

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الآية

تَبَارَكَ الَّذِي جَعَلَ فِي السَّمَاءِ بُرُوجًا وَجَعَلَ فِيهَا سِرَاجًا وَقَمَرًا مُنِيرًا ٦١ وَهُوَ الَّذِي

جَعَلَ اللَّيْلَ وَالنَّهَارَ خِلْفَةً لِمَنْ أَرَادَ أَنْ يَذَّكَّرَ أَوْ أَرَادَ شُكُورًا ٦٢ وَعِبَادُ الرَّحْمَنِ الَّذِينَ

يَمْشُونَ عَلَى الْأَرْضِ هَوْنًا وَإِذَا خَاطَبَهُمُ الْجَاهِلُونَ قَالُوا سَلَامًا ٦٣ وَالَّذِينَ يَبِيتُونَ

إِنَّ عَذَابَهَا لِرَبِّهِمْ سُجَّدًا وَقِيَامًا ٦٤ وَالَّذِينَ يَقُولُونَ رَبَّنَا اصْرِفْ عَنَّا عَذَابَ جَهَنَّمَ

كَانَ غَرَامًا ٦٥ إِنَّهَا سَاءَتْ مُسْتَقَرًّا وَمُقَامًا ٦٦ وَالَّذِينَ إِذَا أَنْفَقُوا لَمْ يُسْرِفُوا وَلَمْ يَقْتُرُوا

وَكَانَ بَيْنَ ذَلِكَ قَوَامًا ٦٧

صدق الله العظيم

سورة الفرقان الآيات (61—67)

المستخلص

لعله من ثمرات الثورة المعلوماتية الانتشار الكبير لشبكات الحاسوب والهاتف المحمول مما أسهم كثيراً في تبادل المعلومات والاتصالات مما أدى الى ظهور مجموعة من التحديات تهدد سلامة المعلومات وهي في طريقها من المرسل الى المستقبل .

تعتبر الثغرات الأمنية في كل مؤسسة هي النقاط الضعيفة والغير محصنة ضد الهجمات وبالتالي تمكن المهاجمين من تبديد موارد المؤسسة في حالة الوصول السلبي للممتلكات، لذلك كله يتناول هذا الكتاب "الثغرات الأمنية للشبكات اللاسلكية" مفاهيم أمن المعلومات وأنواع الشبكات والتهديدات ودوافع المهاجمين كما يشمل الكتاب تعريف وتوصيف للثغرات وأنواعها وسبل وأدوات حمايتها.

يقع هذا الكتاب في أربعة وحدات تحتوي الوحدة الأولى على مفاهيم أمن المعلومات والاتصالات، كما تشمل الوحدة الثانية مواضيع الشبكات اللاسلكية و بنياتها الداخلية وطرق التشبيك وأنواعها وأنواع الموجات والترددات المستخدمة فيها.

تحتوي الوحدة الثالثة على الثغرات الأمنية، تصنيفها وأنواعها، المخاطر وتصنيف المهددات ودوافع المهاجمين والطرق التي يستخدمونها في الهجمات، جرائم المعلوماتية، كما تحتوي الوحدة الرابعة على اهم التقنيات والأدوات المستخدمة في عملية محاربة واقفال الثغرات الأمنية وبعض النصائح لحماية الشبكات اللاسلكية من الاختراق.

Abstract

Perhaps the fruits of the information revolution high prevalence of computer networks and the mobile phone, which contributed greatly to the exchange of information and communication, which led to the emergence of a range of challenges threaten the integrity of the information on its way from sender to receiver.

The security holes in each institution are weak points and non-immune attacks and thus enables attackers to dispel enterprise resources in the case of access downside of the property, so the whole This book deals with "security vulnerabilities for wireless networks" concepts of information security and network types, threats and motives of the attackers also includes book definition and characterization gaps and types and ways and means of protection.

This book is in four units with the first unit include the concepts of information security and communications, the second unit includes wireless networking topics and their internal structures and networking methods, types and kinds of waves and frequencies used.

The unit third contains a security vulnerabilities, classification and types, risk and classification of threats and motives of the attackers and the ways in which they use in the attacks, cybercrime, also contains the fourth unit on the most important techniques and tools used in the process of fighting and close security holes and some tips to protect wireless networks from hackers.

الإهداء

أهدي هذا الكتاب الى روح والدتي العزيزة زينب الشيخ مصطفى الكباشي و
أهدية الى روح الوالدة السعدية عثمان وأسأل الله لهما ولنا الرحمة.

كما أهديه الى أسرتي الصغيرة زوجتي وأطفالي ميار وأحمد لما لهم من كبير
أثر في حياتي.

أهدي هذا المجهود الى كل طلاب العلم والمعرفة وأخص منهم طلابي في
جمهورية السودان.

أهدي هذا الكتاب الى زملائي بجامعة السودان المفتوحة إدارةً وهيئات
تدريس وأخص منهم الدكتور يس بابكر أحمد.

المؤلف

الشكر والتقدير

الشكر لله رب العالمين من قبل ومن بعد على حفظه وتوفيقه ورعايته
ونعمه التي لا تحصى ولا تعد .

وتمتد ألسنة الشكر والتقدير لزميلي الفاضل الدكتور إبراهيم قسم السيد
أستاذ القانون بجامعة السودان المفتوحة على مجهوداته الكبيرة في
سبيل نشر هذا الكتاب، والشكر موصول للإخوة في مطبعة جامعة
السودان المفتوحة لقيامهم بطباعة هذا الكتاب.

كما أود ان أشكر الذين اعتبرهم القدوة الحسنة والذين طوقوني بحبهم
ورعايتهم أسرتي الكبيرة ال الشيخ ابراهيم الكباشي،،،

فهرس المحتويات

رقم الصفحة	الموضوع	رقم الموضوع
أ	الآية	
ب	الإهداء	
ج	الشكر والتقدير	
د	المستخلص باللغة العربية	
هـ	المستخلص باللغة الإنجليزية	
و	فهرس المحتويات	
ك	قائمة الأشكال	
ل	قائمة الجداول	
الوحدة الأولى		
1	مفاهيم أمن المعلومات	1-1
3	المخاطر والثغرات والمهددات	2-1
6	عناصر أمن المعلومات	3-1
49	الإختراق	4-1
10	دوافع الإختراق	5-1

11	طرق الإختراق	6-1
12	التقنيات المستخدمة في الإختراق	7-1
14	الأدوات المستخدمة في الإختراق	8-1
14	أنوع الهجمات	9-1
20	نموزج أمن الشبكات	10-1
الوحدة الثانية		
23	توطئة	1-2
23	تصنيف شبكات الحاسوب	2-2
24	التصنيف حسب الوصول للموارد المشتركة	1-2-2
28	تصنيف الشبكات حسب التوزيع الجغرافي	2-2-2
29	تصنيف الشبكات حسب الوسيط الناقل	3-2-2
30	أصناف الشبكات اللاسلكية	4-2-2
30	مميزات الشبكات اللاسلكية	5-2-2
34	تصنيف الشبكات حسب البنية	6-2-2
37	الحاجة الى الشبكات اللاسلكية	3-2
42	أنواع الشبكات اللاسلكية	4-2
43	الشبكات الافتراضية الخاصة	5-2
43	مكونات الشبكات الافتراضية	1-5-2
47	البنية التحتية للشبكات	6-2
49	بنى الشبكات اللاسلكية	1-6-2
51	مكونات الشبكات اللاسلكية	7-2

52	زبائن الشبكات اللاسلكية	1-7-2
53	أنماط الشبكات اللاسلكية	2-7-2
53	النمط الخاص	3-7-2
54	نمط البنية النجمية	4-7-2
59	الموجات اللاسلكية الكهربية	8-2
60	ماكسويل والموجات الخفية	1-8-2
61	طيف الموجات اللاسلكية الكهربية	2-8-2
62	توزيع حزم الموجات للبعث الإذاعي	3-8-2
63	الموجات الكهرومغناطيسية	4-8-2
63	إنتشار الموجات بالراديو	5-8-2
66	مميزات الحزم الموجية	6-8-2
75	تقنية البلوتوث	9-2
77	طريقة عمل تقنية البلوتوث	1-9-2
79	التشويش الذي يحصل بين الأجهزة	2-9-2
77	أشكال التوصيل بين الأجهزة	10-2
80	الأشعة تحت الحمراء	11-2
81	لوحة الدائرة المطبوعة	12-2
الوحدة الثالثة		
83	تمهيد	1-3
84	مفهوم الأمن في شبكات الحساسات اللاسلكية	2-3
85	معوقات الأمن في شبكات الحساسات اللاسلكية	3-3

86	الإعتداءات الأمنية شبكات الحساسات اللاسلكية	4-3
86	تصنيف الإعتداءات الأمنية	1-4-3
88	أشكال الإعتداءات الأمنية	2-4-3
88	الإعتداءات المستهدفة للطبقة المحسوسة	3-4-3
89	الإعتداءات المستهدفة لطبقة ربط البيانات	4-4-3
91	الإعتداءات المستهدفة لطبقة الشبكة	5-4-3
93	الإعتداءات المستهدفة لطبقة النقل	6-4-3
93	الإعتداءات المستهدفة لطبقة التطبيقات	7-4-3
94	الإعتداءات المستهدفة للبيانات المنقولة	8-4-3
95	الإعتداءات المحسوسة الموجهة ضد عقد الشبكة	9-4-3
96	حماية شبكات الحساسات اللاسلكية	5-3
99	إستعراض الحلول الأمنية	6-3
99	التشفير وإدارة المفاتيح	1-6-3
102	التوجيه الأامن	2-6-3
104	جرائم المعلوماتية	7-3
105	خصائص جرائم المعلوماتية	1-7-3
108	الهكرز الأخلاقي	2-7-3
112	الهندسة الإجتماعية	3-7-3
114	الهدف من الهندسة الإجتماعية	1-3-7-3
114	الوسائل المستخدمة في الهندسة الإجتماعية	2-3-7-3
117	طرق الحماية من الهندسة الاجتامية	3-3-7-3
107	التشريعات القانونية	8-3

الوحدة الرابعة

120	أساسيات ثغرات الفيض	1-4
121	الطرق البرمجية المستخدمة لإقفال الثغرات	2-4
132	معرف الخدمة	1-2-4
134	المعدات المستخدمة في إقفال الثغرات	3-4
135	الجدار الناري	1-3-4
135	الجيل الأول ملفترات العبوة	1-1-3-4
136	الجيل الثاني فلتر محدد الحالة	2-1-3-4
138	الجيل الثالث طبقات التطبيقات	3-1-3-4
144	الجيل الرابع (الجيل الحديث من جدار الحماية)	4-1-3-4
146	الخادمين النيابيين	2-3-4
146	أجهزة تعقب المتطفلين	3-3-4
149	أنواع أجهزة تعقب المتطفلين	1-3-3-4
150	طرق إكتشاف المتطفلين	4-4
155	طرق منع الفخاخ	5-4
156	أجهزة تعقب المتطفلين المتطورة	5-3-4
157	مخدم البروكسي	6-4
167	كيفية عمل البروكسي	1-6-4
157	أنواع البروكسي ووظائفها	2-6-4
167	مزايا مخدمات البروكسي	3-6-4
169	مخاطر إستخدام الوكيل المفتوح	7-4

167	مخاطر إستخدام خدمة بروكسي مجهولة	8-4
169	طرق الحماية الفيزيائية	9-4
171	كيفية إختراق الطرق الفيزيائية	10-4
177	الطرق الوقائية لإقفال الثغرات الأمنية	11-4
188	الخاتمة	
189	المصادر والمراجع	
192	المؤلف في سطور	

قائمة الأشكال

رقم الصفحة	عنوان الشكل	رقم الشكل
6	مكونات نظم أمن المعلومات	1-1
15	الهجوم الخامل	2-1
17	الهجوم النشط	3-1
18	هجوم تعديل الرسالة	4-1
19	هجوم التزوير	5-1
20	إعادة الإرسال	6-1
21	نموزج الإتصال الآمن	7-1
22	نموزج النفاذ الآمن	8-1
26	الشبكات المحلية وشبكات المناطق الواسعة	1-2
27	العلاقة بين الشبكة المعشقة وأطرافها	2-2
29	شبكة الاتصال اللاسلكي	3-2
32	البنية الخطية	4-2
33	البنية النجمية	5-2
34	بطاقة حاسوب لاسلكي	6-2
34	نقطة وصول لاسلكية	7-2
56	بنى الشبكات اللاسلكية	8-2
57	أمثلة للتكرار ضمن البنية اللاسلكية	9-2
139	مخدم البروكسي	1-4
148	طرق تعقب المتطفلين	2-4

150	طرق عمل أجهزة تعقب المتطفلين	3-4
153	البنية التحتية لأنظمة كشف التطفل	4-4
154	مثال لموقع كشف التطفل في الشبكات	5-4
176	مثال لغرفة تأمين الثغرات	6-4

قائمة الجداول

رقم الصفحة	عنوان الجدول	رقم الجدول
48	البنية الأساسية للشبكات	1-2
55	بنى الشبكات اللاسلكية	2-2
56	نموذج لشبكة لاسلكية نجمية	3-2
59	نموذج لشبكة لاسلكية بين نقطتين	4-2
59	نموذج لشبكة معشقة	5-2

1-1 مفاهيم أمن المعلومات والشبكات

ظل مجال امن المعلومات والشبكات حتى أواخر سبعينيات القرن الماضي معروفاً باسم أمن الاتصالات
Communication Security, COMSEC والذي حددته توصيات أمن نظم المعلومات والاتصالات لوكالة
الأمن القومي بالولايات المتحدة بما يلي :

المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أشخاص غير مخولين عبر الاتصالات وضمان
أصالة وصحة هذه الاتصالات وتضمنت النشاطات المحددة لأمن الاتصالات أربعة محاور هي :

- أمن التشفير security Crypto .
- أمن الإرسال Transmission Security .
- أمن الإشعاع Security Emission .
- الأمن الفيزيائي (المادي) Physical Security .

و يتضمن تعريف أمن الاتصالات خاصيتين وهما:

- السرية Confidentiality : وتعنى بالتأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل
أشخاص غير مخولين بذلك.

الخطر risk ، وهو مفهوم يشير إلى التأثيرات السالبة والمحتملة على الأصول والممتلكات القيمة والتي قد تنتج
من عملية حالية أو حدث مستقبلي. بمعنى آخر، الخطر هو احتمال حدوث حدث معين يكون لديه تأثير على
إنجاز الأهداف بدأت في الثمانينات من القرن الماضي ومع النمو المضطرد للحواسيب الشخصية واستخداماتها،

حقبة جديدة من الأمن وهي حقبة أمن الحواسيب Computer Security ، COMPUSEC والتي حددتها

توصيات أمن نظم المعلومات والاتصالات لوكالة الأمن القومي بالولايات المتحدة بما يلي :

المعايير والإجراءات التي تضمن سرية و كمال وتوفر مكونات نظم المعلومات، بما فيها التجهيزات والبرمجيات والبرمجيات المدمجة firmware والمعلومات التي تتم معالجتها وتخزينها ونقلها.

تضمن أمن الحواسيب خاصيتين إضافيتين وهما:

• **التكاملية وسلامة المحتوى Integrity** : وتعنى بالتأكد من أن محتوى الرسائل (المعلومات) صحيح

ولم يتم تعديله أو العبث به. وبشكل خاص لم يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع خلال الإرسال .

• **استمرارية توفر المعلومات أو الخدمة Availability** : التأكد من استمرار عمل نظام المعلومات

والشبكات واستمرار مقدرتها على التفاعل مع المعلومات والمستخدمين، وعدم توقف أو حجب الخدمة وعدم إمكانية النفاذ كنتيجة للهجوم عليها أو تدميرها وتخريبها.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي أمن الاتصالات وأمن الحواسيب لتشكيل ما أصبح

يعرف باسم أمن نظم المعلومات Information Systems Security –INFOSEC . يشتمل مفهوم أمن

نظم المعلومات الخصائص الأربع المذكورة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب، وهي السرية

والموثوقية والكمال والتوفر، كما أُضِيفَتْ إليها خاصية جديدة وهي مكافحة الإنكار، أو منع إنكار التصرف

المرتبط بالمعلومات ممن قام به Non-repudiation ، والقصد هنا هو ضمان عدم إنكار الشخص الذي قام

بتصرف ما متصل بالمعلومات أو مواقعها إنه هو الذي قام بهذا التصرف، بحيث توفر هذه الخاصية المقدرة على إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين.

1-2 المخاطر والثغرات والتهديدات

يعرف الأمن بالحماية من المخاطر والفقدان. بصورة عامة مفهوم الأمن شبيه بمفهوم السلامة. الفارق الدقيق بين المفهومين يتمثل في التركيز الإضافي للأمن على الحماية من المخاطر الخارجية المتمثلة في الأفراد والأنشطة التي تنتهك الحماية وتكون مسؤولة مباشرة عن خرق الأمن. يستخدم تعبير الأمن بصورة عامة كمرادف لتعبير السلامة، ولكن من ناحية فنية يعنى تعبير الأمن ليس فقط السلامة بل العمل على توفير السلامة أيضاً.

هناك مفاهيم محددة تتكرر في مجالات الأمن المختلفة منها:

1) الخطر risk ، وهو مفهوم يشير إلى التأثيرات السالبة والمحتملة على الأصول والممتلكات القيمة والتي قد تنتج من عملية حالية أو حدث مستقبلي. بمعنى آخر، الخطر هو احتمال حدوث حدث معين يكون لديه تأثير على إنجاز الأهداف. في مجال العلوم الهندسية، يعرف الخطر كمياً بحاصل ضرب احتمال حدوث الحادثة و الخسارة في الحادثة الواحدة. ويعتبر الخطر مؤشراً للتهديدات ويعتمد على التهديدات والثغرات والتأثير على العمليات وعدم التأكد. يوجد العديد من الطرق والأساليب لتقييم وقياس الخطر.

في أمن المعلومات والشبكات يحدد الخطر باستخدام ثلاثة متغيرات (عوامل) وهى:

- احتمال أن يكون هناك تهديداً.

- احتمال إن تكون هناك ثغرات.
- التأثير المحتمل للخطر.

إن أصبحت أي من هذه المتغيرات تساوي صفراً، يقترب الخطر الكلي على النظام أو الشبكة من الصفر أيضاً.

إدارة الخطر نشاط إنساني يهدف إلى تكامل تميز الخطر وتقييمه وتطوير الاستراتيجيات لإدارته وتخفيفه باستخدام الموارد الإدارية.

(2) **الثغرات Vulnerability (أو عدم التحصين)** وبصورة عامة تعرف بالحساسية اتجاه الأذى أو الهجوم الجسدي أو النفسي. كما تعني أيضاً عدم توفر الحماية اللازمة للممتلكات والأصول القيمة. في أمن الحاسوب والشبكات يستخدم تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم والتي تتيح للمهاجم الاعتداء على سلامة النظام. وقد يتسبب في الثغرات قصوراً في البرمجيات أو خللاً في التصميم، نتيجة لإهمال المبرمج أو المصمم، أو استخدام المهاجم لبرامج خبيثة مثل برامج الفيروسات.

يمكن تصنيف الثغرات في أمن الحاسوب والشبكات إلى فئتين:

(3) **ثغرات فنية**، وتكون نتيجة لضعف التحصين الناتج من التقنيات المستخدمة في النظم والشبكات، في هذه الحالة يعرف الهجوم على الشبكة بالهجوم التقني.

(4) **ثغرات إدارية**، وتكون نتيجة لأسباب غير فنية ويعرف الهجوم على الشبكة أو الحاسوب في هذه الحالة بهجوم الهندسة الاجتماعية social engineering attack .

كما يمكن تقسيم الثغرات من حيث الصعوبة والسهولة إلى فئتين :

أ- ثغرات المستوى الأعلى High-level Vulnerability ، وهو ثغرات سهلة الاستغلال، ومثال عليها كتابه شفرة برنامج لاستغلال تلك الثغرة .

ب- ثغرات المستوى الأدنى Low-level Vulnerability وهذا النوع من الثغرات يصعب استغلاله ويتطلب الكثير من الجهد والموارد من قبل المهاجم.

(5) التهديدات Threats ، وهو احتمال التطفل على الأصول والممتلكات (المعلومات) بدون إذن صاحبها وقسراً وعبر ثغرة محتملة في النظام، بهدف سرقتها أو تخريبها، وفي حالة حدوثها تمثل التهديدات خطراً على النظام. هناك ثلاثة مكونات أساسية للتهديد وهي:

(6) الهدف، ويمثل في أمن الحاسوب والشبكات المعلومات المخزنة أو المرسلة عبر الشبكات بغرض انتهاك سريتها أو سلامتها أو تواجدها .

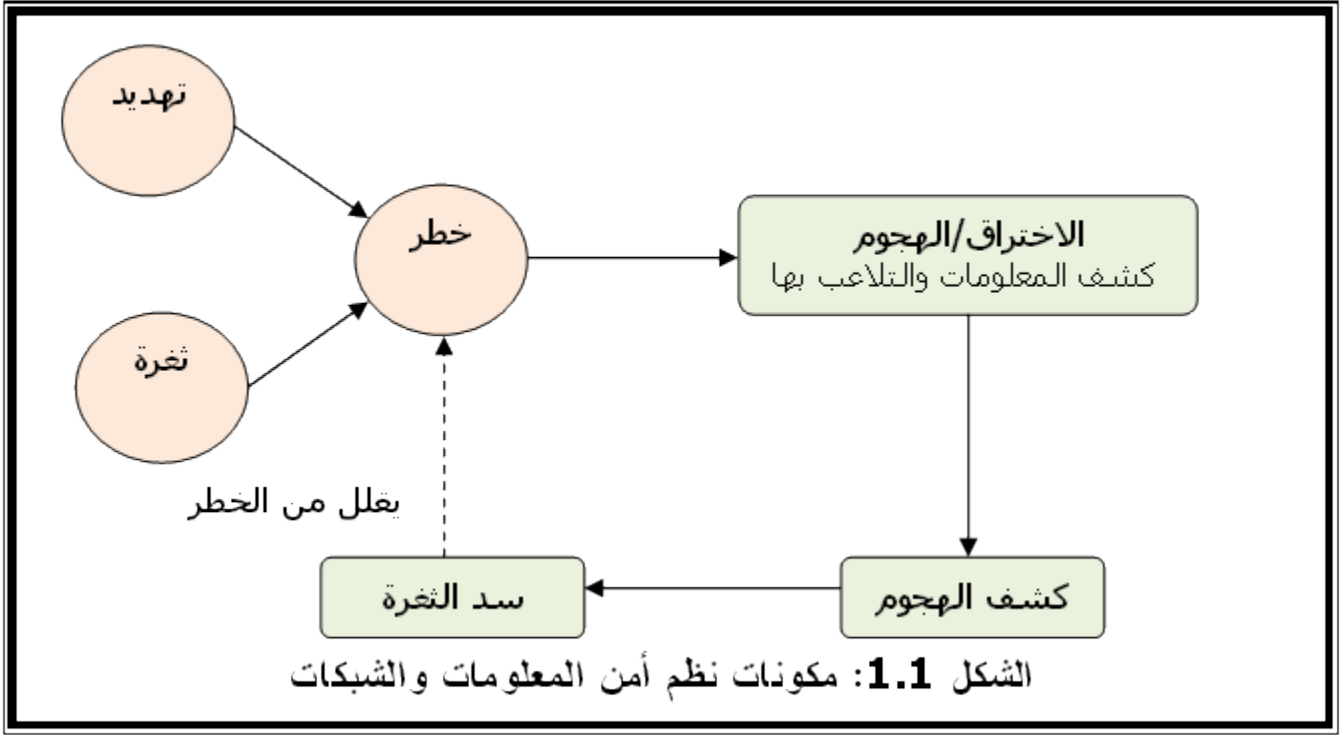
(7) العميل وهي البرامج والأشياء المكونة والمنشأة للتهديد، ويتطلب استخدامها النفاذ إلى الحاسوب أو الشبكات بالإضافة إلى معلومات عن خصائص تشغيلها وآليات الأمن المستخدمة فيها وذلك للبحث عن ثغرة للنفاذ من خلالها إلى النظام أو الشبكة.

* الحدث، ويمثل نوعية التأثير لوضعية التهديد ويستخدم لذلك بطرق عديدة من أهمها إساءة النفاذ المخول

Authorized وغير المخول Unauthorized إلى المعلومات أو النظام. ووضع شفرات خبيثة Malicious

مثل شفرات الفيروسات في النظم.

الشكل 1.1 يوضح العلاقة بين مكونات نظام أمن المعلومات والشبكات وتأثرها ببعضها البعض.



3-1 عناصر أمن المعلومات

تتمحور عناصر أمن المعلومات في عدة مجالات أذكر منها التالي:

- أمن أماكن حفظ البيانات و المعلومات : ويهتم هذا المجال بالعديد من الآليات العلمية والعملية المرتبطة بأماكن حفظ البيانات والبيئة المحيطة بها، وذلك للتأكد من تواجد المعلومات في أماكن آمنة مثل مراكز البيانات Data Centers ، والتي يجب أن تخضع لرقابة دقيقة وإجراءات أمنية مادية عالية في الدخول، بحيث لا يصل إلي الأجهزة إلا من هو مصرح له ومن خلال بوابة آمنة والتي قد

- تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بصمة الإصبع (Printfinger) وقزحية العين (Printeye) أو تردد الصوت أو من خلال الأرقام المتسلسلة أو البطاقات الممغنطة، وغيرها.
- **أمن طريقة حفظ البيانات :** ويتم ذلك من خلال استخدام التقنيات المتقدمة لتشفير المعلومات المحفوظة (Encryption) بمختلف أنواع التشفير المتناظر أو غير المتناظر، وسواء كان معتمداً دولياً أو أسلوب تشفير مطوراً محلياً.
- **أمن وسائط حفظ البيانات :** ويتحقق هذا المحور من خلال الحفظ على الأنسب من الأقراص الصلبة (HDD) أو كروت الذاكرة (CASH) أو الأقراص المدمجة (CD) وغيرها من وسائط الحفظ المناسبة .
- **أمن حماية المعلومة :** ويتم بعدة آليات مثل استخدام برامج الحماية أو الجدران النارية Firewalls للحماية من اختراق الأجهزة المرتبطة بالشبكات ، واستخدام المرشحات Filters لضمان عدم نقل المعلومات غير المسموح بنقلها، واستخدام برامج مكافحة الفيروسات (Anti-Virus) للحماية من الفيروسات المختلفة والنسخ الاحتياطي (Backup) لمعالجة مشكلة فقدان البيانات الرقمية غير المكتوبة والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو فقدان ويتم ذلك بعدد من الآليات.
- **أمن نقل المعلومات والبيانات :** قديماً كانت تستخدم آليات النقل المادي المباشر للبيانات وتحاط بسرية وحماية هذه الآليات بطيئة نسبياً، والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة المعتمدة علي التواصل الإلكتروني. وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من سرعة النقل والدقة هي الأنسب عند أخذ الاحتياطات الأمنية اللازمة في عمليات نقل البيانات، ولذا نرى بأن هذا المجال يهتم بالبيئات الآمنة لنقل البيانات والمعلومات عبر الشبكات والنفوذ إليها.

- **أمن نظم الاتصالات وبيئات النقل المستخدمة :** وذلك عندما يكون الاتصال مباشراً بواسطة خطوط الهاتف أو بالاتصال المباشر بالأقمار الاصطناعية، وعندما يكون حجم البيانات متوسطاً نسبياً . وتكمن الخطورة هنا عند وجود متطفلين يقومون بعمليات بالتطفل Sniffing على خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة وكفاءة عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين.
- **أمن التطبيقات المستخدمة والبروتوكولات :** عندما يكون الاتصال غير مباشر وعبر وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدمات عالي الأهمية الأمنية مثل المصاريف أو للشراء المباشر ببطاقات الائتمان الإلكترونية، يمثل التجسس والاختراق أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة على مستوى طبقة التطبيقات أو طبقة الشبكة، وهنا تظهر أهمية التوقيعات الرقمية والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية .
- **البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها :** تعتبر مصادر الخطر وتهديدات أمن البيانات والشبكات كثيرة جداً و لعل من أهمها خطورة النفاذ إلى البيانات من قبل أشخاص غير مسموح لهم بذلك وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها ويمكن أن يستعين أولئك المهاجمون بالعديد من الوسائل التي توصلهم للبيانات أو تمكنهم من إتلافها أو تغييرها بعدة طرق، كما سنرى لاحقاً في هذه الوحدة.

4-1 الاختراق

يعرف الاختراق Hacking بشكل عام على أنه القدرة على الوصول لهدف معين بطريقة غير مشروعة، وذلك عبر الثغرات في نظام الحماية الخاص بالهدف، وبطبيعة الحال هذه سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوة ودون رغبة منهم وحتى دون علمهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سحبة ملفات وصور تخصهم وحدهم . يمكن تصنيف المخترقين إلى مجموعتين رئيسيتين :

- المجموعة الأولى : وهم الهواة وعامة المخترقين الذين يستخدمون برامج سهلة وبسيطة للاختراق وغالبية هذه البرامج تعمل تحت بيئة نظام التشغيل Windows ، وهؤلاء المخترقون عادة لا يتمكنون من النفاذ إلى بيانات أي جهاز إلا إذا كان متصلاً بشبكة الإنترنت ومصاباً بفيروسات من نوع "حصان طروادة " Trojanhors التي تدعم برامج المخترقين حيث يقوم حصان طروادة بفتح منفذ في الجهاز المصاب يمكن للمخترق من خلاله التحكم في جهاز الضحية والوصول لبياناته فيما يعرف بالباب الخلفي.

- المجموعة الثانية : وهم القلة والأخطر وهم المخترقون المحترفون وعادة ما يكونون مبرمجين أو متخصصين في مجال البرمجيات والشبكات وتقنية المعلومات، ويشكلون تحالفات في عالم الإنترنت الافتراضي. وهؤلاء المخترقون لا يعتمدون فقط على برامج الاختراق بل يقومون باستغلال الثغرات الأمنية في نظم التشغيل والشبكات، حيث يعترضون البيانات والحصول على نسخة منها في نقاط الاتصال سواء كانت أجهزة ربط شبكات مثل الموجهات Routers أو المبدلات القابلة للإدارة

Manageable Switches أو يقومون بالتواصل مع الموجهات Routers وبالتالي يعطلون نطاقات كاملة عن العمل أو قد يتمكنون من ضرب أجهزة الربط والإضرار بقطاع كبير من مستخدمي شبكة الإنترنت.

1-5 دوافع الاختراق

لا يعد الاختراق من المسائل العيئية فهو نشاط منظم وديماً مايراد له الوصول الى أهداف محددة تماماً من قبل المخترقين أنفسهم أو الجهات التي تقف خلفهم ويمكن ان نلخص دوافع الاختراق في التالي:-

- **الدافع السياسي والعسكري :** مما لاشك فيه أن التطور العلمي والتقني أديا إلي الاعتماد بشكل شبه كامل على الحاسوب والشبكات في أغلب الاحتياجات الفنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي و التجسسي بين الدولتين العظميين آنذاك والذي كان على أشده، ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية في المؤسسات والدول، أصبح الاعتماد كلياً على الحاسوب وعن طريقه أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.
- **الدافع التجاري:** من المعروف أن الشركات التجارية الكبرى في حالة حرب مستعرة فيما بينها وقد بينت الدراسات الحديثة أن عدداً من كبريات الشركات التجارية تجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم.
- **الدافع الفردي (التحدي):** بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة الأمريكية كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم، و ما لبثت أن

تحولت تلك الظاهرة إلي تحدُّ فيما بينهم في اختراق النظم بالشركات ثم بمواقع الانترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية.

- الدوافع الفكرية والعقدية:تمثل الإختلافات الفكرية والاجتماعية واحدة من أهم دوافع الاختراق التي برزت في عالم اليوم إذ تحاول المجمعات البشرية ان تبرز نقاط قوتها على صعد متعددة.

1- 6 طرق الاختراق

يتبع المخترقون طرق عدة للوصول الى أهدافهم حيث يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلي ثلاث مجموعات:

- اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق المنظومة الأمنية المتمثلة في الجدران النارية وأجهزة محاربة المتطفلين التي عادة ماتوضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة (الاحتيال) Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام أو عن طريق الوصول من بعيد.
- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات.
- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات المصرفية ATM والبطاقات الذكية Smartcards.

1-7 التقنيات المستخدمة في الاختراق

تقوم الفكرة الأساسية للاختراق على السيطرة على جهاز حاسوب الضحية من بعد من خلال عاملين مهمين:

- البرنامج المسيطر ويعرف بالعميل (الزبون) Client .

- وحدة الخدمة Server Unit الذي يقوم بتسهيل وإدارة عملية الاختراق.

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج

وحدة الخدمة وفي جهاز المخترق يوجد برنامج العميل. تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل

الاختراق، ولكنها جميعاً تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي تزرع به وحدة

الخدمة الخاصة بالمخترق، وجهاز المخترق على الطرف الآخر حيث يوجد برنامج المستفيد أو العميل هناك

عدة طرق شائعة لتنفيذ ذلك:

- عن طريق ملفات أحصنة طروادة Trojan Hors : ولتحقيق الاختراق لابد من توفر برامج تجسس

يتم إرسالها وزرعها من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق أو الصامت وهو

ملف عادة ما يكون صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (وحدة الخدمة) ويمثل حلقة

الوصل بينه وبين المخترق (المستفيد).

- منافذ الاتصال Ports : يتم الاتصال بين العمليات في أي جهازين عبر منفذ اتصال والذي يكون

جزءاً من الذاكرة له عنوان معين يتعرف عليه الجهاز بأنه منطقة اتصال يتم عبره إرسال واستقبال

البيانات مع بروتوكولات طبقة التطبيقات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن 65000.

- استخدام عنوان بروتوكول الانترنت IP Address : عند اتصال جهاز الحاسوب بالإنترنت يكون معرضاً لكشف الكثير من المعلومات الخاصة به، مثل عنوان الجهاز وموقعه ومزود الخدمة الخاص به، كما يمكن تسجيل كثير من تحركاته على الشبكة. حينما يتمكن المحترق من معرفة رقم عنوان بروتوكول الانترنت الخاص بالضحية قد يتمكن من خلاله من الدخول إلى الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلاً بالشبكة فقط،
- عن طريق كعكات الإنترنت Internet Cookies : يمكن أيضاً تحقيق التواصل للاختراق عن طريق كعكات الإنترنت وهي عبارة عن ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب لتسهيل عملية التواصل ، هذا الملف به آليات تمكن الموقع التابع له من خلال جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع كما أنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري ولكنه قد يساء استخدامه من قبل بعض المبرمجين المتمرسين . يتم الاختراق بوضع برنامج وحدة الخدمة بجهاز الضحية ويتم الاتصال به عبر المنفذ الذي فتحه للمستخدم (المحترق) في الطرف الآخر ويكون حلقة الوصل هذه تنقصها المعابر وهي البرامج المخصصة للاختراق.

في مجال أمن الحاسوب والشبكات يستخدم المهاجمون (المخترقون) وأخصائيو الأمن نفس الأدوات لمواجهة بعضهم البعض، في حالة شبيهة بحالة المجرمين والشرطة. تشتم الحزم packet sniffer أداة تسمح للمستخدم بترشيح حزم بروتوكول TCP/IP على الشبكات على أساس مجموعة من الخواص تضع من قبل

المستخدم. مثلا أن يسمح فقط بمرور الحزم التي يكون مصدرها أو مقصدها عنوان بروتوكول انترنت محدد، أو لديها محتويات محددة، إلخ.

8-1 الأدوات المستخدمة في الاختراق

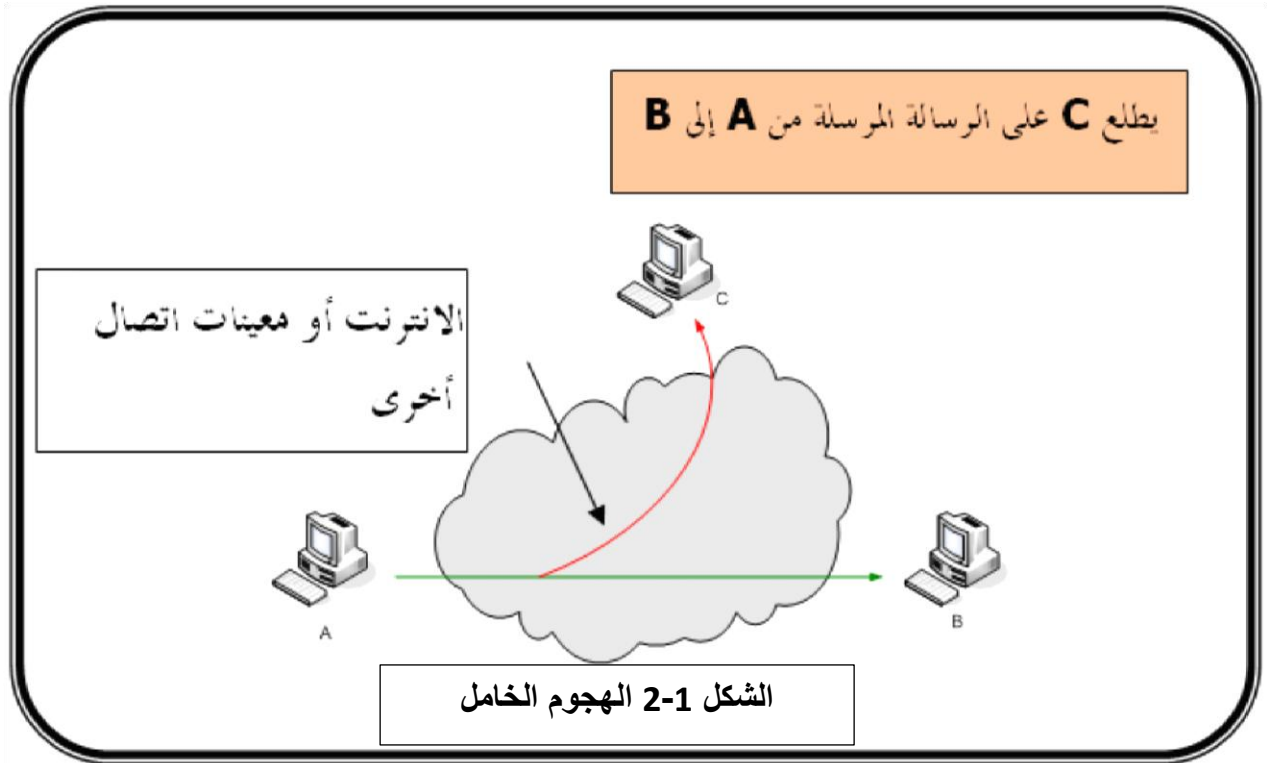
يستخدم المخترقون والمهاجمون مجموعة كبيرة من الأدوات والبرامج يجب على مشرفي الشبكات ومراكز المعلومات معرفتها للوقاية والاحتراز منها و أكثرها شهرةً مايلي:-

- Wireshark
- InSSIDer on Windows and Kismet on Mac, Linux
- AirCrack and coWPAtty
- Nmap
- MAC Shift

9_1 أنواع الهجمات

يهدف الهجوم على نظم المعلومات الالكترونية وشبكات المعلومات إلى تدمير أو تخريب المعلومات أو سرقتها أو منع الوصول إليها أو تنصيب برامج خبيثة malicious software . يقسم الهجوم إلى قسمين رئيسيين وهما الهجوم النشط Active Attack والهجوم الخامل Passive Attack .

في الهجوم الخامل، الشكل (1-2)، يتم باعتراض الرسائل من أجل التعرف على محتوياتها واستخدامها داخليا دون تغيير محتوياتها أو تحليل الحركة. من الصعب اكتشاف هذا النوع من انواع الهجوم ولا بد من اخذ التدابير الاحترازية للحماية منه.



في الهجوم النشط يقوم المهاجمون بمجموعة من النشاطات قد تؤدي الى اتلاف المحتوى الاصلي للرسالة، يعرف هذا الهجوم أيضا بهجوم التنصت على الرسائل Interception Attack ، حيث يراقب المهاجم الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال . Eavesdropping .

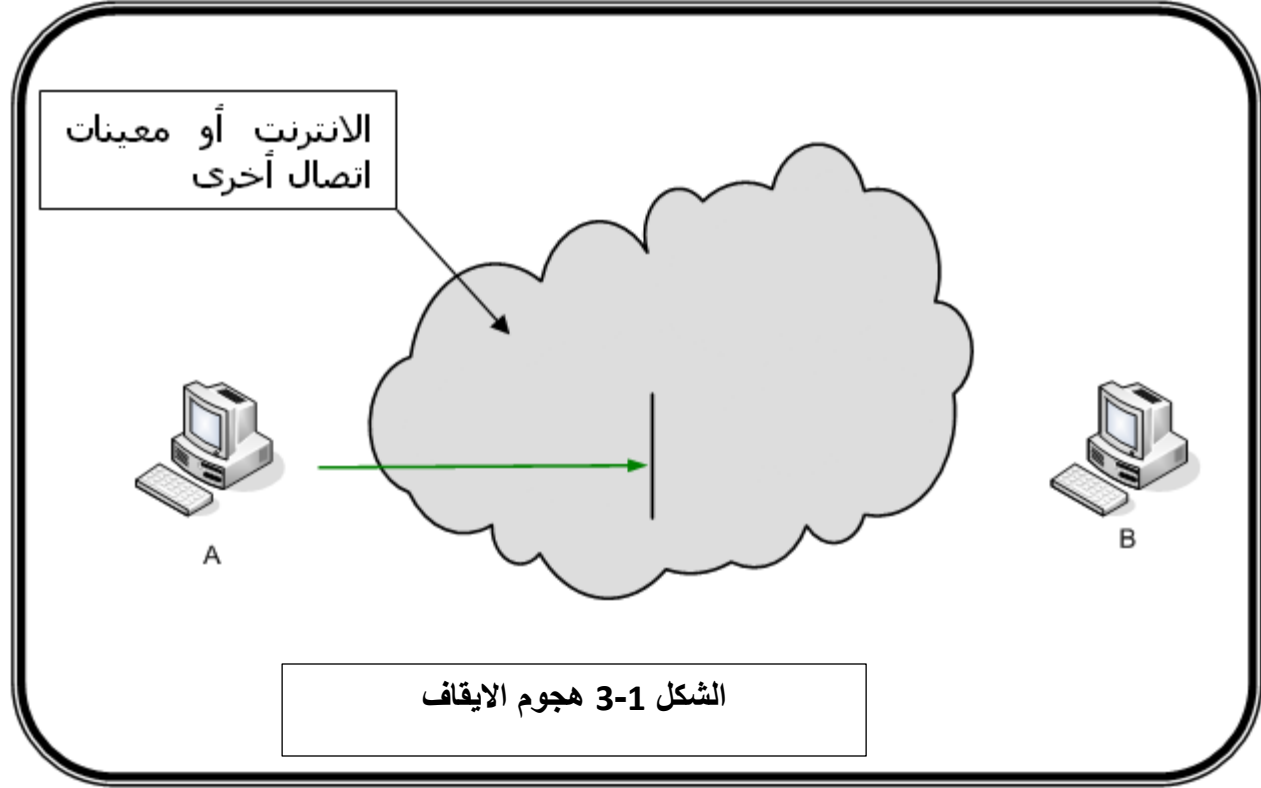
في الهجوم النشط قد يعالج المخترق الرسالة ببراعة ويغير محتواها. يهدف الهجوم النشط إلى تغيير إمكانيات النظام والتأثير على عملياته وذلك بتعديل تتدفق البيانات من اجل:

- انتحال هوية احد أطراف الاتصال.

- إعادة إرسال رسائل سابقة.
- تعديل محتويات الرسالة التي في الانتظار.
- منع أو حجب الخدمة.

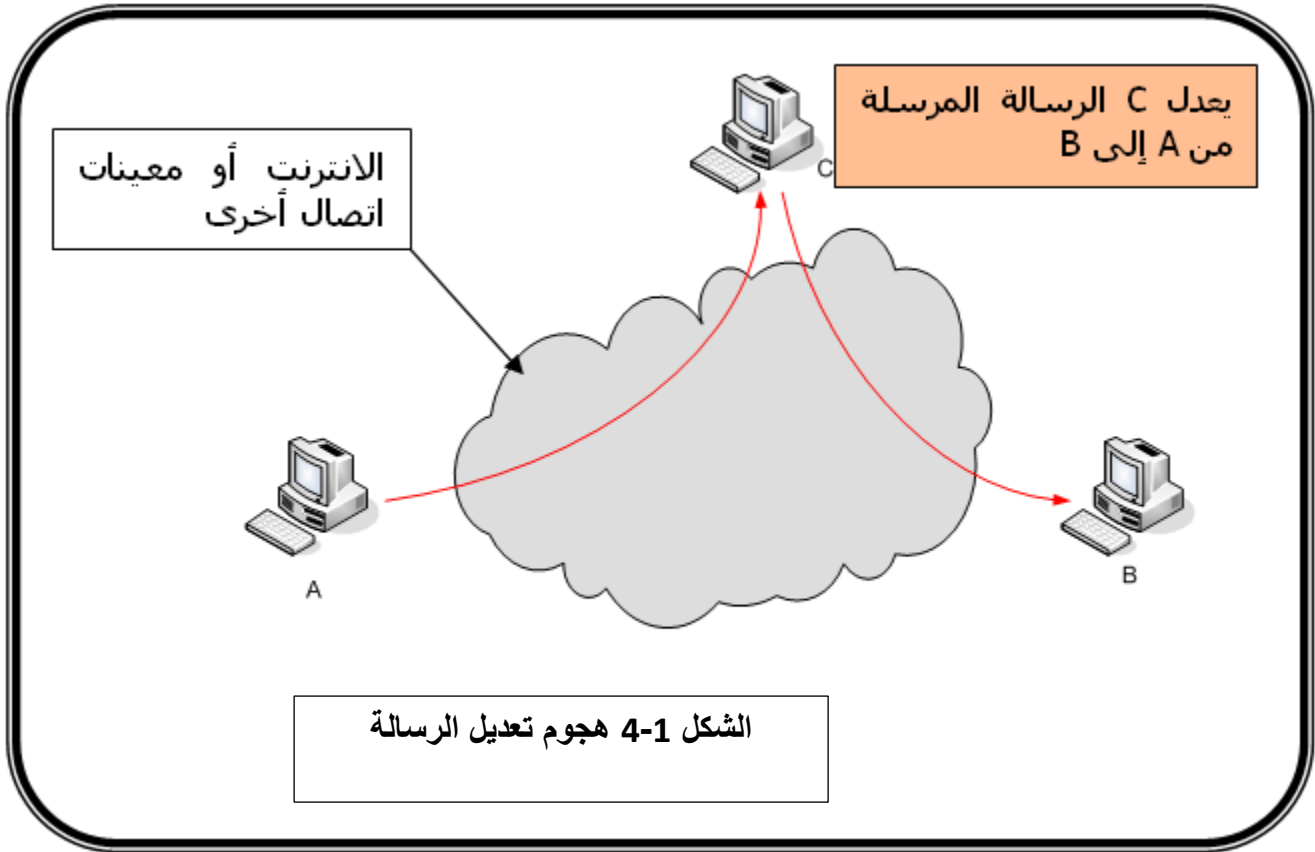
من الصعب منع الهجمات النشطة كلياً نتيجة للثغرات المحتملة في العتاد والبرمجيات والشبكات. وذلك عكس الهجمات الخاملة والتي من الصعب اكتشافها ولكن يمكن منعها كلياً. وتهدف أساليب مكافحة الهجمات النشطة إلى اكتشاف الهجمات والاسترجاع من آثارها، يقسم الهجوم النشط إلى أربعة أقسام رئيسية وهي :

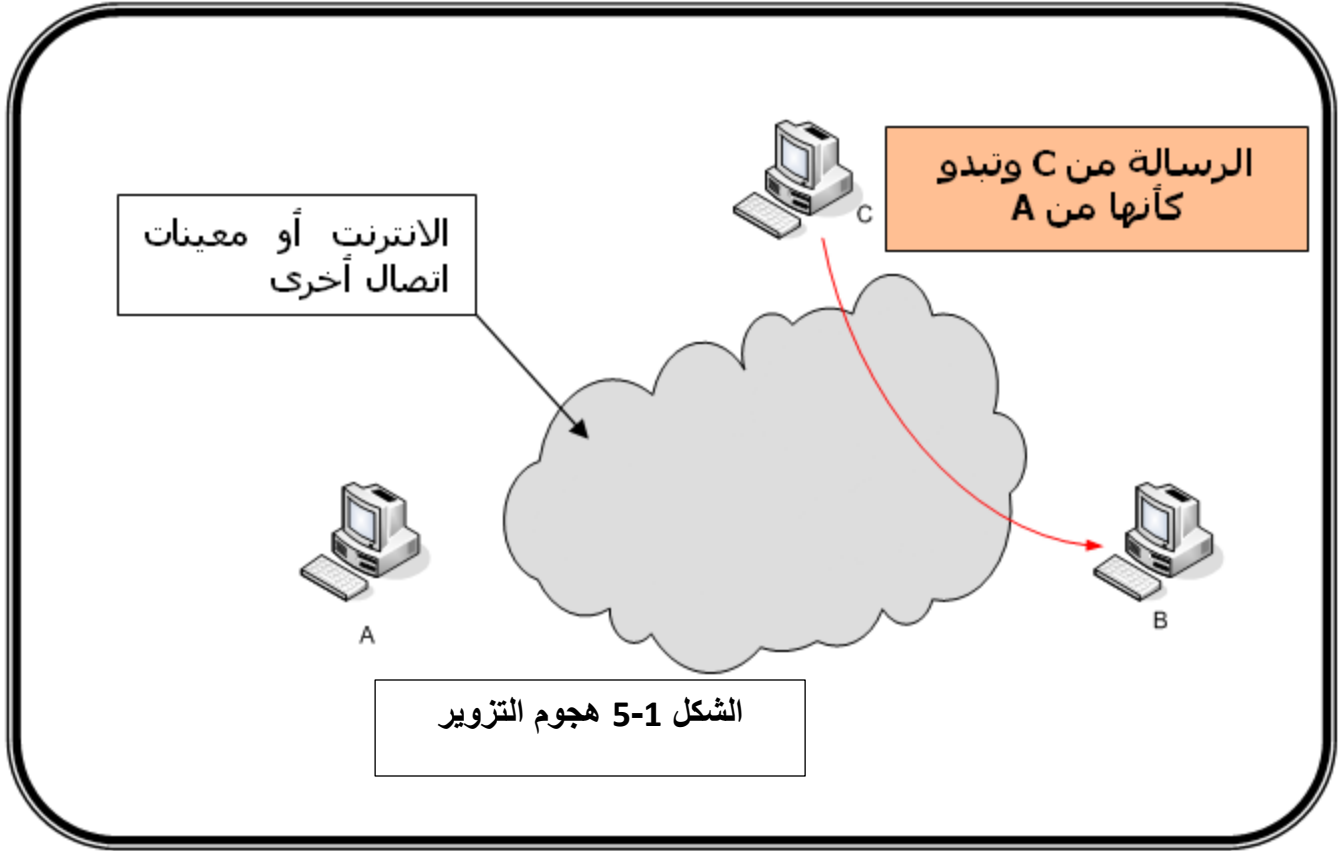
- **هجوم الإيقاف Interruption Attack** ، الشكل (1-3)، هذا النوع يقوم على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض أو حجب الخدمة (Denial of service) ويعتبر هذا النوع من أكثر أنواع الهجمات ضرراً.

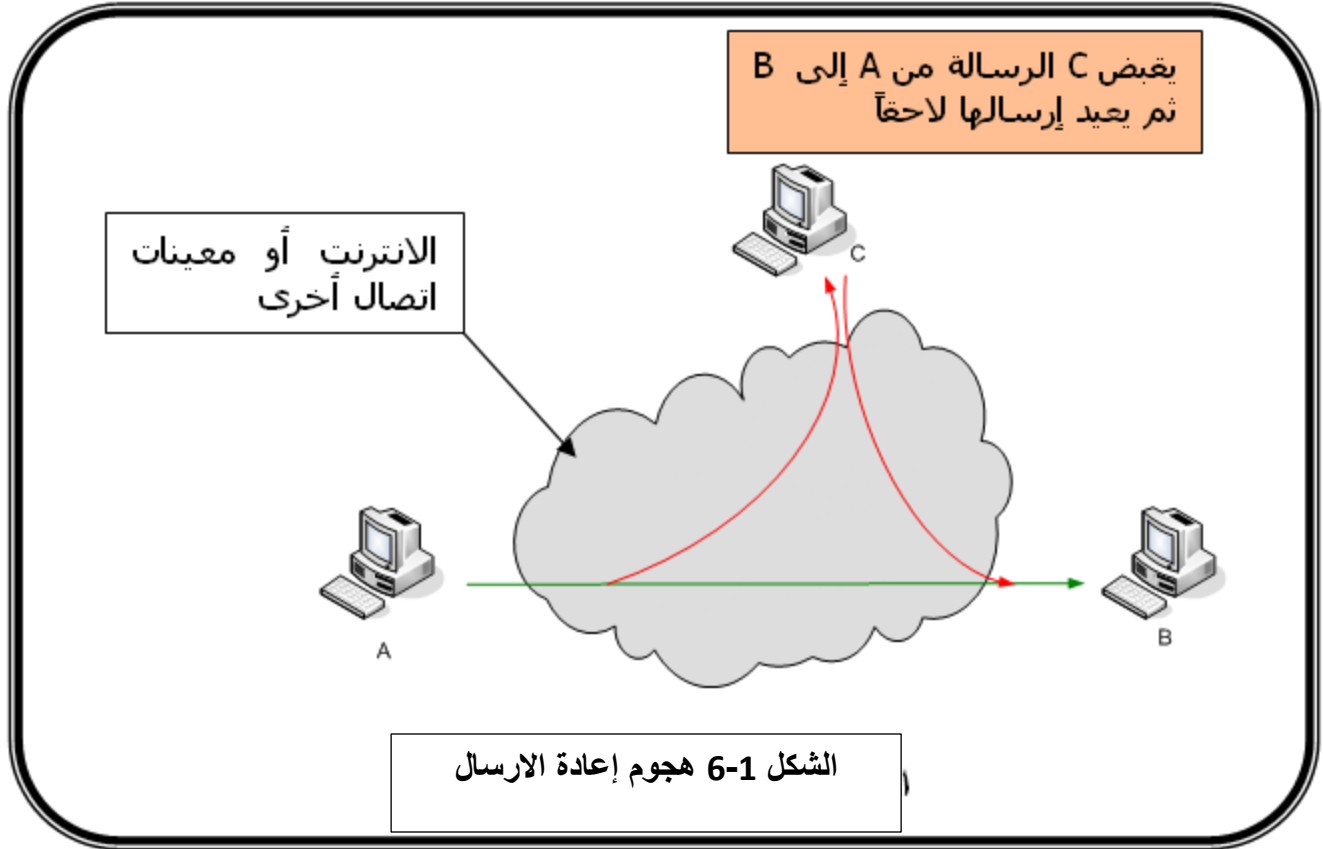


- هجوم التعديل يقوم على تعديل محتوى الرسالة **Modification Attack** ، الشكل (1-4)، هنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيطاً ثالثاً بين المرسل والمستقبل) وعندما تصل الرسالة إلى المهاجم يقوم بتغيير محتوى الرسالة ومن ثم إعادة إرسالها إلى المستقبل، و قد لا يعلم المستقبل بتعديل الرسالة من قبل المهاجم.
- هجوم التزوير أو الفبركة **Fabrication Attack** ، الشكل (1-5)، هنا يرسل المهاجم رسالة إلى أحد أطراف الاتصال مفادها أن جهة موثوق فيها تطلب منه معلومات أو كلمات سرية خاصة به مثلا .

- هجوم إعادة الإرسال Replay attack ، هنا يستلم المهاجم نسخة من الرسالة المرسله من A إلى B ثم يعيد إرسالها لاحقا للتأثير على العمليات في الطرف B أو قد يستخلص منها على معلومات تساعده على مهاجمة النظام مستقبلا، الشكل (1-6).







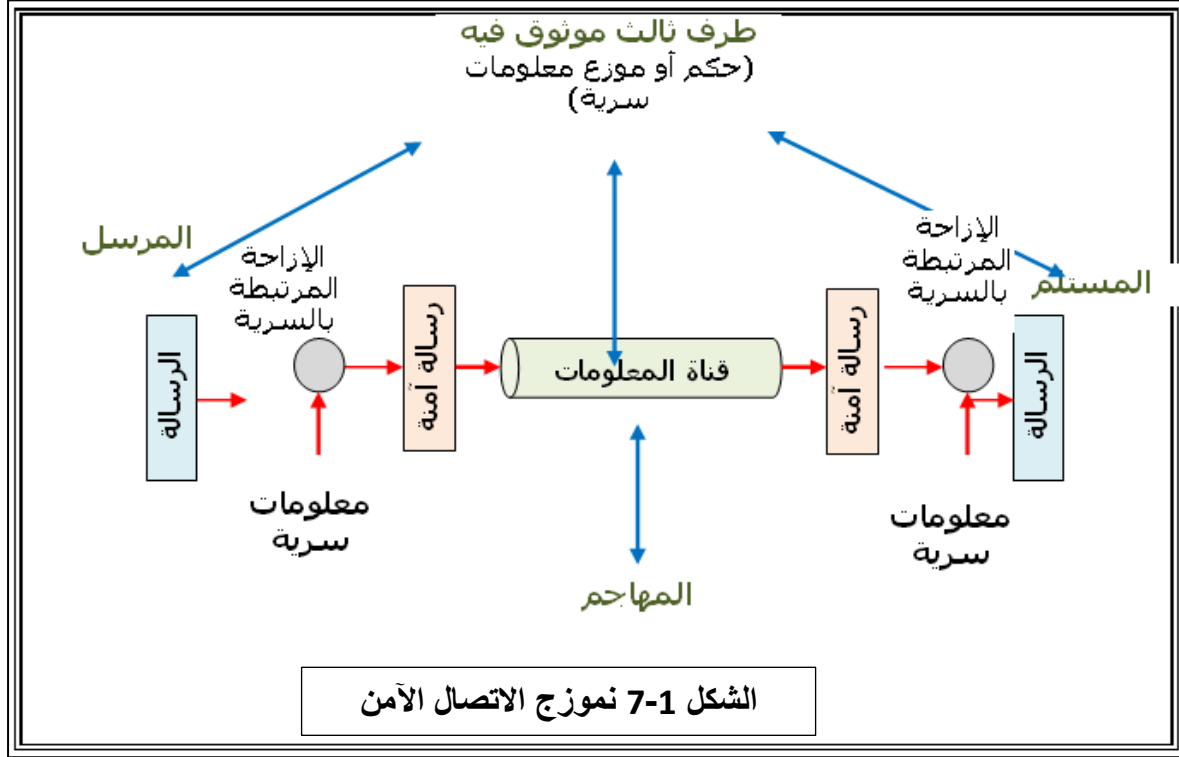
10-1 نموذج أمن الشبكات

الشكل (1-7) يوضح نماذج انسياب المعلومات على قنوات الاتصال الآمنة، في حالة تواجد مهاجم محتمل. يعتمد نموذج الاتصال الآمن هذا على آليات نقل آمنة (استخدام خوارزميات تشفير) مع مفتاح مناسب يمكن أن يتفاوض عليه مع طرف ثالث موثوقٍ فيه. بدراسة هذا النموذج العام تتضح ضرورة القيام بأربع مهام أساسية لتصميم خدمة اتصال آمنة وهي:

- تصميم خوارزمية مناسبة للنقل الآمن (خوارزمية تشفير).
- توليد معلومات سرية (مفاتيح) لاستخدامها مع الخوارزميات.
- تطوير أساليب للمشاركة في المعلومات السرية وتوزيعها.

- تحديد بروتوكول يمكن من أطراف الاتصال من استخدام النقل والمعلومات السرية لخدمة الأمن.

هذه المطلوبات سندرسها بالتفصيل في الوحدات القادمة.

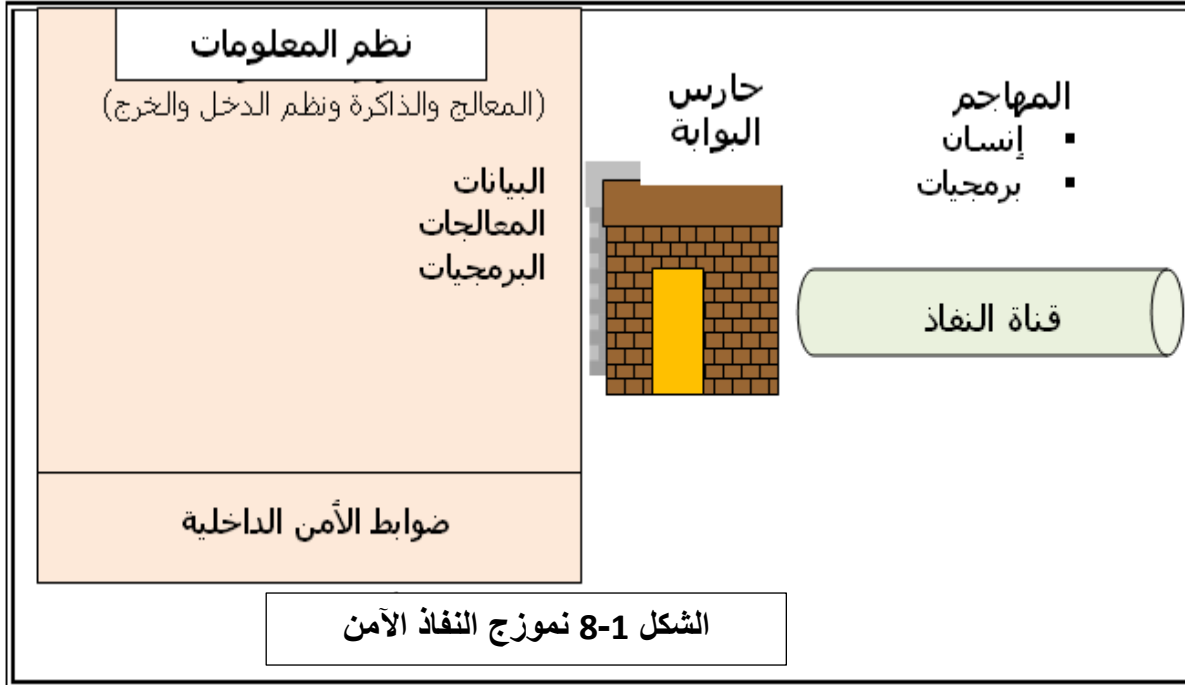


الشكل (1-8)، يوضح نموذج نفاذ أمن إلى الشبكة، حيث يضبط النفاذ إلى المعلومات والموارد في نظم الحاسوب والشبكة وفي حالة تواجد مهاجم محتمل. هنا نحتاج إلى إجراءات مناسبة لضبط النفاذ إلى النظام لتوفير مستوى أمن مناسب، وقد يكون استخدام بعض أساليب التشفير مفيداً هنا

إن استخدام نموذج النفاذ الآمن هذا يتطلب:

- تواجد حارس بوابة (منفذ) للتحقق من المستخدمين.

- تنفيذ ضوابط أمنية للتأكد من نفاذ المستخدمين المخول لهم فقط النفاذ (الوصول) إلى المعلومات والموارد. إن استخدام نظم حاسوب ذات موثوقية قد يكون مفيداً لتنفيذ هذا النموذج، وهذا ما سندرسه في الوحدات القادمة في هذا المقرر.



1-2 توطئة

تعرف الشبكات بصورة عامة بأنها مجموعة من العقد المتصلة ببعضها ، سواء كانت عقد شبكات حاسوب، طرق او اتصالات أو كهرباء ، الخ ..أما شبكات الحاسوب فهي مجموعة مترابطة ومتصلة مع بعضه لغرض تبادل الموارد والمصادر .

في هذه الوحدة سوف يتم التطرق الى انواع وتصنيفات الشبكات و طرق التشبيك المستخدمة

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. قد نتكلم مثلاً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

بناء على ذلك فقد قمت بصياغة مصطلح "أمن الشبكات اللاسلكية" ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات اللاسلكية. تقوم هذه الوحدة بتعريف أمن الشبكات اللاسلكية ضمن سياق أمن المعلومات، أي أننا عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني أمن المعلومات في الشبكات اللاسلكية WLAN.

2-2 تصنيف شبكات الحاسوب

لا يوجد تصنيف عام يمكن ان ينطبق على كل شبكات الحواسيب من الناحية التصميمية التقنية ، ولكن هنالك أربعة معايير أساسية سنركز عليها هي التوزيع الجغرافي وأسلوب الوصول للموارد المشتركة و شكل البنية الفيزيائية ونوع الوسط الناقل.

2-2-1 التصنيف حسب الوصول للموارد المشتركة

في هذا التصنيف يحدد عدد الأجهزة الطرفية التي تتكون منها الشبكة ودرجة صعوبة بناء الشبكة أو بساطتها والسرية والأمان المتاحان في الشبكة ومدى التوسع المستقبلي ودرجة الاستقرار.

(أ) شبكات الند للند

شبكات الند للند Peer to Peer هي شبكات حاسوب محلية تتكون من عدد من الأجهزة وهي مستقلة عن بعضها البعض ولا تتحكم فيها خادم مخصص بل يمكن لكل جهاز أن يكون خادما وزبونا ويطلق على هذا النوع من الشبكات مجموعات عمل حيث تتكون المجموعة من أجهزة تتراوح بين الاثني عشر إلى العشرة. يستطيع أعضاء مجموعة العمل رؤية البيانات والموارد المخزنة على الأجهزة المتصلة بالشبكة والاستفادة منها. ويلاحظ أن مستوى السرية في هذا النوع من الشبكات منخفض كما أنها لا تمتد إلى مسافات بعيدة بل تكون محصورة في مبنى واحد .

(ب) شبكات الزبون/ الخادم Client/Server

في الشبكات المحلية تقوم أجهزة الحاسوب بدور أجهزة الخادم ومحطات العمل. أجهزة الخادم تقوم بإتاحة المكونات المتصلة بها مثل محركات الأقراص والطابعات وأجهزة الاتصال لمحطات العمل. عند اختيار أجهزة الخادم لابد من مراعاة سرعة المعالج الذي يعمل فيه ، وكذلك الحد الأدنى من الذاكرة بحيث تؤدي العمل المطلوب و بكفاءة بحيث تتمحور فكرة هذا النوع من الشبكات في جعل كل الموارد تحت تحكم الوحدة المركزية المتمثلة في الخادم، ومن مميزات شبكة الزبون/ الخادم أنها:

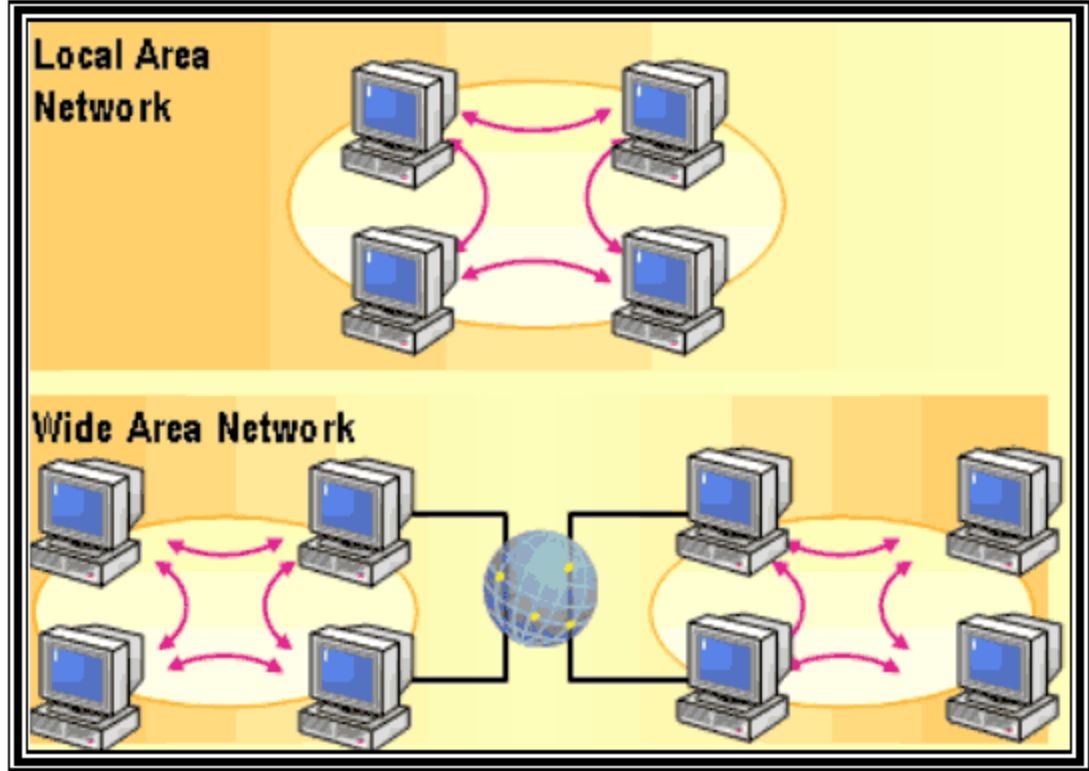
- ذات إعتماذفة عاذفة ومرنة
- تءعم الآلاف من المرءءمءن والتطبفقات
- ءمافة البفاناء من التفف والفققان
- النسخ الاءفاءطف للبفاناء بفورة مننظمة من مكان وااء
- موارء الشبكة متمركرة فف ءهاز الءاءم مما فءعل الوصول للمعلومة أمرا سهلا
- اءم الءاكة إلى شراء أءهزة ءالفة الثمن وبمواصفاء عاذفة للزفائن ءفء فقوم الءاءم بأءلب الأعمال
- ءوففر ءرءة عاذفة من الءمافة ءفء فسمح لمءفر الشبكة فقط ءءكم فف إءارة موارء الشبكة .

2-2-2 ءصنف الشبكات ءسب ءوزفء الءءرافف

ءصنف الشبكات ءسب المساحة الءءراففة ءفء ءشءها إلى:

أ) الشبكات المءلفة Local Area Network

وهف شبكات ذات ملكفة ءاصة عموماً لا ءءاوز أبعاءها عدة كفلومءراء . ءءءءم ءالباً لرفط مءموعة من الءواسفب الشءصففة وكءلك مءطاء العمل فف مكاءب شركة او مصنء؁ لءمكنفها من المشاركة بالمصادر وءبائل المعلومات ففما بفنفا.



الشكل (1-2) : شبكة محلية وشبكة مناطق واسعة

(ب) الشبكات الإقليمية (MAN) Metropolitan Area Networks

ويطلق عليها أيضاً شبكات المدن أو شبكات الانفاق فقد صممت (MAN) لنقل البيانات عبر مناطق جغرافية شاسعة ولكنها ما تزال تقع تحت مسمى المحلية وهي تصلح لربط مدينة او مدينتين متجاورتين ويستخدم في ربط هذا النوع من الشبكات الألياف البصرية او الوسائل الرقمية فهذه التقنية تقدم سرعات فائقة .

(ج) شبكات المناطق الواسعة (WAN) Wide Area Networks

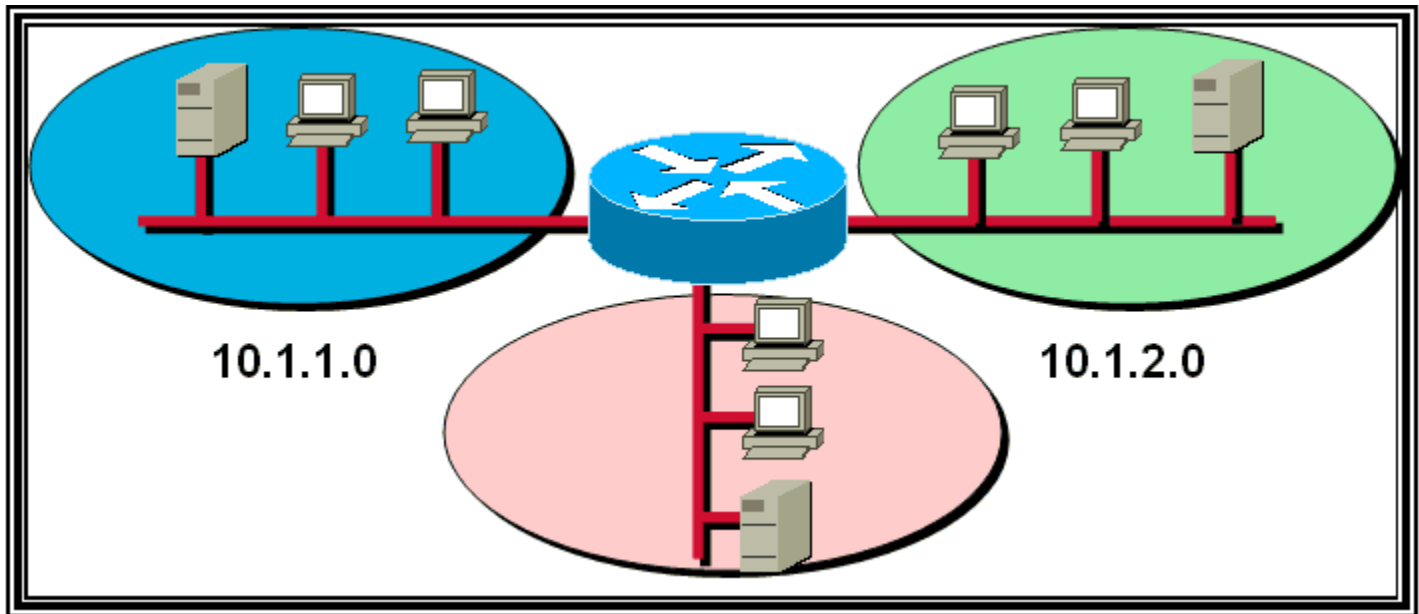
أما شبكات المناطق الواسعة WANS فهي تغطي مساحات كبيرة جدا مثل ربط الدول مع بعضها البعض ومن مميزات هذا النوع أنها تربط آلاف الأجهزة و تنقل كميات كبيرة من البيانات لا يمكن نقلها إلا بهذه الوسيلة. وتضم تقنيات ربط متعددة مثل:

. التبديل بالدوائر Circuit Switched

. التبديل بالحزم Packet Switched

. التبديل بالإطارات Frame Relay

. نمط الإرسال غير المتزامن (ATM Asynchronous Transmission) Mode



الشكل (2-2): العلاقة بين الأجهزة المضيفة والشبكة الفرعية او الواسعة

2-2-3 تصنيف الشبكات حسب الوسط الناقل

يتم انتقال المعلومات بوسائط الانتقال المعروفة Transmission media مثل الأسلاك متحدة المحور

coaxl والأسلاك الملفوفة twisted pair ، وأجهزة اللاسلكي wireless والألياف الضوئية fiber .

كما توجد تقنيات عديدة Communication Techniques تساعد في تحسين عملية الاتصال مثل

التشفير encoding والربط interface والبروتوكولات protocols . كما يستخدم أسلوب الضغط

compression والدمج multiplexing لزيادة فعالية النقل Transmission efficiency

(أ) الشبكات السلكية :

وهي شبكات تستخدم فيها الأسلاك متحدة المحور coaxl والأسلاك الملفوفة twisted pair ، والألياف

الضوئية fiber كوسائط لنقل المعلومات .

(ب) الشبكات اللاسلكية Wireless Networks

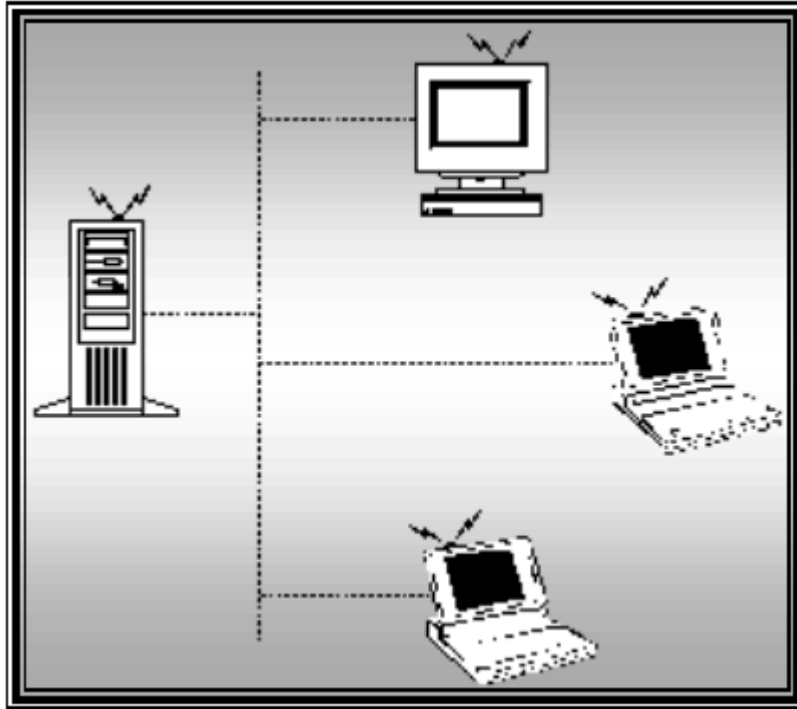
الشبكات اللاسلكية هي أي نوع من الشبكات الحاسوبية التي تعمل على نقل المعلومات بين العقد من دون

استخدام الأسلاك (التوصيلات) إن هذا النوع من الشبكات ينفذ عادةً مع نظم نقل معلومات بالتحكم عن بُعد

من خلال استخدام أمواج كهرومغناطيسية كالأمواج الراديوية كحامل لإشارة المعلومات. وهذا التنفيذ يتم عادةً

في الطبقة الفيزيائية من الشبكة.

كما إنها شبكات حاسوب محلية لاسلكية يتم فيها ربط جميع أجهزة الحاسوب في مكان واحد باستعمال وسط لا سلكي مثل ذبذبة إرسال الراديو (RF Radio Frequency) أو الأشعة تحت الحمراء (IR Infra Red) بدلاً من الأسلاك ويستطيع المستخدمون أن يكونوا على اتصال بالشبكة دون الارتباط فيزيائياً بين الأجهزة ، او شبكات الهواتف الخلوية .



شكل (2-3) شبكة اتصال لاسلكي

2-2-4 أنواع الشبكات اللاسلكية :

يمكن تقسيم الشبكات اللاسلكية لثلاثة أنواع أساسية وذلك بناء على الهيكل البنائي الخاص بها

- شبكات لاسلكية محلية LANS

- شبكات لاسلكية محلية ممتدة Extended LANs
- شبكات لاسلكية لأجهزة متقلة Mobile Computer

2-2-5 مميزات الشبكات اللاسلكية :

قد أصبحت الشبكات اللاسلكية محل اهتمام الكثيرين ممن يعملون في هذا المجال وذلك لان المكونات

اللاسلكية يمكنها القيام بالتالي :

- توفير ما يعرف بالتوصيلات المؤقتة لأي شبكة تستخدم نظام الكابلات .
- المساعدة في توفير بديل احتياطي للشبكات القائمة .
- إمكانية تحويل بعض مكونات الشبكة بأن تكون قابلة للحركة من مكان لآخر .
- إمكانية توسيع ومد الشبكات خارج الحدود المادية القائمة
- إمكانية تغطية الأماكن الصعبة والأثرية
- سهولة تركيب الشبكة

2-2-6 تصنيف الشبكات حسب البنية Network Topology

هنالك عدة مخططات لتوصيل الشبكات وبناءها (Topology) والتي يمكن استخدامها في شبكات البث

الإذاعي .

عندما يكون الممر الرئيسي خط في شبكة البث الإذاعي ، يكون هنالك جهاز واحد في لحظة ما هو

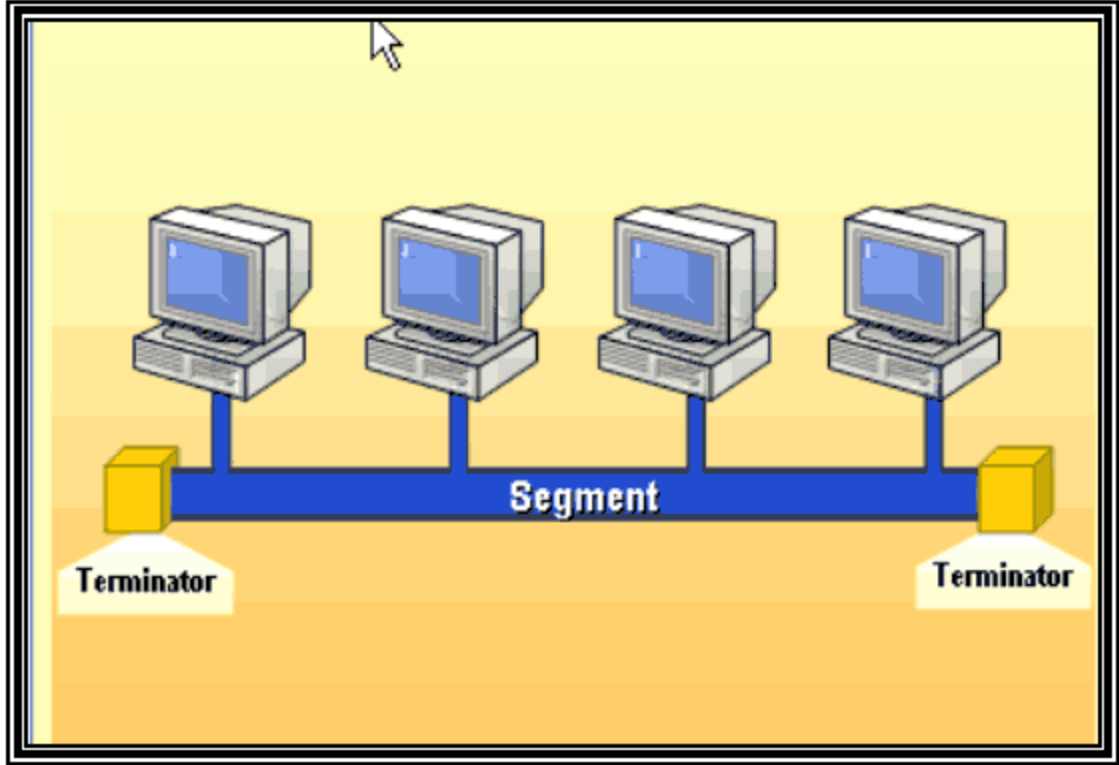
المرسل (Sender) وهو المسموح له بالبث والإرسال على الشبكة، وتمنع بقية الأجهزة من الإرسال خلال

هذه الفترة الزمنية. وهنا تظهر الحاجة لطريقة تساعد في فك التعارض عندما يحاول جهازان الإرسال في آن واحد و يكون الحل من النوع المركزي أو الموزع. وتعتبر تقنية IEEE802.3 المعروفة باسم (Ethernet) هي طريقة غير مركزية تعمل مع الشبكات ذات الممر المشترك وبسرعات مختلفة منها 10/100 Mbps ، وتستطيع الأجهزة التي تعمل على هذه الشبكة أن تقوم بالبث في أي وقت تريده ، فإذا حدث تعارض " تصادم" بين جهازين قاما بالإرسال في فترة زمنية واحده ، فإن كل منهما يقوم بالانتظار لفترة زمنية عشوائية قبل ان يعاودا الإرسال مرة أخرى . أما النوع الآخر من أنظمة البث الإذاعي هو الحلقة ، حيث يتم إرسال كل رسالة عبر الحلقة بشكل مستقل ودون انتظار اكتمال الإطار الذي تنتمي إليه، وعادة ما يستغرق البث المرسل عبر الحلقة ويزمن يساوي تقريباً الوقت اللازم لإرسال عدة رسائل . وهي مثل باقي نظم البث الإذاعي هنالك حاجة لوسيلة تحكم لفض التعارض الناتج من المحاولات المتزامنة للدخول من قبل محطات العمل المختلفة.

ولتخطيط أي شبكة لابد من وضع وتحديد حدود المساحة التي ستغطيها الشبكة ، بالإضافة إلي تحديد التقنية التي تستخدم في هذه الشبكة . وتنقسم شبكات الحاسوب إلى ثلاث بنى شائعة الاستخدام هي:

أ) البنية الخطية Bus Topology

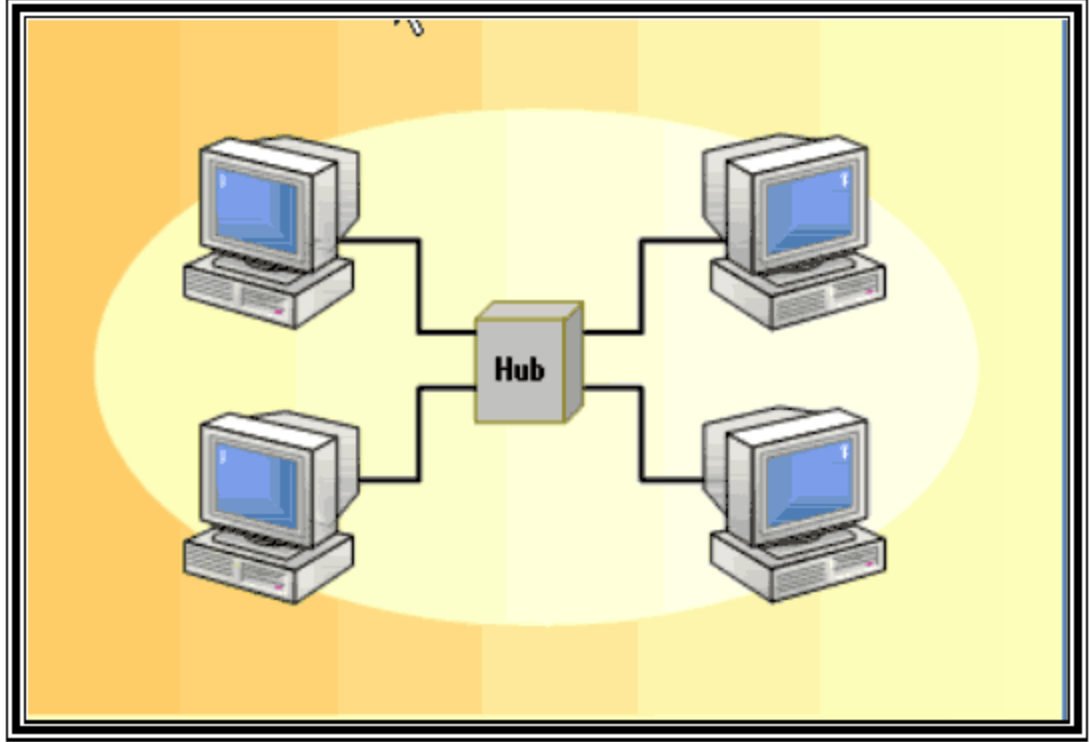
في هذه البنية تتصل كل وحدات الشبكة بسلك واحد مركزي يمثل مسار الاتصال الرئيسي. وهو يربط كل وحدات الشبكة في هذه البنية كما في الشكل (2-4).



الشكل (2-4): البنية الخطية

ب) البنية النجمية Star Topology

في هذه البنية تتصل كل الوحدات مباشرة بوحدة الخدمة المركزية بسلك خاص و بشكل يشبه النجمة. هذه البنية أصبحت شائعة الاستخدام حالياً بعد أن أصبحت تستخدم في شبكات البث الإذاعي لتحل محل البنية الطولية وذلك لتفادي الأعطال التي تحدث في البنية الطولية ، كما هو موضح في الشكل (2-5).



الشكل (2-5): البنية النجمية

ج) البنية الحلقية Ring Topology

هذه الشبكة تربط كل الوحدات في شكل حلقة ليس لها بداية أو نهاية ، وهذه البنية ليست شائعة الاستخدام لأن الشبكة تتوقف كلياً عن العمل بمجرد توقف أو عجز أحد الأجهزة ، على الرغم من أن كل وحدة تعمل على فحص الإشارة عند استقبالها ثم تكبيرها لتمريرها عبر الشبكة إذا لم تكن تلك الإشارة موجهة إليها

2- 3 الحاجة إلى الشبكات اللاسلكية networkswireless

لقد نجح علماء الحاسوب في الآونة الأخيرة الذين منهم إلى استخدام ما يسمى بالشبكات المحلية، والتي يرمز لها LAN اختصاراً لكلمة (Local Area Network) وأن الهدف الأساسي من ذلك تحقيق الفائدة القصوى المرجوة من الموارد التي تتيحها الأجهزة على الشبكة وبالفعل فقد وفرت هذه الشبكات العديد من الخدمات لمستخدميها حيث مكنتهم من التواصل مع بعضهم البعض عن طريق البريد الإلكتروني والاستفادة من البرامج والتطبيقات بالإضافة إلى إمكانية الولوج إلى قواعد بيانات مشتركة لكن هذا لم يمنع من ظهور بعض العوائق والتي بدأت تحد من اتساع استخدام هذه الشبكات يمكن أن نحدد أهم هذه العوائق بما يلي :

الحاجة إلى وصلة فيزيائية حيث يتوجب على الجهاز الاتصال إلى منفذ ثابت مما جعل عدد العقد ضمن الشبكة يميل إلى الثبات، إضافة إلى تقييد المستخدم في مكان معين دون إمكانية التنقل.

إضافة إلى الانتشار الواسع للحواسيب يمكن القول بأن الميزات التي قدمتها ال WLAN للأجهزة المحمولة والمفكرات الإلكترونية قد أدت إلى زيادة الطلب على هذه التقنية الجديدة والتي ستلعب دوراً هاماً في حياتنا الإلكترونية في المستقبل القريب حيث يتوجه العالم في العصر الحديث إلى استبدال النظام السلكي الذي تم الاعتماد عليه في العقود الماضية والانتقال إلى عصر جديد من الأجهزة اللاسلكية.

كما تجدر الإشارة إلى الاختلاف بين ال Wide Area Network (WAN) و LAN (WLAN Wireless) والتي ترسل المعلومات الرقمية إلى مسافات طويلة باستخدام الأنظمة الخلوية بمعدل نقل بيانات منخفض

إضافة حاجتها إلى بنية تحتية ذات تكلفة عالية... نقله لأن هذا الأمر يتطلب قطع الاتصال مع الشبكة وإعادة الاتصال من موقع آخر

أما إذا أردنا إضافة عقدة جديدة إلى الشبكة فهذا يعني المزيد من التوصيلات السلكية

والمزيد من المساحة وهذا ما يؤدي بدوره إلى زيادة التكلفة. إن هذه العوامل قد أدت إلى صعوبة في إنشاء هذه الشبكات وارتفاع سعرها مما دعا إلى ضرورة تعديلها بحيث تتلاءم مع متطلبات العصر، بناءً عليه بدأ التوجه إلى استخدام الشبكات اللاسلكية (Wireless LAN) والتي قدمت الحلول للمشاكل التي عانت منها الشبكات السلكية، حيث أعطت مرونة كبيرة في عملية إضافة عقدة جديدة إلى الشبكة دون الحاجة إلى المزيد من التوصيلات السلكية، والأهم هو إمكانية التنقل بحرية مع الجهاز المحمول ضمن مجال الشبكة، هذا مع الأخذ بعين الاعتبار الكلفة المنخفضة لهذه الشبكات.

مع ظهور الشبكات المحلية اللاسلكية (WLAN) أصبح الآن بإمكان الشخص التنقل في أي مكان يريده وحتى بالأماكن العامة وهو حاملاً جهاز الحاسب المحمول أو ال(لاب توب) وبدون أي أسلاك يستطيع ان يرسل أو يتلقى أي بريد إلكتروني والتصفح في الإنترنت بحرية كاملة وأصبح بإمكان المسافرين في الأول من أبريل 2004 على متن طائرات شركة طيران المانية خلال الرحلات عبرت المحيط الاطلسي استخدام المحمول للاتصال بالإنترنت وكل هذا بفضل التقنيه الجديده وهي الشبكات المحليه اللاسلكيه (WLAN \wireless) (local area network) وتسمح هذه التقنيه بالاتصال بشبكة الإنترنت عبر إشارة الراديو (radio frequency/RF) بدلا من الاتصال عبر الاسلاك. اما النقاط الساخنه فهي عباره عن الأماكن التي يستطيع الشخص فيها استخدام تقنية الربط اللاسلكي بالإنترنت. ان عدد النقاط الساخنه وصل إلى مئات الالاف في جميع أنحاء العالم بحلول عام 2005 تعتمد تقنية النقاط الساخنه على عنصرين رئيسيين للاتصال:

1. بطاقة حاسب لاسلكي

1. بطاقات الحاسب اللاسلكيه (wireless computer cards) وقد تكون موجوده بالجهاز المحمول أو أي جهاز اخر أو قد تكون قابلة للاضافه به.تحتوي هذه البطاقه على هوائي داخلي أو خارجي.



الشكل (2-6) بطاقة حاسوب لاسلكي

شكل (2-7) نقطة وصول لاسلكي

2. نقطة الوصول (access point) التي تصل الشبكات المحليه اللاسلكيه بشبكة الإنترنت. اما بالنسبة للطائرات التي تحتوي على نقاط ساخنه فيتم حل مشكلة نقطة الوصول عبر هوائي خارج الطائرة مرتبط باقمار صناعيه خاصه تصله بالشبكة عبر محطات استقبال ارضيه.

بالنسبة للسرعه والتكلفه فان تقنية الشبكات المحليه اللاسلكيه باستخدام إشارات الراديو (WLAN) بالمقارنه بالتقنيات الأخرى فقد استطاعت التغلب على مشكلة نقل المعلومات لاسلكيا لمسافات بعيدة نسبيا بتكلفه

معتدلة"فمثلا تفوقت على تقنية نقل المعلومات عبر الأشعة تحت الحمراء حيث كانت محدودة لمسافات لا تزيد عن 20 مترا وهي غير قادرة على اختراق الحواجز، أيضا تفوقت على تقنية Universal Mobile Telecommunications System المستخدمة في الهاتف المحمول؛ لأن نقل المعلومات في تقنية WLAN أسرع بكثير وبتكاليف معتدلة؛ ولأن تقنية UMTS في الهاتف المحمول غير متواجدة بكميات كافية في السوق حاليا. هذه مقارنه بين الشبكات السلكية (Wired) واللاسلكية (Wireless LAN) الشبكات اللاسلكيه أصبحت أكثر استعمالا في المؤسسات والبيوت.

2-4 أنواع الشبكات اللاسلكية

1. شبكات PAN (شبكة المناطق الشخصية)

شبكات المناطق الشخصية (Wireless Personal Area Network) هي الشبكات التي تصل بين أجهزة ضمن مساحة صغيرة نسبياً، عادةً ما تكون هذه المساحة ضمن مجال يمكن لشخص الوصول إلى جميع أجزائه. كمثال على ذلك، فإن تقنية البلوتوث تقوم مثلاً بربط حاسوب شخصي مع سماعات. وكذلك فإن تقنية ال ZigBee تدعم تطبيقات هذا النوع من الشبكات.

2. شبكات LAN

شبكات المناطق المحلية (Wireless Local Area Network) هي النوع الأكثر شيوعاً من الشبكات اللاسلكية. تقوم بربط الأجهزة على مسافة أبعد من النوع السابق كمنزل أو مكتب أو حتى بناء وفي بعض الأحيان تمتد لتغطي عدة كيلومترات. معظم الشبكات LAN تعتمد على المعيار IEEE 802.11 الذي يحتوي على معايير للشبكات اللاسلكية المحلية التي تعمل في الحزم الترددية 2.4، 3.6 و 5 GHz وتضم عدداً من

البروتوكولات المختلفة. ان الخصائص المهمة لهذه الشبكة بالمقارنة مع شبكة الـ WAN هي أنها تنقل البيانات بسرعات أعلى بكثير حيث تقوم بنقل البيانات بسرعة 10 إلى حدود 10000 ميجابت لكل ثانيه Mbps. الشبكات المحليه الحاليه - غير اللاسلكية على الأغلب هي مستنده على معيار الايثرنت.

واي فاي وهو اسم مستخدم بصورة شائعة كبديل عن التسمية IEEE 802.11 مع أن هذا الاستخدام خاطئ من الناحية العلمية. لأن Wi-Fi هو شعار لشركة يدل على إمكانية اتصال الأجهزة التي تتبع المعيار السابق معاً.

شبكات لاسلكية محدّدة (Fixed Wireless Data): وهي شبكات لاسلكية تُستخدم لتحقيق اتصال بين جهازين أو شبكتين في مكانين مختلفين. يتم ذلك من خلال استخدام موجات صغيرة أو أشعة ليزرية على مدى خط البصر (of Sight Line) وغالباً ما يُستخدم هذا النوع من الشبكات لربط شبكات في أبنية متجاورة دون الحاجة إلى ربط هذه الأبنية فيزيائياً مع بعضها.

3. شبكات MAN

شبكات المناطق الكبيرة (Wireless Metropolitan Area Network) تقوم بربط عدة شبكات LAN مع بعضها البعض لتحقيق شبكة لاسلكية تمتد على رقعة جغرافية متوسطة الحجم مثل عبر حرم جامعي أو مدينة. الخدمة التي توديتها مشابه للخدمة التي يقوم بها مزود الإنترنت (ISP).

WiMAX هو التعبير المستخدم للإشارة إلى هذا النوع من الشبكات ويتناوله المعيارين IEEE 802.16d و IEEE e802.16 الموضوعين من قبل جمعية مهندسي الكهرباء والإلكترونيات.

هناك ميزتان لهذا النوع من الشبكات

حجم هذا النوع من الشبكات أكبر من الـ LAN. العديد من الـ MAN تغطي منطقة بحجم مدينة وبعضها تغطي مجموعه من البنايات أي ما يعادل مساحه قطر ما بين 5 إلى 50 كيلومتر.

الـ MAN تعمل كشبكة ذات سرعات عاليه لتسمح بمشاركه المصادر المحليه الإقليميه. كثيرا ما تُستخدم لتزويد أو دعم اشتراك الاتصال مع شبكات أخرى باستخدام وصله للـ WAN.

4. شبكات الأجهزة الخلوبية

إن التطور الذي حصل في الآونة الأخيرة في مجال الشبكات الخلوبية مكّننا من نقل معطيات ومعلومات عن طريق هذه الشبكات بالإضافة إلى الهدف الأساسي منها ألا وهو نقل المحادثات بين جهازين خلوبيين:

النظام العالمي للمواصلات الجواله (GSM) Global System for Mobile Communications: وهو معيار لاتصال الأجهزة الهلوبية مع بعضها. يتألف من 3 أنظمة أساسية: النظام القاعدي (Base Station System)، نظام العمليات والمساعدة (Operation and Support System) ونظام التحويل (Switching System). عند القيام بمكالمة، يتم الاتصال أولاً مع النظام القاعدي الذي يقوم بالاتصال مع نظام العمليات والمساعدة الذي يقوم بدوره بالاتصال مع نظام التحويل وأخيراً، يقوم هذا النظام بإيصال المكالمة إلى وجهتها. يعد نظام الـ GSM أكثر أنظمة الاتصالات الخلوبية شيوعاً حيث يُقدّر أن 80% من الهواتف الخلوبية في العالم تعمل على هذا النظام.

خدمة الاتصالات الشخصية PCS Personal Communications Service: وهي شبكة رادوية تُستخدم من قبل بعض مستخدمي الهواتف الخلوبية في أميركا الشمالية.

لعبت الشبكات اللاسلكية دوراً كبيراً في الاتصالات العالمية منذ الحرب العالمية الثانية فعن طريق استخدام الشبكات اللاسلكية، يمكن إرسال معلومات لمسافات بعيدة عبر البحار بطريقة سهلة ،عملية وموثوقة. منذ ذلك الوقت، تطورت الشبكات اللاسلكية بشكل كبير وأصبح لها استخدامات كثيرة في مجالات واسعة، نذكر منها: الهواتف الخليوية تشكل أنظمة شبكات ضخمة حول العالم يزداد استخدامها يوماً للتعامل بين أشخاص من جميع أنحاء العالم.

إرسال معلومات كبيرة الحجم لمسافات شاسعة أصبح ممكناً من خلال الشبكات اللاسلكية من خلال استخدام الأقمار الصناعية للتواصل.

الاتصالات العاجلة - كاتصال أفراد الشرطة مع بعضهم - أصبحت أسهل بكثير باستخدام الشبكات اللاسلكية.

أصبح بإمكان الأفراد والشركات على حدّ سواء استخدام هذه الشبكات لتوفير اتصال سريع سواءً كان ذلك على مسافات قريبة أو بعيدة.

من أهم فوائد الشبكات اللاسلكية هو استخدامها كوسيلة رخيصة وسريعة للاتصال بالإنترنت في المناطق التي لا توجد فيها بنية تحتية تسمح بتوفير هذا الاتصال بشكل جيد كما هو الحال في معظم الدول النامية.

من أهم إيجابيات الشبكات اللاسلكية التي جعلتها تنتشر بشكل كبير وتحلّ محلّ الشبكات السلكية:

المرونة (wirelessness): للشبكات اللاسلكية فوائد أكثر من الشبكات السلكية وإحدى هذه الفوائد المرونة إذ تمر موجات الراديو بالحيطان والحاسوب اللاسلكي يمكن ان يكون في أي مكان على نطاق الاكسس بوينت.

سهولة الاستخدام: الشبكات اللاسلكية سهلة إلى الإعداد والاستعمال فقط برنامج مساعد وتجهيز الحاسوب النقل أو الدسك توب ببطاقة شبكة اصالات لاسلكية وهناك حواسب مجهزه بهذه البطاقه مثل أجهزة سنترينو.

التخطيط: ان الشبكات السلكية واللاسلكية يجب أن تكون مخططة بدقه ولكن الاسوء في الشبكات السلكية انه يجعل منظر الجدران غير مرتب وتعدد الاجهزة يكلف في عملية الصيانه ان مكونات الشبكات السلكية هي (كابلات ،سويتش، هب، مسير.....الخ) لذلك يجب أن نخطط لها بعنايه ام بالنسبة للشبكات اللاسلكية فهي أسهل بكثير من ذلك المنطق ولكن يجب أن نخطط لهذه الشبكات لانماط الاستعمال الفعليه

مكان الاجهزه: الشبكه اللاسلكيه يمكن تكون مخفيه يمكن ان توضع من وراء الشاشات وهي هذه الشبكات مناسبه تماما للأماكن أو المواقع التي يكون من الصعب ربط شبكه سلكيه فيها مثل المتحف البنايات القديمه.

المتانه: شبكات اللاسلكي ممكن ان تكون متينه ولكن ممكن ان تعاني من التداخل الاذاعي من الأجهزة الأخرى والأداء يمكن ان يضعف عند محاولة المستخدمين استعمال نفس الاكسس بوينت.

الاسعار: ان اسعار الشبكات اللاسلكيه كانت غاليه كانت بطاقة الـ PCI اللاسلكيه تكلف 100 يورو عام 2000 وفي نهاية 2004 أصبحت تكلف 30 يورو فقط وهذا يعني ان الاسعار الآن ليست عاليه وان الشبكات اللاسلكيه أصبحت اختيار الكثير من مستخدمي البيوت.

على الرغم من هذه الفوائد، فإن الشبكات اللاسلكية لا تخلو من بعض المشاكل لعل أهمها:

مشكلات التوافق: فالأجهزة المصنوعة من قبل شركات مختلفة قد لا تتمكن من الاتصال مع بعضها أو قد تحتاج إلى جهد إضافي للتغلب على هذه المشاكل.

إن الشبكات اللاسلكية تكون غالباً أبطأ من الشبكات النوصولة مباشرةً باستخدام تقنيات الإيثرنت Ethernet.

الشبكات اللاسلكية أضعف من حيث حماية الخصوصية لأن أي شخص ضمن مجال تغطية شبكة لاسلكية يمكنه محاولة اختراق هذه الشبكة. من أجل حل هذه المشكلة، يوجد عدة برامج تؤمن حماية للشبكات اللاسلكية مثل الخصوصية المكافئة للشبكات السلكية (Wired Equivalent Privact (WAP التي لم تؤمن الحماية الكافية للشبكات اللاسلكية وال (Wi-Fi Protected Access (WPA التي أظهرت نجاحاً أكبر في منع الاختراقات من سابقتها.

2- 5 الشبكات الافتراضية الخاصة (VPN)

الشبكة الخاصة الافتراضية (Virtual Private Network) هي شبكة افتراضية لوجود لها في الواقع ولكنها مع ذلك تؤدي واجبها على اكمل وجه كأكثر أنواع الشبكات أمانا واكثرها شيوعا وحتى استخداما بين الشركات الكبيرة

و كونها شبكات افتراضية فلا بد من وجود داعم حقيقي يحمل هذه الافتراضية إلى أرض الواقع.. لا بد لهذا الداعم ان يكون مستيقظا كل الوقت جاهزا ومستعدا في أي لحظة وهنا كانت الشبكة العنكبوتية لتثبت انها دائما الأرض الخصبة لكل من اراد بقليل من الجهد.

هذه الشبكات الافتراضية هي نفسها الشبكة العنكبوتية لكن تم توظيف خصائصها لتلائم سرية نقل البيانات والحفاظ على امن المعلومات، كما تتم حماية البيانات بشكل عام عادة بتشفيرها بحيث يصعب فهمها إذا ما تمت سرقتها... لكن أيضا حتى تشفير المعلومات لا يكفي أحيانا إذا وضعنا بعين الاعتبار وجود أنواع كثيرة من آليات التشفير والتي يمكن كسرها بطريقة أو بأخرى وما أكثر الامثلة هنا ابتداءا بسرقة ارقام البطاقات

الائتمانية وانتهاءا بسرقة البرامج القيد البرمجة من اصحابها وغيرها الكثير من الامثلة... لذلك كان لابد دائما من اتباع لوغارتومات قوية ومؤكدة من شركات كبيرة وذات اسم لامع في عالم التشفير كنقطة مبدئية للعمل على هذه الشبكات الافتراضية.

2-5-1 مكونات الشبكة الافتراضية

بشكل عام تتكون الشبكات الافتراضية من مكونين أساسيين اولهما العميل وثانيهما بوابة الاتصال (GateWay)

الشبكة الافتراضية تتم حمايتها في ثلاث نقاط عبور وهي :

1. بوابة الاتصال (GateWay)

2. الشبكة الهدف (Target Network)

3. العملاء (Clients)

والشبكة الخاصة الافتراضية عبارة عن توصيل جهازين أو شبكتين معا عن طريق شبكة الإنترنت كما هو موضح في الصورة وهي تقنية تعتمد في عملها على بروتوكول حيث يطلق عادة على عملية إنشاء اتصال خاص بين جهازي كمبيوتر من خلال شبكة وسيطة كالإنترنت اسم نقل البيانات عبر مسار امن (Tunneling) حيث يتم إنشاء هذا المسار بين جهازي الكمبيوتر مباشرة.

تستخدم الشبكات الافتراضية البروتوكولات المعتمدة عليها تقنية VPN ، PPTP ، Point-T-Point Protocol Tunneling : Layer Two Tunneling Protocol Tunneling وهما البروتوكولان الرئيسيان

المعتمد عليهما ال IP Security Protocol : VPN IPSec وهو بروتوكول النظام الأمني لل VPN يتضمن IPsec بعض تقنيات التشفير القوية لحماية البيانات.

6-2 مميزات وعيوب استخدام VPN

المميزات :

1. يوفر الكثير من المال خاصة في تكاليف الأجهزة.

2. يسهل ادارته واكثر يسرا

عيوبه :

1. إذا لم تقوم بتوثيق المستخدمين والشبكات بشكل قاطع ستصبح هناك فرصة للمتطفلين للوصول إلى

بياناتك ومصادك

2. ما زال IPsec وحتى الآن في طور التجربة.

تتطلب هذه التقنية في الجهاز المراد الاتصال به خدمة Real IP address والتي هي عبارة عن ميزة يتم الحصول عليها من مزود خدمة الإنترنت الذي تدخل عن طريقه إلى شبكة الإنترنت وهي الحصول على عنوان IP ثابت لجهازك يبقى ثابتاً في كافة الأحوال، أي حتى إذا انقطع الاتصال وأعيد وصله.

ان فكرة الشبكات الافتراضية الخاصة أو ما يعرف بال Virtual Private Networks وتذكر اختصاراً ب VPN، قد ساهمت في تخفيض تكاليف نقل المعلومات الخاصة بالشركات والمؤسسات بين فروعها البعيدة عن

المقر الرئيسي لها وبين المستخدم المنزلي الذي يريد الوصول إلى معلوماته المتوفرة في جهاز الحاسب المنزلي.

قد تملك شركة من الشركات مكتباً واحداً، وقد تملك مكاتب كثيرة متوزعة في أنحاء مختلفة من البلاد أو خارج البلاد. قد يعمل موظفوها من المكتب الرئيس hdoifh لها أو من خلال المكاتب المتوزعة في أنحاء البلاد أو حتى من خلال بيوتهم أو مواقعهم البعيدة كحقول النفط في البحار. في مثال الشركة ذات المكتب الواحد، استخدام الشبكة العادية أو ما يعرف بالLocal Area Network والتي تعرف اختصاراً بال LAN باستخدام تقنية الايثرنت، قد يكفي لايصال وربط كافة أجهزة الكمبيوتر الموجودة في المكتب مع بعضها البعض، ولكن للمكاتب البعيدة كأمثلة التي ذكرناها في الأعلى، فان الشركة تحتاج إلى شيء آخر غير ال LAN.

في الماضي، كان المستخدم البعيد أو الموظف الذي يعمل من منطقة بعيدة عن المقر الرئيس للشركة يتصل من خلال مودم عادي للشركة باستخدام خطوط الهاتف. يقوم سرفر ومودم اخر موجودان في مقر الشركة بالرد على اتصال الموظف ليقوم بعمله ويتم اقفال الخط بعد الانتهاء من العملية. سلبيات هذه الطريقة كانت من عدة نواحي منها كلفة فواتير الهاتف المتصل من المستخدم البعيد، ايجار الخطوط، سرعة الاتصال البطيئة، بالإضافة إلى اشغال خط الهاتف أثناء فترة الاتصال. رغم هذه السلبيات كانت العملية نوعاً ما آمنة لأنها كانت تصل الطرفان بشبكة مغلقة ومسار خاص. كانت الشركات المقتدرة تستخدم خطوط عالية السرعة تسمى بالLeased Lines لتتغلب على مشكلة السرعة لكنها كانت تدفع مبالغ ضخمة في مقابل هذه الخدمة لربط النقطتين بشكل متواصل وبسرعة عالية وبشبكة خاصة آمنة نوعاً ما.

عندما انتشرت شبكة الإنترنت في كل مكان، كانت هناك فرصة استخدامها كوسيط لنقل المعلومات وكشبكة يمكن من خلالها نقل المعلومات من مكان إلى آخر بأسعار زهيدة مقارنة بالطريقة السابقة، ولم يكن هناك داعٍ لتوصيل نقطتين مع بعضها فيمكن الاتصال من أي جهاز في العالم بأي جهاز في العالم ان كانا متصلين بالإنترنت. وان كانت نوعية الاتصال بين الجهازين هو الـ ADSL فان التكلفة تكون ثابتة ومناسبة والاتصال قائم بشكل مستمر .

المشكلة المنتظر ان يتم الاتصال بها للوصول إلى المعلومات الخاصة بها، ويقوم الجدار الناري بابعاد مستصفحي الإنترنت ومنعهم من الدخول أو الوصول إلى السرفر الخاص بالشركة إلا من خلال كمبيوترات معينة تختارها الشركة.

الفكرة الرئيسة في مسألة الشبكة الافتراضية الخاصة هي عبارة عن بناء "نفق" خاص بين الجهازين كما في الصورة، النفق أو الـ VPN Tunnel هو عبارة عن معلومات خاصة ومشفرة يتم تبادلها بين الجهازين الذين يقومان بفك التشفير عند استلام المعلومات من الطرف الآخر من النفق الافتراضي بعد أن يبعد الجدار الناري أي اتصال غير مرخص له من مدير النظام أو المسؤول عن الشبكة في الشركة أو فرعها. الفكرة هي حماية المعلومات من خلال النفق المشفر للبيانات وأيضاً التأكد من هوية الجهاز المتصل من خلال الجدار الناري الذي لن يقبل أي اتصال غريب .

في هذه الطريقة هي ان اتصال الجهازين عبر شبكة الإنترنت يعرضهما مع المعلومات الخاصة بالشركة إلى الاختراق، وهذا الاتصال يعتبر غير آمن ولن تقبل به الشركات والمؤسسات لما يحمله من مخاطر، فكان لا بد من ايجاد حل لمشكلة الامن هنا ولهذا تم اصدار الشبكات الافتراضية الخاصة.

الشبكة الافتراضية الخاصة توفر الأمن للشبكة الخاصة بالإضافة إلى الأسعار المناسبة باستخدام شبكة الإنترنت.

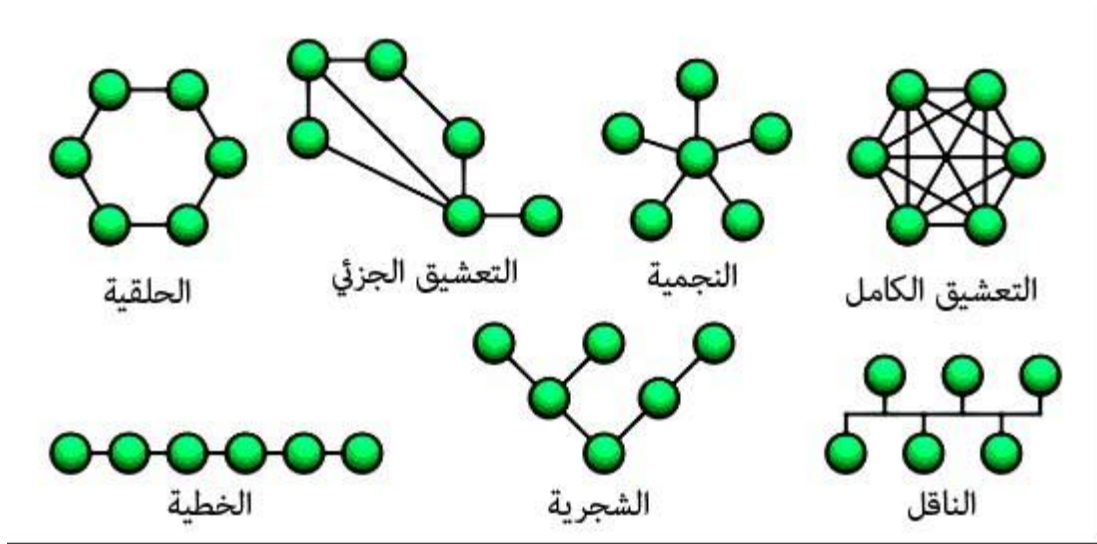
هنا يجب فصل الطرفين عن الإنترنت من الناحية الطريقة، عن طريق وضع الأجهزة في نطاق IP معين وخاص كشبكات محلية خاصة بكل جهة. يجب وضع جدار ناري أو Firewall للجهة التي ستستلم الاتصال

6-2 البنية التحتية للشبكات

بنية الشبكة هي مخطط ربط الوصلات بين نقاط شبكة ما. تتخذ الشبكات أشكالاً مختلفة تبعاً لكيفية توصيل النقاط المكونة للشبكة مع بعضها البعض. يمكن توصيف بنية الشبكة بأسلوبين: فيزيائياً أو منطقياً. تمثل البنية الفيزيائية توزيع الأسلاك، الحواسيب وتجهيزات الشبكة الأخرى في حين تمثل البنية المنطقية الطبقة النظرية الأعلى كأسلوب ومسار نقل البيانات بين النقاط على سبيل المثال فيما يلي شرح موجز لمجموعة من بنى الشبكات الأساسية جداول (1-2).

الشرح	البنية
ترتبط جميع النقاط بسلكٍ مشترك. تعمل شبكات الإيثرنت عادةً وفق بنية الناقل.	الناقل Bus
ترتبط كل نقطة مباشرةً مع مجمّع مركزيّ أو مركزٍ للشبكة. تعبر جميع البيانات في البنية النجمية المجمع المركزي قبل بلوغ وجهتها. يشيع استخدام هذه البنية في شبكات الإيثرنت والشبكات اللاسلكية.	النجمية Star
مجموعة من النقاط المرتبطة ضمن خط. ترتبط كل نقطة مع النقطتين المجاورتين لها ما عدا نقاط الطرفية التي تملك كل منها نقطةً مجاورةً واحدةً.	الخطية Line
وهي دمج لبنيتي الناقل والنجمية. تتألف من مجموعةٍ من النقاط المرتبطة بشكلٍ نجمي تتصل بعمودٍ فقاريّ على شكل ناقل.	الشجرية Tree
تترتبط جميع النقاط مع بعضها البعض على شكل حلقةٍ مغلقةٍ بحيث ترتبط كل نقطة مباشرةً مع نقطتين أخريين. تستخدم عادةً في الأعمدة الفقارية للبنية التحتية من الألياف الضوئية.	الحلقية Ring
وصلة مباشرة بين كل زوجٍ من النقاط. إن التعشيق الكامل لـ n نقطة يتطلب $n(n-1)/2$ وصلةً مباشرةً. مع أن هذه البنية تعتبر مكلفةً إلا أنها عالية الوثوقية. تستخدم بشكلٍ رئيسٍ في التطبيقات العسكرية.	التعشيق الكامل Full Mesh
يتم ترتيب بعض النقاط بأسلوب التعشيق الكامل أما البقية فتربط بنقطةٍ واحدةٍ أو نقطتين فقط. تعتبر هذه البنية أقل كلفةً من بني التعشيق الكامل إلا أنها بالتأكيد أقل وثوقيةً نتيجة تخفيض عدد الوصلات الإضافية.	التعشيق الجزئي

جدول (1-2) توصيف بني الشبكات الأساسية



شكل (8-2) بنى الشبكات الأساسية

6-2-1 بنى الشبكات اللاسلكية

فيما يلي أقدم بعض الملاحظات العامة لمساعدة على استيعاب كيف ولماذا يمكن أو لا يمكن استخدام بعض بنى الشبكات أثناء تصميم الشبكات اللاسلكية. قد تبدو هذه الملاحظات بديهية إلا أن استيعابها يعتبر أساسياً للتصميم الناجح للشبكات اللاسلكية.

- لا يتطلب الإتصال اللاسلكي أي ناقل

في حين لا يتطلب الإتصال اللاسلكي أية أسلاك أو ماشابه فإنه لا يحتاج أيضاً لأي ناقل آخر كالهواء، الفراغ أو أي مادة ناقلة. إن الخط المرسوم في مخطط شبكة لاسلكية يكافئ وصلة "محتملة" يتم إنجازها، أي أنه لا يمثل سلكاً أو أي رابط فيزيائي.

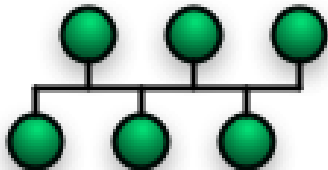
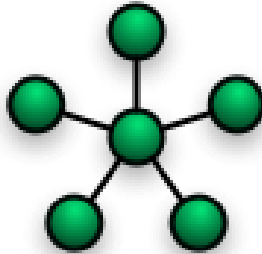
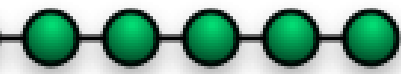
- الإتصال اللاسلكي ثنائي الإتجاه دائماً

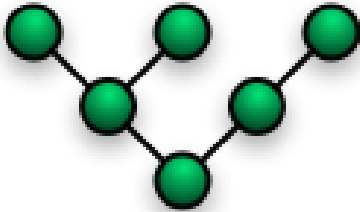
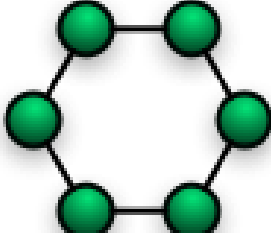
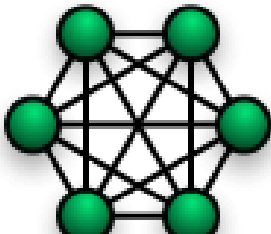
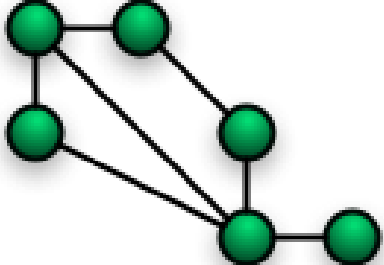
لا توجد قاعدة بلا استثناء، ففي حالة التحسس الخامل Passive Sniffing أو التلصص لا يكون الإتصال ثنائي الإتجاه.

تتحقق هذه الثنائية بغض النظر عما إذا كنا نتحدث عن المرسلات أو المستقبلات، الأسياذ أو الزبائن.

مرسل الراديو لا يعدو مجرد كونه مرسل راديو، وتتحدد مهامه وفقاً للبرمجيات المستخدمة

تحدد البرمجيات المستخدمة كيفية تصرف مرسل الراديو حتى الطبقتين الأولى والثانية من نموذج OSI المعياري (أي الطبقتين الفيزيائية ووصلة البيانات) الجدول (2-2) يوضح البنى التحتية للشبكات اللاسلكية.

العلاقة بالشبكات اللاسلكية	التمثيل البياني	البنية
لا يمكن تطبيقها. نلاحظ لدى دراسة بنية الناقل بأن كل نقطة ترتبط بجميع النقاط الأخرى لكن وبما أن موقع التقاء خط واحد مع الخطوط الأخرى غير موجود في حالة الشبكة اللاسلكية فإن هذه البنية تكافئ تماماً شبكة معشقة بالكامل تعمل ضمن قناة واحدة.		الناقل Bus
نعم، وهي البنية المعيارية للشبكات اللاسلكية.		النجمة Star
نعم، مع عنصرين أو أكثر. الخط بين نقطتين يمثل وصلة من نقطة إلى نقطة .PtP		الخط Line

نعم، تستخدم عادةً من قبل مزودي خدمات الإنترنت اللاسلكية.		الشجرة Tree
نعم، ممكنة إلا أنها نادرة الاستخدام.		الحلقة Ring
نعم، إلا أنها على الأغلب معشقة جزئياً.		التعشيق الكامل Full Mesh
نعم.		التعشيق الجزئي Partial Mesh

جدول (2-2) بني الشبكات اللاسلكية

7-2 مكونات الشبكات اللاسلكية

1. نقطة الولوج Access Point

تشكل نقطة الولوج "مجمّعاً" لاسلكياً. يربط المرسل/المستقبل النقاط اللاسلكية ببعضها البعض كما يقوم أيضاً بربطها مع الشبكة السلكية. ممن الممكن أن تربط مجموعة من نقاط الولوج ببعضها البعض وفق ترتيبٍ معيّن

لبناء شبكةٍ لاسلكيةٍ كبيرةٍ، كما تقوم نقطة الولوج من وجهة نظر المستخدم اللاسلكي - أو الزبون - (مثل

الحواسيب المحمولة أو المحطات النقالة) بتوفير سلكٍ إفتراضي يصل بين محطات المستخدمين. يربط هذا "السلك اللاسلكي" محطات المستخدمين ببعضها البعض كما يربط هذه المحطات بالشبكة السلكية.

يجب التمييز بين نقطة الولوج والموجّهات اللاسلكية Wireless Routers والمنتشرة بكثرة في الأسواق هذه الأيام. يتألف الموجّه اللاسلكي من نقطة وولوجٍ بالإضافة إلى موجّه للشبكة، لذلك فهو قادرٌ على القيام بمهام أكثر تعقيداً من تلك التي تقوم بها نقطة الولوج. يمكنك اعتبار الموجّه اللاسلكي جسراً لاسلكياً Wireless Bridge (يصل بين الشبكة اللاسلكية وشبكة الإنترنت السلكية) وموجّهاً (يقوم بتوفير ميزات توجيه حزم بروتوكول الإنترنت IP Routing).

يتصل الزبائن بنقاط الولوج بعد معرفة "أسماء" هذه النقاط. يسمى هذا الأسلوب للتعريف بمعرف مجموعة الخدمات Service Set Identifier (SSID) والذي يجب أن يتشاركه جميع الأعضاء في شبكة لاسلكية محددة. ينبغي أن يتم إعداد جميع نقاط الولوج وزبائن الشبكة اللاسلكية الموجودين ضمن مجموعة خدماتٍ موسّعة واحدة Extended Service Set (ESS) لاستخدام نفس المعرف (SSID).

لتبسيط الفكرة يمكنك اعتبار معرف مجموعة الخدمات SSID كـ "صاقة تعريف منفذ الإنترنت". أي أنّ الإتصال مع شبكة لاسلكية تملك المعرف SSID (س) يكافئ ربط حاسبك الشخصي بشبكة سلكية عبر منفذ إنترنت على الحائط يحمل لصاقة تعريفٍ كتب عليها (س).

1-7-2 زبائن الشبكة اللاسلكية Wireless Clients

زبون الشبكة اللاسلكية هو أي محطة لاسلكية تتصل بشبكة محلية لاسلكية لمشاركة مواردها. يتم تعريف المحطة اللاسلكية بأنها أي حاسوبٍ يحتوي على بطاقة شبكة لاسلكية ترسل وتستقبل الإشارات الراديوية RF.

من زبائن الشبكة اللاسلكية الشائعة: الحواسيب المحمولة، أجهزة الحواسيب الكفّية PDA، تجهيزات المراقبة اللاسلكية وهواتف نقل الصوت عبر بروتوكول الإنترنت VoIP اللاسلكية.

2-7-2 أنماط الشبكات اللاسلكية

تعرّف مجموعة معايير 802.11 نمطين أساسيين للشبكات اللاسلكية:

- الشبكات الخاصة
- شبكات البنية التحتية

لا بدّ من الإنتباه إلى أنّ بنية الشبكة قد لا تعكس هذه الأنماط مباشرةً وعلى الدوام. مثلاً، قد تعمل وصلةً لاسلكيةً بين نقطتين Point-to-Point ضمن النمط الخاص أو ضمن نمط البنية التحتية، كما يمكنك أن تجد شبكةً نجميةً مبنيةً بالإعتماد على وصلاتٍ خاصة.

يمكن اعتبار نمط الشبكة اللاسلكية كأحد الإعدادات الأساسية لبطاقة شبكةٍ لاسلكيةٍ محددةٍ وليس كأحدى خصائص البنية التحتية بأكملها.

3-7-2 النمط الخاص (IBSS) Ad hoc Mode

يعتبر النمط الخاص (والذي يعرف أيضاً بنمط الند للند Peer-to-Peer) أحد أساليب الربط المباشر بين زبائن الشبكة اللاسلكية. إن السماح لزبائن الشبكة اللاسلكية بالعمل ضمن النمط الخاص يلغي الحاجة إلى استخدام أيّ نقاط وولوجٍ مركزية. تستطيع جميع النقاط ضمن شبكةٍ لاسلكيةٍ خاصةٍ التواصل مباشرةً مع النقاط الأخرى.

ينبغي إعداد بطاقات الشبكة اللاسلكية في جميع زبائن الشبكة اللاسلكية الخاصة للعمل ضمن النمط الخاص واستخدام نفس معرف مجموعة الخدمات SSID ورقم القناة "Channel Number".

تتألف الشبكة اللاسلكية الخاصة عادةً من مجموعة صغيرة من الأجهزة المتوضّعة قرب بعضها البعض. ينخفض أداء الشبكة اللاسلكية كلما ازداد عدد النقاط الموجودة ضمنها. يتطلب ربط الشبكة اللاسلكية الخاصة بشبكة محلية سلكية أو بالإنترنت إعداد بوابة مخصصة لهذا الغرض، كلمة "Ad hoc" لاتينية الأصل وتعني "لهذا الغرض" إلا أنها غالباً ما تستخدم للتعبير عن الحلول أو الأحداث المرتجلة أو غير المعد لها.

تستخدم معايير IEEE 802.11 مصطلح (مجموعة الخدمات الأساسية المستقلة Independent Basic Service Set IBSS) للإشارة إلى النمط الخاص للشبكات اللاسلكية.

1. الحالة 1: الربط بين نقطتين

يمكنك استخدام النمط الخاص للربط بين نقطتين بشكل مباشر (إذا ما رغبت على سبيل المثال بربط بنائين معاً). كما يمكن استخدام هذا النمط لربط مجموعة من محطات العمل ضمن المكتب، إذا كانت إحدى النقطتين مربوطة مع شبكة محلية أو مع الإنترنت فإنها قد تتيح أو تمنع الوصول إلى هذه الشبكة من النقطة الأخرى.

2-7-4 نمط البنية التحتية (BSS) Infrastructure Mode

تحتوي الشبكات العاملة ضمن نمط البنية التحتية - خلافاً للشبكات الخاصة التي لا تتضمن عنصراً مركزياً - على عنصرٍ يقوم بمهمة التنسيق: نقطة وولوج أو محطة مركزية. يمكن لزبائن الشبكة اللاسلكية الوصول إلى الشبكة السلكية عبر نقطة الولوج فيما إذا كانت هذه النقطة موصولةً بالشبكة السلكية.

عند احتواء الشبكة على عدّة نقاط وولوج وعدد من الزبائن ينبغي إعدادها جميعاً لاستخدام نفس المعرف SSID. إذا ما رغبت في التأكد بأن شبكتك اللاسلكية تعمل باستطاعتها القصوى عليك ألا تقوم بإعداد جميع نقاط الولوج الموجودة ضمن نفس الموقع الفيزيائي لاستخدام نفس القناة. يقوم الزبائن باكتشاف (عبر مسح نطاق الترددات) القناة التي تستخدمها نقطة الولوج وبالتالي لا حاجة لهذه الزبائن في معرفة رقم القناة مقدماً.

تستخدم معايير IEEE 802.11 مصطلح (مجموعة الخدمات الأساسية Basic Service Set BSS) للإشارة إلى نمط البنية التحتية للشبكات اللاسلكية.

2. الحالة 1: الشبكة النجمية

تعتبر البنية النجمية أكثر بنى الشبكات اللاسلكية انتشاراً، وهي البنية المعتمدة عادةً في بقع التغطية اللاسلكية Hot Spot سواء وجدت في مطار أو ضمن مركزٍ للولوج البعيد Telecenter. يستخدم مزودو خدمات الإنترنت اللاسلكية بشكلٍ عامٍ البنية النجمية (وذلك لوصول نقطةٍ إلى عدة نقاط). غالباً ما يتم توسيع هذا النوع من الشبكات إلى البنية الشجرية أو إلى تجميعها مع أشكالٍ أخرى للشبكات اللاسلكية.

الإعداد	نقطة الولوج / البوابة	النقطة x1
النمط	بنية تحتية	بنية تحتية
معرف مجموعة الخدمات SSID	تحدد المعرف MY_SSID	تتصل بالمعرف MY_SSID
القناة	ينبغي أن يتم تحديد القناة بالتوافق بين النقطتين	ينبغي أن يتم تحديد القناة بالتوافق بين النقطتين
عنوان الإنترنت IP	(يمكن التوجيه)	عادةً ما تحصل على عنوان الإنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP

جدول (2-3) إعداد نموذجي لشبكة لاسلكية نجمية

3. الحالة 2: الربط بين نقطتين

تعتبر الوصلات بين نقطتين Point-to-Point (PtP) إحدى العناصر الأساسية للبنية التحتية للشبكة اللاسلكية. يمكن أن توجد هذه الوصلات على مستوى بنية الشبكة اللاسلكية كجزء من شبكة نجمية، كوصلة بسيطة بين نقطتين أو ضمن أية بنية أخرى. يمكن أن تعمل الوصلة بين نقطتين ضمن النمط الخاص أو نمط البنية التحتية.

الإعداد	النقطة 1	النقطة 2
النمط	أي نمط	أي نمط
معرف مجموعة الخدمات SSID	MY_SSID	MY_SSID
القناة	تحدد القناة س	تكتشف القناة س
عنوان الإنترنت IP	عادةً ما يكون ثابتاً	عادةً ما يكون ثابتاً
العنوان الفيزيائي MAC	يمكن أن يتم تثبيته تبعاً للعنوان الفيزيائي للنقطة المقابلة	يمكن أن يتم تثبيته تبعاً للعنوان الفيزيائي للنقطة المقابلة

جدول (2-4) إعداد نموذجي لوصلة لاسلكية بين نقطتين. يمكن للوصلة أن تعمل ضمن النمط الخاص أو

نمط البنية التحتية لكن ينبغي أن يتم إعداد النقطتي للعمل ضمن نفس النمط.

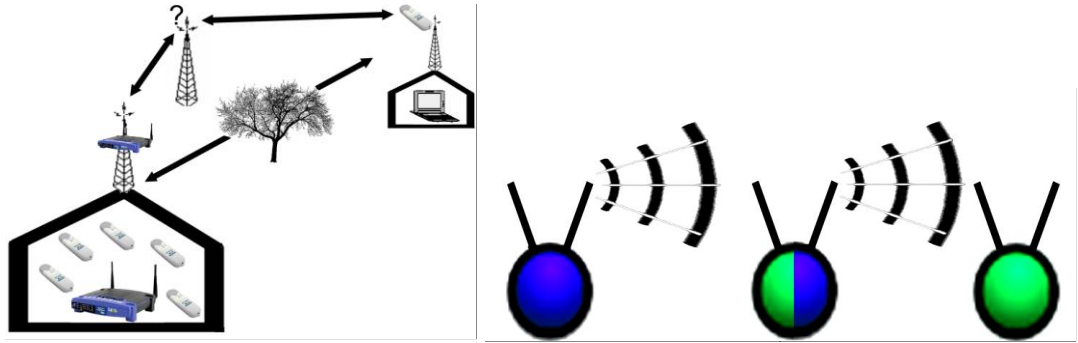
يتوجب في حالة الوصلات بين نقطتين ذات المدى البعيد إجراء بعض الإعدادات المتقدمة لتحسين أداء

الوصلة.

4. الحالة 3: التكرار Repeating

تبرز الحاجة إلى التكرار في حال وجود عوائق تعترض خط النظر أو عندما تكون المسافة طويلة جداً بحيث لا يمكن تغطيتها بوصلة واحدة. يعتبر المجمع في الشبكات السلكية مكافئاً للتكرار في الشبكات اللاسلكية. يعتمد إعداد التكرار بشكل كبير على معايير خاصة بالتجهيزات والبرمجيات المستخدمة مما يجعل توصيفه بشكل عام أمراً صعباً، قد تتألف وحدة التكرار من جهاز فيزيائي واحد أو جهازين كما قد تحتوي جهاز إرسال راديوي واحد أو اثنين. يمكن أيضاً اعتبار وحدة التكرار كزبون مستقبل ونقطة وروج لإعادة الإرسال. يتم استخدام معرف مجموعة الخدمات SSID نفسه عادةً لكلٍ من هذه الوحدات الثلاثة.

في كثيرٍ من الأحيان ترتبط وحدة التكرار بعنوان فيزيائي بالإضافة إلى معرف SSID.



الشكل (2-9) مثالين للتكرار ضمن البنى التحتية للشبكات اللاسلكية

5. الحالة 4: الشبكات المعشقة Mesh

تعتبر الشبكات المعشقة Mesh خياراً جيداً في المناطق الحضرية بشكلٍ أساسي إضافةً إلى المواقع النائية التي يصعب فيها تركيب البنى التحتية المركزية. من الحالات الشائعة لاستخدام الشبكات المعشقة الشبكات البلدية Municipal Networks، شبكات الحرم الجامعي Campus Networks وشبكات المجتمعات المتجاورة Neighbourhood Communities.

تستخدم الشبكات المعشقة واحدةً من بنيتين أساسيتين للوصلات: البنية المعشقة بالكامل Full Mesh أو البنية المعشقة جزئياً Partial Mesh. ترتبط كل نقطة في الشبكة المعشقة بالكامل بجميع النقاط الأخرى، أما في الشبكات المعشقة جزئياً فإن كل نقطة ترتبط مع بعض النقاط الأخرى وليس جميعها.

لاحظ بأنّ هذا التعريف لا يشير إلى أي اعتمادٍ على أي عاملٍ زمني، أي أنه ليس من الضروري أن تتضمن الشبكة المعشقة أي شيء ديناميكي. مع أنه في السنوات الأخيرة انتشر استخدام مصطلح "الشبكة المعشقة" كمرادفٍ للشبكات "الخاصة Ad hoc" أو "النقالة Mobile"، ينبغي أن تتضمن جميع النقاط ضمن الشبكة المعشقة نفس برنامج (بروتوكول) التوجيه، لكنها قد تحتوي أنظمة تشغيلٍ مختلفةٍ أو تتألف من تجهيزاتٍ مختلفةٍ.

يعتمد إعداد الشبكة المعشقة على بروتوكول التوجيه المستخدم وكيفية تشغيله. يظهر الجدول التالي بعض الإعدادات الشائعة.

النقطة x2	النقطة x1	الإعداد
خاص	خاص	النمط
MY_SSID	MY_SSID	معرف مجموعة الخدمات SSID
القناة س	القناة س	القناة
عادةً ما يكون ثابتاً ويتم إعداده يدوياً	عادةً ما يكون ثابتاً ويتم إعداده يدوياً	عنوان الإنترنت IP
يمكن أن يتم تثبيته تبعاً للعنوان الفيزيائي للنقطة المقابلة	يمكن أن يتم تثبيته تبعاً للعنوان الفيزيائي للنقطة المقابلة	العنوان الفيزيائي MAC

جدول (2-5) إعداد نموذجي لشبكة معشقة.

ليس من السهل استخدام بروتوكول الإعداد التلقائي للمضيف DHCP في الشبكات المعشقة، لذلك ينصح باستخدام عناوين الإنترنت IP الثابتة. تتطلب البوابات إعدادات إضافية لتصبح قادرة على التعريف بوجودها، لا تغطي هذه الوحدة كيفية إجراء هذه الإعدادات.

2-8 الموجات اللاسلكية الكهربية

تنتشر الموجات اللاسلكية الكهربية بسرعة 300000 كيلومتر في الثانية، أي بسرعة الضوء. و يطلق عليها اسم موجة لأنها تنتشر على شكل الموجات التي تنجم عن إلقاء حجر في بركة ماء ساكنة، و يجري قياس الموجات اللاسلكية الكهربية بالأمتار طولا، و الطول هنا بالمسافة بين قيمتي موجتين متتاليتين أو بين نقطتين متشابهتين في هاتين الموجتين.

كما و تقاس الموجات بترددتها، و التردد هنا (أو الذبذبة) هو عدد الموجات في الثانية الواحدة، و يعرف

أيضا بالدورة في الثانية (سايكل) أو بالهرتز. و بما أن عدد الموجات الراديوية فانه من السهل معرفة العلاقة بين طولها بالأمتار و ذبذبتها بالكيلوهرتز.

*هنريش هرتز فزيائي ألماني طور التجهيزات اللازمة لبث واستقبال الموجات الكهرومغناطيسية وذلك في الثمانينات من القرن التاسع عشر.

*أثبتت معادلات العالم الرياضي ماكسويل انه بالإمكان إنتاج موجات كهرومغناطيسية بتيار كهربائي يتغير اتجاهه بتردد سريع.

*تيار القطاع الكهربائي بقوة 220 فولت يتغير اتجاهه 100 أو 120 مرة في الثانية. إنه تيار متردد يقال عنه انه بتردد أو بذبذبة 50 أو 60 هرتز نسبة إلى العالم الفيزيائي هرتز.

*لكي يتم إنتاج موجات راديوية ,يجب على التيار الكهربائي أن يتذبذب بسرعة أقوى تبلغ بضعة آلاف أو ملايين مرة في الثانية، صنع هرتز آلة تحدث تيارات كهربائية متذبذبة (نواس) وذلك باستعمال بكرات ناقلة للقوة الكهربائية تنتج ذبذبات بتواتر عالي.

2-8-1 ماكسويل والموجات الخفية J.Maxwell

أي علاقة توجد بين الكهرباء والمغناطيسية ؟ هذا هو السؤال الذي تكلف العالم الإيرلندي جيمس ماكسويل (1830- 1879) بالإجابة عنه. لقد فكر هذا العالم المنظر مليا في المر مستعينا بالعمليات الرياضية والفيزيائية.

في سنة 1864 رأى ماكسويل على انه بالإمكان إحداث " موجات " في الهواء بواسطة تيار متغير داخل جهاز موصل و تماما كما يفعل حجر عندما يسقط في الماء محدثا تموجات دائرية , لذلك أطلق اسم الموجات الكهرومغناطيسية على تلك الموجات المغناطيسية التي يتم استقبالها بأجهزة كهربائية.

تحدث ماكسويل سوى شكلا مرئيا لموجات كهرومغناطيسية ، وان كل هذه الموجات تنتشر بسرعة الضوء ، وهو المر الذي أكدته التجارب العلمية بعد ماكسويل.

2-8-2 طيف الموجات اللاسلكية الكهربائية

ينقسم طيف الموجات، حسب أطوال الموجات المستخدمة في البث و الإستقبال، إلى تسع حزم من الذبذبات، ابتداء من 3 كيلوهرتز و حتى 3000 جيجا هرتز. و فيما يلي قائمة بحزم الذبذبات الأكثر استخداما، و قد استثنينا منها الحدين الأقصى و الأدنى من حزم الذبذبات.

من 30 إلى 300 كيلوهرتز = (LF .ذبذبة واطئة BANDS5) حزمة 5

موجات يقاس طولها بالكيلومترات (موجات طويلة) : من 10 إلى 1 كيلومتر.

من 30 إلى 3000 كيلوهرتز = (MF .ذبذبة متوسطة BANDS6) حزمة 6

موجات متوسطة من 1000 إلى 100 متر.

من 3 إلى 300 ميغاهرتز = (HF .ذبذبة عالية BANDS7) حزمة 7

موجات يقاس طولها بعشرات الأمتار (موجات قصيرة) من 100 إلى 10 متر.

من 30 إلى 300 ميغاهرتز = (VHF .ذبذبة عالية جدا BANDS8) حزمة 8

موجات يقاس طولها بالأمتار من 10 إلى متر واحد.

من 300 إلى 3000 ميغاهرتز = (UHF .ذبذبة فوق العالية BANDS9) حزمة 9

موجات يقاس طولها بعشرات السنتيمترات من 10 إلى 1 سنتيمتر.

من 3 إلى 30 جيجا هرتز = SHF. الذبذبة أكبر من العالية BANDS10 حزمة 10

موجات يقاس طولها بالسنتيمترات من 10 إلى 1 سنتيمتر.

من 30 إلى 300 جيجا هرتز = (EHF). الذبذبة الفائقة العلي BANDS11 حزمة 11

موجات ميليمترية: من 10 ملليمتر إلى ملليمتر واحد.

LOW FREQUENCY (L.F.) ذبذبة واطئة:

MEDIUM FREQUENCY (M.F.) ذبذبة متوسطة:

HIGH FREQUENCY (H.F.) ذبذبة عالية:

VERY HIGH FREQUENCY (V.H.F.) ذبذبة عالية جدا:

ULTR HIGH FREQUENCY (U.H.F.) الذبذبة فوق العالية:

SUPER HIGH FREQUENCY (S.H.F.) الذبذبة أكبر من العالية:

EXTRA HIGH FREQUENCY (E.H.F.) الذبذبة الفائقة العلي:

2-8-3 توزيع حزم الموجات للبت الإذاعي:

من السهل ملاحظة أن هذه الحزم الموجية المخصصة للبت الإذاعي تشغل منطقة صغيرة جدا ضمن طيف

الذبذبات حيث تبدأ ب10 كيلوهرتز وتنتهي ب275 جيجا هرتز، أي ما يعادل 275000000 كيلوهرتز. أما

باقي الحزم الموجية فقد خصصت لأنواع الكثيرة الأخرى من الاتصال، وجدير بالذكر أن الذبذبات التي تم

تحديدها للبت الإذاعي وللاتصالات اللاسلكية في المؤتمر العالمي الإداري للإذاعات الذي عقد عام 1979،

قد بدأت بالدخول في حيز التنفيذ اعتبارا من عام 1982 وبشكل تدريجي.

2-9-4 الموجات الكهرومغناطيسية

*تعتبر الموجات الكهرومغناطيسية شكلا من أشكال الطاقة . تنتشر هذه الموجات انطلاقا من مصدرها على شكل تركيبات كهربائية ومغناطيسية . تخترق هذه الموجات الهواء وعددا من المواد وحتى الخواء الكائن بين النجوم.

*لا نستطيع سماع الموجات الكهرومغناطيسية ولا الإحساس بها ، لكننا نستطيع رؤية بعض من أشكالها

كالأشعة الضوئية التي هي شكل من أشكال الإشعاع الكهرومغناطيسي .

*يمكننا مع ذلك الإحساس بتأثير بعض هذه الموجات في شكل حرارة مثلا.

*موجات الراديو هي شكل آخر من أشكال الموجات الكهرومغناطيسية كالأشعة

السينية و الموجات micro-ondes.

*تسافر الموجات الكهرومغناطيسية بسرعة الضوء (299 792 كلم في الثانية) . يمكن لهذه الموجات أن

تدور سبع مرات ونصف المرة حول الكرة الأرضية في زمن لا يتعدى ثانية واحدة.

*تختلف الموجات الكهرومغناطيسية عن بعضها البعض باختلاف " طول الموجة " وهي المسافة التي تفصل

نقطة معينة من الموجة عن النقطة المقابلة لها على الموجة التالية.

*يبين الرسم أسفله طيف الموجات الكهرومغناطيسية مع بعض أطوال الموجات النموذجية.

2-8-5 انتشار الموجات بالراديو:

تنتشر موجات الراديو في خط مستقيم. ولهذا السبب و باعتبار أن الأرض كروية الشكل، فإن هذه الموجات

تبتعد عن سطح الكرة الرضية بشكل مستمر يؤدي بها التلاشي في الفضاء. ولكن ذلك لا يحدث بفضل

الانعكاسات التي تحدثها طبقات الجو العليا تتلقى جزيئاتها الإشعاعات الشمسية فتشحن كهربيا- وهي الظاهرة المعروفة باسم التأين- بحيث تصبح قادرة على رد بعض الموجات اللاسلكية الكهربائية التي تعود إلى سطح الأرض من جديد بقفزات متعاقبة. ويطلق على هذه الطبقات المتأينة من الجو اسم (طبقات الجو الأيونية) أو (الأيونوسفير) أو الغلاف الأيوني.

وينقسم الغلاف الأيوني إلى عدة طبقات، توجد على ارتفاعات تختلف باختلاف قوة الإشعاع الشمسي الذي تتعرض له .و يؤدي ذلك إلى انتشار موجات الراديو ذات الذبذبات المتفاوتة بطرق مختلفة. فالموجات الطويلة ذات التردد المنخفض لا تنحرف في الغلاف الأيوني وتساير موازية لسطح الأرض حتى تبعد عن كوكبنا نهائيا. ومدى هذه الموجات ثابت، سواء كان الوقت نهارا أم ليلا، بعض النظر عن الفصل من السنة وعن الدورة الشمسية.

أما الموجات المتوسطة ففيها مركب أرضي وآخر أيونوسفيري. وفي النهار تمتص الطبقة السفلى من الغلاف "ولا توجد إلا في النهار وينحصر وجودها D الأيوني المركب اليونسفيرى، وتعرف هذه الطبقة باسم " طبقة بين 50 و 60 كيلومتر بعدا عن سطح الأرض . وتأين هذه الطبقة ضعيف جدا ويتناسب مع ارتفاع الشمس بحيث يكون أقصى حد للتأين في فترة الظهيرة خاصة في شهور القيظ. ولا تقدر هذه الطبقة الجوية على إحداث انحراف في موجات الراديو و لكنها تتميز بمقدرتها على امتصاص الموجات ذات الذبذبة المنخفضة والمتوسطة.

فإن إشارات الموجة المتوسطة تصبح قادرة على الوصول D أما في الليل، عندما تتلاشى طبقة إلى طبقات أعلى من الغلاف الأيوني وهو ما يؤدي إلى انتشارها على مسافات بعيدة عن سطح الأرض. و الطبقة التالية في الغلاف الأيوني هي الطبقة الواقعة في المسافة بين 60 كم و 144 كم بعيدا عن سطح

الأرض، و لا توجد إلا في النهار. و تصل هذه الطبقة إلى الحد الأقصى من التأين وقت الظهيرة و تلعب دورا هاما في انتشار الموجات القصيرة نهارا عبر مسافات لا تتعدى 1600 كم و في انتشار إشارات الموجة المتوسطة ليلا.

نوع من الفقاعات المتحركة ذات التأين الفائق الشدة القادرة على إحداث D و كثيرا ما تتكون داخل طبقة (المشنتة) والتي E وتتشكل هذه الفقاعات الطبقة المعروفة باسم (طبقة VHF. انحراف حتى في موجات تتسبب في إحداث ظواهر الانتشار الشاذة.

هي أهم طبقات الغلاف الأيوني لانتشار الموجات القصيرة لمسافات طويلة. و أثناء الليل توجد هذه F و طبقة الطبقة على مسافة من الأرض تتراوح بين 270 و 320 كم . و تنخفض درجة تأينها بعد غروب الشمس و تصل على معدلها الأدنى قبل بزوغ الشمس.

وأثناء النهار تنقسم طبقة F إلى طبقتين: F1 و F2 و توجد طبقة F1 في المنطقة الواقعة بين 160 و 240 كم بعيدا عن سطح الأرض. أما طبقة F2 فتقع بين 250 كم و 420 كم بعيدا عن سطح الأرض و فيها تتحرف معظم إشارات الموجة القصيرة أثناء النهار.

و يعود انحراف الموجات في طبقة أو أخرى من طبقات الغلاف الأيوني، بل و يعود عدم انحرافها، بامتصاصها من قبل هذه الطبقات أو باختراقها لها، يعود أساسا إلى ذبذبة الموجة. فالإشارات ذات الذبذبات الأكثر انخفاضا تتسم بكونها أضعف قوة مما يجعل امتصاصها أو انحرافها في الطبقات الواطئة أمرا ممكنا. أما الإشارات ذات الذبذبات الأعلى فإنها تتحرف في الطبقات العليا أو تخترقها و ذلك نظرا لكونها أشد قوة و أكثر طاقة.

ويحدث تأين هذه الطبقات من الغلاف الأيوني بسبب الإشعاعات الصادرة عن الشمس. وكلما ازدادت شدة

الإشعاعات الشمسية يزداد شحن الغلاف الأيوني كهربائياً وتزداد مقدرته على كسر الموجات الراديوية التي يتاح لها و الحالة هذه أن تسافر عبر مسافات طويلة بسهولة أكبر. ويزداد الإشعاع الشمسي بزيادة عدد البقع التي يمكن رصدها في الشمس. و رغم أن العلاقة بين الظاهرتين ليست معروفة بشكل جيد بعد فإنه بإمكاننا القول بأن عدد البقع الشمسية يساعد على حساب درجات الإشعاع الشمسي و درجة التأين وانتشار الموجات اللاسلكية الكهربية.

2-8-6 ميزات الحزم الموجية:

1.الموجة الطويلة:

تخصص الموجة الكيلومترية أو الطويلة للبث الإذاعي. أما في أمريكا و آسيا و استراليا فتخصص للخدمات العاملة كالاتصالات اللاسلكية للملاحة البحرية وخدمات الأرصاد الجوية التابعة للطيران المدني. وتتميز هذه الحزمة من الموجات بالنشاط المستمر ليلا ونهارا ويبلغ مداها عدة مئات من الكيلومترات.

2.الموجة المتوسطة:

(في عالم البث الإذاعي AM الموجة الهيكومتريية أو المتوسطة تبث عموما ضمن التعديل الواسع) قاطبة. ويمكن أن تظل صالحة للاستخدام طيلة أربعة وعشرين ساعة يوميا.

3.الحزم الموجية الاستوائية:

نستخدم الحزمة الاستوائية ضمن المناطق الواقعة بين مدار السرطان ومدار الجدي بشكل تقريبي. وهناك أربع حزم موجية تقليدية لهذه المناطق: حزمة أ ل 120 مترا (من 2300 إلى 2495 كيلوهرتز) وحزمة أ ل 90 مترا (من 3200 إلى 340 كيلوهرتز) وحزمة أ ل 75 مترا (من 3950 إلى 4000 كيلوهرتز) وحزمة أ ل 60 مترا من 4750 إلى 4995 كيلوهرتز ومن 50005 إلى 5060 كيلوهرتز.

4. الموجة القصيرة :

تزاوُل هوائية الراديو أو أَل (دي إكس) ضمن حزم الموجة القصيرة بما فيها الموجات الاستوائية. ونظرا للميزات المختلفة لكل من هذه الموجات فإنه من الضروري تقديم شرح مختصر لها كي يكون بمثابة الدليل بالنسبة لهواة الموجة القصيرة الجدد، حزمتي 49 و 41 متر (5950-6020 و 7100-7300 كيلوهرتز تلائم هاتان الحزمتان الموجيتان البث الإذاعي لمسافات قصيرة في الليل أطول بكثير منه في النهار وفي فصلي الخريف والشتاء تصبح هاتان الحزمتان ملائمتين بشكل خاص للمسافات الطويلة بعد غروب الشمس مباشرة وبعد بزوغها، أي عندما يكون مستوى الشحنة الكهربائية الاستاتيكية منخفضا.

ب) حزمة 31 متر 9500-9775 كيلوهرتز

تبدأ الإذاعات الدولية للمسافات البعيدة بهذه الحزمة الموجية ويمكن أن يكون استقبالها ممتاز بين 300 و 3000 كيلومتر.

ج) حزمة 250 متر من 11700-14975

يتوفر أفضل استقبال لها أثناء النهار على المسافات المتوسطة. أما ليلا، وخاصة في فصل الصيف، فيمكن لها أن تصل إلى مسافات بعيدة. وتتسم هذه الحزمة من الذبذبات بأنها ذات استقبال مستقر على مدار السنة وعلى مسافة تتراوح بين 1000 و 3500 كيلومتر.

د) حزمة 19 متر 15100-15450 كيلوهرتز

تستخدم هذه الحزمة للمسافات البعيدة ويتحقق أفضل استقبال لها خلال فترة المساء وحتى غروب الشمس وإثر بزوغها مباشرة. وتتميز هذه الحزمة الموجية بالاستقبال الجيد على المسافات المتوسطة بين آخر الساعات الصباحية وأولى ساعات المساء.

هـ) حزمة 16 متر من 17700-17900 كيلوهرتز

تتأثر هذه الحزمة من الذبذبات بطروف الغلاف الأيوني أكثر من تأثر أل 19متر بها. وتتسم بالاستقبال الجيد بين الربيع والخريف.

و) حزمة 13 متر 21450-21750 كيلوهرتز

تتأثر هذه الحزمة الموجية تأثرا كبيرا بالبقع الشمسية. فإذا نشطت هذه البقع يصبح الاستقبال النهاري لهذه الذبذبات صالح للمسافات الطويلة. وبالإمكان التقاط إشارات واضحة وقوية أثناء المساء وحتى منتصف الليل في فصول الربيع والصيف والخريف، لاسيما إذا كان هناك نشاط قوي للبقع الشمسية.

ز) حزمة 11 متر من 25600-26100 كيلوهرتز

تعتمد هذه الحزمة الموجية تماما على نشاط البقع الشمسية. وتظل هذه الموجات صامتا تماما خلال عدة سنوات ثم يجري التقاطها من جديد لسنوات أخرى في كافة أنحاء العالم. وقد وقع ذلك حديثا خلال عامي 1980-1981.

UHF -VHF:(5الذبذبات العالية جدا)

في البث الإذاعي بالذبذبات VHF ملائمتان للمسافات القصيرة. وتستخدم حزمة UHF -VHF حزمنا وتستخدم كلتاها في بث الصوت والصورة للتلفزيون. ونظرا لطبيعة هاتين الحزمتين فإن (FM) المعدلة مداهما لا يتعدى الأفق، و مع ذلك فبإمكانهما اختراق الغلاف الأيوني دون أن تتأثر به. (ي)جهاز الإستقبال:

إن أول ما يجب أن يتوفر لدى (الديكسي) أي هاوي الراديو والموجة القصيرة هو جهاز استقبال أو مذياع. وبما أن هناك عدد كبير من الماركات التجارية و الأطرزة في أسواق البلدان المختلفة فإنه لا يجوز والحالة هذه

أن نجازف بالإشارة على القارئ بأن يقوم باقتناء ماركة أو طراز معينين من أجهزة الاستقبال. ولكن يتعين على مشتري جهاز الاستقبال أن يهتم بثلاثة عناصر هامة قبل إقدامه على شراء الجهاز. وهذه العناصر هي:

*الحساسية أو الدقة:

ليست الإشارات التي يلتقطها جهاز الاستقبال بالإشارات القوية دائما، و بالطبع فإنه يتعين على الجهاز أن يحولها إلى إشارات مسموعة. ويعتمد ذلك على مقدرة الجهاز على تضخيم الإشارات السمعية.

تقاس إشارات الدخول عبر الهوائي بالميكروفولت بينما تقاس إشارات الصوت بالديسيبل. وبالطبع فإن جهاز استقبال يتطلب ميكروفولت واحد في الهوائي (النتين) ليحوّله إلى 20 ديسيبل في السماعه لهو أكثر حساسية بكثير من جهاز استقبال آخر يحتاج إلى 5 أو 6 ميكروفولت من إشارات الدخول ليحوّلها إلى نفس إشارة الاستماع أي 20 ديسيبل.

*الانتقائية:

تتلخص هذه على مقدرة جهاز الاستقبال على انتقاء الإشارة المرغوب بالاستماع إليها أو مقدرته على الفصل بين إذاعة و أخرى بسهولة. أي أن الانتقائية هي مقدرة المذياع على التقاط إذاعة تبث على ذبذبة معينة بدون الخلط بينهما وبين إشارات أخرى بحيث من السهل التمييز بين الإشارات المختلفة تقاديا للتشويش.

و مقدرة الجهاز على انتقاء الذبذبات ترتبط ارتباطا وثيقا بعرض حزمة الذبذبات. فإذا عرض الحزمة أمكننا معرفة سبب أهمية الانتقائية في جهاز الاستقبال أما العروض المختلفة لحزم الاتصال اللاسلكي واللبث الإذاعي فهو كما يلي:

UHF. (ذات الذبذبة العالية جدا FM180) كيلوهرتز للبت الإذاعي ب

في منطقتي 1 و 3 AM9. كيلوهرتز للبت الإذاعي بالموجة المتوسطة والطويلة ب

10 كيلوهرتز في المنطقة 2.

AM5. كيلوهرتز للبث الإذاعي بالموجة ب

3 كيلوهرتز حزمة جانبية وحيدة (558) للاتصال الصوتي.

C.W 100. (كيلوهرتز حزمة جانبية وحيدة للاتصال البرقي بالموجة المتواصلة)

*الاستقرار:

لا يقل العنصر الثالث في جهاز الاستقبال أهمية عن العنصرين الآخرين، وهو عنصر الاستقرار. ويمكن هذا العنصر في مقدره الجهاز على الاحتفاظ بإشارة تم التقاطها بدون أن تنتقل هذه الإشارة من مكانها على لوحة الالتقاط في الجهاز. ويحدث هذا الانتقال لأسباب عدة منها تغير درجات الحرارة والتغيرات التي تطرأ على الضغط في التيار الكهربائي.

مفاتيح أخرى إضافية في جهاز الاستقبال:

بالإضافة إلى العناصر الثلاثة المذكورة آنفا فإنه بإمكاننا أن نجد أجهزة الاستقبال مزودة بتجهيزات تقنية أوسع من ذلك بكثير وتكون هذه الأجهزة بالمفاتيح التالية:

S-Meter: مفتاح قياس القوة

هو مقياس بصري لإشارات البث التي يلتقطها جهاز الاستقبال.

مفتاح التحكم بزيادة الذبذبة:

(أو إشارة الدخول عبر RF يقوم هذا المفتاح بالتحكم بحساسية جهاز الاستقبال لزيادة الذبذبة الإذاعية)

الهوائي.

التحكم بالهوائي:

تحتوي بعض أجهزة الاستقبال على هذا المفتاح لتعديل قوة دخول الإشارات عبر الهوائي وذلك حسب كل واحدة من الذبذبات المستخدمة وذلك لاستغلال الهوائي على أفضل وجه ممكن.

مفتاح عيار الذبذبات:

تحتوي أجهزة الاستقبال المتطورة، لاسيما تلك الخاصة بالاتصال اللاسلكي، على مقياس للذبذبات يستخدم للتحقق من دقة لاقط الذبذبة و عرض حزمة الذبذبات أي من صحة ما تشير إليه إبرة لوحة الاستقبال من ذبذبة . وعادة ما يكون معيار الذبذبات مصنوع من زجاج الكوارز . وقد تم تنسيق عمل معيار الذبذبات مع جهاز ضابط وذلك لتصحيح الخطأ المحتمل أو التغيير الذي يمكن أن يطرأ على دقة الإبرة في لوحة الاستقبال. مختار الحزم الموجية:

ينقسم طيف الذبذبات في كل أجهزة الاستقبال تقريبا إلى عدة حزم . ولذا فإنه يوجد في هذه الأجهزة مفاتيح أو أزرار للاختيار ، بحيث تكون لكل حزمة زر معين.

بالإضافة إلى ما ذكرنا هناك المزيد من المفاتيح أو أزرار التحكم التي يمكننا ذكرها فيما يلي على سبيل المثال و بإمكان القارئ أن يعثر عليها بسهولة في مذياعه أو في جهاز الاتصال اللاسلكي:

3- مفتاح الحد من الضجيج.4-مفتاح مضاعف أل-BF1 .مفتاح التحكم بالانتقائية.2-فلتر

، (الخ -5 Standby .مفتاح إسكات المذياع)

وننصح القارئ بأن يقوم قبل تشغيل مذياعه بقراءة دفتر التعليمات المرفق به بإمعان.

ك-الهوائيات الأنتينات:

إذا كان لديك جهاز استقبال من نوع جيد فعليك أن تفكر بنوع معين من الهوائيات. ومن الأفضل أن يتوفر الهوائي الجيد مع جهاز استقبال متوسط النوعية بدلا من أن يكون جهاز الاستقبال ممتاز النوعية والهوائي

المرفق به غير ملائم له. ولهذا فإنه بإمكاننا أن نؤكد أن أهمية الهوائي تعادل أهمية المذياع بل وتتفوق عليها. سنشرح فيما يلي بعض أنواع الهوائيات الإستقبالية.

1. الهوائي الحديدي:

تكثر في أيامنا هذه أجهزة الترانزيستور الصغيرة النفاثة التي تحتوي على هوائي صنع من مركب حديدي. ويتمتع هذا الهوائي بحساسية تعتمد كثيرا على اتجاهه، فإذا غيرنا وضع أو اتجاه الهوائي لاحظنا أن تغيرا يطرأ على جودة الاستقبال. و لا يصلح هذا الهوائي للاستماع للموجة القصيرة وتقتصر صلاحيته على استقبال إذاعات الموجات الطويلة والمتوسطة المحلية.

2. الهوائي التلسكوبي:

تحتوي أجهزة استقبال أخرى على هوائيات تلسكوبية (متداخلة الأجزاء) تمتاز عموما بجودتها، باستثناء أن يجري تشغيل المذياع داخل شقة في قلب المدينة وفي منطقة تكثر فيها بنايات المرتفعة المبنية من الإسمنت المسلح والمزودة بالنوافذ المعدنية. ويعود ذلك إلى أن العناصر المعدنية تمتص الموجات اللاسلكية الكهربية ويؤدي ذلك إلى انخفاض جودة إشارات الاستقبال.

3. هوائي القضيب الرأسي:

إذا أردنا الاستماع إلى الموجات القصيرة فمن الأفضل أن نقوم بتركيب هوائي خارجي. ومن أكثر الهوائيات بساطة وسهولة في التركيب هي المعروفة باسم (هوائي القضيب الرأسي) وهو ملائم بشكل خاص لأولئك الذين يعيشون في الشقق في المدجن الكبيرة. ويتألف هذا الهوائي من قضيب صغير القطر يتراوح طوله بين 3 و 5 أمتار. ويمكن تركيب القضيب مع عازلين مثبتين على عمود أو على جدار الشرفة أو جدار المدخنة على

السطوح أو على إطار النافذة. ويجب أن يكون الهوائي على أكبر ارتفاع مكن ومن الفضل أن يكون سلك التوصيل محجوب بمادة واقية وأن يكون الهوائي بعيد عن شبكة التوزيع الكهربائي ويجب أن لا يكون إطلاقاً موازياً لأي من أسلاك الشبكة.

وهوائي القضيب الرأسي ذو حساسية في كافة الاتجاهات أي انه يتلقى الإشارات من كافة الاتجاهات مما يؤدي إلى كونه حساس لكل أنواع التشويش والضجيج المنبعثين عن العوامل الجوية.

4. الأفقي الثنائي القطب ونصف الموجي:

هو هوائي متغير الاتجاه، أي انه يجب أن يكون موجهاً لدى تركيبه نحو محطة الإذاعة المرغوب باستقبال برامجه وذلك كي تصل الموجات بشكل عمودي على الهوائي، ويطلق هذا الهوائي من جزأين متساويين يتم وصلهما بواسطة عازل. ويجب أن يكون طول كل من الجزأين مساوياً لربع طول الموجة. فإذا كنت تفضل الاستماع لحزمة موجات 41 متر فإن الطول الكامل لسلك الهوائي يجب أن يبلغ 20.5 متراً. فإذا قسمناه على جزأين متساويين كل منهما 10 متراً. أما سلك التوصيل فيتعين أن يكون مزدوجاً أي مؤلفاً من سلكين متوازيين أو أن يكون مؤلف من سلك ملفوف ذو مقاومة تبلغ 75 أوم . ويتعين في هذه الحالة وصل السلك الموصل الرئيسي بمدخل الهوائي في جهاز الاستقبال بينما يجري توصيل الشبكة الملفوفة عليه بمدخل التفريغ الأرضي في الجهاز. وفي حالة أن يكون جهاز الاستقبال مزود بمدخلين للهوائي يجري وصل طرف السلك بالموصل بالمدخل الأول ويصل طرف الشبكة بالمدخل الثاني.

5. ثنائي القطب و متعدد الحزم الموجية:

يعتمد هذا الهوائي أيضاً على التوجيه و يتألف من عدة هوائيات ثنائية القطب خاصة بحزم موجية مختلفة. و

بثلاثة من هذه الهوائيات يمكن تغطية كلى حزم الذبذبات . و يجب أن يكون سلك التوصيل ملفوف و بمقاومة 75 أوم.

6.ثنائي القطب العمودي:

يصلح هذا الهوائي لكافة الاتجاهات. فإذا تم تركيبه خصيصا لحزمة موجية معينة كانت له فعالية كبيرة. و بالإمكان أن يثبت طرفه بإفريز السطح بينما يثبت الطرف الآخر في الأرض، كما يبين في الرسم التالي ومن الملائم دائما أن يكون سلك التوصيل ملفوفا وان نكون قوة مقاومته 75 أوم. أما باقي مواصفات هذا الهوائي فهي مشابهة لمواصفات الهوائي الأفقي الثنائي القطب.

ويمكن في حالة الضرورة تركيب هوائي المعين في غرفة ولكنه يجب عندئذ وصل طرفي المعين بنفس السلك وان يكون سلك التوصيل فرديا. كما ويتعين في هذه الحالة أن يكون سلك الهوائي بعيدا عن الحائط وموازيا لها على مسافة 5 سنتيمتر. هذا ويجب مراعاة أن لا يكون سلك الهوائي موازيا لشبكة التوزيع الكهربى إطلاقا.

8.هوائيات أخرى:

توجد إلى جانب الهوائيات التي تعرضنا لها أنواع أخرى كثيرة من الهوائيات. ويمكن للقارئ أن يجد شروحات لها في النشرات المختصة. وسنكتفي هنا بذكر بعض هذه الأنواع لإفادة القارئ في إجراء مقارنة تقنية بين أنواع الهوائيات المختلفة إذا أتاحت له الفرصة: أ-هوائي ربع الموجة العمودي.ب-هوائي ربع الموجة الأفقي أو العمودي المزود بأسلاك متوازية قوتها 300 أوم.ج-هوائي المنشه العمودي أو الأفقي والمعروف أيضا باسم ويندوم .د-هوائي بيفاريج أو الهوائي الطويل السلك ه-هوائي لوب ، إلخ..

9.التفريغ الأرضي:

كثيرا ما يكون إبريز أو فيشة التفريغ الرضي غير ضرورية بالنسبة لأجهزة استقبال الموجة القصيرة. ولكن مما

لاشك فيه أن استخدام هذا الإبريز في المذياع يؤدي إلى تخفيض مستوى الضجيج وتحسين نوعية الاستماع، ويمكن إتمام عملية التفريغ الرضي بوصل المدخل الخاص به في المذياع بصفحة من النحاس أو بقضيب معدني يجري دفنه في الأرض على عمق يتراوح بين 30 و 50 سنتمتر. و بالنسبة لأولئك الذين يقيمون في شقق فيكفيهم أن يصلوا مدخل التفريغ الرضي في المذياع بماسورة للماء البارد. ولكن يتعين عليهم في أوقات العواصف أن يتخذوا الإجراءات الكفيلة بالحيلولة دون وقوع أضرار في جهاز الاستقبال لا يمكن إصلاحها . وذلك بتركيب الأدوات الخاصة بمنع وقوع مثل هذه الأضرار .

2- 9 تقنية البلوتوث:

تعود تسمية بلوتوث إلى ملك الدنمارك الذي توفي في العام 986 Harald Blåtand وكلمة Bluetooth تعني باللغة الإنكليزية. وهو الملك الذي قام بتوحيد الدنمارك والنرويج وأدخلهم في الديانة المسيحية. واختير هذا الاسم لهذه التكنولوجيا للدلالة على مدى أهمية الشركات الدنماركية والنرويجية والسويدية والفنلندية في صناعة الاتصالات، بالرغم من أن التسمية لا علاقة لها بمضمون التكنولوجيا. الجدير بالذكر أن هذا الملك كان مولعاً بأكل العنب البري Blueberries حتى تلونت أسنانه باللون الأزرق فسمي بصاحب السن الأزرق. Bluetooth، فكرة البلوتوث فكرة قديمة جداً في بال مهندسي شركة Ericsson للصناعات الالكترونية. قبل أن تقوم الشركات IBM, Intel, Nokia و Toshiba بتبنيها ووضعها قيد الاستعمال. و بلوتوث هو اسم تقنية مفتوحة المصادر للاتصال اللاسلكي القريب بين الأجهزة الالكترونية. و هي تقنية عالمية موحدة لربط كافة أنواع الأجهزة مع بعضها البعض مثل الكمبيوتر والهاتف النقال والكمبيوتر الجيبى والأجهزة السمعية والكاميرات الرقمية. بحيث تتمكن هذه الأجهزة من تبادل البيانات

ونقل الملفات بينها وبين شبكة الانترنت لاسلكياً.

حيث توفر هذه التقنية للمستخدمين نقل المعلومات بدون أدنى جهد. وقد تم تطوير تكنولوجيا الاتصال

اللاسلكي البلوتوث بواسطة مجموعة من المهتمين يطلق عليهم اسم Bluetooth Special Interest Group
GIS.

وصممت الرقاقة المسؤولة عن بلوتوث لتحل محل كبل التوصيل في الأجهزة الالكترونية. حيث تقوم بتشفير

المعلومات وإرسالها بشكل أمواج بتردد معين إلى مستقبل بلوتوث في الجهاز الثاني. ويقوم المستقبل بدوره بفك

تشفير هذه المعلومات وإعادتها إلى شكلها الرئيسي لتستخدم في أجهزة الكمبيوتر والموبايل....الخ. وهذه التقنية

رخيصة جداً مقارنة بما تقوم به من جهد في نقل المعلومات، وذلك لأنها تعتمد على رقاقة أو اثنتين ذات

تكاليف تصنيع رخيصة

تكاد حياتنا اليومية الآن تغص بكلمة بلوتوث، وكثير منا لا يعلم شيئاً عن هذه التقنية ولا عن طريقة عملها،

وإنما نعرفها أنها هي التي ترسل الصور والفيديو والنغمات من جهاز موبايل إلى جهاز آخر، ونكاد لا نرى

أحداً نعرفه إلا ونسأله "عندك ايه جديد؟" ونسارع إلى طلب إرسال لإحدى الصور مثلاً "ابعتلي الصورة دي

على البلوتوث" ثم وبعد أن ننهي هذا "الارسال" نقوم بإيقاف عملها وننساها. ولا نذكرها مرة أخرى إلا حين

نتباهي أمام الناس بالموبايل الذي نحمله. هذا برأيي الشخصي إجحاف بحق هذه التقنية الرائعة وهنا سنتعلم كل

شيء عنها بالتفصيل.

2- 10 مشاكل التوصيل بين الأجهزة:

إن توصيل جهازين الكترونيين مع بعضهما البعض يحتاج إلى توافق في العديد من النقاط، من هذه النقاط نذكر

1- كمية الأسلاك اللازمة لتوصيل جهازين: ففي بعض الأحيان يكون سلكين فقط مثل توصيل الأجهزة الصوتية بالسماعات وفي أحيان أخرى يتطلب الأمر 8 أسلاك ويصل حتى 25 سلك كالوصلات المستخدمة في الكمبيوتر وأجهزته الطرفية.

نوعية التوصيل المستخدم بين الأجهزة لتبادل المعلومات: هل هو على التوالي أم على التوازي؟ فمثلاً الكمبيوتر يستخدم الطريقتين للتوصيل من خلال المخارج المثبتة في اللوحة الأم فتصل الطابعة مع الكمبيوتر على التوازي أما لوحة المفاتيح والمودم فيتصلا مع الكمبيوتر على التوالي.

نوعية البيانات المتبادلة بين الأجهزة: وكيف تترجم إلى إشارات خاصة تستجيب لها الأجهزة. هذا ما يعرف باسم البروتوكول Protocol. وهذه البروتوكولات يتم استخدامها من قبل جميع الشركات المصنعة فمثلاً يمكن توصيل جهاز فيديو من نوع Sony مع جهاز تلفزيون من نوع JVC وذلك لأن البروتوكولات المستخدمة لتبادل المعلومات موحدة مسبقاً.

هذه النقاط التي استخدمها المنتجون (الشركات المصنعة للأجهزة الالكترونية) جعلت من الصعب التحكم في كمية الوصلات المستخدمة حتى ولو تم استخدام أسلاك ملونة للتمييز بينها، كما أنه لا يمكن ربط كافة الأجهزة الالكترونية مع بعضها البعض، مثل الكمبيوتر وملحقاته وأجهزة الاتصالات وأجهزة الترفيه المنزلية لأن ذلك يتطلب إعداد بروتوكولات جديدة وإضافة المزيد من الأسلاك، أما الآن فقد أضحت بلوتوث تقوم بكل ما سبق فهي تقنية موحدة في جميع الأجهزة، وتقوم على بروتوكول موحد وبطريقة لاسلكية.

وهي تقنية صحية جداً، وغير مضرّة أبداً بصحة المستخدم -كما شاع من إشاعات- لأن إشارة أوضاعها

ضعيفة ولا تتجاوز 1 ميلي وات بينما إشارة أجهزة الموبايل تبلغ 3 وات.

الاتصال اللاسلكي مستخدم في العديد من التطبيقات، مثل التوصيل من خلال استخدام الأشعة تحت الحمراء

وهي أشعة ضوئية لا ترى بالعين وتعرف باسم الأشعة تحت الحمراء لأن لها تردد أصغر من تردد الضوء

الأحمر. تستخدم الأشعة تحت الحمراء في أجهزة التحكم عن بعد في التلفزيون (Remote Control) وتعرف

باسم Infrared Data Association وتختصر بـ IrDA كما أنها تستخدم في العديد من الأجهزة الطرفية

للكمبيوتر. لكن الأجهزة المعتمدة على الأشعة تحت الحمراء لها ثلاث مشاكل هي:

المشكلة الأولى: أن التكنولوجيا المستخدمة فيها الأشعة تحت الحمراء تعمل في مدى الرؤية فقط line of

sight أي يجب توجيه جهاز التحكم عن بعد إلى التلفزيون مباشرة للتحكم به.

المشكلة الثانية: أن التكنولوجيا المستخدمة فيها الأشعة تحت الحمراء هي تكنولوجيا واحد إلى واحد one to

one أي يمكن تبادل المعلومات بين جهازين فقط فمثلاً يمكن تبادل المعلومات بين جهاز الكمبيوتر العادي

وجهاز الكمبيوتر المحمول بواسطة الأشعة تحت الحمراء أما تبادل المعلومات بين الكمبيوترين وجهاز الهاتف

المحمول فلا يمكن.

المشكلة الثالثة: وتتجلى في كون الشركات المصنعة لأجهزة الموبايل مثلاً تقوم باعتماد بروتوكولات نقل

مختلفة. وعلى سبيل المثال فإن جهاز من إنتاج شركة Samsung لا يستطيع إرسال المعلومات إلى جهاز

من إنتاج Siemens. ومثال آخر هو أن أجهزة Nokia 6610 7210 6100 مثلاً لا تستطيع إرسال أي

معلومات من خلال فتحة IrDA ولا تستطيع استقبال المعلومات إلا من جهاز كمبيوتر.

جاءت تكنولوجيا البلوتوث للتغلب على المشاكل المذكورة أعلاه، حيث قامت شركات عديدة مثل Siemens و

radio و Toshiba, Motorola و Ericsson بتطوير مواصفات خاصة مثبتة في لوحة صغيرة

module تثبت في أجهزة الكمبيوتر وأجهزة الموبايل وأجهزة التسلية الالكترونية لتدعم هذه الأجهزة تقنية

البلوتوث وستمكن بعدها من الاستفادة من ميزاتها على النحو التالي:

1- أجهزة بدون أسلاك: وهذا يجعل نقل الأجهزة وترتيبها في السفر أو في البيت سهلاً وبدون متاعب.

2- تقنية رخيصة التكاليف: غير مكلفة بالمقارنة بالأجهزة الحالية.

3- سهولة التشغيل: تستطيع الأجهزة أن تتواصل مع بعضها البعض بدون تدخل المستخدم وكل ما عليك هو

الضغط على زر التشغيل واترك الباقي للبلوتوث ليتحاور مع الجهاز المعني بالأمر من خلال الـ (Module)

ليقوم بتبادل الملفات بكافة أنواعها.

2-9-1 طريقة عمل تقنية البلوتوث

تعمل تقنية البلوتوث عند تردد 2.45 جيجا هيرتز وهذا التردد يتفق مع الأجهزة الطبية والأجهزة العلمية

والصناعية مما يجعل انتشار استخدامه سهل. فمثلاً يمكن فتح الأبواب في الوقت الحالي من خلال الأشعة

تحت الحمراء التي يقوم بإصدارها جهاز خاص لذلك ولكن باستخدام البلوتوث يمكن فتح هذه الأبواب باستخدام

جهاز الهاتف النقال.

2-9-2 التشويش الذي يحصل عند استخدام بلوتوث

من المحتمل أنه قد خطر لك التساؤل: إذا كانت الأجهزة تتبادل المعلومات والبيانات بإشارات راديو تعمل عند

تردد 2.45 جيجا هيرتز. فماذا عن التداخلات التي قد تسبب التشويش الذي نلاحظه على شاشة التلفزيون

عندما تتداخل مع إشارات لاسلكية، مشكلة التداخل تم حلها بطريقة ذكية حيث أن إشارة البلوتوث ضعيفة وتبلغ

1 ميلي وات إذا ما قورنت بإشارات أجهزة الموبايل التي تصل إلى 3 وات. هذا الضعف في الإشارة يجعل

مدى تأثير إشارات البلوتوث في حدود دائرة قطرها 10 متر ويمكن لهذه الإشارات اختراق الجدران مما يجعل التحكم في الأجهزة يتم من غرفة لأخرى دون الحاجة للتواجد مقابل الجهاز المعني مثلاً، عند تواجد العديد من الأجهزة الالكترونية في الغرفة يمكن أن يحدث تداخل لأنني ذكرت أن مدى تأثير البلوتوث في حدود 10 متر وهو أكبر من مساحة الغرفة ولكن هذا الاحتمال غير وارد لأن هناك مسح متواصل لمدى ترددات إشارة البلوتوث، وهذا ما يعرف باسم Spread-Spectrum Frequency Hopping حيث أن المدى المخصص لترددات البلوتوث هي بين 2.40 إلى 2.48 جيجا هيرتز ويتم هذا المسح بمعدل 1600 مرة في الثانية الواحدة. وهذا ما يجعل الجهاز المرسل يستخدم تردد معين مثل 2.41 جيجا هيرتز لتبادل المعلومات مع جهاز آخر في حين أن جهازين في نفس الغرفة يمكن أن يستخدموا تردداً آخر مثل 2.44 جيجا هيرتز ويتم اختيار هذه الترددات تلقائياً وبطريقة عشوائية مما يمنع حدوث تداخلات بين الأجهزة، لأنه لا يوجد أكثر من جهازين يستخدمان نفس التردد في نفس الوقت. وإن حدث ذلك فإنه يكون لجزء من الثانية.

2-11 الأشعة تحت الحمراء

تبدو وظيفة جهاز التحكم عن بعد أكثر تعقيداً مما نراها نحن بتلك البساطة والتلقائية فهو يقوم بتحويل ضغطة المستخدم على الزر إلى إشارة ضوئية بالأشعة تحت الحمراء يلتقطها التلفاز . وبإزالة الغطاء الخلفي للجهاز سنجد أن هناك جزءاً واحداً فقط يمكن رؤيته وهو "لوحة الدائرة المطبوعة" والتي تحتوي على المكونات الإلكترونية ومكان توصيل البطارية .

والمكونات التي تراها هنا متماثلة في جميع أجهزة التحكم عن بُعد، فسترى وحدة دائرة متكاملة وتعرف أيضاً باسم الشريحة Chip ، وهي مركبة فيما يعرف بوحدة ثنائية ذات 18 رأساً من الخطوط الداخلية المزدوجة، وسترى إلى يمين الشريحة صماماً ثنائياً (دايود)، وصماماً ثلاثياً (ترانزيستور) ذا لون أسود وذا ثلاثة رؤوس،

وصمام رنين ذا لون اصفر. ومقاومتين خضراوين. ومكثفا ازرق غامقا، ويوجد بجوار موصلات البطارية مقاومة خضراء ومكثف عبارة عن قرص اسمر. وتستطيع الشريحة في هذه الدائرة الإحساس بأي ضغطة على أي زر وتقوم عندئذ بترجمة هذه الضغطة إلى سلسلة من النبضات شبيهة بشفرة مورس (المستخدمة في التلغراف)، ولكل زر (مفتاح) سلسلة نبضات مختلفة وخاصة به. وتقوم الشريحة بإرسال هذه الإشارة (النبضات) إلى الصمام الثلاثي الذي يقوم بدوره بتكبيرها وتقويتها .

2-12 لوحة الدائرة المطبوعة

هي عبارة عن لوحة رفيعة وصغيرة مصنوعة من مادة الألياف الزجاجية، مطبوع بالحفر على سطحها أسلاك نحاسية رفيعة، ويتم تركيب المكونات الإلكترونية على هذه اللوحة. وتستخدم هذه الدوائر لأنه من السهل إنتاجها وتجميعها بأحجام كبيرة. وكما أنه من غير المكلف نسبيا طباعة الحبر على صفحة من الورق. فكذلك من غير المكلف طباعة أسلاك النحاس على صفحة (لوحة) من الألياف الزجاجية، ومن السهل أيضا تركيب المكونات الإلكترونية (الشريحة والترانزيستور وغيرها) آليا على هذه اللوحة ولجمعها لتوصيلها بالأسلاك النحاسية، وتحتوى اللوحة على مجموعة من نقاط التوصيل لأزرار الجهاز، وهي مصنوعة من رقيقة مطاطية، ولكل زر قرص موصل للكهرباء (اسود اللون). وعندما يتم ضغط الزر يمس هذا القرص نقاط التوصيل على اللوحة ويوصل بينها فتحس الشريحة بهذا الاتصال. ويوجد في نهاية اللوحة صمام باعث للضوء بالأشعة تحت الحمراء يمكن النظر إليه كلمبة ضوئية صغيرة .

تصدر جميع الصمامات الباعثة للضوء ضوءا مرئيا إلا أن الصمامات الخاصة بأجهزة التحكم عن بعد تبتث أشعة تحت الحمراء وهي أشعة غير مرئية للعين البشرية. ولكنها ليست مستعصية على كل الأبصار على أية حال فعلى سبيل المثال يمكن لآلة تصوير الفيديو رؤية هذه الأشعة، فيتم توجيه جهاز التحكم عن بعد إلى آلة

التصوير والضغط على أي زر فيمكن رؤية الأشعة تحت الحمراء تومض على الشاشة. ووحدة الاستقبال في التلفاز قادرة على رؤية هذه الأشعة أيضا، ويعمل جهاز التحكم عن بعد كالتالي: عندما يضغط أي زر تتم توصيلة كهربية تحس بها الشريحة وتحدد الزر المضغوط وتصدر إشارة خاصة بهذا الزر شبيهة بشفرة المورس. ويقوم الترانزيستور بتكبير الإشارة وإرسالها إلى الصمام الباعث للضوء الذي يقوم بتحويلها إلى أشعة تحت الحمراء يراها جهاز الإحساس في التلفاز وبرؤيته لها يقوم بتنفيذ المطلوب.

3-1 تمهيد

ان للشبكات اللاسلكية اخطاراً تهدد امنها كغيرها من الشبكات الأخرى، سواء كانت هذه المخاطر مشتركة بين الشبكات السلكية و اللاسلكية ، او كانت مخاطر مخصصة او موجودة فقط في الشبكات اللاسلكية وما تحويه من معايير و غيرها، ومن المعروف ان من أخطر ما يهدد الشبكات هذه الايام هي هجمات حجب الخدمة التي قد تتعرض لها و في كثير من الاحيان يصعب تفاديها ان تمت بصورة دقيقة و مركزة. ان منفاذي هجمات حجب الخدمة الموزعة DDoS او Service Distributed Denial of يحتاجون الى عدد كبير من الاجهزة لكي ينفذوا هجماتهم، فتراهم يبرمجون برمجيات تعمل على اتمتة الهجوم و الاستيلاء على اجهزة الحاسب و من ثم الانتقال الى الاجهزة المجاورة و غيرها بصورة تلقائية سريعة، و اذا كان جهاز الحاسب غير محمي بصورة كافية فانه سيقع ضمن قائمة الاجهزة التي تنتظر الاوامر من المهاجمين لتنفيذ الهجوم. في العادة فان الاجهزة المصابة لا يتم حذف الملفات منها، لكن يتم استعمالها جميعاً في وقت واحد في الهجوم على شبكة معينة او موقع معين و تلك الاجهزة تسمى بالzombies.

يحتوي هذا الفصل على تعريف للمخاطر والمهاجمون وسوف يتم التركيز على الثغرات الأمنية الموجودة في الشبكات اللاسلكية بمزيد من التفصيل .

3-2 مفهوم الأمن في شبكات الحساسات اللاسلكية

يتمثل تحقيق الأمن في شبكات الحساسات اللاسلكية بتوفير الحماية الفيزيائية للحساسات ، حماية الاتصالات بين مكونات الشبكة، و أخيراً حماية البيانات ، ويمكن تلخيص المتطلبات الأمنية لشبكات الحساسات اللاسلكية في النقاط التالية :

سرية البيانات: و تعني إخفاء البيانات عن الأطراف غير المصرح لهم بالاطلاع عليها، السرية المتقدمة: و تعني منع أي عقدة من قراءة أي رسالة بعد مغادرتها للشبكة، السرية الرجعية: و تعني منع أي عقدة جديدة من قراءة أي رسالة قديمة نقلت قبل انضمام العقدة للشبكة، موثوقية البيانات: و تشمل ضمان استلام الرسائل من مصادر موثوقة ، التصريح و تحديد الصلاحيات: السماح فقط بالعقد المصرح لها بالمشاركة في أعمال الشبكة، ضبط الوصول: و الذي يمنع الوصول غير المصرح به لموارد الشبكة، صحة البيانات: و هي التأكد من أن البيانات سليمة و لم يتم تخريبها أو تحويرها أثناء نقلها خلال الشبكة ، حداثة البيانات: أي ضمان ان جميع البيانات و الرسائل المتبادلة حديثة ومنع إعادة إرسال بيانات قديمة، عدم الإنكار: ألا يكون بمقدور أي عقدة إنكار إرسال أي رسالة، استمرارية الشبكة و متانتها: أن تكون الشبكة صلبة في مواجهة الاختراقات الأمنية و أن تحتوي المضاعفات الناتجة عنها، سرعة التغلب على الاعتداءات، و القدرة على ضمان استمرارية الشبكة، تفاوت مستويات الأمن: و يعنى قدرة الشبكة على تغيير درجة الأمن بناء على تغير الموارد المتوفرة في الشبكة، و يمكن تصنيف الوسائل الأمنية القابلة للتطبيق في شبكات الحساسات اللاسلكية إلى:

1. وسائل وقائية: و التي تمنع الاختراقات الأمنية من الحدوث أو أن تجعل منها على الأقل مهمة صعبة
2. وسائل كاشفة: و التي تمكن الشبكة من اكتشاف الاختراقات عند حدوثها و التفريق بينها و بين حالات الفشل غير المقصودة.

3. وسائل تفاعلية: و التي قد تتفاوت من تجميد جميع أعمال الشبكة حتى يزول مصدر الخطر إلى آليات أكثر

تعقيداً تعمل على تعطيل الجزء المصاب من الشبكة مع استمرارية عمل باقي الأجزاء

و تختلف درجة الأمن المتوفرة في شبكة الحساسات اللاسلكية بناء على عوامل أساسية نذكر منها:

1- طبيعة المنطقة التي تم نشر الحساسات فيها

2- توفر محطات المراقبة في الشبكة

3- عدد العقد المكونة للشبكة ، خصائصها، و تحركاتها

4- احتمالات حدوث الاعتداءات

5- البروتوكولات المستخدمة في إدارة الشبكة

6- المتطلبات الأمنية للتطبيق البرمجي الذي يستخدم الشبكة

3-3 معوقات الأمن في شبكات الحساسات اللاسلكية

نستعرض فيما يلي القيود التي تجعل من تحقيق الأمن في شبكات الحساسات اللاسلكية أمراً معقداً و صعب المنال إن لم يكن مستحيلاً:-

1. حدود الحساسات: و التي تتصف بمحدودية الموارد فيما يتعلق بموارد الطاقة، سرعة المعالجة، سعة التخزين

و قنوات الاتصال مما يوجد تضارباً بين تخفيض استهلاك الموارد و رفع مستوى الأمن في الشبكة. كما أن

هذه الحساسات سريعة الفشل و غير مقاومة للتلاعب. وقد يزيد الأمر تعقيداً إذا كانت الحساسات قابلة للحركة

و الانتقال من موقع لآخر فالاختراقات التي تنشأ من عقد متحركة تكون صعبة الاكتشاف. هذا بالإضافة إلى

ارتفاع عدد الحساسات المستخدمة في تكوين الشبكة و التي يتم نشرها في مساحات واسعة و بيئات عنيفة تزيد

من فرص استغلال ثغرات الشبكة الأمنية و يوجد الحاجة إلى إدارة أمنية موزعة عوضاً عن الاعتماد على نقطة أمنية مركزية.

2. حدود الشبكة: تتغير جغرافية الشبكة بشكل دائم مما يجعلها فريسة سهلة للاختراقات التي يمكن أن تأتيها من جميع الاتجاهات على خلاف الشبكات السلكية التي تتوفر فيها بوابات و جدران نارية تحمي حدودها. كما أن عمليات إزالة و إضافة العقد المستمرة تخلق هيكلاً توجيهياً غير ثابت، هذا بالإضافة إلى اعتماد شبكات الحساسات اللاسلكية على الاتصالات اللاسلكية التي تعاني من العديد من الثغرات الأمنية.

3. حدود فيزيائية: و التي تنشأ من نشر الحساسات في بيئات مفتوحة و عنيفة مما يجعلها عرضة للتخريب و الأسر بالإضافة إلى افتقار الحساسات إلى وسائل الحماية و مقاومة التلاعب التي تم غض النظر عنها لارتفاع تكلفتها المصنعية.

3-4 الاعتداءات الأمنية في شبكات الحساسات اللاسلكية

3-4-1 تصنيف الاعتداءات الأمنية

تتعرض شبكات الحساسات اللاسلكية إلى أشكال مختلفة من الاعتداءات الأمنية التي يمكن تصنيفها من زوايا متعددة. تصنف الاعتداءات من حيث نشاطها إلى اعتداءات صامتة و اعتداءات فاعلة ، فالاعتداءات السلبية التي تتمثل بالاطلاع على البيانات فقط دون إجراء تخريب أو تحوير فيها و الاعتداءات النشيطة التي تتمثل بتحويل و تخريب و تعديل البيانات واستغلال عملية الاتصال. و بحسب المتطلبات الأمنية للشبكة تصنف الاعتداءات إلى اعتداءات على سرية و موثوقية البيانات، اعتداءات على استمرارية الشبكة، و اعتداءات خفية تستهدف نزاهة خدمات الشبكة. و يصنف باثان و من معه ، 2006 الاعتداءات إلى نوعين، النوع الأول

يستهدف الآليات الأمنية المستخدمة في الشبكة، النوع الثاني يستهدف الآليات الأساسية في الشبكة كآلية التوجيه. كما يصنف [هيلي و من معه، 2009] [كافيتا و سريدهان ، 2010] الاعتداءات بحسب قدرات المعتدي إلى اعتداءات تستخدم الحساسات التي تنتمي للشبكة أو أجهزة تحاكيها في القدرات، و اعتداءات تستخدم أجهزة أكثر قوة كالمبيوتر المحمول، و من جهة أخرى يصنف الاعتداءات بحسب نقطة الوصول إلى اعتداءات خارجية صادرة من كائنات خارج الشبكة، و اعتداءات داخلية صادرة من عقد تنتمي للشبكة. كما توجد اعتداءات تستهدف طبقات البروتوكول المختلفة في الشبكة [هيلي و من معه، 2009] [كافيتا و سريدهان ، 2010] ، الطبقة المحسوسة ، طبقة ربط البيانات، طبقة الشبكة، طبقة النقل، و طبقة التطبيقات. و كل طبقة تتعرض لأشكال مختلفة من الاختراقات الأمنية سنأتي على ذكرها في الجزء اللاحق من البحث.

إن أي معندي على شبكات الحساسات اللاسلكية يتم تصنيفه بناءً على دوافعه و الغرض من اعتدائه، و كذلك المعرفة و الموارد التي يمتلكها. وعند التوجه إلى تأمين شبكات الحساسات اللاسلكية علينا التفكير في إجابة الأسئلة التالية [طاهر و شاه ، 2008]: ما الذي نسعى إلى حمايته؟ هل نسعى إلى حماية البيانات المتبادلة و المحافظة على سريتها؟ هل نسعى إلى ضمان بقاء الشبكة و استمرارية عملها عند تعرضها لاعتداء ما؟ ما هي القدرات التي يملكها المعتدي؟ ما هي الاستراتيجية المتبعة في الاعتداء؟ و ماهي النتائج المترتبة على وقوع الاعتداء؟

و يصنف [دي بيترو و من معه ، 2009] المعتدي بحسب أهدافه إلى : الفضولي - الذي يسعى إلى الاطلاع على البيانات المنقولة و المخزنة داخل الشبكة، الملوث - الذي يسعى إلى تشويش و تضليل الشبكة من خلال تغذيتها ببيانات مزيفة، المزيل - و الذي يهدف إلى منع مجمع الشبكة من تلقي بعض البيانات، المستبدل - الذي يعمل على استبدال بيانات صحيحة ببيانات مزيفة. إن الأضرار الناتجة عن

الاعتداءات الأمنية التي تتعرض لها شبكات الحساسات اللاسلكية تختلف باختلاف طريقة نشر و تجميع البيانات المتبعة داخل الشبكة [ناكياما و من معه ، 2007]، فالمعتدي على الشبكات المستوية لن يتمكن من السيطرة على كامل الشبكة بمجرد سيطرته على أحد عقدها، أما في الشبكات الهرمية فإن بمقدرو المعتدي أن يسيطر على كامل الشبكة بمجرد سيطرته على العقدة الجذر، مما يؤكد اختلاف الوسائل الأمنية باختلاف نوع الشبكة.

3-4-2 أشكال الاعتداءات الأمنية

نقوم في هذا الجزء من البحث بإلقاء الضوء على أهم الاعتداءات التي تتعرض لها شبكات الحساسات اللاسلكية. حيث نبدأ باستعراض الاعتداءات المستهدفة لطبقات البروتوكول [كافيتا و سريدهان ، 2010] [وانغ و من معه ، 2006] [كومار و سارما، 2008]، ثم ننتقل إلى الاعتداءات التي تستهدف البيانات المنقولة [باتان و من معه ، 2006] [هملانين و من معه ، 2006] [هيلي و من معه، 2009] [كافيتا و سريدهان ، 2010] ، و أخيراً ندرج الاعتداءات المحسوسة الموجهة ضد عقد الشبكة [هملانين و من معه ، 2006] [زيا و زومايا، 2006] [هيلي و من معه، 2009] [طاهر و شاه ، 2008].

3-4-3 الاعتداءات المستهدفة للطبقة المحسوسة

1.التشويش الإذاعي

و يصنف التشويش الإذاعي على أنه أحد أشكال حجب الخدمة الذي يهدف من خلاله المعتدي إلى تعطيل الشبكة عن طريق بث إشارة عالية الطاقة. و يمكن تقسيم التشويش الإذاعي إلى أنواع [كافيتا و سريدهان ، 2010]: التشويش المستمر: الذي يعمل على إفساد حزم البيانات المنقولة، التشويش المخادع: الذي يرسل بيانات مزيفة تظهر كجزء شرعي من حركة البيانات داخل الشبكة، التشويش العشوائي: الذي يبديل بين حالتي النوم و التشويش لتوفير الطاقة، التشويش التفاعلي: الذي يعمد إلى إرسال إشارات التشويش عندما يشعر

بحركة البيانات في الشبكة. و قد يستخدم المعتدي مصدر تشويش عالي الطاقة قادر على تعطيل كامل الشبكة و إن لم يتوفر ذلك فبمقدور المعتدي أن يستخدم مصادر أقل طاقة موزعة بشكل استراتيجي.

2. التلاعب المحسوس

و الذي يعد سهلاً لعدة أسباب: ارتفاع عدد الحساسات و انتشارها على مساحات واسعة بالإضافة إلى عدم حماية الحساسات بتغليف مضاد للتلاعب. و عند تمكن المعتدي من الوصول إلى الحساسات فإن بإمكانه سرقة المعلومات الحساسة المخزنة عليها، أو أن يستبدلها بحساسات أخرى يتحكم بها. و على عكس الاعتداءات الأخرى التي يمكن تلافى الأثر الناتج عنها ، ينتج التلاعب المحسوس أثراً دائماً لا يمكن التخلص منه.

3-4-4 الاعتداءات المستهدفة لطبقة ربط البيانات

1. التصادم و استنزاف الموارد

يحدث التصادم عندما تحاول عقدتين الإرسال في نفس الوقت و على نفس التردد، و عندما تتصادم حزم البيانات فإن البيانات التي تحملها تتعرض للتغيير مما يدفع العقد إلى إعادة الإرسال من خلال قناة الاتصال بشكل مستمر الأمر الذي يحرم بقية العقد من استخدامها. و ما لم يتم اكتشاف عمليات إعادة الإرسال و إيقافها فإن موارد الطاقة في العقد المرسل و العقد المجاورة لها سيتم استنزافها. وقد يستخدم هذا النوع من الاعتداء لحجب خدمات الشبكة بشكل غير مباشر عندما تسود حالة من الإجحاف في استخدام موارد الشبكة [وانغ و من معه ، 2006]، يمكن للمعتدي أن يسبب التصادم من خلال تغيير جزء من البيانات الموجودة في الحزم المنقولة و بذلك يوجد خطأ يدعو لإعادة الإرسال. كما يمكن أن يحدث التصادم عندما تخالف العقدة

الخبیئة شروط بروتوكول التحكم في الدخول و تقوم بالإرسال في أي وقت شاءت، و قد تدعي العقدة الخبيئة أنها عقدة شرعية لتستحوذ بذلك على صلاحيات الإرسال.

2. الاستجاب

يستغل هذا الاعتداء بروتوكول المصافحة المستخدم في تحقيق الاتصال بين العقد، حيث يتمكن المعتدي من استنزاف موارد العقدة المستهدفة من خلال إرسال حزم طلب الإرسال بشكل متكرر مما يدفع العقدة الضحية إلى إعادة إرسال رد جاهزية الاستقبال إلى الحد الذي يستهلك مواردها [كافيتا و سريدهان ، 2010].

3. اعتداء سيبيل

وهنا يعمد المعتدي إلى انتحال هوية أكثر من عقدة داخل الشبكة مما يؤثر على موثوقية و صحة البيانات، و من خلال تزيف الهوية يمكن للمعتدي أن يخترق التخزين الموزع للبيانات، آلية التوجيه المستخدمة في الشبكة، آلية تجميع البيانات، و توزيع الموارد [إيثان و من معه ، 2006]. و إذا دمجت الهويات المزيفة مع مواقع مزيفة يصبح بإمكان المعتدي أن يظهر في مواقع مختلفة من الشبكة بهويات مختلفة [طاهر و شاه ، 2008] مما يزيد من احتمالية اختيار عقدة سيبيل كجزء شرعي من مسار التوجيه. و قد تعمل مجموعة من العقد المزيفة إلى إرسال تعزيزات سلبية تطعن في صحة مجموع البيانات التي أرسلتها العقد [كومار و سارما، 2008].

3-4-5 الاعتداءات المستهدفة لطبقة الشبكة

1. اعتداء المجمع

يقوم المعتدي باستغلال خوارزميات التوجيه من أجل توجيه حركة البيانات إلى عقدة ضحية تعمل بمثابة المجمع التي تجرف إليها كل الرسائل المنقولة خلال الشبكة. و قد يستخدم هذا المجمع - الذي قد يقطع الطريق بين العقد و المحطة الطرفية في الشبكة- لتحقيق اعتداء الثقب الأسود أو الثقب الدودي.

2. طوفان حزم الترحيب

وفقاً للعديد من بروتوكولات التوجيه فإن العقد تعلن عن وجودها بإرسال حزم ترحيب إلى العقد المجاورة لها، و قد يعتمد المعتدي إلى استخدام كمبيوتر محمول - أو أي جهاز آخر له هوائي إرسال قوي- ليرسل من خلاله حزم ترحيب إلى جميع العقد في الشبكة مما يوهم هذه العقد بأن جهاز المعتدي عقدة شرعية تنتمي إلى الشبكة مخولة لاستلام الرسائل الأمر الذي يؤدي إلى هدر طاقة العقدة و فقدان البيانات.

3. اعتداء الثقب الأسود

تستخدم شبكات الحساسات اللاسلكية التوجيه متعدد النقاط الوسيطة مما يعني أنها تفترض أن جميع العقد المشاركة في توجيه الرسائل تعمل على تمرير الرسائل بإخلاص و بدون تغيير مسارها و تقع العقد ضحية للمعتدي عندما يقنعها بأنه على بعد قفزة واحدة لتمرر الرسائل إليه و عند استلامه للرسائل قد يرفض تمرير بعض الرسائل و يهملها مشكلاً بذلك ثقباً أسود تخنفي داخله الرسائل أو أن يمرر الرسائل بشكل انتقائي فيسمح بمرور بعضها و يهمل البعض الآخر و يظهر في الشكل رقم 2 عقدة خبيثة تعمل بمثابة الثقب الأسود الذي

يتوسط بين عناقد الشبكة [مارتنز و جونييه، 2010].

4.الثقب الدودي

في هذا الاعتداء يقوم المعتدي بإنشاء نفق افتراضي تمرر من خلاله الرسائل، و يمكن إيجاد هذا النفق من خلال عقدتين متواجديتين في جزئين مختلفين في الشبكة، و تزداد خطورة الثقب الدودي عندما يتوضع المعتدي على مقربة من المحطة الطرفية ليوهم العقد في الشبكة بأنه على بعد قفزة واحدة مما يتيح له استلام جميع الرسائل كما هو موضح في الشكل رقم 3 حيث يجذب الثقب الدودي رسالة العقدة أ دون أن تمر بالعقد الشرعية.

4.التوجيه الخاطئ

تعمل العقدة الخبيثة الموجودة في مسار التوجيه على إرسال حزم البيانات في مسارات خاطئة لتمنع من وصولها إلى مستقبلها الشرعي. و بإمكان المعتدي أن يغير معلومات التوجيه كذلك ليخلق حلقات توجيه داخل الشبكة، ليغير أطوال مسارات التوجيه، أو ليجذب حزم البيانات باتجاه عقدة معينة أو يبعدها عنها [وانغ و من معه ، 2006].

5.تزييف إقرار الاستلام

تتطلب بروتوكولات التوجيه المستخدمة في شبكات الحساسات اللاسلكية استخدام إقرار التسليم للتأكد من وصول الرسائل، وقد يقوم المعتدي بالتصنت على حزم البيانات المنقولة و من ثم يقوم بتزييف إقرار الاستلام لهذه الحزم مما يوهم العقد المرسله باستلام المستقبل الشرعي لها الذي قد يكون خارج الخدمة في الحقيقة، فباستخدام هذه الثغرة يستطيع المعتدي أن يعطي معلومات غير صحيحة عن حالة العقد في الشبكة.

6.الاعتداء الموجه

من خلال تحليل حركة البيانات في الشبكة يستطيع المعتدي أن يحدد العقد ذات المسؤوليات الخاصة في الشبكة كرأس العنقود أو مدير المفاتيح الأمنية، ليتمكن من السيطرة على الشبكة عن طريق شن هجمات التشويش الإذاعي و حجب الخدمة على هذه العقد. [كافيتا و سريدهان ، 2010].

3-4-6 الاعتداءات المستهدفة لطبقة النقل

1. اعتداء الطوفان

و الذي يقع عندما يقوم المعتدي بتكرار إرسال طلبات الاتصال إلى عقدة ما ليعمل على استنزاف مواردها. و يمكن الحماية من هذا الاعتداء بوضع حد لعدد طلبات الاتصال المرسله من كل عقدة.

2. اعتداء اللاتزامن

يهدف هذا النوع إلى إرباك الاتصالات القائمة في الشبكة، حيث يقوم المعتدي بتكرار إرسال رسائل مزيفة إلى أحد أو كلا طرفي الاتصال مما يدفع العقد إلى طلب إعادة الإرسال و إذا استخدم المعتدي التوقيت المناسب بإمكانه أن يمنع العقد المتصلة من تبادل أي معلومات صحيحة لتستمر في استنزاف مواردها طلباً لتصحيح الإرسال.

3-4-7 الاعتداءات المستهدفة لطبقة التطبيقات

1. اعتداء الإرباك

و الذي يقع عندما يقوم المعتدي بغمر العقد بمثيرات للحساسات مما يضخم حجم البيانات المرسله من العقد إلى المحطة الطرفية. و يهدف هذا النوع من الاعتداء إلى هدر طاقة العقد و استهلاك عرض نطاق الشبكة.

و يمكن الحد من آثاره من خلال ضبط الحساسات بحيث تعمل عند وجود مثيرات محددة كأن تتحسس حركة المركبات لا أي حركة عشوائية تحدث حولها.

2. إعادة البرمجة الغامرة

إن نظم برمجة الشبكات تسمح بإعادة برمجة العقد عن بعد، و إذا لم يتم تأمين هذه العملية فإن بإمكان المعتدي أن يختطف العملية ليتحكم بالعقد المكونة للشبكة.

3-4-8 الاعتداءات المستهدفة للبيانات المنقولة

في شبكات الحساسات اللاسلكية ترسل الحساسات إلى المحطة الطرفية تقاريراً بالتغييرات التي تحدث في المعالم التي تراقبها، و قد تتعرض هذه التقارير إلى مجموعة من الاعتداءات نذكرها فيما يلي.

1. المقاطعة

في هذا النوع من الاعتداء تصبح قناة الاتصال غير متاحة مما يهدد استمرارية عمل الشبكة و يساعد في تحقيق حالة حجب الخدمة.

2. الاعتراض

يهدف هذا الاعتداء -الذي قد يعرف باسم التصنت أو الرصد الصامت [سين ، 2009] إلى اختراق سرية الرسائل المتبادلة بين العقد من خلال التصنت عليها أو من خلال السيطرة على أحد عقد الشبكة و البيانات المخزنة داخلها. و من الصعب اكتشاف هذا النوع من الاعتداء لأنه لا يجري أي تعديل على البيانات إلا أنه من الممكن التقليل من نسبة حدوثه من خلال استخدام آليات التشفير المناسبة.

3. التعديل

يهدد هذا الاعتداء صحة و نزاهة البيانات عندما يتمكن المعتدي من الوصول إلى البيانات و تعديلها مما يخلق تشويشاً بين العقد التي تتبادل البيانات. فقد يغير المعتدي بيانات المرسل، المرسل إليه، محتوى الرسالة نفسها، أو يمسح بعض الحزم مما يفسد الرسالة.

4.التصنيع

يستهدف هذا الاعتداء موثوقية البيانات المنقولة داخل الشبكة عندما يقوم المعتدي بتغذية الشبكة ببيانات مصنعة من قبله. الغرض الأساسي لهذا الاعتداء هو تضليل العقد المكونة للشبكة. و من الممكن أن تساعد في تحقيق حجب الخدمة عندما تغمر العقد بطوفان من الحزم المصنعة.

5.إعادة الإرسال

يؤثر هذا الاعتداء على حداثة البيانات عندما يعيد المعتدي إرسال رسائل قديمة ليوهم العقد بحدائتها. و تبرز هذه الثغرة في الشبكات التي لا تستخدم البروتوكولات المدركة للزمن.

3-4-9 الاعتداءات المحسوسة الموجهة ضد عقد الشبكة

1.اعتقال العقدة

عادة ما يتم نشر شبكات الحساسات اللاسلكية في مواقع مفتوحة مما يجعلها عرضة للاعتقال. و بمجرد اعتقالها فإن بإمكان المعتدي أن يسرق المعلومات الحساسة المخزنة عليها، تدميرها، أو إعادة برمجتها. إن اعتقال عقدة واحدة يعرض الشبكة بأكملها للخطر.

2.العقدة المزيفة

بإمكان المعتدي أن يضيف عقدة مزيفة إلى الشبكة لتعمل على تغذية الشبكة ببيانات خاطئة، و قد تتمكن من استدراج العقد المجاورة لها لترسل لها بياناتها. و يعد هذا الاعتداء من أخطر الاعتداءات لأنه بإمكان العقدة المزيفة أن تنتشر أكوادها الخبيثة إلى سائر العقد في الشبكة .

3.استنساخ العقدة

يقوم المعتدي بإضافة عقدة مستنسخة من أحد العقد المتواجدة في الشبكة بحيث تحمل العقدة المستنسخة هوية العقدة الضحية فتصبح قادرة على تزيف معلومات التوجيه داخل الشبكة بالإضافة إلى تمكنها من الوصول إلى معلومات سرية كمفاتيح التشفير و عند وضع العقد المستنسخة في مواقع استراتيجية يستطيع المعتدي التحكم بنطاقات مختلفة من الشبكة مع إمكانية إحداث فصل الشبكة و يمكن أن تكون هناك أكثر من نسخة بنفس الهوية على عكس اعتداء سبيل الذي تظهر فيه عقدة واحدة بهويات مختلفة.

4.الحرمان من وضع السكون

يهدف هذا الاعتداء إلى حرمان العقد من وضع السكون مما يؤدي إلى استنزاف موارد طاقتها حتى تموت. و قد يحدث ذلك بغمر العقدة بعدد كبير من الرسائل أو بطلب تنفيذ حسابات كثيفة تظهر و كأنها طلبات شرعية.

3-5-5 حماية شبكات الحساسات اللاسلكية

في هذا الجزء من البحث نلقي الضوء على بعض القضايا المتعلقة بحماية و تأمين شبكات الحساسات اللاسلكية، يبدأ هذا الجزء بتعريف الإطار العام الذي تعمل وفقه معظم الحلول الأمنية ، كما ينتهي بعرض لمبادئ عمل بعض الأنظمة الأمنية في شبكات الحساسات اللاسلكية.

3-5-10 الإطار العام لتصميم حلول أمنية

يشير [هيو و من معه ، 2004] إلى ثلاث أهداف رئيسة في مجال تأمين شبكات الحساسات اللاسلكية: إدارة مفاتيح التشفير وهي قضية حاسمة الأهمية لكنها تضحى مهمة صعبة في شبكات الحساسات اللاسلكية نظراً لطبيعة الشبكات العشوائية، الاتصال المتقطع، و محدودية العقد من حيث الموارد. تقليدياً فإن إدارة المفاتيح تتم عن طريق جهات مانحة موثوقة، إلا أن استخدام جهة مانحة وحيدة في شبكات الحساسات اللاسلكية يعد أمراً خطيراً لأنه باختراق الجهة المانحة تسقط الشبكة بأكملها، التوجيه الآمن تتعرض بروتوكولات التوجيه المستخدمة في شبكات الحساسات اللاسلكية إلى الكثير من الاعتداءات الداخلية و الخارجية، و التحدي يكمن في إيجاد بروتوكولات آمنة في ظل جغرافية الشبكة الدينامكية، العقد غير الحصينة، بالإضافة إلى قدرات الحساسات المحدودة المصحوبة بمحدودية الطاقة، منع هجمات حجب الخدمة و الذي يعد أمراً بالغ الصعوبة و ذلك لقدرة المخترق على تنفيذه في جميع طبقات بروتوكول الشبكة. و يؤكد [كافيتا و سريدهان ، 2010] على ضرورة تأمين جميع طبقات بروتوكول الشبكة لتحقيق أمن متكامل لشبكات الحساسات اللاسلكية و أن تكون الآليات الأمنية قابلة للتكيف مع طبيعة الشبكات الموزعة و التشكيل الديناميكي. كما يؤكد على أهمية ألا تتعدى كلفة الآليات الأمنية الكلفة المقدرة للآثار الناتجة عن الاختراق الأمني. بينما يتجه [طاهر و شاه ، 2008] إلى توضيح طريقتين للكشف عن الاختراقات الأمنية: النهج المركزي - الذي تتولى فيه عقدة مركزية مسؤولية الكشف عن الاختراق و من ثم تحديد الآليات اللازمة للتعافي من هذا الاختراق و منع حدوثه مستقبلاً. المنهج الموزع حيث تشترك جميع العقد في اكتشاف الاختراق، و في حال تواجده فإنه يتم الاتصال بالعقدة المركزية من أجل إجراء التعديلات اللازمة على جغرافية الشبكة و معلومات التوجيه. و من سلبيات الطريقة الأولى أنها تسبب زيادة في كثافة حركة البيانات باتجاه العقدة المركزية، كما أن الطريقة الثانية تعد مناسبة للشبكات المكونة من عدد صغير من العقد، و في حال ارتفاع عدد العقد فإن بإمكان المخترق أن

يسيطر على الشبكة دون أن تشعر العقدة المركزية بذلك. إن تصميم أي حل أمني يعتمد على طبيعة الشبكة من حيث هدف التشغيل، النطاق، ومدى اهتمام المعتدين باختراقها [ناكياما و من معه ، 2007] بالإضافة إلى كلفة تنفيذ هذا الحل الأمني و خصوصاً فيما يتعلق باستهلاك موارد العقد. حيث يفيد [تشيجان و من معه، 2004] أن استهلاك موارد العقد بفعل الآليات الأمنية قد يؤدي إلى حالة من حجب الخدمة غير المقصودة في الشبكة و هي ما تعرف بحجب الخدمة الأمني. و يفرق [كاريكهوف ، 2007] بين نوعين من تكاليف الطاقة المصاحبة لتنفيذ الآليات الأمنية: تكاليف ثابتة - وهي الطاقة المستهلكة في الترقب للاختراقات الممكنة، تكاليف متغيرة - و هي الطاقة اللازمة لاستكشاف العقد المخترقة و من ثم تخفيف الأثر الواقع على معلومات التوجيه داخل الشبكة. يلخص [باتان و من معه ، 2006] مجموعة من الإنجازات البحثية في ابتكار وسائل لتأمين شبكات الحساسات اللاسلكية و يذكر [كافيتا و سريدهان ، 2010] بعض المقاييس التي يمكن أن تستخدم في تقييم الحلول الأمنية لشبكات الحساسات اللاسلكية:

- المرونة - ينبغي أن يضمن الحل الأمني استمرارية عمل الشبكة و حمايتها حتى بعد تعرضها للاختراق، كما ينبغي أن يكون قادراً على التكيف مع أي نموذج لنشر الحساسات.
- استخدام الطاقة بفاعلية - يجب ألا يسبب استهلاك الحل الأمني للطاقة توقف الشبكة عن العمل.
- التكيف مع الأعطال - على أي حل أمني أن يستمر في توفير الأمن للشبكة حتى في حال حدوث الأعطال
- القابلية للتوسع - ينبغي أن يكون الحل الأمني قابلاً للتوسع دون التأثير على مستوى الأمن

- الشفاء الذاتي - في حال فشل بعض الحساسات في الشبكة فإنه ينبغي إعادة ترتيب الحساسات المتبقية للمحافظة على مستوى الأمن.

- الضمان - و يعني ضمان نشر المعلومات لمستخدميها.

3-6 استعراض الحلول الأمنية

يهدف هذا الجزء من الكتاب إلى تزويد القارئ بمبادئ عمل الحلول الأمنية المصممة خصيصاً لشبكات الحساسات اللاسلكية و تحديداً التشفير و إدارة المفاتيح، بروتوكولات التوجيه الآمنة، وسائل الحماية من هجمات حجب الخدمة، و أخيراً وسائل كشف التسلل.

3-6-1 التشفير و إدارة المفاتيح

إن آليات التشفير المصممة للشبكات السلكية غير قابلة للتطبيق في شبكات الحساسات اللاسلكية لأن تطبيقها يتطلب زيادة في استهلاك قدرات العقد الحاسوبية و موارد طاقتها كما أنه قد يزيد من حدوث تأخير في الإرسال أو فقدان لحزم البيانات [باثان و من معه ، 2006]. و يقترح [هيلي و من معه ، 2007] آلية لتقليل تكاليف التشفير و ذلك عن طريق استغلال مورد متوفر على معظم الحساسات و هو وحدة التشفير الموجودة في رقاقة Chipcon CC2420 . و من جهة أخرى قام [تشانج و من معه ، 2008] بدراسة استهلاك الطاقة في تنفيذ عمليات التشفير البرمجية و يدرج مبادئ توجيهية لتطبيق التشفير في شبكات الحساسات اللاسلكية بفاعلية كما يقدم [سليجبيسفاك و من معه، 2002] نموذجاً أمنياً تتناسب فيه تكلفة التشفير مع حساسية البيانات المشفرة حيث يوفر ثلاث مستويات أمنية: المستوى الأول - مخصص للكود المتنقل الذي يعد أكثر البيانات حساسية في الشبكة و يستخدم أقوى مستويات التشفير، المستوى الثاني - و الذي يستخدم تشفيراً أقل قوة لمواقع

الحساسات التي يتم تبادلها ، المستوى الثالث - و هو أدنى مستويات التشفير المستخدم للبيانات الخاصة بالتطبيق.

ومن المتفق عليه أنه على آلية التشفير المستخدمة في شبكات الحساسات اللاسلكية أن تتماشى مع قيود العقد المكونة للشبكة و أن تكون مناسبة من حيث حجم الكود اللازم لتشغيلها، حجم البيانات الناتج عن استخدامها، الوقت المستغرق في تنفيذها، و مستوى الطاقة التي تستهلكها. و يستعرض الباحثون في [وانغ و من معه ، 2006] [دو و تشين، 2008] [تشين و من معه ، 2009] [سين ، 2009] [كافيتا و سريدهان ، 2010] آليات التشفير المقترحة للتطبيق داخل شبكات الحساسات اللاسلكية و مما خلصوا إليه أن آليات التشفير المتناظرة تتفوق على الآليات اللامتناظرة- أو مايعرف بالتشفير باستخدام المفتاح العام - من حيث السرعة في التنفيذ والتقليل من مستوى استهلاك موارد العقد المحدودة مما يجعل التشفير المتناظر الاختيار الأمثل بالنسبة لشبكات الحساسات اللاسلكية. إلا أنه من أكبر العقبات أمام آليات التشفير المتناظر تأمين عملية توزيع المفاتيح بين الأطراف المتواصلة في الشبكة.

إن تطبيق التشفير في شبكات الحساسات اللاسلكية يثير بعض الأسئلة المهمة فيما يخص إدارة مفاتيح التشفير. و تعد بروتوكولات إدارة مفاتيح التشفير من أكثر القضايا تناولاً في مجال تأمين شبكات الحساسات اللاسلكية حيث يتطلب منها إدارة المفاتيح بين العقد بطريقة آمنة و موثوقة و بما أن العقد في شبكات الحساسات اللاسلكية تعاني من قدرات و طاقات محدودة فإن هذه البروتوكولات تواجه تحديات يمكن تلخيصها في العناصر التالية [هيو و من معه ، 2004] [سين ، 2009]: التوزيع المسبق للمفاتيح و الذي قد يكون صعب التطبيق نظراً لحجم الذاكرة المحدود في الحساسات، اختيار آلية اكتشاف العقد المجاورة و التي يجب أن تكون قوية لمنع المخترق من استغلالها في اكتشاف المفاتيح السرية، تغيير المفتاح تلقائياً و الذي لن يكون

سهل التحقيق بسبب صعوبة توقع الوقت اللازم لاكتشاف المفتاح و صعوبة تحديد طول الفترة التي تمثل صلاحية المفتاح، معالجة العقد المخترقة و التي قد يستغلها المعتدي للتوصل إلى المفتاح، بالإضافة إلى تأمين الوصول المباشر من طرف لطرف و التأخير المصاحب لعمليات إنشاء المفاتيح.

و بالرغم من التحديات التي تواجه إدارة المفاتيح في شبكات الحساسات اللاسلكية تمكن العديد من الباحثين من تقديم بروتوكولات يصنفها [وانغ و من معه ، 2006] بحسب هيكل الشبكة إلى بروتوكولات مركزية و أخرى موزعة و بحسب احتمالية الاشتراك في المفتاح بين عقدتين إلى بروتوكولات احتمالية و أخرى حتمية. وفي البروتوكولات المركزية يوجد ما يسمى بمركز توزيع المفاتيح و الذي يتولى مسؤولية إصدار و توزيع المفاتيح، مما يشكل نقطة ضعف يمكن أن تستغل لاختراق الشبكة فبمجرد اختراق مركز توزيع المفاتيح تسقط الشبكة بأكملها في قبضة المعتدي. و على النقيض من ذلك نجد أن البروتوكولات الموزعة توظف أكثر من جهة لتوزيع و إنشاء المفاتيح مما يعزز قوتها في مواجهة الاختراق لذا نجد أن أغلب البروتوكولات تستخدم المنهجية الموزعة. و يصنف البروتوكول على أنه حتمي إذا كان يضمن وجود مفاتيح مشتركة بين أي عقدتين وسطيتين في الشبكة، على العكس من البروتوكول الاحتمالي الذي لا يضمن ذلك. و نحن ندعو القارئ للرجوع إلى [وانغ و من معه ، 2006] [تشين و من معه ، 2009][سين ، 2009] للوقوف على تفاصيل عمل البروتوكولات التي استعرضها الباحثون و للتعرف على مستوى أدائها من ناحية قدرتها على الاتساع، سرعتها في التغلب على الاعتداءات، و تكلفة استخدامها من حيث التخزين، المعالجة، والاتصال.

و يركز الباحثون في [سيمبليشيو و من معه ، 2009] على استعراض مجموعة من بروتوكولات التوزيع المسبق للمفاتيح بحكم أنها الأنسب لشبكات الحساسات اللاسلكية المتجانسة التي تعد الأكثر شيوعاً. و قد عرض الباحثون تقييماً مفصلاً لمجموعة كبيرة من البروتوكولات تنتمي إلى تسع فئات مختلفة ، و لإجراء

التقييم عرف الباحثون معايير لقياس فعالية و مرونة البروتوكول تتلخص في: حجم الذاكرة المستهلكة في تخزين المفاتيح، عدد دورات المعالج اللازمة لإصدار المفاتيح، كمية البيانات المتبادلة بين العقد خلال عملية إصدار المفاتيح، حجم الطاقة المستهلكة في إصدار المفاتيح، ضمان ترابط العقد من خلال توفر مفاتيح مشتركة بينها، عدم الاعتماد على المعرفة المسبقة لمواقع العقد داخل الشبكة، القدرة على العمل في نطاق واسع و سهولة إضافة عقد جديدة للشبكة.

تتعدد أنواع المفاتيح المستخدمة داخل شبكات الحساسات اللاسلكية لتشمل [مارتنز و جونه، 2010]:
المفاتيح الشاملة - حيث تشترك جميع عقد الشبكة في نفس المفتاح و الذي يستخدم في تشفير و فك تشفير جميع الرسائل المتبادلة ، المفاتيح الزوجية للعقد - و الذي يفترض أنه إذا كان للعقدة عدد (س) من العقد المجاورة فإن عليها تخزين (س) من المفاتيح المختلفة للتواصل مع جيرانها ، المفاتيح الزوجية للمجموعات - حيث تستخدم العقد داخل العنقود مفتاح مشترك و يتم التواصل بين رؤوس العناقيد باستخدام مفاتيح زوجية، المفاتيح الفردية - حيث يخصص لكل عقدة مفتاح خاص ، معلوم من قبل مجمع الشبكة فقط. و نستطيع القول أن المفاتيح الزوجية أقوى من المفاتيح الشاملة لأنه في حال اختراقها سيفشل جزء محدود من الشبكة على عكس المفاتيح الشاملة التي قد يسبب اختراقها انهيار الشبكة بأكملها.

3-6-2 التوجيه الآمن

تم إنشاء العديد من بروتوكولات التوجيه الآمنة للشبكات اللاسلكية العشوائية إلا أنها غير مناسبة لشبكات الحساسات اللاسلكية بسبب كثافة الحوسبة المصاحبة لها و لعدم توافقها مع حركة البيانات في شبكات الحساسات اللاسلكية [دو و تشين، 2008]. و يشير [كافينا و سريدهان ، 2010] إلى الخصائص الأمنية

الواجب توفرها في بروتوكولات التوجيه الآمنة: التحقق من الهوية، التأكيد ثنائي الاتجاه، تقييد جغرافية الشبكة، اعتماد اللامركزية و الإرسال متعدد المسارات. و يضيف [هيو و شارما ، 2005] أنه يتوجب على البروتوكول أن يكون قادراً على عزل العقد غير المصرح لها خلال عملية اكتشاف الطريق، المحافظة على سرية جغرافية الشبكة، حماية المسارات من التضليل، منع اختراق الرسائل المتبادلة خلال عملية اكتشاف الطريق، و القدرة على تمييز رسائل التوجيه المزيفة.

يمكن تصنيف بروتوكولات التوجيه الآمنة إلى [سين ، 2009] : بروتوكولات توجيه مستوية - و التي تعطي لعقد الشبكة أدوراً متكافئة في عملية التوجيه، بروتوكولات توجيه هرمية - و التي تعطي لعقد الشبكة أدوراً متباينة في عملية التوجيه، بروتوكولات توجيه جغرافية - و التي توجه البيانات اعتماداً على مواقع العقد في الشبكة. و من الملاحظ أن معظم البروتوكولات تخدم الشبكات الساكنة دون أي اعتبار لإمكانية حركة العقد [وانغ و من معه ، 2006].

يوفر [مديركزاني و من معه ، 2010] تحليلاً مفصلاً لمجموعة من البروتوكولات المتعددة المسارات من حيث المتطلبات الأمنية المتحققة من خلال استخدامها، بالإضافة إلى تحديد بروتوكولات إدارة المفاتيح و آليات التوثيق التي تستخدمها. و قد وجد الباحثون أنه يتم تحقيق التوثيق و نزاهة البيانات في معظم البروتوكولات المختارة مما يؤكد قدرتها على مواجهة اعتداءات مثل اعتداء سيبيل و غيره كما يشير الباحثون إلى ضرورة تحقيق التوازن بين المستوى الأمني و الموارد المستهلكة عند اختيار أي بروتوكول.

كما يقدم [دو و بينغ ، 2009] دليلاً يساعد المختصين في اختيار البروتوكول المناسب للتطبيقات المختلفة لشبكات الحساسات اللاسلكية و تحديداً مراقبة البيئة و المسكن، التطبيقات العسكرية و الطبية، التطبيقات

المنزلية والمكتبية، و تطبيقات مراقبة الإنتاج. و يحدد لكل بروتوكول عدداً من الخصائص منها على سبيل المثال الاعتداءات التي قد يتعرض لها، جغرافية الشبكة، نموذج نشر البيانات، و مستوى الطاقة المستهلكة

3-7 جرائم المعلوماتية

يقصد بالجريمة المعلوماتية كل استخدام ، في صورة فعل أو امتناع ، غير مشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على أي مصلحة مشروعة سواء أكانت مادية أم معنوية ، تعتبر الجرائم المعلوماتية ثمرة من ثمار التقدم السريع في شتى المجالات العلمية الذي يتميز به عصرنا الحاضر ؛ فهناك ثورة في مجال الجينات والصبغيات نتيجة للتقدم في فرع الهندسة الوراثية ؛ وهناك ثورة في مجال وسائل الاتصال والمعلومات Information Revolution ترجع إلى استخدام الكمبيوتر (الحاسوب) ... الخ .

ولقد صاحب هذا التقدم السريع في مجال العلوم والتقنية واستخداماتها لخير البشرية ؛ تقدم آخر مواز في مجال الجريمة ؛ فلم تصبح الجريمة مقصورة على طبقة معينة من طبقات المجتمع دون أخرى ؛ وذلك لوضوح إجرام الفساد الذي يتورط فيه كبار المسؤولين في الدول المختلفة ؛ علاوة على إجرام ذوي الياقات البيضاء ؛ الذي يتورط فيه كبار المسؤولين في الشركات العملاقة ؛ وإجرام الاتجار بالمخدرات .

وعلى مستوى ثورة الاتصالات والمعلومات نجد أن الصراع مستمر بين جانبي الخير والشر في هذه الثورة ؛ ففي جانب الخير نجد أن هذه الثورة ساعدت على عولمة المعلومات ؛ وتسهيل كثير من الخدمات والأعمال ؛ فقد توصلت البشرية إلى السيطرة على المعلومات من خلال استخدام الحاسب الآلي computer لتخزين ومعالجة واسترجاع المعلومات ؛ فضلا عن استخدامه في عمليات التصميم والتصنيع والتعليم والإدارة ؛ ناهيك عن تطوير تطبيقاته لتشمل أداء خدمات عديدة مثل التعليم والتشخيص

والخدمات التمريرية وتسهيل المعاملات والخدمات البنكية والحجز الآلي لنقل الأشخاص وإدارة المكاتب الحديثة وقيادة المعارك ؛ وعلى وجه العموم دخل الحاسب الآلي في شتى نواحي الحياة الإنسانية .

فضلا عن أنه جعل المعلومات في متناول الجميع من خلال شبكات الإنترنت ؛ أي شبكات المعلومات المحلية والإقليمية والعالمية ؛ وأصبح العالم بذلك مزدخراً بكم هائل من المعلومات لا تعرف الحواجز الجغرافية ولا المسافات ؛ بصورة يمكن معها القول بأن العالم صار أشبه بمجتمع كبير تترايط فيه الحاسبات و شبكات المعلومات ؛ لتعلن بزوغ فجر ثورة جديدة هي الثورة المعلوماتية La revolution informatique أو الثورة الصناعية الثالثة التي تدفع بالإنسانية إلى عصر جديد هو عصر أو مجتمع المعلومات.

وعلى جانب الشر والاستخدامات غير الشرعية نجد أن الإنسان متأثراً بنزواته وشهواته ونواقصه يسعى استخدام ثورة الاتصال والمعلومات ؛ فإذا كانت الكثير من المؤسسات كالبنوك والشركات الكبرى تستخدم الحاسب الإلكتروني ؛ فإنه من خلاله ترتكب كثير من الجرائم مثل السحب الإلكتروني من الرصيد بواسطة الكارت الممغنط إذا كان مزوراً أو من غير صاحب الصفة الشرعية، كذلك يمكن تصور التجسس عن بعد وسرقة بيانات تتعلق بالأمن القومي ؛ ومن الممكن أن يترتب علي الإصابة بالفيروس المعلوماتي تدمير برامج مهمة ، علاوة على أنه من المتصور أن يحدث مساساً بحياة الأفراد الخاصة وانتهاكها من خلال استخدام الحاسب الآلي وشبكة الانترنت ، والمثل يقال بالنسبة للجرائم الماسة بالآداب .

3-7-1 خصائص جرائم المعلوماتية

في واقع الأمر أن جرائم المعلوماتية تتميز بعدة خصائص لعل من أبرزها ما يلي : -

لا يتم في الغالب الأعم الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير . لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة ؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها . فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة ؛ والعدد الذي تم اكتشافه ؛ هو رقم خطير . وبعبارة أخرى ؛ الفجوة بين عدد هذه الجرائم الحقيقي ؛ وما تم اكتشافه فجوة كبيرة ، ومن الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني ؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها .

لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها ؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت . فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها .

تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم . إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها . فهي جرائم تتسم بالغموض ؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية . الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى .

عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم ؛ فهذه الجرائم هي صورة صادقة من صور العولمة ؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة ؛ ومن الناحية الزمنية تختلف المواقيت بين الدول ؛ الأمر الذي يثير التساؤل حول : تحديد القانون الواجب التطبيق على هذه الجريمة .

3-8 التشريعات القانونية

ونسبة لكل هذه المخاطر كان من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا الإجراء غير التقليدية ، مواجهة تتعامل بشكل عصري متقدم مع جرائم المعلوماتية المختلفة التي يأتي في مقدمتها بناء ونشر برامج فيروسات الحاسب الآلي والدخول غير المشروع علي شبكات الحاسبات، والتحايل علي نظم المعالجة الآلية للبيانات وإتلاف البرامج وتزوير المستندات المعالجة إلكترونياً، فضلاً عن الجرائم التي تحدث في مجال البنوك.

غير أن هذه المواجهة قاصرة حتى الآن والتشريعات القانونية غير كافية وغير فعالة كأن الجرائم المعلوماتية ماردا جبارا خرج من القمم تستعصي عليه أية مواجهة تشريعية ، أو بعبارة أخرى ؛ المواجهة التشريعية تسير بسرعة السلحفاة في مواجهة (الجرائم المعلوماتية) التي تنطلق كالصاروخ بسرعة الضوء .

فلا جدال في أن صور السلوك الخطر والضرار بمجتمع المعلوماتية تكسب أرضاً جديداً يوماً بعد يوم ، في الوقت الذي تعجز فيه التشريعات القائمة عن مواجهة هذا الخطر الداهم ؛ الذي يهدد في الصميم الأفراد في ممتلكاتهم وخصوصياتهم ؛ والمؤسسات في كيانها المادي والاقتصادي ؛ والاقتصاد في بنيانه وحركة التعامل في مفرداته .

3-7-2 الهاكر الاخلاقي Ethical Hacker

الهكر الأخلاقي "قرصان أبيض القبعة" هو مصطلح يُطلق على المُخترق الذي يملك جميع المعلومات والدراسات التي تجعله هكر غير أخلاقي " قبعة سوداء " و متمكّن من اختبار اختراق الأنظمة والمخدمات ودراسة سلوكها، ولكن مع ذلك يكون هيبته انه لا يلتفت إلى صغائر الأمور ولا يشجع أبداً على أي اختراقات أو تدمير كان بل يساعد الشركات في استعادة مواقعها ودراسة كيفية تم المخترق " قبعة سوداء " من السيطرة على السيرفر وبذلك يقوم فوراً بتوفير الحماية اللازمة من تلك الطرق والأساليب والثغرات المستخدمة من قبلهم، ويعتبر شخص يمتلك القدرة على الاختراق والحماية من الاختراق، يمتلك احدى الشهادات المخصصة لممارس طبيعة عمله كهاكل اخلاقي، كما يسخر تلك الفنون "الاختراق والقرصنة" لخدمة المجتمع أما بتقديم خدمات أمنية احترافية أو باكتشاف الثغرات في تطبيقات وأنظمة دولية وأشعار الشركات المتضررة بخطورة تلك الثغرات، ولكن لا يتم كل ذلك إلا بعد توقيع اتفاقيه وتخطيط مسبق مع الجهة المراد اختبارها،اي انه لا يجوز له الدخول لأي مكان واختراقه "بحجة" فحصه ! يجب ان يأخذ الموافقة الازمة لذلك قبل اي خطوة متبعة.

للهاكل الاخلاقي شروط وأحكام يجب عليه اتباعها والموافقة عليها بالتوقيع على اتفاقية تسمى Code Of

Ethic وهي اتفاقية أخلاقية تهدف إلى أن الهاكر الأخلاقي يجب أن يحافظ على السرية التامة في أي اختبار

اختراق ولا يقوم بتسريب أي معلومات عن الجهة المختبرة أو الثغرات المكتشفة وعلى أن يقوم بتقديم تقرير

كامل يوضح فيه جميع الثغرات الأمنية والحلول مما يساعد الجهة المعنية بالاختبار تأمين مصادرها من

المخترقين، كما أن أي إخلال بأحد نصوص الوثيقة الأخلاقية قد يعرض الهاكر الأخلاقي للمطالبة القانونية

والمحاكمة امام الجهات المختصة.

هناك مدارس ومعاهد يتبعها مختبرون الاختراق منها التي تركز على تطبيقات الويب مثل OWASP ومنها الذي يركز على النظام وجمع المعلومات مثل OSSTMM و NIST ولكن في كل الأحوال تتبع خطوات ليست بالضرورة أن تكون إجبارية أثناء الاختبار ولكن هي خطوات تساعد المختبر باتباع تقنيات مجربة وآمنة في الاستخدام. يجتمع المختبر والجهة المعنية بالاختبار لتحديد خطة العمل وتحديد نوع الاختبار المطلوب وعدد الخوادم أو التطبيقات المراد اختبارها، بعد ذلك يتم توقيع اتفاقية بين كل من المختبر والجهة المعنية بالاختبار اتفاقية وتحديد موعد الاختبار والأجهزة المستخدمة ورقم ال IP للمخترق.

بعد الانتهاء من توقيع الاتفاقية يقوم المختبر بجمع أكبر عدد من المعلومات المتوفرة عبر الانترنت ويكون ذلك من خلال استخدام تقنيات في الاختراق تسمى Hack Google مع العلم ان هناك شرحا مفصلا لدي من خلال كتيبات الكترونية لمن يريد معرفة تفاصيل أكثر، وهذه التقنية التي تستخدم محرك البحث جوجل كمساعد لها في معرفة المعلومات المتوفرة عبر الانترنت، ففي بعض الأحيان يخطئ مديرو النظام عندما يظنوا أن ملفاتهم الموجودة على الخادم وأن وضعت في مكان غير ظاهر للمستخدم هي مخفية عن متناوله، فباستخدام هذا الأسلوب وأساليب أخرى يستطيع المخترق والمختبر معرفة جميع الملفات الموجودة على الخادم الموقع، على سبيل المثال لو وضعنا التالي في محرك البحث جوجل `site:teedoz.com shehab` سوف نلاحظ أن جوجل حصر البحث في موقع كمبيوتر فقط وقام بالبحث عن كلمة shehab فقط. بعد مرحلة جمع المعلومات يقوم المختبر بالتعرف على الهدف المراد اختباره بشكل أكبر عن طريق مسح المنافذ الموجودة ومعرفة أنواع التطبيقات والخدمات المتوفرة في الهدف مع أتباع خطوات معينة لعرض جميع الخدمات المرتبطة بشكل مباشر وغير مباشر في الهدف.

كما يتقدم عمل المختبر ليكون أشمل وأوسع عبر تحليل التطبيقات ومعرفة عدد المتغيرات في التطبيق وقيم المتغيرات ومعرفة إصدارات التطبيقات والخدمات. في المرحلة الرابعة يقوم المختبر بتحليل النواتج من المرحلتين السابقتين ويحاول اكتشاف نقاط الضعف واستغلالها لتكون ثغرات يطبقها فور اكتشافها لكي يثبت حقيقة وجودها في التطبيق أو النظام المختبر، في هذه المرحلة بالتحديد يقضى المختبر معظم فترة المشروع المتفق عليها باكتشاف نقاط الضعف وتحليل تلك النقاط وبرمجة برمجيات معينة أن لزم الأمر لاستثمار نقاط الضعف.

بعد الانتهاء من اكتشاف نقاط الضعف واختبارها يقوم المختبر بكتابة تقرير مفصل عن جميع المخاطر ونقاط الضعف والثغرات المكتشفة مع تقديم نصائح وإرشادات لإغلاق تلك الثغرات والنقاط بشكل مفصل وتقني وتحديد خطورة النقاط والثغرات المكتشفة عبر تصنيفها بثلاث مراتب وهي «خطيرة» High متوسطة الخطورة Medium وقليلة الخطورة Low ويتم ذلك بعد الرجوع لمصادر معتمدة في تقييم المخاطر الأمنية ودراسات أمنية تتم من قبل المختبر.

لو تحدثنا عن الويب فأكثر أساليب الاختراق شيوعا في وقتنا الحالي هي الاختراقات التي تستهدف تطبيقات الويب والبرامج المساعدة في تشغيل المواقع وإدارتها كما يكون مستخدمها موضع خطر في بعض الأحيان. وتعود أسباب كثرة اختراقها لكثرة استخدامها من قبل مديري المواقع والصلاحيات التي توفرها بعد الاختراق، مما شجع مكتشفي الثغرات والمخترقين بالتدقيق والبحث عن نقاط الضعف في تلك التطبيقات التي فيما بعد تستثمر لتكون ثغرات جاهزة في أيدي المخترقين وأطفال السكريبتات «Script Kiddies» فمن أكثر الثغرات توجد في وقتنا الحالي «Cross-site scripting» XSS و «SQL Injection» و «Cross Site Request» CSRF و «Forgery» و «Information Leakage and Improper Error Handling» وهي تسرب المعلومات عن

طريق الانترنت مما يجعل مهمة المخترق سهله بوجود ما يسمى Google Hack وهو استخدام محرك البحث جوجل في البحث عن المعلومات المتعلقة في الموقع ومحاولة كشف أي تسرب للمعلومات أو الملفات المراد إخفاؤها من قبل مدير التطبيق أو النظام، وأيضا يمكن تسرب المعلومات عن طريق إحداث أخطاء في التطبيق مما تساعد المخترق بجمع أكبر عدد من المعلومات عن التطبيق ومعرفة طبيعة التطبيق الجدير بالذكر أن الموضوع لا يتوقف عند اختراق الموقع بل يمتد ليشمل باقي المواقع الموجودة على الخادم «server» لأن المخترقين في العادة يحاولون رفع صلاحياتهم على النظام من مستخدمين لمديري نظم Administrator في بيئة ويندوز، وroot في بيئة لينكس ويكون ذلك باستخدام ثغرات تدعى Local Root Exploit في لينكس و escalation administrator privilege في بيئة ويندوز والتي تعتمد في الغالب على أخطاء النظام نفسه أو خطأ في أحد تطبيقات المنزلة في النظام والتي تساعد المخترقين باستغلالها، ولو فرضنا وصادف أن يكون النظام محمياً بشكل جيد وجميع التطبيقات تخلو من الأخطاء والثغرات الأمنية يبدأ المخترقون باستخدام أساليب وطرائق أخرى مثل تحميل ما يدعى ال phpshell لتكون في المقام الأول أبواب خلفية لهم للعودة إلى النظام متى أرادوه وأداه للتجوال داخل الخادم واستعراض ملفات المستخدمين الآخرين ومن ثم اختراقهم، مع الأخذ بالاعتبار أنه تم اكتشاف حل لمشكلة ال phpshell فيما سبق وهي عن طريق تفعيل ما يدعى php safe mode في أنظمة لينكس مما كان يحد من عمليات الاختراق الداخلي، غير أنه ومع مرور الوقت اكتشف المخترقون طرائق عديدة لتخطي ال php safe mode فكان الحل الوحيد هو تعطيل بعض الدوال الخطيرة في php وتغيير صلاحيات ملفات معينة مع تركيب بعض البرمجيات التي تشل حركة المخترق داخل السيرفر وتقلل الضرر على موقع واحد فقط، ولكن بقدر ما يحاول خبراء الأمن تطوير وتحسين القاعدة الأساسية

للأمن يحاول المخترقون بدورهم إيجاد طرائق بديلة لتخطى الجدران المنيعه، فقد كانت ال phpshell مثال من مئات الأمثلة لما يستخدمه المخترقون لتخطي قواعد الأمن المعدة مسبقا من قبل مدير النظام.

3-7-3 الهندسة الاجتماعية

هناك عدة تعريفات للهندسة الاجتماعية ومن أشهرها أن الهندسة الاجتماعية هي طريقة الهجوم المستخدمة من قبل العديد من المهاجمين، و التي تستفيد من طبيعة البشر ونقاط الضعف فيها، للتلاعب عليهم وخداعهم بكسب ثقتهم وذلك من أجل الحصول على المعلومات السرية سواء كانت كلمات المرور الخاصة بالأشخاص أو أي معلومة حساسة مالية أو غيرها من حساسية المعلومات الشخصية، "وقد يكون الغرض منها هو تثبيت برامج تجسس بشكل سري أو أي برامج أخرى خبيثة، أو دخول الأشخاص الغير مخول لهم إلى نظام الكمبيوتر.

وفي الغالب نجد أن المهندسين الاجتماعيين (المهاجمين) لا يملكون أي مهارات تقنية وإنما يستغلون الجانب البشري لأنه أضعف جزء في أمن الشركة أو المنظمة حيث يستخدمون مهارات التعامل مع البشر لاستدراجهم وسؤالهم ويعتمدون على خداعهم ،وكثيرا ما نسمع في حياتنا اليومية عن مصطلح المهندس الاجتماعي وقد يتبادر إلى الأذهان أنه الشخص المصلح ، بينما هو في الحقيقة عكس ذلك ، فهو الشخص المهاجم الذي يهاجم من أجل الحصول على المعلومات الشخصية ، أو من أجل اختراق أنظمة الشركات أو القطاعات الحكومية.

وقد بدأت الهندسة الاجتماعية مع أكبر مهاجم وهو كيفين ميتنيك، الذي يعد من أبرع من استخدم أساليب الهندسة الاجتماعية والذي صرح في مقابلة معه أن 50% من الاختراقات التي يقوم بها كانت بسبب تمكنه من

الحصول على معلومات سرية وخطيرة من المسؤولين في المراكز الحساسة ، ومن هذا الاعتراف نستنتج أن استغلال الجانب البشري هو من أنجح الأساليب والطرق المستخدمة من قبل المهندسين لتحقيق هدفهم وذلك " عن طريق انتحال شخصية موظف مصرح له، و عادة ما يستخدم منتحل الشخصية(الهاكرز) الهاتف أو البريد الالكتروني كأدوات لهذا الهجوم ولكن الهندسة الاجتماعية لا تقتصر فقط على المكالمات الهاتفية ورسائل البريد الالكتروني وإنما هناك عدة طرق لتنفيذ هذه الهجمات.

وفي آخر الإحصائيات التي تم إجراؤها في سنة 2006 من معهد للحاسبات في الولايات المتحدة الأمريكية " اتضح أن بنسبة 90% من 503 شركات أظهروا تقارير للاختراق المعلومات، ومن هذا الإحصاء يتضح انه لا بد من الحذر من الهاكرز (منتحل الشخصية) فهو غالباً ما سيبدو باحترام وذي أخلاق رفيعة ويزيد من واقعية الانتحال يقدم هو معلومات صحيحة للموظف (الضحية) كاسم مدير القسم أو أسماء موظفين يعملون في نفس الشركة فلا بد استخدام طرق للحماية ضد هذه الهجمات من خلال وضع سياسات أمنية للشركة وتدريب موظفيها وتنقيفهم وزيادة الوعي عندهم ، واستخدام الحلول والطرق التقنية كذلك ، الكلمات المفتاحية ، الهندسة الاجتماعية ، انتحال الشخصية ، المهاجمين (المهندسين الاجتماعيين) ، سرقة المعلومات السرية. نظرا لخطورة الهندسة الاجتماعية وانتشارها فإنه في هذا المقال سوف نوضح مفهوم الهندسة الاجتماعية، والهدف منها، وأنواعها، وسوف نبين الوسائل المستخدمة في كل نوع، وطرق الحماية منها

3-7-3 الهدف من الهندسة الاجتماعية

نستنتج من التعريف السابق، أن هدف المهندسين الاجتماعيين (المهاجمين) هو خداع الأشخاص للحصول على المعلومات السرية كما سبق ذكره، أو للدخول الغير شرعي للأنظمة واختراقها أو تدميرها.

3-7-3 أنواع الهندسة الاجتماعية

يمكن أن تصنف الهندسة الاجتماعية إلى نوعين

النوع الأول: يعتمد على الجانب البشري وهو الغالب والأكثر شيوعاً ، حيث يتفاعل المهاجم مع الأشخاص للحصول على المعلومات المطلوبة.

النوع الثاني: يعتمد على تقنية الكمبيوتر، حيث يستخدم المهاجم برامج من خلالها يسترجع المعلومات المطلوبة

3-3-7-3 الوسائل المستخدمة في الهندسة الاجتماعية

في النوع الأول هناك عدة وسائل والتي سوف أقوم بشرحها في الأسطر التالية، حيث يستخدمها المهاجم للكشف عن المعلومات السرية التي لا تتحصر في كلمة السر فقط و إنما تتعداها إلى المعلومات الحساسة الخاصة بالشركة فعلى سبيل المثال خطط عمل الشركة أو خطط التسويق المستقبلية ومن أشهر هذه الوسائل التالي:-

1.الهجوم المباشر

حيث أن المهاجم يسأل الضحية مباشرة ليكمل له المهمة(مثلاً، مكالمة السكرتارية و سؤالها عن اسم المستخدم و كلمة السر) و لأن هذه الطريقة هي أسهل طريقة و أكثرها مباشرة فهي نادراً ما تنجح، و إن كان الضحية ذا حس أمني فسوف يسارع بتغيير بياناته.

3. الانتحال

انتحال شخصيات مثل عميل أو مراجع أو موظف تقني للحصول على الأرقام السرية أو أي معلومات تساعد على اختراق النظام عن طريق الموظف نفسه وبشكل مباشر دون استخدام أي تقنيات الكترونية، فهم يقومون باستخدام مهارات الهندسة الاجتماعية للحصول على اسم المستخدم، أو اسم النظام، أو الرقم السري أو طلب كتابة أوامر تساهم في فتح ثغرات في النظام أو تُعطي صلاحيات خاصة. مثال على ذلك، أن يتم الاتصال الهاتفي بالموظف أو مقابلته في مقر عمله على أن هناك مشكلة تحتاج إلى إصلاح أو أمر طارئ يستدعي الدخول على النظام مع إيهام الموظف انه إن لم يقدم المساعدة فإن المدير سيغضب منه، وقد يتم ذلك عن طريق عرض المساعدة في تركيب برامج أو ضبط إعدادات الحاسب الآلي أو قد يدعي احدهم بأنه موظف جديد ويحتاج لمساعدة مستغلين بذلك الزمالة الوظيفية وحسن النية وحب مساعدة الآخرين، وبالتالي تتم عملية الاختراق والحصول على معلومات قد تستخدم في عمليات إرهابية أو تتعرض لأسرار أمنية أو مالية للشركات وللأجهزة الحكومية والأهلية.

3. البحث في سلة المهملات

حيث يقوم المهاجم بالبحث في صناديق القمامة عن قوائم لكلمات السر التي تم رميها مسبقاً، أو عن أي معلومات تخص الطابعات، أو تخص دليل المستخدم لأي نظام، ومن ثم يستخدمها كوسيلة في هجماته.

4. النظر من خلف مستخدمي الكمبيوتر وهم يضعون كلماتهم السرية Shoulder surfing

وهي طريقه يستخدمها المهاجم لرؤية الشخص عند كتابته للرموز السرية إما أن يختلس النظر أو أن يكسب ثقة الشخص بحيث لا يمانع وجوده في نفس المكان وبذلك يستطيع أن يضمن رؤيته للرموز عند ضغطها على الحاسوب أو كتابتها .

في النوع الثاني ومع تطور التكنولوجيا نجد أن المهاجمين دمجوا التكنولوجيا في مخططاتهم، لشن هجمات أكثر إبداعا، وتطورا، وتدميرا، ومن أشهر التقنيات المستخدمة:

1.التصيد Phishing

في أمن المعلومات ، يعرف التصيد على انه عملية احتيالية " لمحاولة الحصول على معلومات حساسة مثل أسماء المستخدمين ، كلمات السر وتفاصيل بطاقات الائتمان عن طريق التكر ككيان موثوق فيه في الاتصالات الالكترونية التي قد تكون من خلال البريد الالكتروني أو مواقع الشبكات الاجتماعية ، أو مواقع الدردشة التي يتساهل فيها المستخدم بنشر معلوماته الشخصية متجاهلا خطورتها، الاحتيال عن طريق رسائل البريد الالكتروني و المواقع على شبكة الانترنت ومن ضمنها،البريد الالكتروني يوفر الفرص العظيمة للمهاجم فعلى سبيل المثال ، قد يتلقى الشخص رسالة في بريده الإلكتروني التي تبدو أنها آتية من مصدر موثوق فيه ، كالبانك الخاص به أو غيرها من المؤسسات المالية التي تطلب منه تحديث معلومات حسابه، و في هذه الرسالة ، يوضع رابط مزيف أو وهمي على الشبكة العنكبوتية و الذي يظهر كأنه رابط حقيقي للموقع الالكتروني الخاص بالبنك أو المؤسسة ، فإذا قام الشخص بإدخال اسم المستخدم وكلمة السر الخاصة به وغيرها من معلوماته الشخصية فإن المهاجم يتمكن من سرقة هذه المعلومات لينتحل شخصية هذا الشخص بدون علمه.

والتصيد عن طريق رسائل البريد الإلكتروني غالبا ما يتضمن أخطاء إملائية، وسوء استخدام قواعد اللغة، والتهديدات، والمبالغات ، وفي رسائل البريد الإلكتروني قد يرفق المهاجم ملفات فيها فيروسات " ومن أشهر

الفيروسات هي ، ' I LoveYou ' Anna Kournikova

2. النوافذ المنبثقة

وهي النوافذ التي تظهر على الشاشة وتختبر المستخدم بأنه قد فقد اتصاله بالشبكة، ويحتاج إعادة إدخال اسم المستخدم وكلمة السر الخاصة به، لكن توجد برامج مخفية تقوم بجمع المعلومات الخاصة بالمستخدم وإرسالها إلى البريد الإلكتروني الخاص بالمهاجم.

3-7-3-4 طرق الحماية من الهندسة الاجتماعية

تعد الهندسة الاجتماعية من الثغرات الأمنية التي يصعب منعها وحصرها، لأنها تعتمد و بشكل كبير على طبيعة البشر. لذا نلاحظ أن هناك الكثير من هذه الهجمات يمكن صدها إذا كان الناس يدركون بما يحيط بهم.

وفيما يلي قائمة من التوصيات حول كيفية منع هذه الهجمات وطرق للحماية منها:-

1.السياسة الأمنية:

يجب إنشاء سياسة أمنية قوية للشركة ووضع تعليمات للموظفين و قد تكون بشكل أوامر تصدر من إدارة الشركة، أو تكون في شكل عقد يوثق من قبل الطرفين (الشركة والموظف) وتكون هناك عقوبات صارمة للموظفين عند التخلف عن إتباع هذه السياسة إذ تتكون السياسة الأمنية من النقاط التالية:-

- ما الذي يجب عمله عندما تتكشف كلمة السر

- من هم الأشخاص المخول لهم بالدخول إلى أماكن العمل

- ماذا تفعل عندما ترد عليك أسئلة من موظف آخر للكشف عن المعلومات المحمية

- يجب التحقق من هوية أي شخص يطلب معلومات عن جهازك أو حسابك أو معلوماتك

الشخصية أو أي معلومات عن حساب لموظف آخر وذلك بالاتصال بهيئة التحقق من خصائص الهوية.

- لا تقم بإتباع تعليمات غريبة أو مريبة تتعلق بالأجهزة الإلكترونية وكذلك لابد من التحقق من هوية

الشخص المصدر لهذه التعليمات والأوامر وأحقيته في إصدارها حتى لو ادعى أن الأمر طارئ. لا تشارك

بالاستبيانات الهاتفية حتى لو كانت من داخل الجهاز نفسه لأنه قد تستغل لدس أسئلة بين الاستبيان للحصول

على معلومات تساعد على الاختراق.

-تحميل برنامج مكافحة الفيروسات، وتجديده ما بين كل فترة وأخرى.

-التخلص من الأوراق فور الانتهاء منها باستخدام آلة تقطيع الورق ويفضل استخدام النوع الذي

يقطع الورق بشكل عامودي وأفقي

و يفضل أن تكون هذه السياسة متضمنة خطة الحفاظ على استمرارية العمل أثناء وبعد حصول الهجمة.

2. التدريب:

يعد تدريب الموظفين من العوامل المهمة لمنع هذه الهجمات ، ويتم تعليمهم عن السياسة المتبعة في الشركة

وتدريبهم بإقامة دورات تثقيفية يشرح لهم فيها ماهية الهندسة الاجتماعية و الهدف المنشود وراءها وكيفية

التصدي لها ويفضل أن يكون تدريبهم بشكل مرح وشامل لجميع النواحي ، ويفضل أن تكون هذه الدورات ما

بين كل فترة وأخرى كأن تكون من أربع إلى ستة أشهر ، ولا بد في هذا التدريب أن نركز على التقنيات التي يستخدمها المهاجم والأثر المترتب على الأفراد من جراء حصول مثل هذه الهجمات.

ومن الممكن منح مكافآت للموظفين الذين يقبضون على من يحاول بالهجوم، وتختلف هذه المكافآت على حسب الشركة فقد تكون شهادة تقدير أو مال نقدي أو إجازة لمدة يوم.

3. الوعي بأمن المعلومات:

كثير من الشركات والأفراد يكون جل اهتمامهم بالهاكرز ويركزن على الجانب التقني فقط و يغفلون الجوانب الأخرى وينسون كذلك أن الهندسة الاجتماعية هي احد أنواع الهجمات لذا يجب على الشركة توعية الناس بكل أنواع الهجمات وتوضيح لهم كيفية تقليل خطر التعرض للهجوم من جميع الجهات.

4-1 أساسيات ثغرات الفيض Buffer Overflow

تتبع أهمية ثغرات البوفر اوفر فلو ان اي برنامج او اي ادارة مستخدمة يتم برمجتها من خلال لغة برمجية ما ويقوم المبرمج بتجميع اكواد هذه الأداة ليحصل في النهاية على برنامج او اداة . ان اغلب المبرمجين يهتمون في بداية عملهم البرمجي ،هي الحصول على النتيجة المطلوبة دون ادنى اهتمام بنسبة الأمان الذي يجب ان يكون متوفر في هذا البرنامج او الأداة الي جانب النتيجة المطلوبة ،فعند برمجة برنامج يقوم بتشغيل ملفات الصوت مثلا اهم ما يتوجه اليه المبرمج ان يعمل هذا المشروع البرمجي وان يقوم هذا البرنامج فعلا بتشغيل الصوتيات دون الاهتمام بالجانب الامني المهم جدا ،وهذا الجانب هو الذي يضمن استمرارية استخدام هذا البرنامج ان ثغرات الفيض تهتم بهذا الجانب الامني . فهية تبحث عن الخطأ الذي وقع فيه المبرمج خلال برمجته للبرنامج او اي نقص برمجي . ليتم بعد ذلك استغلال هذا الخطأ والتحكم في الذاكرة ،ان التعامل مع امثال هذه الثغرات تحتاج لخبرة لا بأس بها في لغات برمجة ومن اهمها لغة التجميع (اسمبلي) .

كما يعتبر البوفر هو المكان الذي يتم فيه تجميع وتخزين البيانات المؤقت ،واوفر فلو هو الفيض الذي يحدث بأن تحمل شئ ما اكثر من ما هو مسموح له . ملئ كاس من الماء اكثر من قدرته استيعابه .

ماهي المسجلات Registers : سجلات يتم استخدامها لتنفيذ عملية التحكم والسيطرة ويتم استخدامها من قبل البروسيوسور .

المؤشر EBP : هو المؤشر المسؤول عن استدعاء او طلب دالة معينة يتم الضغط عليها الى العودة وتشير الى اعلى المكس .

نقطة الضعف points Vulnerability : هو الخلل البرمجي الذي يسمح للمخترق بتنفيذ اشياء ضارة .

المنقح العام GDB : يتم استخدامه لمتابعة البرامج ومعرفة الملفات الموجودة بداخلها .

الكومة Stack : تحدث الكومة مع البرامج التي تمنح حجم ذاكرة محدد في الاستخدام فعند حدوث الكومة يقوم البرنامج باستخدام ذاكرة اكبر من ما هو مخصص له .

ويستخدم الستيك ايضا في عملية Program Crash . وهية فيض في عملية جلب واستدعاء الدوال .

المساحة Heap : هية المساحة المخصصة للبرنامج .

عنوان العودة Returning Address : وهو امر يستخدم داخل البرنامج ليتم الرجوع بعد ذلك لنقطة الادخال

تعتبر هذه مقدمة في الاساسيات وليست كل الأساسيات في ثغرات البوفر اوفر فلو . وهية بداية لسلسلة دروس سنتحدث بها عن هذا النوع من الثغرات .

4-2 الطرق البرمجية لإقفال الثغرات

4-2-1 معرف الخدمة

يعتبر معرف الخدمة (Identifier Set Service) من الدوات الأساسية حيث ان كل اتصال تملك معرف يكون عبارة عن كلمة او رقم او خليط بين حروف وارقام. يقوم هذا المعرف بالتعريف عن نقطة الاتصال ولفرض ان نقطة اتصال معينة تملك SSID معين على سبيل المثال هو "ميّار"، ان اي شخص موجود في مدى التغطية التي تغطيها نقطة الاتصال هذه (المدى يعتمد على امور عديدة قد تصل الى كيلو مترات، سواء كان في نفس البيت او المبنى او كان في الشارع المجاور للبيت) يستطيع ان يدخل الى الشبكة الخاصة بنقطة الاتصال ذات المعرف "ميّار" اذا عرف ان كلمة "ميّار" هي SSID الخاص بها. أغلب نقاط الاتصال تحمل

اعدادات افتراضية و يكون المعرف لها معروفاً و في الغالب يكون كلمة (default). اذا لم يتم تغيير هذا المعرف الى اي شي آخر، فان اي شخص يقع في ضمن مدى نقطة الاتصال يستطيع الدخول للشبكة الخاصة بها بدون عوائق.

من الامور الموجودة في الاعدادات الافتراضية الخاصة بال SSID هو ال Broadcasting SSID. تقوم نقاط الاتصال بالتعريف عن نفسها بشكل مستمر على مدى التغطية التي تغطيه، فتقوم بصورة مستمرة بارسال اشارات تقوم بالتعريف عن نفسها و بمعرفها الخاص. بهذه الطريقة يمكن لاي شخص يملك جهاز خاص، او كمبيوتر محمول به كرت شبكة لاسلكية ان يتجه الى المنطقة التي تغطيها نقطة الاتصال فيحصل بشكل تلقائي على الاشارة مع رقم المعرف، فيعرف انه الان يمكنه الاتصال بشبكة نقطة الاتصال (الموسوعة) من موقعه. يجب تعطيل هذه الخاصية التي تأتي بصورة افتراضية في العادة حتى لا يتمكن ضعاف النفوس من الذين يملكون اجهزة محمولة ذات كروت شبكة لاسلكية من الاقتراب و معرفة الاماكن (القريبة) من المنزل او المبنى و التي من خلالها يستطيعون الدخول على الشبكة اللاسلكية. يفضل قدر الامكان تغيير المعرف بصورة مستمرة بين حين و آخر، حتى ان حصل احد الذين يحاولون اختراق الشبكة على المعرف الخاص بنقطة الاتصال في وقت معين، فانه عند تغييره بصورة مستمرة ستصعب مهمته اكثر.

من الممكن ايضا تقليل نسبة الارسال لدة نقطة الاتصال بحيث ان يكون مداها قدر الامكان على المحدود المطلوبة و المسموح بها لا ان تتخطى هذه الحدود و تغطي مساحات خارج نطاق المنزل او الشركة و التي قد يستغلها البعض في الدخول للشبكة الخاصة، نستطيع تمثيل مسألة خروج مدى التغطية عن حدود المؤسسة او المنزل الى مسافات لا داعي لها، كوصول المدى الى الشارع المجاور ، بتوزيع اسلاك و كيبيلات خاصة

بالشبكة الداخلية، ماعلى الناس الا ان يحضروا اجهزتهم و يوصلون كروت الشبكة بالكييلات و الاسلاك و يدخلون على الشبكة الداخلية وهم جالسون في الشارع المجاور.

من أكثر الجهات التي ينصب اهتمام المهاجمين على الاستيلاء على اجهزتها ، هي الشركات الكبيرة و الجامعات و الكليات التي تحمل عدد كبير من اجهزة الحاسب المتصلة بالانترنت بشكل متواصل و ان لم يتخذ المسؤولين عن هذه الشبكات الحذر من امور عديدة، فان نسبة تعرض اجهزة شبكتهم للاشتراك في هجوم امر وارد، و بما ان اغلب الشركات و الجامعات بدأت بالتوجه الى استعمال الشبكات اللاسلكية، فان نسبة الخطر في ضلوع اجهزتها بطبيعة الحال ترتفع لاسباب عديدة اولها ان الاجهزة لن تكون في العادة موجودة في مكان ثابت، بل تتحرك و ربما تخرج من مبنى الشركة نفسها لذا وجب الحذر من اتخاذ كافة الوسائل الممكنة من جعل الشبكة اللاسلكية آمنة قدر المستطاع.

ان الاجهزة المحمولة التي تملك كرت شبكة لاسلكي موصل بمقوي للارسال، بإمكانها ان تشارك في نقل الملفات و التعامل كما لو كانت في مبنى الجامعة او الشركة او الكلية و في الحقيقة من الممكن ان تبعد كيلومترات عنها! و اذا كانت نقاط الاتصال الموجودة في المؤسسة او الجامعة لم يتم تضبيط اعداداتها بطريقة سليمة،و لم يتم تعديل الاعدادات الافتراضية المعروفة لدى كل باحث، فان اي شخص على بعد أميال (باستخدام مقوي للارسال)يستطيع الدخول بكل سهولة على الشبكة.

ان أغلب الامور التي من الممكن ان يتم استغلالها هي الاعدادات الافتراضية لنقاط الاتصال Access Points، و في ما يلي بعض الامور التي ستساعد في تقليل مخاطر الاعدادات الافتراضية:

1. ترشيح العنوان الفيزيائي للشبكة MAC Address

كل كرت شبكة في العالم يحمل رقم يميزه عن غيره، تقوم الشركات المنتجة بوضع ارقام خاصة على اساس النظام السداسي العشري لتميز كروت الشبكة عن بعضها و من المفترض ان لا تكون هذه الارقام مكررة ابدأً. بطبيعة الحال نقطة الاتصال تعتبر من الطبقة الثانية في نمزج النظم المفتوحة (OSI Model) او Open System Interconnect يعني في طبقة ربط البيانات (Data Link) كالسويتشات فان تعاملها يكون مع ال MAC Address وليس مع IP Address. و هنا يستطيع المسؤول عن الشبكة اللاسلكية ان يحدد الاجهزة التي يسمح لها باستخدام نقطة الاتصال الخاصة به.

كما نعرف فان كل جهاز حتى يتصل بالشبكة اللاسلكية يجب ان يحتوي على كرت شبكة لاسلكية، و كل كرت شبكة لاسلكية تملك رقم خاص مميز وهو MAC Address و من المفترض ان المسؤول عن الشبكة يعي و يعلم عدد الاجهزة الموجودة لديه او لدى شركته و التي يريد ان تستخدم شبكته اللاسلكية. عندها يستطيع ترشيح استخدام نقط الاتصال لديه و يحدد الاجهزة بواسطة اضافة ارقام العناوين الفيزيائية الخاصة بها في قائمة الاجهزة المسموح لها باستخدام الشبكة او استخدام نقط الاتصال و لا يسمح بغير هذه الاجهزة مهما كانت باستخدام نقاط الاتصال الخاصة بشكيبته.

2. تشفير البيانات باستخدام WEP

أغلب نقط الاتصال تملك امكانية التعامل مع البيانات المشفرة. باستخدام تقنية WEP او Wired Equivalent Privacy فانه و تفعيلها في نقطة الاتصال، يمكن تشفير استلام و تمرير البيانات المشفرة فقط. لذا يجب على كل مستخدم يريد استخدام الشبكة اللاسلكية ان يفعل خاصية WEP اي التشفير في جهازه، كي

يتم تبادل البيانات بصورة مشفرة تصعب في معظم الاحيان معرفة محتواها ان تم نسخ هذه البيانات اثناء مرورها بين الاجهزة.

و كخط دفاع ثاني، عند استخدام ميزة التشفير، يجب تبادل مفتاح التشفير المسمى WEP Key فهو عبارة عن ارقام على اساس النظام السداسي العشري ، تحدد درجة التشفير ، و كلما زاد حجم الرقم زادت صعوبة كسر التشفير و ايضا زادت المدة التي يتم نقل البيانات بعد تشفيرها و استلامها و من ثم فك تشفيرها، كما يعتبر المفتاح خط دفاع ثاني لانه يجب على الاطراف المستخدمة للشبكة معرفة هذا المفتاح كي يتم تشفير البيانات على اساسه، و يفضل تغييره بين فترة و اخرى حتى ان وقع في يد احد المتطفلين فانه لن يستخدمه لفترة طويلة.

3. الكلمة السرية الافتراضية (Default Password)

دائماً ما تأتي نقط الاتصال من الشركات المنتجة لها بكلمة سرية معينة موحدة و معروفة، يجدها المستخدم في الدليل الخاص بنقاط الولوج (Access Point)، و في بعض الاحيان تكون الكلمة السرية خالية ، يعني ان عند تسجيل الدخول لنقطة الاتصال لتغيير الاعدادات، يكون اسم المستخدم هو مثلا admin و الكلمة السرية غير موجودة من الواضح انه يجب تغييرها الى كلمة سرية صعبة مكونة من ارقام و حروف .هذه هي الاعدادات الافتراضية التي وجدت لتسهل العملية على المستخدمين لكن ان بقيت هكذا فانها قد تؤدي لى مصائب كبيرة، يمكن تفاديها بسهولة باتباع التعليمات و النصائح.

4. تأمين بروتوكول الأنترنت IPsec

كما نعرف انه بلا اخذ الامن بعين الاعتبار ، فان الشبكة والبيانات التي تمر فيها يمكن ان تتعرض للعديد من

انواع الهجمات المختلفة ، بعض الهجمات تكون غير فعالة Passive مثل مراقبة الشبكة Network Monitoring ، ومنها ما هو الفعال Active مما يعني انها يمكن ان تتغير البيانات او تسرق في طريقها عبر كوابل الشبكة. وفي هذا الدرس سوف نستعرض بعض انواع الهجمات على الشبكات، وكيفية منع IPSec حدوثها او كيفية الوقايه منها عن طريق IPSec نستخدم التالي:-

1. التقاط حزم البيانات Eavesdropping sniffing snooping

حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكة بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ، ويعالجها IPSec عن طريق تشفير حزمة البيانات، عندها حتى لو التقطت الحزمة فانه الفاعل لن يستطيع قراءتها او العبث بها، لان الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل(بالاضافه الى الطرف المرسل) .

2. تعديل البيانات Data modification

حيث يتم بذلك سرقة حزم البيانات عن الشبكة ثم تعديلها واعادة ارسالها الى المستقبل، ويقوم IPSec بمنع ذلك عن طريق استخدام الهاش (Hash) وهي من طرق التشفير الكتلي المعروفة ووضعها مع البيانات ثم تشفيرها معا ، وعندما تصل الحزمة الى الطرف المستقبل فان الجهاز يفحص Checksum التابع للحزمة اذا تمت مطابقته ام لا، فاذا تمت المطابقة مع الهاش الاصلي المشفير تبين ان الحزمة لم تعدل، لكن اذا تغير الهاش نعرف عندها ان حزمة البيانات قد تم تغييرها على الطريق.

3. انتحال الشخصية spoofing Identity

بحيث يتم استخدام حزم البيانات على الشبكة والتقاطها وتعديلها لتبين هويه مزوره للمرسل، اي خداع المستقبل بهوية المرسل، ويمنع ذلك عن طريق ثلاثة طرق والتي يستخدمها IPSec وهي:

1. بروتوكول الكيربيرس Kerberos Protocol

2. الشهادات الالكترونيه Certificates Digital

3. مشاركة مفتاح معين Preshared key

حيث لا تتم عملية بدأ المحادثه وارسال البيانات قبل التأكد من صحة الطرف الثاني عن طريق احدى الطرق المذكوره أعلاه.

4. رفض الخدمه او حجبتها Denial of Service

حيث تعمل هذه الهجمه على تعطيل خدمه من خدمات الشبكه للمستخدمين والمستفيدين منها ، مثلا كإشغال جهاز الخدمة الرئيسي (server) في الشبكه بعمل إغراق عن طريق الرسائل (flood) مما يشغله بالرد على هذه الامور وعدم الاستجابه للمستخدمين. ويعمل IPsec على منع ذلك عن طريق امكانيه غلق او وضع قواعد للمنافذ المفتوحه Ports .

5. الطرف الثالث Man in The Middle

من اشهر الهجمات في الشبكات، وهي ان يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسله من طرف لآخر وامكانية العمل على تعديلها او العمل على عدم ايصالها للجانب الاخر، ويعمل IPsec على منعه عن طريق طرق التحقق من الموثوقيه Authentication methods.

6. سرقة مفتاح التشفير Key interception

حيث يتم سرقة المفتاح المستخدم للتشفير او التعرف عليه عن طريق برامج كسر التشفير اذا لم يكن بالقوه المطلوبه، هنا لا دور IPsec بها ، ولكن الدور لنظام التشغيل لانه يقوم بتغيير المفاتيح المستخدمه للتشفير بشكل دوري ودائم مما يقلل من خطورة كشفه او سرقاته.

7. الهجمات على طبقة التطبيقات Application Layer Attacks

حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في اجهزة الشبكة وايضا تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الامثله عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الانظمه او البرامج او حتى اخطاء المستخدمين. يعمل IPsec على حمايه من ذلك بكونه يعمل على طبقة IP Layer فيعمل على اسقاط اي حزمة بيانات لا تتطابق والشروط الموضوعه لذلك ، لذا فتعمل الفلاتر على اسقاطها وعدم اوصولها للانظمه او البرامج.

بشكل عام إن IPsec يحمي من معظم الهجمات عن طريق استخدامه ميكانيكية التشفير المعقده ، حيث يوفر التشفير الحماية للبيانات والمعلومات ايا كانت اثناء انتقالها على الوسط (ايأ كان) عن طريق عمليتي التشفير Encryption والهاش Hashing .

طريقة التشفير المستخدمه في IPsec عباره عن دمج لعدة خوارزميات ومفاتيح حيث ،الخوارزمية عباره عن العملية الحسابيه التي تمر فيها البيانات لكي تشفر،المفتاح وهو عباره عن رقم(شفره) سرية يتم من خلالها قراءه او تعديل او حذف او التحكم في البيانات المشفره بشرط مطابقتها للزوج الثاني الذي قام بعملية التشفير.

يستخدم IPsec عن طريق ما يعرف بالسياسات Policies IPsec والتي تطبق في الشبكة ، حيث ان كل مجموعة من القواعد التي تريد تطبيقها تشكل لنا سياسه، والIPsec يستخدم هذه النظرية ، الامر الذي يجب الانتباه له هو اننا لا نستطيع عمل اكثر من سياسة لكل جهاز كمبيوتر ، لذلك يجب عليك تجميع كل القواعد والامور التي ترغب في تطبيقها في سياسه واحده تطبق على مستوى الاجهزه لا على مستوى الافراد . قبل القيام بوضع القواعد وتطبيق السياسه ، يجب علينا مراعاة مايلي:

1. نوع الحركه Type of traffic

حيث انك تقوم باستخدام المرشحات لتحديد نوعية الحركة التي تريد أن تطبق عليها هذه القواعد ، فمثلا تستطيع ان تطبق مرشح يعمل على مراقبة بروتوكول HTTP و FTP فقط دون الباقي. بعد ذلك يجب ان تقوم بتحديد IPsec ماذا سيفعل بعد تطابق الحركة مع المرشح ، وهو ما يسمى Filter Action والذي تستخدمه لتخبر السياسة Policy ماذا ستفعل اذا تم مطابقة الحركة حسب المرشح، فمثلا يمكنك ان تجعل IPsec يقوم بمنع الحركة على بورت بروتوكول نقل الملفات FTP ، وايضا تجعله يعمل على تشفير الحركة على بورت بروتوكول HTTP . وايضا تستطيع من خلال Filter Action بتحديد اي انظمة التشفير والهاش التي تريد ان تستخدمها Encryption and Hashing Algorithms يجب على السياسة ان تستخدم، طريقة التحقق من الموثوقية Authentication Method .

2. استخدام احدى نظامي IPsec وهما Tunnel or Transport mode

1. نوع الاتصال او الشبكة التي سيتم تطبيق السياسة عليها What connection type the rule applies

to ، حيث ان السياسة يمكن ان تحدد IPsec في نطاق الشبكة المحليه LAN ، او ان يعمل على اساس الوصول من بعد Remote access او ما يعرف بWAN ، او الاثنين معا.

8. انواع السياسة في نظامي التشغيل Win2000 & 2003 ، حيث توجد ثلاثه انواع ، وكل واحد من هذه الأنواع تحتوي على اعدادت خاصه تناسب الغرض التي ستطبق لاجله، و في الشركات الصغيره او المتوسطه ، لكن كلما كبر حجم الشركه وزادت التعقيدات زادت الحاجه الى استخدام سياسه مبتكره من قبل الشركه .

1. Client Respond only

افضل ما تطبق هذه السياسة على Domain Group security policy وذلك لكي تضمن لنا امكانية رد المستخدم على طلبات الاجهزه الاخرى باجراء تشفير عن طريق IPsec ، اذا تعتبر هذه السياسة اساسيه في

اي شبكه سيعمل فيها ولو سيرفر واحد على IPsec ، حيث في هذه السياسه لن يقوم المستخدم بارسال طلب المحادثه والتشفير عن طريق IPsec وانما سيقوم بالاجابه والدخول في الطلبات التي يتسقبلها لذلك من الاجهزه الاخرى في مجال IKE ، اذا كنت تفكر في تطبيق IPsec على اي جزء من اجزاء الشبكه فالاجهزه بعد ذلك ان يتم تطبيق هذه السياسه على مستوى المجال (Domain).

2.Server Request Security

تطبق هذه السياسه في العاده على السيرفرات التي ستتحدث مع اجهزة Win2000 او حتى اجهزة Nonwin2000 مثل Unix وغيره ، في هذه الحاله ، اذا كان المستخدم يستطيع التعامل مع IPsec فان جميع المحادثات بينهما ستكون مشفرة فيه ، اما اذا لم يملك المستخدم القدره على استخدام IPsec فانه يستعامل مع السيرفر بطرق المحادثه والاتصال العاديه، تطبق هذه السياسه في حالة وجود خليط من الاجهزه في الشبكه حيث يكون بعضها يستخدم IPsec والبعض الاخر لا ، فتكون هذه هي الانسب لذلك.

3.Secure Server Require Security

تضمن هذه السياسه للمخدرات عدم التكلم وسقوط جميع انواع المحادثه والاتصال مع الاجهزه التي لا تستخدم او لا تدعم IPsec ، حتى لو كانت هذه الشبكه او هذا الجهاز موجوده في المجالات الموثوقه. وافضل ما تستخدم هذه السياسه اذا دعت الحاجه الى تشفير كل شيء يصدر عن مخدم محدد كمخدمات البنوك وغيره، وبسبب تشدد هذه السياسه فانه يجب علينا في بعض الاحيان وضع اعفاءات واستثناءات من استخدام IPsec كما يحصل في بروتوكول Simple Network Management Protocol_SNMP .

9.إستخدام تقنية الطبقات الأمانة (SSL) Secure Socket Layer

تقوم هذه الطريقة على قيام اتصال امن مشفر Encrypted ضمن تعقيدات متفاوتة فمنها Bit40 ومنها bit128 ، فتم استخدام SSL لتشفير وحماية قنوات الاتصال التي تنتقل عبرها البيانات مثل SMTP او Database communications ، وتم استخدام ما يعرف بـ SSL over HTTP في المواقع التجاربه ومواقع البريد الالكتروني فاصبحت تسمى HTTPS و Secure Hyper Text Transfer Protocol واستخدم منفذ 443 بدلا من المنفذ 80 الخاص ببروتوكول النصوص التشعبية (HTTP) ، وانتشر واشتهر بشكل كبير .

ثم ظهرت تقنيه مشابه له ولاستخدامه وهي TLS : Transport Layer Security وهي تقنيه محسنه من بروتوكول الطبقات الأمانة ولكنهما يختلفان في طريقة اداء العمليه ، والطريقتان تحتاجان للشهادات الالكترونيه Certificates ، وظهرت تقنيه اخرى داخل الشبكه نفسها وليس على شبكه عالميه كالانترنت ، وهي SMB Signing ، الجميع يعلم ان Server Message Block : SMB هي ال packets الي يتم ارسالها بين الخادم والاجهزه في عملية المشاركه في الملفات وغيره ، وللحمايه من طريقة سرقة المعلومات اثناء مرورها في الاسلاك Man In The Middle وهذه الطريقه تدعى يتم بواسطتها اضافة ال Hash (وهي طريقة يتم من خلالها استخلاص رمز معين حسب حسابات رياضيه من الرساله ، ومن الامثله عليه SHA-1 , MD5 , MD4) ويتم تشفير هذا الهاش و اضافته للرساله وبذلك نحافظ على صحة وتكاملية الرساله .

لكن ظهرت المشكله الكبرى بكون جميع هذه الوسائل تعمل على طبقة التطبيقات في نمونم المفتوحة (OSI) لأن وظائفها محدده جدا ، لا تستطيع تشفير الا ما بنيت لاجله ، ، لذلك كان لا بد من ابتكار طريقة

تمكننا من تشفير كل الحزم التي تصدر من اي جهاز ، فتم ابتكار تقنيه تأمين بروتوكول الانترنت التي تم ذكرها أنفاً والتي تقوم بتشفير كل شيء يصدر عن الجهاز ترسله على الشبكة .

3-4 المعدات المستخدمة في اقفال الثغرات

في مقدمة هذا الفصل تم الحديث عن الطرق البرمجية للوقاية وسد الثغرات الأمنية في الشبكات اللاسلكية فيما يلي نستعرض بعض الأجهزة المستخدمة لهذا الغرض.

1-3-4 الجدار الناري Fire Wall

يعمل جدار الحماية أو الحائط الناري كجهاز عزل وترشيح يفصل ما بين الشبكة الداخلية للمؤسسات والشبكات الخارجية مثل شبكة الإنترنت ، وظيفة جدار الحماية الأساسية هي تنظيم بعض تدفق أزمنة الشبكة بين شبكات الحاسوب المكونة من مناطق ثقة المتعددة. ومن الأمثلة على هذا النوع الإنترنت و التي تعتبر منطقة غير موثوق بها وأيضا شبكة داخلية ذات ثقة أعلى، ومنطقة ذات مستوى ثقة متوسطة، متمركزة بين الإنترنت والشبكة الداخلية الموثوق بها، تدعى عادة بالمنطقة منزوعة السلاح.

والوظيفة الأخرى لجدار الحماية هي الحماية من داخل الشبكة هو مشابه إلى أبواب الحريق في تركيب المباني بحيث في الحالة الأولى يستعمل في منع اختراق الشبكات الخاصة، وفي الحالة الثانية يفترض به أن يحتوي ويؤخر حريق الموجود في بناء معين من الانتقال إلى بناء آخر، من دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة، فممارسات الأمان المعيارية تحكم بما يسمى بمجموعة قوانين "المنع أولاً"

جدار الحماية، الذي من خلاله يسمح بمرور وصلات الشبكة المسموح بها بشكل تخصيصي فحسب. ولسوء الحظ، فإن إعداد مثل هذا يستلزم فهم مفصل لتطبيقات الشبكة ونقاط النهاية اللازمة للعمل اليومي للمنظمات. العديد من أماكن العمل ينقصهم مثل هذا الفهم وبالتالي يطبقون مجموعة قوانين "السماح أولاً"، الذي من خلاله يسمح بكل البيانات بالمرور إلى الشبكة ان لم تكن محددة بالمنع مسبقاً.

على الرغم من أن مصطلح "Firewall" قد اكتسب معنى جديد في الوقت الحالي، إلا أن تاريخ المصطلح يعود إلى أكثر من قرن، حيث أن العديد من البيوت قد تم بناؤها من طوب موضوع في الحائط بشكل يوقف انتقال النيران المحتملة، هذا الطوب الحائط سمي بال"حائط الناري".

ظهرت تقنية الجدار الناري في أواخر الثمانينات عندما كانت الإنترنت تقنية جديدة نوعاً ما من حيث الاستخدام العالمي. الفكرة الأساسية ظهرت استجابة لعدد من الاختراقات الأمنية الرئيسية لشبكة الإنترنت التي حدثت في أواخر الثمانينات. في العام 1988 قام موظف في مركز ابحاث "Ames" التابع لناسا في كاليفورنيا بإرسال مذكرة عن طريق البريد الإلكتروني إلى زملائه قائلاً فيها "نحن الآن تحت الهجوم من فيروس من الإنترنت، لقد أصيبت جامعات بيركلي، سان دييغو، لورنس ليفير مور، ستانفورد وناسا ايمز".

دودة موريس نشرت نفسها عبر العديد من نقاط الضعف في الأجهزة في ذلك الوقت. على الرغم أنها لم تكن مؤذية في النية لكنها كانت أول هجوم من الحجم الكبير على أمن الإنترنت المجتمع الموصول على الشبكة لم يكن يتوقع هجوماً أو جاهزاً للتعامل معها وفيما يلي نعرض بعض أنواع جدار الحماية:

4-3-1-1 الجيل الأول مفلترات العبوة (Packet Filters)

أول بحث نشر عن تقنية الجدار الناري كانت عام 1988، عندما قام مهندسون من (DEC) بتطوير نظام فلترة عرف باسم جدار النار بنظام فلترة العبوة، هذا النظام الأساسي يمثل الجيل الأول الذي سوف يصبح عالي التطور في مستقبل أنظمة أمان الإنترنت. في مختبرات T&AT قام بيل شيزويك وستيف بيلوفين بمتابعة الأبحاث على فلترة العبوات وطوروا نسخة عاملة مخصصة لشركتهم معتمدة على التركيبة الأصلية للجيل الأول.

تعمل فلترة العبوات بالتحقق من "العبوات" (packets) التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الإنترنت. إذا كانت العبوة تطابق مجموعة قوانين فلترة العبوة فإن النظام سيسمح بمرور العبوة أو يرفضها (يتخلص منها ويقوم بإرسال استجابة "خطأ" للمصدر).

هذا النظام من فلترة العبوات لا يعير اهتماماً إلى كون العبوة جزءاً من تيار المعلومات (لا يخزن معلومات عن حالة الاتصال). وبالمقابل فإنه يفلتر هذه العبوات بناءً على المعلومات المخزنة في العبوة نفسها (في الغالب يستخدم توليفة من مصدر العبوة المكان الذاهبه إليه، النظام المتبع، ورقم المرفأ المخصص لـ (UDP) (TCP) الذي يشمل معظم تواصل الإنترنت، ولأن (TCP) و (UDP) في العادة تستخدم مرافئ معروفة إلى أنواع معينة من قنوات المرور، فإن فلترة عبوة "عديم الحالة" يمكن أن تميز وتتحكم بهذه الأنواع من القنوات (مثل تصفح المواقع، الطباعة البعيدة المدى، إرسال البريد الإلكتروني، إرسال الملفات)، إلا إذا كانت الأجهزة على جانبي فلترة العبوة يستخدمان نفس المرافئ الغير اعتيادية.

4-3-1-2 الجيل الثاني فلتر محدد الحالة ("Filters Stateful")

هنا يقوم جدار الحماية بمراقبة حقول معينة في المظروف الإلكتروني، ويقارنها بالحقول المناظرة لها في المظاريف الأخرى التي في السياق نفسه، ونعني بالسياق هنا مجموعة المظاريف الإلكترونية المتبادلة عبر شبكة الإنترنت بين جهازين لتنفيذ عملية ما. وتجري غريلة المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده: لأن هذا دليل على أنها زرعت في السياق وليست جزءاً منه، مما يثير الشكوك بأنها برامج مسيئة أو مظاريف أرسلها متطفل.

4-3-1-3 الجيل الثالث طبقات التطبيقات (Firewall Application Layer)

بعض المنشورات بقلم جين سبافورد من جامعة بورديو، بيل شيزويك من مختبرات T&AT، وماركوس رانوم شرحت جيلاً ثالثاً من الجدران النارية عرف باسم "الجدار الناري لطبقات التطبيقات" (Application Layer Firewall)، وعرف أيضاً بالجدار الناري المعتمد على الخادم النيابي (Proxy server). وعمل ماركوس رانوم قاد ابتكار أول نسخة تجارية من المنتج. قامت "DEC" بإطلاق المنتج تحت اسم "SEAL".

أول مبيع للمنتج من "DEC" كان في 13 أغسطس 1991 إلى شركة كيميائية متمركزة على الساحل الشرقي من الولايات المتحدة، الفائدة الرئيسية من الجدار الناري لطبقات التطبيقات أنه يمكن أن "يفهم" بعض التطبيقات والأنظمة (مثل نظام نقل الملفات "DNS" تصفح المواقع)، ويمكنه أن يكتشف إذا ما كان هنالك نظام غير مرغوب فيه يتم تسريبه عبر مرافئ غير اعتيادية أو إذا كان هنالك نظام يتم إساءة استخدامه بطريقة مؤذية ومعروفة.

4-1-3-4 الجيل الحديث من جدار الحماية

في العام 1992 قام كا من لبوب برادين وانبيت ديشون في جامعة جنوب كاليفورنيا كانوا يقومو بعمل تحسينات على مبدأ الجدار الناري، وكان اسم المنتج "Visas" الذي كان النظام الأول الذي له واجهة إدخال مرئية مع ألوان وأيقونات، الأمر الذي سهل عملية تطبيقه والوصول له على حاسوب مشغل بأنظمة تشغيل مثل APPLE MACOS ، MICROSOFT WINDOWS. وفي العام 1994 قامت شركة إسرائيلية اسمها CHECK POINT SOFTWARE TECHNOLOGIES ببناء مثل هذا النظام داخل برنامج متوفر بشكل كبير اسمه "FireWall-1"، وظيفة التحقق العميق للعبوة الحالية للجدران الحديثة يمكن مشاركتها مع أنظمة منع الاختراق (IPS)، كما قامت مجموعة الصندوق الأوسط للاتصالات من قوة مهام هندسة الإنترنت (IETF) تعمل حالياً على تحديد الأنظمة الاعتيادية لتنظيم الجدران النارية والصناديق الأوسطية الأخرى.

هنالك العديد من فئات الجدران النارية بناءً على مكان عمل الاتصال، ومكان تشفير الاتصال والحالة التي يتم تتبعها نذكر منها التالي:-

1. طبقات الشبكة ومفلاترات العبوات (Network Layer and Packet Filters)

الجدار الناري ذو طبقات الشبكة الذي يسمى أيضا مفلاترات العبوة، تعمل على رصة أنظمة TCP/IP منخفضة المستوى، ولا تسمح للعبوات بالمرور عبر الجدار الناري دون أن تطابق مجموعة القوانين المحددة. يمكن للمسؤول عن الجدار الناري أن يحدد الأوامر، وإن لم يتم هذا تطبق الأوامر الطبيعية. المصطلح فلتتر العبوة نشأ في نطاق أنظمة تشغيل "BSD".

الجدار الناري ذو طبقات الشبكة عادة ينقسم إلى قسمين فرعيين اثنين، ذو الحالة وعديم الحالة. تتحفظ الجدران النارية ذات الحالة بنطاق يتعلق بالجلسات المفتوحة حالياً، ويستخدم معلومات الحالة لتسريع معالجة العبوة. أي اتصال شبكي يمكن تحديده بعدة امور، تشتمل على عنوان المصدر والوجهة، مرفئ UDP " و "TCP"، والمرحلة الحالية من عمر الاتصال (يشمل ابتداء الجلسة، المصافحة، نقل البيانات، وإنهاء الاتصال). إذا كانت العبوة لا تطابق الاتصال الحالي، فسوف يتم تقدير ماهيتها طبقاً لمجموعة الأوامر للاتصال الجديد، وإذا كانت العبوة تطابق الاتصال الحالي بناءً على مقارنة عن طريق جدول الحالات للحائط الناري، فسوف يسمح لها بالمرور دون معالجة أخرى، الجدار الناري العديم الحالة يحتوي على قدرات فلترة العبوات، ولكن لا يستطيع اتخاذ قرارات معقدة تعتمد على المرحلة التي وصل لها الاتصال بين المضيفين.

الجدران النارية الحديثة يمكنها ان تفلترالقنوات معتمدة على كثير من الجوانب للعبوة، مثل عنوان المصدر، مرفأ المصدر، عنوان الوجهة أو مرفأها، نوع خدمة الوجهة مثل "WWW" و "FTP"، ويمكن أن يفلتر اعتماداً على أنظمة وقيم "TTL"، صندوق الشبكة للمصدر، اسم النطاق للمصدر، والعديد من الجوانب الأخرى.

فلاتر العبوات لنسخ متعددة من "UNIX" هي، "IPF" (لعدة)، (FREEBSD /MAC " (OS X) IPFW، (IPTABELSIPCHAINS (LINUX، "PF" (OPEN BSD AND ALL OTHER BSD).

2. طبقات التطبيقات (Application Layer)

تعمل الجدران النارية لطبقات التطبيقات على مستوى التطبيق لرصة "TCP/IP" (مثل جميع أزمة المتصفح، أو جميع أزمة "TELNET" و "FTP"، ويمكن أن يعترض جميع العبوات المنتقلة من وإلى التطبيق). ويمكن أن

يجب العبوات الأخرى دون إعلام المرسل عادة. في المبدأ يمكن لجدران التطبيقات النارية منع أي اتصال خارجي غير مرغوب فيه من الوصول إلى الأجهزة المحمية.

عند تحري العبوات جميعها لإيجاد محتوى غير ملائم، يمكن للجدار الناري أن يمنع الديدان (worms) والأحصنة الطروادية (Trojan horses) من الانتشار عبر الشبكة. ولكن عبر التجربة تبين أن هذا الأمر يصبح معقداً جداً ومن الصعب تحقيقه (مع الأخذ بعين الاعتبار التنوع في التطبيقات وفي المضمون المرتبط بالعبوات) وهذا الجدار الناري الشامل لا يحاول الوصول إلى مثل هذه المقاربة.

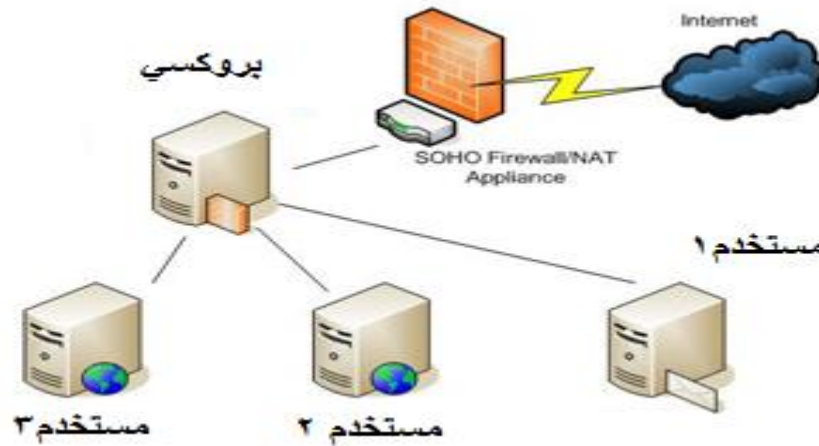
4-3-2 الخادمين النيابيين (Servers Proxy)

الخادم النيابي (سواء أكان يعمل على معدات مخصصة أو برامج الأجهزة المتعددة الوظائف) قد يعمل مثل كجدار ناري بالاستجابة إلى العبوات الداخلة (طلبات الاتصال على سبيل المثال) بطريقة تشبه التطبيق مع المحافظة على حجب العبوات الأخرى.

يجعل الخادم النيابي العبث بالأنظمة الداخلية من شبكة خارجية أصعب ويجعل إساءة استخدام الشبكة الداخلية لا يعني بالضرورة اختراق أمني متاح من خارج الجدار الناري (طالما بقي تطبيق الخادم النيابي سليماً ومعداً بشكل ملائم). بالمقابل فإن المتسللين قد يختطفون نظاماً متاحاً للعامة ويستخدمونه كخادم نيابي لغاياتهم الشخصية، عند إن يتتكر الخادم النيابي بكونه ذلك النظام بالنسبة إلى الأجهزة الداخلية. ومع أن استخدام مساحات للمواقع الداخلية يعزز الأمن، إلا أن المشقين قد يستخدمون أساليب مثل "IP Spoofing" لمحاولة تمرير عبوات إلى الشبكة المستهدفة.

4 ترجمة عنوان الشبكة (Network Address Translation)

عادة ما تحتوي الجدران النارية على وظيفة ترجمة عنوان الشبكة (NAT)، ويكون المضيفين محميين خلف جدار ناري يحتوي على مواقع ذو نطاق خاصة، كما عرّفت في "RFC 1918". تكون الجدران النارية متضمنة على هذه الميزة لتحمي الموقع الفعلي للمضيف المحمي. وبالأصل تم تطوير خاصية "NAT" لتخاطب مشكلة كمية "IPv4" المحدودة والتي يمكن استخدامها وتعيينها للشركات أو الأفراد وبالإضافة إلى تخفيض العدد وبالتالي كلفة إيجاد مواقع عامة كافية لكل جهاز في المنظمة. وأصبح إخفاء مواقع الأجهزة المحمية أمراً متزايد الأهمية للدفاع ضد استطلاع الشبكات.



شكل 1-4 يوضح مخدم البروكسي

تشكل الشبكة السلكية نظاماً مغلقاً وحاجزاً مادياً طبيعياً (physical perimeter) يعتبر الحاجز الدفاعي الأول الذي يتصدى للاختراق، إلا أن الشبكات اللاسلكية، وما قدمت لمستخدميها من حرية الحركة والانتقال معتمدة على الأمواج الراديوية RF التي تثبت في الهواء، ألغت بذلك حاجز الدفاع الأول المتوفر في الشبكات السلكية. لذلك كان من الضروري إيجاد البديل الأمني له. سوف نلقي بعض الضوء من خلال هذا المقال على بعض

ظواهر الاختراق للشبكات الحاسوبية اللاسلكية وسويات الحماية المختلفة التي توفرها بروتوكولات هذه الشبكات. ظواهر الاختراقات للشبكات اللاسلكية لم يأخذ موضوع أمن الشبكات المحلية اللاسلكية والتي تدعى بـ Wi-Fi القسط الكافي من وقت الباحثين خلال تصميمها، وبرزت مخاطرها وعواقبها بُعيد انتشارها الواسع. وبسبب ضعف الوعي بالمشاكل الأمنية لنظم المعلومات لدى معظم مستخدمي الشبكات، فقد مر لا يمكن استغلال العديد من الأشخاص حقيقة وجود الآلاف من الشبكات اللاسلكية المحلية في الإستخدام دون مستوى الحماية اللازم، ونشطوا في اختراقها. وظهرت في الآونة الأخيرة هواية تدعى Wardriving، وهي تعني قيادة السيارة والبحث على جانبي الطريق عن شبكات Wi-Fi اللاسلكية غير المحمية، واختراقها باستخدام حاسوب محمول (laptop) أو جهاز حاسوب كفي Handheld computer. توسعت هذه الهواية وأصبح لديها مئات الآلاف من الرواد، وعدة مئات من صفحات الوب المخصصة لشرح هذه الهواية وتقديم إرشادات لممارسيها، وحتى ابتكار أو تعديل أجهزة Wi-Fi بغية تحسين مداها وقدراتها على التقاط الشبكات البعيدة وضعيفة الإشارة. يبين الشكل (1) سيارة VAN عائدة لأحد ممارسي هواية Wardriving تحتوي هوائياً عالي الانقراط (high-gain antenna) يستطيع التقاط الشبكات اللاسلكية المحلية من مسافة تصل إلى بضعة أميال عن مركز الشبكة وقد استفاد المخترقون من خدمات الأقمار الصناعية GPS في البحث عن أماكن هذا النوع من الشبكات، وتعيين إحداثيات المناطق التي تشاهد فيها شبكات الـ Wi-Fi غير المحمية على خريطة إلكترونية. يبين الشكل (2) شخصاً يمارس هواية Wardriving بمساعدة نظام الأقمار الصناعية للملاحة GPS، مفهوم الأمن في الشبكات الحاسوبية يلحُ باحثوا أمن المعلومات على أن تؤخذ بالاعتبار المتطلبات الأمنية لنظام ما خلال مراحل التحليل والتصميم، إذ تُعتبر إضافتها لاحقاً إلى النظام بعد الانتهاء من التصميم أمراً محفوفاً بالمخاطر، وقد يؤدي إلى العديد من الثغرات التي قد لا تتكشف إلا في مرحلة متأخرة. هذا ما يحصل، ويا للأسف الشديد في أغلب

الأحيان (وخاصة في نظم وبروتوكولات الاتصالات)، لذلك، بعد ان ينتهي المصممون من العمل، يطرح أحدهم السؤال التالي: لكن ماذا يحصل عندما يقوم الأشرار بأمر ما يهدد الشبكات ، عندئذٍ يُستدعى خبراء الأمن ويطلب منهم تصميم نظام أمني إن أحد أهم المبادئ الأساسية في المفاهيم الأمنية هو: اجعل دفاعاتك في عدة طبقات، فإذا أخفقت إحدى الطبقات، فسيكون هنالك طبقة أخرى تتفد حياتك. ليس من الضروري أن تكون هذه الطبقات مادية، بل قد تكون طبقات منطقية، أو افتراضية لتخفيف حدة الهجوم ومنع بعض المهاجمين من الوصول. تتركز الأهداف الرئيسية لنظم الأمن في تطبيقات الاتصالات على تقديم ثلاث خدمات:

1- الاستيقان أو التوثيق (Authentication): وهي المعنية بالتحقق من صلاحية الجهة المشاركة في الشبكة.

2- السرية/الخصوصية (Confidentiality/Privacy) ويقصد بها مجموعة القواعد والنظم التي تتحقق من خلالها سرية المعلومات وحمايتها من الإختلاس أو الاطلاع عليها من قبل غير المخولين بذلك. 3- التكامل (Integrity): وتضم الإجراءات والنظم التي تؤمن عدم السماح بالتغيير أو التلاعب في مضمون المعلومات سواءً خلال تبادلها عبر الشبكة أو تخزينها. تركز بعض نظم الأمن على تقديم حلول للمشاكل الثلاث السابقة، على حين يقوم البعض الآخر على حل واحدة أو اثنتين من هذه المشاكل وترك بقية المهام لنظم أخرى. مثل بروتوكول الحماية WEP أدرك الباحثون في معهد IEEE هشاشة الشبكات اللاسلكية في مواجهة المخاطر الأمنية، لذلك قامت هذه الهيئة بتصميم بروتوكول حماية أطلقت عليه اسم الخصوصية المكافئة للشبكات السلكية (Wired Equivalent Privacy) والذي عرف لاحقاً WEP، وتتلخص الأهداف الرئيسية لبروتوكول WEP في توفير خصائص الخدمات الأمنية الأساسية الثلاث، وهي: الاستيقان، والخصوصية وتكامل المعلومات. اعتمد بروتوكول WEP في بنيته على خوارزمية تشفير تدعى RC4 لتشفير المعطيات وتحقيق

الخصوصية. يمكن تشبيه خوارزمية RC4 بعلبة سوداء تأخذ بايتاً واحداً من المعطيات مدخلاً، وتنتج بايتاً مقابلاً مُخرَجاً مختلفاً عن بايت المُدخل، ويدعى هذا النوع من التشفير بالتشفير التدفقي (stream cipher).
بذلك يبدوالمخرج وكأنه سلسلة من رموزٍ عشوائية من الصعب معرفة نصها الأصلي. أما عملية فك التشفير فتتم بتسلسل معاكس للعمليات السابقة، لذلك تدعى هذه الخوارزمية بخوارزمية تشفير متناظرة (symmetric algorithm). يبين الشكل (3) مخطط عمل هذه الخوارزمية الشكل (3) يوضح خوارزمية التشفير التدفقية RC4 اعتمد البروتوكول WEP تطبيق خوارزمية RC4 لتشفير كل طرد من المعلومات على حدة، أي يعامل كل طرد على أنه دفق جديد من المعطيات، وعلى هذا، في حال ضياع طرد ما تبقى قادرين على فك تشفير باقي الرسالة، وتدعى هذه الخاصة بالتزامن الذاتي (self synchronization). تستخدم خوارزمية RC4 مفتاحاً مشتركاً بطول يساوي 40 بتاً أو 104 بتاً. يوجد أسلوبان لاستخدام المفاتيح في WEP:1. تستخدم كل الأجهزة ومحطة النفاذ مجموعة وحيدة من المفاتيح تسمى بالمفاتيح الافتراضية. عند البدء باستخدام يجري تحميل المفتاح الافتراضي في الأجهزة، ويُبرمج المفتاح المختار في محطة النفاذ، وتبرز المشكلة عندما يقرر بعض المستخدمين تغيير المفتاح الافتراضي، وذلك لأنه إذا حدث تغيير المفتاح أولاً في محطة النفاذ فسوف ينقطع اتصال جميع المشتركين، أما إذا أرسلت رسالة إلى المشتركين بأن يغيروا المفتاح الافتراضي إلى مفتاح آخر، فلا شيء يضمن أن كل المشتركين قد وصلتهم رسالة التغيير، لأنهم ببساطة قد لا يكونون جميعاً على اتصال بالشبكة حينذاك.2. يستخدم كل جهاز مفتاحاً مميزاً لا يعرفه إلا هذا الجهاز ومحطة النفاذ، وتعرف هذه المفاتيح بمفاتيح المقابلة Key mapping key. الفكرة الأساسية هنا هي إعطاء كل مستخدم قيمة مفتاح خاصة به. ولكن المشكلة تظهر عند إرسال محطة النفاذ رسالة بث للجميع broadcast. وقد أمكن إيجاد حلٍ لها في هذا البروتوكول باستخدام مفتاح افتراضي مشترك، على هذا يجري تحميل مفاتيح عند كل

مستخدم.ولكن العملية أصبحت أصعب بالنسبة إلى محطة النفاذ، إذ عليها الآن أن تحتوي قائمة مؤلفة من مئات المفاتيح. وكلما وصل إليها طرد مشفر عليها أن تبحث في القائمة عن المفتاح الخاص بهذا المستخدم لفك تشفير الطرد، إضافة إلى أن هذه القائمة تحتاج إلى حجم كبير في الذاكرة. وكل محطة نفاذ عليها أن تحتوي نسخة من هذه القائمة، لذا أصبحت الإدارة أصعب وخاصة في الأنظمة الكبيرة.جزا الله كل خير لمن شارك في هذا الموضوع المفيد والهام جدا مع تحيات evil_eye[عدل] نقاط ضعف البروتوكول WEP في توفير الحماية عندما بدأ بروتوكول WEP بالانتشار والتوسع بالاستخدام، ظهرت مقالات وأبحاث عديدة لإثبات ضعف التقنيات المستخدمة فيه، من ناحية توفير الحماية للشبكات اللاسلكية| واكتشف العديد من الثغرات الأمنية الخطيرة في WEP، يمكننا تصنيف المشاكل التي يتعرض لها بروتوكول WEP إلى: عدم شمولية التدابير الوقائية. المشاكل والثغرات في تصميم البروتوكول يمكن الباحثون من تعرّف ثلاث نقاط أساسية في تصميم WEP، وتتوضع نقاط الضعف هذه في الوظائف التالية:

1. عملية التوثيق: ضعيفة ويمكن التغلب عليها بسهولة مطلقة.2. التشفير: استعمال غير مناسب لمفاتيح التشفير وطريقة تبادلها، حيث يمكن اختراقها بسهولة.3. التكامل: ضعيف ويجب إعادة النظر في التقانات المستخدمة، إذ إن التصميم المعتمد قد أخفق في منع المهاجمين من تعديل الرسائل.سنستعرض على سبيل المثال المشاكل التصميمية في عملية التوثيق في البروتوكول WEP.هناك متطلبات أساسية لعملية التوثيق في الشبكات اللاسلكية وهي:

1- يجب أن تكون المفاتيح المستخدمة في التوثيق مستقلة عن مفاتيح العمليات الأخرى (كالتشفير).

2- يجب أن تكون عملية التوثيق ثنائية الجانب3- وجود طريقة للحفاظ على هوية الشخص الموثوق به للتحقق من صلاحية عملية التوثيق في جميع الإجراءات وعمليات الإرسال اللاحقة4- منع الانتحال وعدم

إمكان استعمال هوية الشخص الموثوق به من قبل المخترق. لكن بروتوكول WEP أخفق في تحقيق هذه المتطلبات وذلك لأن المفتاح المستخدم في عملية التوثيق هونفس مفتاح WEP المستخدم في عملية التشفير، لهذا لم يحقق البند الأول من متطلبات التوثيق. عملية التوثيق في WEP أحادية الجانب، أي تجري من جهة واحدة، تتم من خلالها تحقق جهاز النفاذ إلى الشبكة والمعروف باسم Access Point من صلاحية الجهة الراغبة في الإتصالات Mobile device. ومن ثم لا يستطيع المستخدم التحقق من موثوقية محطة النفاذ أي موثوقية الشبكة اللاسلكية، مما يسمح لطرف آخر بزعم أجهزة نفاذ، والحصول من خلالها على مفاتيح الحماية ومعلومات الدخول. يجب أن تجري عملية التوثيق باستمرار طوال مدة الاتصال، إذ لا يكفي القيام بهذه العملية عند بداية الاتصال فقط، وهذا غير محقق في البروتوكول WEP. نستنتج مما سبق أن البروتوكول WEP أخفق عملياً في تحقيق المتطلبات الأمنية للشبكات اللاسلكية، إضافة إلى أنه تجاهل بعض متطلبات الأمن الأساسية. ولهذا يعتبر بروتوكول الـ WEP غير آمن من الناحية العملية، مع العلم أن أكثر الشبكات .

4-3-3 أجهزة تعقب المتطفلين IDS

إن أجهزة محاربة المتطفلين أو intrusion detection system عبارة عن نظام حماية تستطيع تشبيهه بي مضاد الفيروسات الموجود على جهازك يقوم بتحليل كل الترافيك المار عبر الشبكة من خلال إرسال نسخة من هذا الترافيك إليه وتتركز وظيفته الأساسية على التحليل العملي فقط وذلك اعتماداً على Rules يمكن تحميلها من الأنترنت أو إعدادها يدوياً كما سوف نشاهد لاحقاً بالإضافة إلى قواعد بيانات تحوي معلومات عن الفيروسات والديدان أستطاعت النفاذ من خلال جدار الحماية الموجود على الشبكة وتعتمد إليه عمل النظام على مقارنة الـ Signature الخاص بكل فايروس والتي تكون مخزنة في قاعدة البيانات ولكن مايعيب هذا

النظام أنه لايقوم بأي ردة فعل اتجاه هذا الفيروسات فكل مايقوم به هو إرسال تحذير إلى مدير الشبكة بوجود شيء غير طبيعي في الترافيك المار ومن هنا نستطيع ان نستنتج ان كلمة detection لاتعني إلا الكشف وقد يخطر على البال سؤال صغير ماذا نستفيد من هذه العملية ؟ وبكلام آخر ماذا سوف أستفيد إذا دخل الفيروس إلى الشبكة ؟ الأجابة على هذا السؤال يجب أن نعلم أولاً أن هذا النوع من الأنظمة مفيد في عدة حالات:-

- الحالة الأولى كشف الثغرات الموجودة في أنظمة الحماية
- الحالة الثانية أرشفة كل أنواع التهديدات التي تحدث للشبكة
- الحالة الثالثة تحديد الأخطاء التي وقع فيها مسؤولوا الحماية وتصحيحها

ومايميز هذا النوع أيضا هو أمكانية وضعه بعيدا عن السار الحقيقيي للترافيك بحيث لا يؤثر على سرعة نقل البيانات بعدد من الأوجه سيتم سردها كمايلي:-

- أنظمة تعقب المتطفلين على الشبكة (Network intrusion detection systems (IDSs) هي وظيفة مشابهة لأسلوب (الكشف عن الفيروسات - virus detection جرس الإنذار ضد اللصوص burglar alarm)الهدف منه هو أنه يخبر مدير الشبكة Administrator بأي دخيل محتمل suspected intrusion مثل حدوث هجوم attack occurring .
- المراقبة الثابتة Constant monitoring مهم جداً للحصول على منافع تعقب المتطفلين فيما عدا ذلك فإن تعقب المتطفلين لا يمثل أكثر من سجل تدقيق audit log للتاريخ الماضي.
- النسخة المحسنة من نظام تعقب المتطفلين (IDSs) هو نظام " منع دخول المتطفلين ومفهوم ال IPS أن الهجوم تم صده attack is blocked فور اكتشافه.

4-3-3-1 أنواع أنظمة تعقب المتطفلين

1. Host based

عبارة عن جهاز يعمل أو أداة تعمل بصورة شبيهة لمراقب النشطة

مثل device أداة – particular computer host وهو يراقب الأنشطة على (حاسب مضيف معين

host-based IDS على الأدوات الأخرى لن ترى بواسطة موجهاة الاشارات. الراوترى

2. Network based

يراقب جهاز محاربة المتطفلين و packet sniffer بأسلوب مشابه لجهاز مراقبة الحركة. وهو يراقب الحركة

يمكن أن يرى الهجمات على اتصالات مشوشة او غير شرعية IDS و. network link الأنشطة عبر

discreet switched network connections ولكن ليس عبر promiscuous connections

من اكتشاف الهجمات الحادثة على IDS system يمكن أن يمنع ال network switch ال فتصميم

أخرى switch ports إلى systems connected

4-4 طرق إكتشاف المتطفلين

1. Statistical

تحميل وحدة المعالجة المركزية network traffic تستخدم النظام الإحصائى لحساب (الحركة على الشبكة

إذا كانت هناك هجمات تحدث والأنظمة الإحصائية معرضة لأن لتحديد ما (memory loading الذاكرة

لأغلب الشبكات تكون متقطعة (traffic patterns) لأن نماذج المرور false alarms تعطى إنذارات كاذبة

والتي قد تمر بدون يقدم النظام الإحصائى ميزة أنه قادر على اكتشاف الهجمات الجديدة (sporadic)

signature-based system ملاحظة فى حالة الاستخدام .

Signature .2

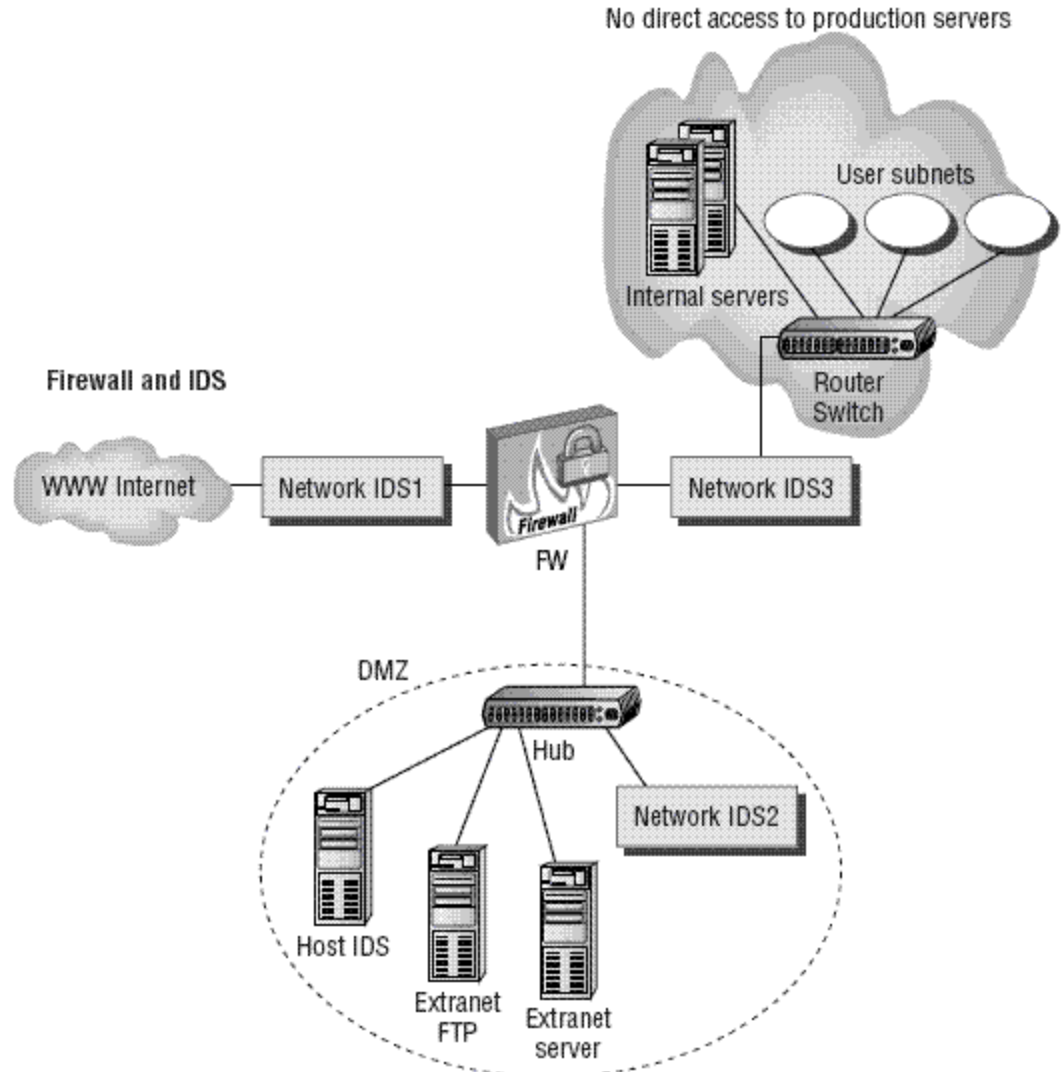
. Signature-based IDS على قاعدة بيانات لتقنيات الهجمات يعتمد database of attack techniques signature-based virus scanner مشابه في تصميم signature-based IDS techniques ال يبحث عن السلوك الذى يشير إلى نوع معين من الهجوم المعروف ... ولسوء الحظ فإن IDS حيث أن ال Database . لا يستطيع اكتشاف الهجمات التى لم تدرج فى قاعدة البيانات signature-based IDS

Neural .3

بدأ تطبيقه على أنظمة تعقب المتطفلين Neural-based learning networks . والهدف هو إنشاء نظام تعليمى (learning system) يكون هجين الهجين و ما بين النظامين الإحصائى

signature-based statistical التوقيع -

Intrusion detection system



شكل (2-4) طرق تعقب المتطفلين

أنظمة تعقب المتطفلين (Intrusion detection systems) تساعد على تمييز الهجمات على الشبكات بعض أفضل التقنيات تكون بعمل (سيرفر - server شبكة فرعية) subnet تظهر كهدف مغرى للهجوم (enticing target for the attacker) والهدف من هذه الأنظمة هي أن تكون " هدف فخ (decoy) "

(target)الهجمات على الفخ توفر إنذار مبكر (early warning) إلى الموظفين الملائمين.
الفخ يمكن أن يكون (عالي التفاعل high interaction في بيئة إنتاج مقلدة simulated production environment

منخفض التفاعل low interaction مع مضيف ساكن (static host)

4-5 طرق منع الفخاخ

1. جرة العسل (Honey pot)

جرة العسل (Honey pot) هي " خدمة لجذب اهتمام المهاجمين sacrificial Server " يوضع بأسلوب مناسب لجذب اهتمام المهاجمين جرة العسل honey pot ليس له أي قيمة في مجال العمل ما عدا أنه ينذر المنظمة بوقوع هجوم يمكن لجرة العسل (honey pot) أن يستعمل أي من (host-based IDS

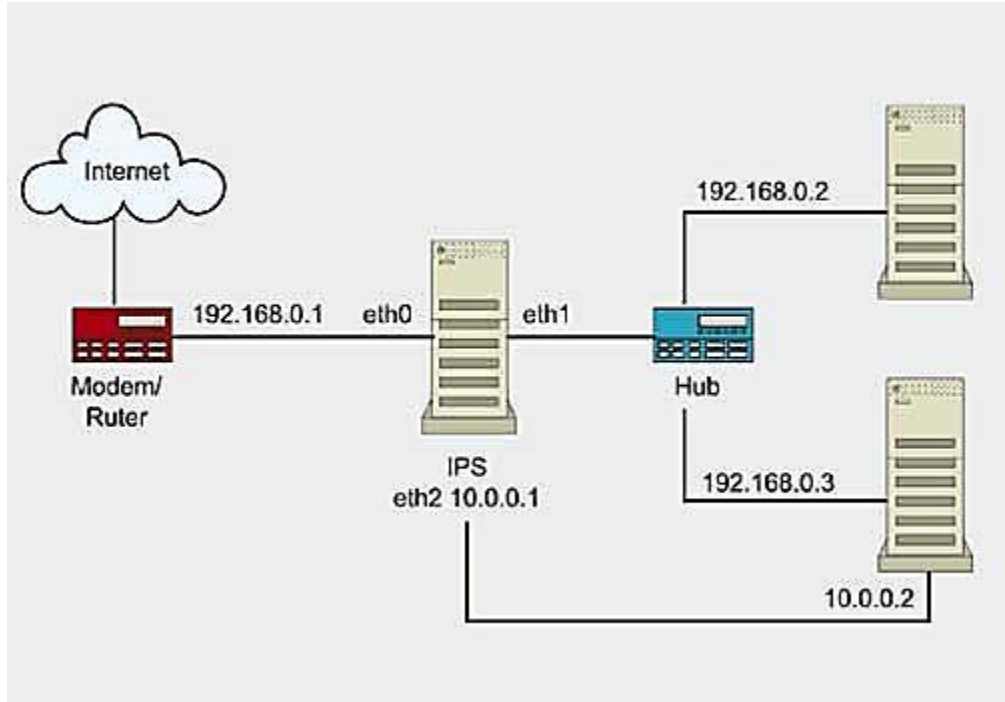
network-based IDS)

2. شبكة العسل (Honey net)

شبكة العسل (Honey net) هي " شبكة فرعية لجذب الاهتمام sacrificial subnet " بها عدد قليل من الماكينات ، تم تصميمها لتجذب اهتمام المهاجمين وأي مرور (traffic) من " شبكة العسل " يعتبر مريب لأنه ليس هناك أي نشاط إنتاجي حقيقي يحدث على هذه الشبكة ... والغرض من هذا التصميم هو أنه يمنح رجال الأمن الفرصة للحصول على تحذير مسبق (advance notice) بأن هناك هجوم محتمل ضد بيئة الإنتاج الحقيقي ، كما تشاهدون الخادم موجود على منفذ آخر وكل مانقوم به هو إرسال نسخة من هذه الحركة (traffic)إليه وبذلك نكون قد ضمنا أن سرعة النقل أو عبور الداتا لن يتأثر أبدا بعمل النظام .

4-3-4 أجهزة تعقب المتطفلين المتطورة IPS

أجهزة تجنب المتطفلين نسخة مطورة من النظام السابق فهو يقوم بعملية الكشف Detection أولاً وبعدها يقوم بتنفيذ ردة فعل معينة Prevention مثل عمل Drop للباكيت الضارة لذا يتوجب وضعه على ممر الترافيك مباشرة الشكل (3-4) يوضح هذه العملية.



شكل 3-4 يوضح طريقة عمل أجهزة تعقب المتطفلين

نلاحظ أن النظام هنا هو برنامج تم تنصيبه على نظام تشغيل لكي يعمل IPS للترافيك وما يميزه أيضا هو طريقة الاستجابة للترافيك الخطر فهو يستطيع أن يمنعه ويستطيع أيضا أن يقوم بأرسال إعدادات لأجهزة الأمن الموجودة على الشبكة مثل الجدران النارية أو الروترات لكي تقوم هي بإيقافه

وأخيرا لهذه الخادمت كما ذكرت سابقا برامج واجهزة عتاد وقد قمت بعملية بحث صغيرة على الأنترنت فوجدت الكثير من البرامج التي تقوم بهذه الوظيفة وأستخلصت لكم برنامج يدعى Snort وهو برنامج مفتوح المصدر يمكن تنصيبه على انظمة مايكروسوفت ولينوكس وطبعا أنا أنصح دائما لمثل هذه الأشياء أنظمة لينوكس فهي مستقرة وتعمل لفترات طويلة ولاتستهلك كثيرا من أماكنيات الجهاز بالإضافة إلى كونها أمن وطبعا البرنامج مجاني وتستطيع أيضا تحميل Rules جاهزة وهذا رابط البرنامج

أما العتاد فهي أيضا كثيرة جدا فهناك أجهزة من سيسكو وأجهزة من com3 وأجهزة من جونيبر والخ....

كما يمكنك شراء Module خاص بهذا النظام ووضعه على روترات أو جدران نارية خاصة بسيسكو مثل هذا Module الخاص بي أجهزة 1841 and 2800 3800

إن أنظمة كشف التطفل مهمة جدا لمن يريد حماية معلوماته أو أجهزته من السرقة ، أو لإبقاء المعلومات سرية وفي الكتمان فهي تكتشف وجود المتطفلين إذا تم اختراق الجهاز لتنبه المستخدم فيقوم بالاحتياطات اللازمة إما بقتل البرامج أو تشغيل جهاز الحماية ونحو ذلك. بدون هذه البرامج والأنظمة قد لا يتنبه المستخدم لمن يخترق الجهاز ويقوم بعمليات تساعد المخترق وتسهل عليه كشف المعلومات السرية وسرقتها. ففي هذه الأوقات التقنيات المستخدمة في الانترنت متطورة و متشعبة ، وقد يستخدمها البعض للاختراق والهجوم التي لا يرغب الجميع بها لما تسببه من أضرار جسيمة في الأجهزة ، والشبكات أو في الأموال ، فمن الأهداف الأساسية لهذه الأنظمة أو أي نظام في امن المعلومات هي خصوصية وسلامة البيانات والقدرة للوصول إليها وهذا

تفصيل لكل هدف :

- الخصوصية: تكمن في إطلاع من يجب إطلاعهم على معلومات أو بيانات محددة من غير سواهم.
- السلامة : تكمن في ضمان سلامة محتوى المعلومات أو بيانات محددة من عدم تغييرها من قبل جهة غير

مسؤولة عن البيانات.

- القدرة على الوصول : تكمن في ضمان وصول المخولين للبيانات والمعلومات المسؤولين عنها وعدم حرمانهم ذلك من أي شخص غير مخول لذلك.

المشكلة التي تحلها كل الأنظمة الأمنية هي محاولة المخترقين لكسر الأهداف الأمنية واختراقها بشتى الأشكال . فالخصوصية يمكن اختراقها وانتهاكها في عدة آليات منها البحث في الشبكة ، التجسس على المستخدم من

غير علمه ، سرقة كلمات المرور . إما السرية فيتم انتهاكها عن طريق الفيروسات ، القنابل المنطقية _ التي

تعتبر من البرامج الخبيثة _ أو إحداث ثغرات خلفية في النظام مما يفتح المجال لتدميره ، إحداث تغييرات خبيثة

أو تبديل المعلومات بمعلومات أخرى إما بالتأثير بالقدرة في الوصول إما بواسطة أجهزة أو خلل في البرامج كما

توجد حالات أخرى تنتج عن الظروف الطبيعية من الحرارة والبرودة أو من زيادة الضغط الجوي وما شابه ذلك

، وأشهر الطرق استخدام تقنية منع الخدمة لتخريب قدرة تواصل الشركات والمؤسسات ومثال ذلك إرسال آلاف

الرسائل الاتوماتيكية من عدد كبير من الأجهزة في وقت واحد لموقع معين مما يسبب انهيار في النظام.

بداية نريد أن نقوم بتعريف التطفل أو التجسس في مجال الانترنت وشبكات الاتصال، فهي الدخول إلى جهاز

أو كائن من غير تصريح ولا ترخيص ، وهو إضافة غير مرغوب فيها أو غير ملائمة. فالمستخدم أو صاحب

الأجهزة يقوم بحماية أجهزته بعدة أنظمة للحماية من مثل هذه التدخلات منها أنظمة كشف التطفل .

أما آلية عمل هذه الأنظمة هي كالتالي : تقوم هذه الأنظمة على تعقب المتطفلين أو محاولة إيجاد أية إشارة

تدل على وجود نشاط غير مألوف أو اعتيادي ، عملها شبيه بما تقوم به برامج الحماية من الفيروسات. وهناك

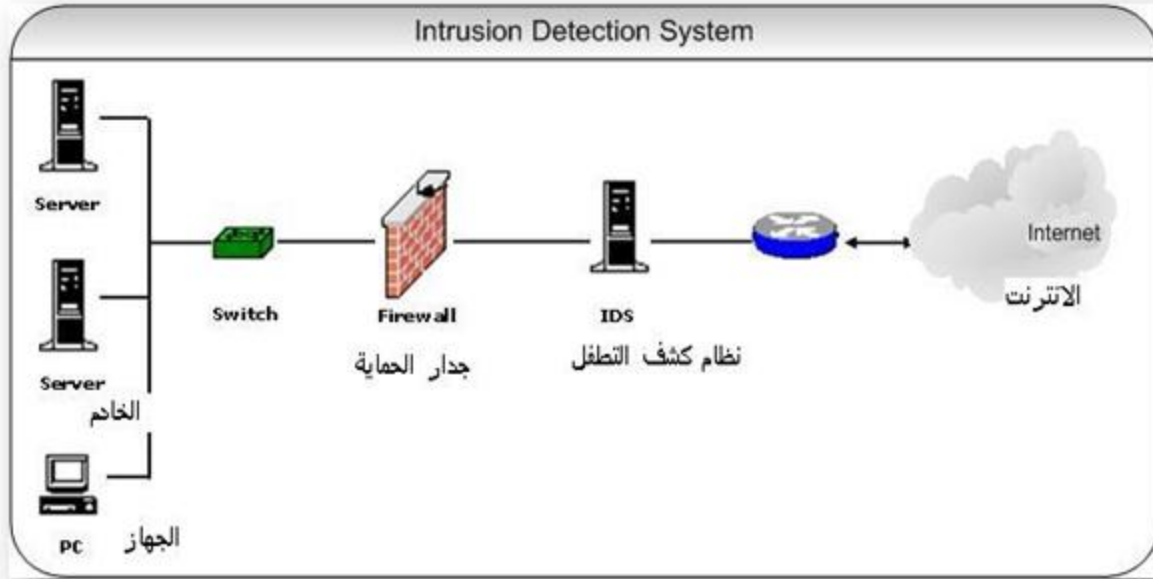
أنواع مختلفة تعتمد عليها هذه الأنظمة فهناك أنظمة تعتمد على تعقب شبكات الاتصال (NIDS) أو قد

تعتمد على التعقب في مجال المضيف أو الجهاز نفسه (HIDS).



شكل 4-4 يوضح البنية التحتية لانظمة كشف التطفل

إن أنظمة كشف التطفل المعتمدة على الشبكات Intrusion Detection System NIDS Network وهي توضع في نقاط مدروسة في الشبكة التي يراد حمايتها أو قد تكون في عدة نقاط موزعة بالشبكة، بحيث تقوم بمراقبة جميع العمليات على الشبكة الصادرة والواردة إليها، وأية نشاط مريب يقوم النظام بتتبيه المسئول عن الشبكة أو من يحل محله. ولكن المراقبة المستمرة لكل الأمور في الشبكة الخارجة منها والداخلية قد يؤدي إلى ضعف السرعة العامة في الشبكة وهذا شيء غير جيد بالنسبة للشبكات.



شكل 4-5 يوضح مثال لموقع نظام كشف التطفل في الشبكة

- أنظمة كشف التطفل المعتمدة على المضيف (Intrusion Detection System HIDS Host) في هذه الحالة تكون الأنظمة تعمل على المضيف أو الأجهزة الموجودة بالشبكة، في هذه الحالة النظام يراقب النشاطات في الجهاز نفسه وما يدخل ويخرج إليه من رزم. في حال وجود أية ملاحظات يقوم بتنبيه المستخدم للجهاز أو من يحل محله. ونلاحظ هنا عدم وجود نقطة الضعف التي كانت موجودة في النوع السابق.
- عندما يقوم النظام بحجب عملية التطفل ومنعها يكون في هذه الحالة النظام نشط ، أما إذا قام النظام بالاكتماء بإرسال تنبيه للمستخدم فيكون النظام في هذه الحالة غير نشط ، وما يستطيع نظام كشف التطفل عملها التالي:-
- يستطيع أن يتتبع نشاط مستعمل من نقطة الدخول إلى نقطة التأثير
 - يستطيع أن يعرف ويبلغ عن تعديلات البيانات
 - يستطيع أن يكتشف متى الجهاز في موضع هجوم

- يستطيع أن يكتشف الأخطاء في ترتيب الجهاز
 - يستطيع معرفة أحدث الهجمات من مراقبة الانترنت
 - يخول إدارة الأشخاص ضعيفي الخبرة للأمن بكل سهولة
 - ومالا يستطيع نظام كشف التطفل عمله :
 - لا يستطيع تحليل كل المرور على شبكة مشغولة
 - لا يستطيع التعويض للضعف في الشبكة
 - لا يستطيع التعامل مع بعض مميزات الشبكات والأجهزة الحديثة
 - لا يستطيع إجراء تحقيقات الهجمات بدون تدخل إنساني
- فمن ما لاحظناه أنها لا تحل جميع مشاكل الأمن بل مختصة بأمور معينة تساعدنا فيها.

4-6 مخدم البروكسي Proxy Server

في الشبكات تعتبر وحدة الخدمة النائية أو البروكسي بمثابة خادم قد يكون عبارة عن أحد نظم الكمبيوتر أو أحد البرامج التطبيقية يعمل كحلقة وصل بين الطلبات الواردة من أجهزة الزبائن التي تبحث عن المصادر المطلوبة من وحدات الخدمة الأخرى. ويمكن الإشارة إلى وحدة الخدمة البديلة باسم وحدة خدمة بروكسي أو يمكن الاكتفاء بكلمة بروكسي. فالجهاز الزبون يتصل بوحدة خدمة بروكسي للحصول على إحدى الخدمات سواء كانت ملف أو صفحة ويب أو الدخول على موقع ما أو الوصول إلى أي مصدر من أية وحدة خدمة أخرى. وعليه، تقوم وحدة خدمة البروكسي بتقييم الطلب المُقدّم وفقاً لقواعد فلترة البيانات الخاصة بها. على سبيل المثال، قد تقوم بفلتره البيانات حسب عنوان الآي.بي.أو، كما يطلق عليه أحياناً، بروتوكول IP. وإذا تم التحقق من الطلب بعد مروره بعملية الفلترة، يقوم البروكسي بتوفير الطلب من خلال الاتصال بوحدة الخدمة ذات الصلة نيابةً عن الجهاز التابع. وقد تقوم وحدة خدمة البروكسي - اختياريًا - بتبديل طلب الجهاز التابع أو عملية الاستجابة الخاصة بوحدة الخدمة. وفي بعض الأحيان، قد توفر الطلب دون الاتصال بوحدة الخدمة المحددة؛ وذلك لأنها تقوم "بتخزين" رد وحدة الخدمة على الطلب. وفي هذه الحالة إذا أراد الجهاز التابع

الحصول على الطلب نفسه فيما بعد، فإنها تقوم بتوفيره مباشرةً دون الحاجة للاتصال بوحدة الخدمة المحددة مرة أخرى أسباب استخدام وحدات خدمة بروكسي كميلي:

- عدم التعرف على الأجهزة وراء البروكسي وجعلها مجهولة (بغرض التأمين) Linux.org .How-to.
- زيادة سرعة الوصول إلى المصادر المطلوبة (بالاستفادة من خاصية التخزين الموجودة على وحدات خدمة البروكسي) - حيث تستخدم في الغالب لتخزين صفحات الويب التي توفرها وحدات خدمة الويب. (2006). Thomas, Keir. Beginning Ubuntu Linux: From Novice to Professional. Apress. "A proxy server helps speed up Internet access by storing frequently accessed pages"

الجدير بالذكر أن وحدات خدمة البروكسي التي تقوم بتمرير الطلبات وعمليات الاستجابة عليها دون تغييرها تسمى عادةً Gateway (وتعني بوابة مرور) أو أحياناً تُسمى Tunneling Proxy (وهو بروكسي يعمل عن طريق إجراء عملية تضمن أمنة باستخدام بروتوكول SSL بين جهاز الكمبيوتر ووحدات الخدمة). علاوةً على ذلك، يمكن تثبيت وحدة خدمة بروكسي في جهاز الكمبيوتر المحلي الخاص بالمستخدم أو في مواضع أخرى متعددة بين جهاز المستخدم ووحدات الخدمة المستهدفة أو الإنترنت. أما البروكسي المقابل أو العكسي (Reverse Proxy) فيعمل كواجهة استخدام من أجل زيادة سرعة تلبية الطلبات وتخزين المصادر المطلوبة (مثل صفحات الويب).

4-6-1 كيفية عمل البروكسي

البروكسي (proxy) هو عبارة عن تطبيق يتم تركيبه على أجهزة خادمة، عند ذلك يدعى باسم خادم البروكسي (proxy server)، وتعتمد عليه الشبكات الداخلية ومزودو خدمات الإنترنت والشركات عند تزويدها للخدمة لأي من مشتركها، بحيث يعمل كوسيط بين مستخدمي الشبكة والإنترنت، كذلك يعمل على عزل الشبكة عن الشبكة الخارجية العالمية ويوفر لها السرعة والأمان (firewall)، فعلى سبيل المثال عند طلبنا لتصفح موقع معين يعمل البروكسي من خلال الوظائف التالية :

1-التخزين (Caching): يتضمن البروكسي ذاكرة تخزين أو قاعدة بيانات كبيرة السعة من شأنها تقليل الزمن اللازم لتحميل صفحة من الشبكة إلى كمبيوتر الزبون، فعند طلبنا لموقع معين سيرسل هذا الطلب لخادم البروكسي (proxy server) الذي يبحث في هذه الذاكرة فإذا وجد ما هو مطلوب فإنه يعيد إرسالها

للزبون، وفي حالة الاخفاق فإنه يجوب الشبكة العالمية باحثاً عما طلب منه بحيث يتم تخزينه لديه في البداية ومن ثم إرساله للزبون.

2-الفلتر (filtering): كثير من الناس هذه الأيام يشكون من أن مواقع الويب المفضلة لديهم يتم حظرها سواء في العمل أو في المدرسة أو حتى في البلد كله، عرفت ماالسبب؟ يتم كل هذا عن طريق عملية تنقيح يقوم بها البروكسي لبعض المواقع عن غيرها، بحيث يسمح بالوصول لبعض المواقع ويمنع المواقع الأخرى، وهو مايعرف بالمواقع المحجوبة.

3-الأمان (firewall):يمكن أن يعمل البروكسي كجدار ناري، مثلاً على مستوى شبكة محلية خاصة بمؤسسة أو شركة فان هذا البروكسي يساعد على حماية هذه الشبكة من اي هجوم أو اعتداء خارجي على شبكتها.

4-6-2 أنواع البروكسي ووظائفها

تقوم وحدات خدمة بروكسي بتنفيذ واحدة أو أكثر من الوظائف التالية:

1. بروكسي التخزين

يعمل بروكسي التخزين - Caching proxy على زيادة سرعة تلبية طلبات الجهاز التابع عن طريق استرجاع المحتوى أو الاستجابة التي تم تخزينها بناءً على طلب سابق تقدم به الجهاز التابع نفسه أو حتى غيره من الأجهزة. هذا وتحفظ وحدات خدمة بروكسي التخزينية نسخاً محلية من المصادر التي يتكرر طلبها باستمرار، مما يسمح للمؤسسات الكبيرة بتقليل استخدام وتكلفة سعة نقل البيانات من شبكات الاتصال البعيدة بشكل ملحوظ مع الحفاظ على السرعة في الأداء. يمتلك معظم مقدمي خدمات الإنترنت والشركات الكبيرة هذا النوع من وحدات الخدمة. جدير بالذكر أن أجهزة البروكسي يتم تصميمها لتقدم أعلى أداء لمنظومة حفظ الملفات (في الغالب، باستخدام تقنية RAID التي توفر للمستخدمين أعلى مستوى من تخزين البيانات وتقسيمها على محركات الأقراص الصلبة وكذلك تقنية Journaling وهو نظام تخزين يقوم بتسجيل أية تغييرات تحدث في الملفات والأدلة في سجلات يومية). وتحتوي هذه الأجهزة أيضاً على نسخ محدثة من بروتوكول TCP المختص بتوفير وسيلة موثوقة لنقل البيانات عبر الإنترنت. وتجدر الإشارة هنا إلى أن وحدات خدمة بروكسي التخزينية تعتبر أول نوع من وحدات خدمة بروكسي عموماً. يحتوي كل من بروتوكول HTTP 1.0 وغيره من البروتوكولات التي تليه في الإصدار على العديد من العناوين لتعريف المحتويات الثابتة (القابلة للتخزين) والتحقق من مدى حداثة المحتوى باستخدام ETAG علامات ترميز تُستخدم للتحقق من إجراء تعديلات بمحتوى موقع ما من خلال المقارنة بين كيانين أو أكثر من نفس

المصدر)، وكذلك باستخدام If-Modified-Since لمعرفة ما إذا كان تاريخ آخر تعديل للموقع يتطابق مع التاريخ المسجل بذاكرة التخزين الخاصة بأخر تعديل بالموقع) و Expiry (التحقق من سلامة البيانات اعتماداً على التاريخ)، وما إلى ذلك. وهناك نوع آخر من البروتوكولات مثل DNS الذي يدعم خاصية Expiry فقط الخاصة بالصلاحيات ولا يحتوي خاصية التحقق من سلامة وصحة البيانات. وهناك بعض الجوانب السلبية التي تعيب بروتوكول التخزين رديء التصميم (مثل عدم القدرة على استعمال خاصية توثيق المستخدم أي التحقق من هويته). وبعض المشكلات يتم التعبير عنها كالاتي: RFC 3143 (وتُعرف باسم مشكلات HTTP Proxy/Caching). هذا، ومن الاستخدامات المهمة الأخرى لوحدة خدمة بروتوكول تقليل تكلفة المكونات الخاصة بالكمبيوتر. فقد تمتلك المؤسسة الواحدة عدة نظم على شبكة واحدة أو متصلة بوحدة خدمة واحدة، وذلك كي تمنع إمكانية اتصال كل نظام على حدة بشبكة الإنترنت. في مثل هذه الحالة، يمكن ربط الأنظمة المفردة ببروكسي واحد، بحيث تكون وحدة الخدمة البروكسي تلك متصلة بوحدة الخدمة الرئيسية.

2. بروتوكول الويب

يطلق على البروكسي الذي يركز على بيانات شبكة الويب الدولية (WWW) "بروكسي الويب - Web proxy". والاستخدام الأكثر شيوعاً لبروكسي الويب هو استخدامه كذاكرة تخزين على الويب. توفر معظم برامج البروكسي (مثل Squid) وسائل يمكن من خلالها منع الوصول إلى بعض عناوين المواقع (URL) المدرجة في القائمة السوداء وذلك لحجب هذه المواقع - الأمر الذي يُعرف باسم فلتر المحتوى. وتُستخدم مثل هذه البرامج في الشركات عادةً، على الرغم من أنه مع زيادة استخدام نظام التشغيل Linux في الشركات الصغيرة والمنازل أيضاً، فإن الاستفادة من خدمة فلتر المحتوى التي يوفرها نظام Linux أيضاً لم تعد تقتصر على الشركات الكبيرة فقط. هذا، ويقوم عدد من وحدات خدمة بروتوكول الويب بإعادة تنسيق بعض صفحات الويب لكي تتناسب مع أغراض معينة أو جمهور محدد (مثل إمكانية عرضها على شاشات الهواتف المحمولة وأجهزة المساعد الشخصي الرقمي [PDA]). اعتاد عملاء أمريكا أون لاين (AOL) على مرور طلباتهم ببروكسي موسع للعمل على "ضغط" أو تقليل التفاصيل في صور JPEG. وقد أدى هذا إلى زيادة سرعة الأداء، لكنه تسبب في حدوث عدد من المشكلات مثل الحاجة إلى وجود درجة وضوح أعلى في الصور أو الحصول على نتائج غير صحيحة نتيجة لعملية الضغط التي تحدث. وكان هذا هو السبب في وجود رابط "AOL Users Click Here" في العديد من صفحات الويب في بداية استخدام شبكة الويب، وذلك لتخطي وحدة خدمة بروتوكول الويب وتجنب الأخطاء الناجمة عن استخدام نظام "الضغط".

3. أجهزة بروكسي الويب المختصة بفلتره المحتويات

توفر وحدات خدمة بروكسي الويب المختصة بعملية فلتره المحتويات رقابة إدارية على المحتوى الذي يتم نقله من خلال البروكسي. ويشيع استخدام هذا النوع من البروكسي في المؤسسات التجارية وغير التجارية أيضاً (وخاصةً في المدارس) لضمان استخدام الإنترنت بما يتفق مع سياسة الاستخدام المقبول. ولكن في أغلب الأحيان، يعمل الأفراد الذين يختلفون مع هذه السياسة على تنزيل واستخدام أنواع أخرى من البروكسي. هناك العديد من الأساليب التي يتم استخدامها في فلتره المحتوى وفقاً لها، ومنها: الفلتره وفق عناوين مواقع معينة أو وفق القوائم السوداء الخاصة بأسماء النطاقات (DNS) أو وفق التعبيرات المتكررة في عناوين المواقع (URL regex) أو الفلتره باستخدام معيار MIME أو وفقاً لتكرار كلمة رئيسية بعينها في المحتوى. جدير بالذكر أن بعض المنتجات عُرف عنها استخدامها لتقنيات تختص بتحليل المحتوى من أجل البحث عن السمات المستخدمة في الغالب من قبل أنواع معينة من الجهات المزودة للمحتويات. في كثير من الأحيان، يدعم البروكسي المختص بفلتره المحتويات خاصية توثيق المستخدم أو التحقق من هويته وذلك كوسيلة للتحكم في إمكانية الدخول على شبكة الويب. وهو عادةً ما ينشئ مجموعة من السجلات إما لإعطاء معلومات مفصلة عن عناوين المواقع التي يزورها بعض المستخدمين أو لمراقبة إحصائيات استخدام البانديث (سعة نقل البيانات) عبر الإنترنت. قد يقوم هذا البروكسي أيضاً بالاتصال ببرنامج مضاد للفيروسات يعتمد على Daemon و/أو بروتوكول ICAP، لتوفير الأمن والحماية من الفيروسات وغيرها من البرامج الضارة من خلال فحص المحتوى القادم قبل وصوله إلى الشبكة.

4. وحدات خدمة البروكسي السري

تحاول وحدات خدمة البروكسي السري والتي يطلق عليها أحياناً بروكسي الويب عموماً جعل التصفح على شبكة الويب مجهول المصدر، وهناك أنواع عديدة ومختلفة من البروكسي السري. ويتمثل أحد أكثر هذه الأنواع شيوعاً في البروكسي المفتوح. ولأن هذا النوع عادةً من الصعب تعقبه، فإنه يعتبر مفيداً بوجه خاص لمن يسعون إلى إخفاء هويتهم في أثناء الاتصال بالإنترنت، مثل المعارضين السياسيين أو حتى مرتكبي جرائم الإنترنت. التحكم في الدخول على شبكة الإنترنت: تفرض بعض وحدات خدمة بروكسي إجراء تسجيل دخول قبل تصفح شبكة الإنترنت. ففي المؤسسات الكبيرة، يجب على المستخدمين المصرح لهم بالدخول على شبكة الويب ملء بيانات تسجيل الدخول أولاً. وبهذا، يمكن للمؤسسة التحكم في استخدام الشبكة من قبل المستخدمين.

5. البروكسي المُعادي (Hostile Proxy)

بالإضافة إلى الاستخدامات العديدة لأجهزة البروكسي، يمكن أيضًا استخدامها في التجسس على البيانات التي تنتقل بين الأجهزة التابعة والشبكة. فكل صفحات الويب التي يتم الدخول عليها، وكذلك كل النماذج التي يتم تقديمها، يمكن رصدها وتحليلها من قبل مشغل وحدة خدمة البروكسي. لهذا السبب، يجب دائمًا تبادل كلمات المرور الخاصة بخدمات الإنترنت (مثل البريد الإلكتروني والمعاملات المصرفية) عبر قناة اتصال مشفرة وأمنة، مثل بروتوكول SSL.

6. وحدات خدمة البروكسي الاعتراضي

وبالنسبة للبروكسي الاعتراضي (Intercepting proxy) الذي يعترض طريق الطلبات المرسله ويقوم بتخزين الإجابات عليها، ويعيد استخدام هذه الطلبات المخزنة فيما بعد والمعروف أيضًا باسم "البروكسي الشفاف - Transparent proxy" لأنه لا يخفي عنوان بروتوكول الإنترنت، وإنما يقوم بعمل ملحوظة بمن تم توجيهها إليه، فإنه يقوم بربط وحدة خدمة البروكسي ببوابة المرور. فعمليات الاتصال التي يتم إجراؤها من قبل برامج التصفح الموجودة على الأجهزة التابعة عبر بوابة المرور يُعاد توجيهها عبر البروكسي دون أن يقوم الجهاز التابع بضبطها (أو حتى يكون على علم بوجودها). يكثر استخدام البروكسي الاعتراضي في المؤسسات التجارية لمنع عدم الالتزام بسياسة الاستخدام المقبول وتخفيف العبء الإداري حيث لا يتطلب استخدامها تهيئة المتصفح الموجود على الأجهزة التابعة. من الممكن في أحيان كثيرة الكشف عن استخدام هذا النوع من وحدات خدمة بروكسي عن طريق مقارنة عنوان بروتوكول الإنترنت الخارجي بالعنوان الظاهر لدى وحدة خدمة الويب الخارجية، أو عن طريق فحص رؤوس HTTP الخاصة بوحدة الخدمة الخارجية.

7. البروكسي الشفاف وغير الشفاف

في كثير من الأحيان، يحدث العكس ويُستخدم مصطلح "البروكسي الشفاف - Transparent Proxy" للإشارة بشكل خاطئ إلى "البروكسي الاعتراضي - Intercepting Proxy" (لأن الجهاز التابع لا يكون في حاجة إلى توصيف البروكسي ولا يمكنه معرفة أن طلباته تمر عبر بروكسي). يمكن تشغيل البروكسي الشفاف باستخدام بروتوكول WCCP الخاص بشركة "سيسكو". وهذا البروتوكول يكون موجود عند الموجه (Router) ويتم توصيفه من خلال ذاكرة التخزين - مما يسمح لذاكرة التخزين بتحديد المنافذ والبيانات التي تُرسل إليها من قبل الموجه عن طريق عمليات إعادة التوجيه. ومن الممكن أن تتم عملية إعادة التوجيه هذه

من خلال إحدى الطريقتين التاليتين: GRE Tunneling (OSI Layer 3) أو MAC rewrites (OSI Layer 2). وعلى الجانب الآخر، فإن RFC 2616 (Hypertext Transfer Protocol) -- (http://1.1

البروكسي الشفاف - Transparent Proxy: عبارة عن بروكسي لا يقوم بتعديل الطلب أو الاستجابة لأقصى مما هو مطلوب لبيانات لتوثيق وتعريف هوية وحدة خدمة بروكسي.

'البروكسي غير الشفاف - Non-Transparent Proxy': عبارة عن بروكسي يقوم بتعديل الطلب والاستجابة من أجل توفير بعض الخدمات المضافة لبرامج أو تطبيقات الجهاز التابع، مثل خدمات إضافة تعليقات من قبل المجموعات أو تحويل نوع الوسائط أو تقليل البروتوكول أو إجراء عملية فلتره بغرض السرية.

8. البروكسي الجبري

يشير مصطلح "البروكسي الجبري - Forced proxy" بعض الغموض. فهي يحمل في طياته اثنين من المعاني المتناقضة من حيث كونه "بروكسي اعتراضي" (لأن هذا النوع يقوم بفلتره جميع البيانات التي تمر عبر بوابة المرور الوحيدة المتاحة للدخول على الإنترنت)، ويعتبر في الوقت نفسه "بروكسي غير اعتراضي" (لأنه يجبر المستخدم على توصيف البروكسي ليتمكن من الدخول إلى الإنترنت). في بعض الأحيان، يكون من الضروري استخدام البروكسي الجبري نتيجة للمشاكل التي تحدث عند اعتراض طلبات بروتوكولي TCP و HTTP. على سبيل المثال، يمكن أن يؤثر اعتراض طريق طلبات بروتوكول HTTP على إمكانية استخدام ذاكرة تخزين البروكسي. كما يمكنه أن يؤثر على آليات توثيق معينة بشكل كبير. ويعود ذلك في الأساس إلى أن الجهاز التابع يعتقد أنه يتواصل مع وحدة خدمة، وبالتالي فإنه لا يمكن تمييز رؤوس الطلبات المطلوبة من قبل البروكسي عن الرؤوس التي قد تطلبها وحدة خدمة عليا في تسلسل وحدات الخدمة (وخاصةً رؤوس طلب ترخيص بالحصول على بيانات). كما أن مواصفات بروتوكول HTTP تمنع تخزين عمليات الاستجابة إذا كان الطلب يحتوي على رأس طلب ترخيص بالحصول على بيانات.

9. وحدة خدمة بروكسي المفتوحة

قد يسيء البعض استخدام وحدات خدمة بروكسي المفتوحة (Open Proxy)، ولذلك فقد قام مديرو الأنظمة المختلفة بتطوير عدد من الأساليب التي يمكن من خلالها رفض الطلبات المقدمة من وحدات خدمة بروكسي المفتوحة. هذا، وتقوم العديد من شبكات IRC تلقائياً بفحص نظم الأجهزة التابعة الخاصة بالأنواع المعروفة

من وحدات خدمة بروتوكول المفتوحة. وبالمثل، يمكن توصيف وحدة خدمة البريد الإلكتروني لتفحص تلقائياً رسائل البريد الإلكتروني المرسله إلى وحدات خدمة بروتوكول المفتوحة.

وتقوم مجموعات IRC ومشغلو البريد الإلكتروني بتشغيل تقنية DNSBL لنشر قوائم عناوين بروتوكول الإنترنت التي يريد أن يتجنبها البعض والخاصة بأنواع معينة من وحدات خدمة بروتوكول المفتوحة، مثل AHBL وCBL وNJABL وSORBS. يعتبر موضوع الفحص التلقائي للأجهزة التابعة التي تستخدم وحدات خدمة بروتوكول المفتوحة مثيراً للجدل من الناحية الأخلاقية. إذ يعتقد بعض الخبراء مثل فيرنون شرايفر أن هذا الفحص التلقائي يعادل اختراق الأجهزة التابعة المضيئة عن طريق فحص المنافذ المفتوحة (Portscanning) للأجهزة. بينما يعتقد آخرون أن مستخدم الجهاز التابع عندما يتصل بوحدة خدمة تفتضي شروط الاتصال بها الخضوع لهذا الفحص، فإنه يجب أن يبدي موافقته على إجراء هذا الفحص، وبالتالي فهذا الأمر لا يعد انتهاكاً أو تعدياً على خصوصياته.

10. البروكسي المقابل

يقصد بمصطلح البروكسي المقابل أو العكسي - Reverse proxy هذا النوع من وحدات خدمة بروتوكول الذي يتم تثبيته بين واحدة أو أكثر من وحدات خدمة الويب. وسُمي البروكسي بذلك الاسم لأنه يقوم مقام المرآة العاكسة لوحدة الخدمة الأولى وذلك بتخزين كل ما تنطوي عليه من محتويات لحسين أداء شبكة الويب. وبذلك، تمر جميع البيانات القادمة من الإنترنت لتتجه إلى إحدى وحدات خدمة الويب عبر البروكسي المقابل. أما عن أهميته، فهناك العديد من الأسباب التي تدعو لاستخدامه مثل:

- التشفير / SSL Acceleration: عند إنشاء مواقع ويب آمنة، لا يتم في الغالب إجراء عملية التشفير من خلال بروتوكول (SSL) باستخدام وحدة خدمة الويب نفسها، لكنها تتم بواسطة بروتوكسي مقابل يشتمل على جهاز SSL Acceleration. انظر (Secure Socket Layer (SSL). علاوةً على ذلك، يمكن لوحدة الخدمة المضيئة أن توفر "بروكسي SSL" واحد فقط، لإجراء عملية تشفير باستخدام بروتوكول SSL لعدد كبير جداً من وحدات الخدمة المضيئة. وبهذا، لا تكون هناك حاجة لوجود SSL Server Certificate لكل وحدة خدمة مضيئة. ومع ذلك، يتمثل الجانب السلبي في هذا الأمر في أن جميع وحدات الخدمة المضيئة التي تستخدم بروتوكسي SSL تضطر إلى الاشتراك في اسم DNS شائع أو عنوان بروتوكول إنترنت واحد في عمليات الاتصال التي تتم عبر بروتوكول SSL.

- موازنة العبء- Load balancing: يمكن لوحدة خدمة بروكسي العكسية توزيع العبء الناتج عن العدد الكبير من طلبات الاتصال على العديد من وحدات خدمة الويب، بحيث تقوم كل وحدة خدمة منها بتنفيذ مهامها في نطاق التطبيق الخاص بها. وفي مثل هذه الحالة، فإن البروكسي المقابل قد يحتاج لإعادة كتابة عناوين المواقع في كل صفحة ويب (أي ترجمتها من عناوين المواقع المعروفة خارجيًا إلى عناوين المواقع الداخلية).
- حفظ المحتوى الثابت: يمكن للبروكسي المقابل تخفيف العبء الواقع على وحدات خدمة الويب عن طريق حفظ وتخزين المحتوى الثابت الموجود في بعض المواقع مثل الصور أو غيرها من المحتويات الرسومية الثابتة، وبالتالي، سيتم توفير هذه المحتويات عند طلبها دون الحاجة للاتصال بوحدة خدمة الويب المحددة.
- ضغط المحتوى: يمكن للبروكسي المقابل أن تقوم بضغط المحتوى للإسراع من عملية التحميل.
- توصيل الرد على مراحل: يقوم البروكسي المقابل بتقليل استخدام المصدر عن طريق تخزين محتوى الرد الذي أرسلته وحدة خدمة الويب ثم توصيله شيئاً فشيئاً للجهاز التابع البطئ. وهذا الأمر يعتبر مفيداً بوجه خاص للصفحات التي يتم إنشاؤها ديناميكياً.
- التأمين: يعتبر البروكسي المقابل بمثابة طبقة دفاع إضافية تستطيع توفير الحماية ضد بعض نظم التشغيل وبعض الهجمات التي تتم ضد وحدات خدمة الويب. ومع ذلك، فهي لا توفر حماية من الهجمات التي تتم ضد تطبيقات الويب أو الخدمة المقدمة نفسها - الأمر الذي يمثل أكبر تهديد في حد ذاته.
- النشر عبر شبكة إكسترانت خاصة: يمكن للبروكسي المقابل المستخدم عبر الإنترنت أن يُستخدم أيضاً في الاتصال بوحدة خدمة محمية داخل مؤسسة ما مع إتاحة الفرصة لأداء بعض المهام عن طريق الاتصال بشبكة إكسترانت بينما تظل وحدات الخدمة محمية. ولكن ينبغي توخي الحذر عند استخدام البروكسي المقابل بهذه الطريقة؛ إذ يجب اتخاذ إجراءات تأمين لحماية البنية الداخلية عندك في حالة أن تكون وحدة الخدمة هذه عرضة للهجمات من شبكة الإنترنت.

11. أساليب المراوغة

يُقصد بأسلوب المراوغة (Circumventor) اختراق سياسات حجب مواقع معينة تفرضها بعض الجهات مستخدمة في ذلك وحدات خدمة بروكسي. ومن المثير للسخرية، أن أغلب أساليب المراوغة تستخدم وحدات خدمة بروكسي - ويحدث ذلك على درجات متفاوتة من التعقيد. وتعتمد عملية المراوغة في مضمونها على استخدام صفحة ويب تقوم بأخذ الموقع الممنوع وتحاول فتحه بالحيلة في موقع ويب آخر غير محظور - لتسمح للمستخدم بمشاهدة صفحاته المحجوبة. ويعد أحد الأمثلة الشهيرة على ذلك بروكسي elgooG الذي

مكّن المستخدمين في الصين من الوصول إلى موقع Google بعد أن تم منعه هناك، لكن تختلف وحدة خدمة البروكسي هذه عن الأخرى بأنها صُممت لتجاوز عملية حجب واحدة. في سبتمبر 2007 أصدر معمل Citizen Lab تقريرًا يوضح فيه أنواع معينة من وحدات خدمة بروكسي التي تُستخدم في أغراض المراقبة، مثل Proxify و StupidCensorship [2]، و <http://www.CGIProxy>

ويمكن بدلاً من ذلك، أن يتواصل المستخدمون في دولة معينة مع أفراد آخرين بعيدًا عن نطاق المراقبة الذي يخضع له الإنترنت في هذه الدولة؛ وذلك باستخدام بروكسي من نوع Psiphon <http://psiphon.civisec.org> أو Peacefire/Circumventor.

<http://peacefire.org>. كما أن هناك أسلوب أكثر تطورًا يقترح استخدام برامج مجانية مثل UltraSurf <http://www.ultrareach.com> و FreeGate، <http://www.dit-inc.us> أو

استخدام غيرها من البرامج مدفوعة الأجر، مثل Anonymizer <http://anonymizer.com> و Ghost Surf. <http://tenebril.com> هذا بالإضافة إلى أنواع أخرى من البرامج المجانية لتضمين البيانات لنقلها

بشكل آمن، مثل Gpass <http://gpass1.com> و <http://www.http-tunnel.com> وتطبيقات تضمين البيانات مدفوعة الأجر، مثل Relakks <https://www.relakks.com> وأخيرًا تقدم شبكات الاتصال السري JAP

[http://anon.inf.tu-](http://anon.inf.tu-dresden.de/index_en.html) ANON

<http://www.i2p.net> I2P و <http://tor.eff.org> Tor و [dresden.de/index_en.html](http://www.dresden.de/index_en.html) مجموع

ة كبيرة من الوسائل التي تمكن المستخدمين من التصفح والتواصل بطريقة آمنة عبر شبكة الإنترنت يمكن للطلاب الوصول إلى المواقع المحجوبة (مثل شبكات التواصل الاجتماعي ومواقع الألعاب وغرف الدردشة والمانجر والمواقع التي تقدم محتويات إباحية أو هجومية) باستخدام وحدات خدمة بروكسي تستخدم أساليب المراقبة وبالسرعة نفسها التي يحجب بها برنامج الفلترة صفحات الويب الخاصة بوحدات خدمة بروكسي المستخدمة للمراقبة، تظهر غيرها من الصفحات الأخرى. لكن في بعض الحالات، قد يظل الفلتر يعترض طريق البيانات المتدفقة إلى البروكسي المراقب، وبالتالي فإن الشخص الذي يدير الفلتر تظل لديه القدرة على رؤية المواقع التي تتم زيارتها. يستخدم أيضًا الأشخاص الذين يتم منعهم من الدخول على مواقع معينة في شبكة الويب بروكسي المراقبة. كما يُستخدم أيضًا بروكسي المراقبة بحيث يمكن لأي شخص في أي دولة أخرى من دول العالم لاستفادة من الخدمات التي تُقدّم في دول معينة لمواطنيها فقط. على سبيل المثال، يمكن الاستفادة من الخدمات المتاحة في دول بعينها فقط والتي يستطيع من خلالها المواطنون إعادة

إنتاج وسائل معينة أو بث معين خاص بالويب. جدير بالذكر أن بروتوكول المرادغة يعتبر آمناً في الغالب إلا في حالة واحدة وهي أن تكون مواقع الويب التي يُستخدم فيها هذا البروتوكول يتم إدارتها من قبل طرف ثالث غير موثوق به وغير مُعلن لنواياه - والتي قد تكون جمع بيانات شخصية عن المستخدمين. ونتيجة لذلك، يُنصح المستخدمون دائماً بعدم إدخال أي بيانات شخصية أو مهمة، مثل أرقام بطاقات الائتمان أو كلمات المرور، في أثناء استخدامهم لهذا النوع من البروتوكول. وإحدى الطرق التي يمكن من خلالها التحايل على بروتوكول حجب المواقع والمسئول عن فلترة المحتويات هي نقل البيانات مضمنة باستخدام بروتوكول آمن إلى بروتوكول آخر (يتحكم فيها مستخدم يمتلك حق دخول غير مقيد على أي موقع على الإنترنت). وكثيراً ما يتم ذلك عن طريق إنشاء اتصال آمن تكون فيه حزم البيانات المرسله بتنسيق بروتوكول VPN أو بروتوكول SSH مضمنة داخل بروتوكول آخر ناقل (فيما يُعرف باسم Tunneling)، لئتم في النهاية فك تضمينها من قبل الجهاز المستلم الذي يتم الدخول عليه من خلال أحد المنافذ المفتوحة. جدير بالذكر أن المنفذ رقم 80 يظل مفتوحاً دائماً للسماح باستخدام HTTP، كما هو الحال بالنسبة للمنفذ رقم 443 الذي يظل مفتوحاً أيضاً للسماح باستخدام HTTPS. ومن خلال استخدام التشفير، لا يكون فقط من الصعب كشف نقل البيانات المنقولة بطريقة Tunneling إلى وحدة خدمة بروتوكول بعيدة - بشرط أن تكون وحدة خدمة البروتوكول البعيدة نفسها مؤمنة جيداً - بل يكون من الصعب اعتراضها أيضاً. في بعض عمليات توصيف الشبكات، يتم إعطاء العملاء الذين يحاولون الوصول إلى وحدة خدمة بروتوكول مستويات مختلفة من امتيازات الوصول تعتمد على مكان جهاز الكمبيوتر الخاص بهم أو حتى على عنوان ماك (MAC) الخاص ببطاقات الشبكة. ومع ذلك، إذا كان في وسع أحد الأشخاص الوصول إلى نظام باستخدام امتيازات دخول أعلى، فيمكنه استخدام هذا النظام كوحدة خدمة بروتوكول يمكن للأجهزة التابعة الأخرى استخدامه للدخول على وحدة خدمة البروتوكول الأصلية، وبالتالي تغيير امتيازات الدخول الخاصة بهم.

12. فلترة المحتوى

هناك العديد من أماكن العمل والمدارس والكلية التي تقوم بحجب الدخول على بعض المواقع والخدمات على شبكة الإنترنت. ومن أجل القيام بذلك، يتم استخدام إما وحدة خدمة بروتوكول مختصة بفلترة المحتويات (ويمكن الحصول على هذا النوع من وحدات خدمة البروتوكول إما مجاناً أو مقابل دفع أجر)، أو باستخدام بروتوكول مثل ICAP الخاص بفلترة أو تهيئة المحتويات والذي يسمح باستخدام برامج إضافية للوصول إلى ذاكرة التخزين بأكملها. يجب أن تمر الطلبات التي يتم إرسالها إلى الإنترنت عبر فلتر خاص بوحدة خدمة بروتوكول خارجية أولاً. وتوفر الشركة التي تقدم خدمة فلترة محتوى شبكة الويب قاعدة بيانات مدرج فيها أنماط معينة

من عناوين المواقع (تشتمل على التعبيرات المعتادة) ويرتبط فيها المحتوى بسمات معينة أيضاً. ويتم تحديث قاعدة البيانات هذه أسبوعياً عن طريق الاشتراك في خدمة التحديث التي يوفرها موقع الشركة، كما هو الحال بالنسبة للاشتراك في خدمة تحديث برامج الحماية من الفيروسات. ويقوم المدير المسئول عن إدارة خدمة فلترة المحتوى بحجب نطاق كبير من أنواع المحتويات المختلفة الموجودة على شبكة الإنترنت (مثل مواقع الرياضة أو المواقع الإباحية أو مواقع التسوق عبر الإنترنت أو مواقع المقامرة أو شبكات التواصل الاجتماعي). ويتم على الفور رفض الطلبات المشتملة على عناوين تتطابق مع أحد أنماط عناوين المواقع الممنوعة. أما إذا افترضنا أن عنوان الموقع المطلوب مقبول وغير ممنوع، فإن وحدة خدمة البروكسي تقوم على الفور بإرسال المحتوى. عندئذٍ، يمكن استخدام فلتر ديناميكي عند مسار الإرجاع الخاص بصفحة الويب. فعلى سبيل المثال، يمكن حجب ملفات الصور JPEG استناداً إلى مواصفات الصور المحددة أو قد تقوم فلاتر اللغة باكتشاف وجود لغة غير مرغوب في وجودها بالمحتوى. وإذا تم رفض المحتوى، يتم عندئذٍ رد الطلب ولا يتم تخزينه. جدير بالذكر أن معظم شركات فلترة محتويات الويب تستخدم محرك بحث عبر الإنترنت يقوم بتخمين احتمالية انتماء محتوى ما إلى نوع معين (على سبيل المثال، : "ربما تشتمل هذه الصفحة على محتويات إباحية بنسبة 70% ومحتويات رياضية بنسبة 40% ومحتويات إخبارية بنسبة 30%). بعد ذلك، يتم تصحيح قاعدة البيانات الناتجة يدوياً بناءً على الشكاوى أو الأخطاء المعروفة في خوارزميات مطابقة للمحتوى. لا يمكن لبروكسي الويب المختص بفلتر المحتويات اكتشاف العمليات التي تتم عن طريق بروتوكول HTTP مؤمن. ونتيجة لذلك، فإن المستخدمين الذين يريدون اجتياز فلترة المحتوى يقومون بالبحث على الإنترنت عن وحدات خدمة بروكسي HTTPS مفتوحة وسرية وشفافة. وعليه، يقوم المستخدمون ببرمجة المتصفح الموجود على أجهزتهم ليحيل جميع الطلبات التي تمر عبر فلتر الويب إلى هذا البروكسي السري. وتباعاً يتم تشفير جميع هذه الطلبات باستخدام بروتوكول HTTP مؤمن. على الجانب الآخر، لا يستطيع فلتر الويب تمييز هذه العمليات عن أي وصول قانوني لموقع ويب خاص بالمعاملات المالية. وهكذا، يتبين أن هذا النوع من وحدات خدمة بروكسي يثبت فاعليته فقط في حالة وجود طلبات بسيطة وغير معقدة مثل المذكورة سابقاً. علاوةً على ما سبق، تجدر الإشارة إلى وجود نوع خاص من وحدات خدمة بروكسي يسمى "بروكسي CGI". وهي عبارة عن مواقع ويب تتيح للمستخدم فرصة الدخول من خلالها على أي موقع محبوب. وتقوم هذه المواقع عموماً باستخدام PHP أو CGI لتتمكن من العمل كوحدة خدمة بروكسي. وتستخدم هذه الأنواع من البروكسي عادةً للدخول على مواقع الويب التي يتم حجبتها في الشركات أو المدارس. ونظراً لأن هذه الأنواع من البروكسي تقوم أيضاً بإخفاء عنوان بروتوكول الإنترنت الخاص

بالمستخدم عن مواقع الويب التي يدخل عليها من خلال هذا البروكسي، فإنه يتم استخدامه أحياناً من أجل الحصول على درجة من السرية - الأمر الذي يطلق عليه Proxy Avoidance.

13. وحدات خدمة البروكسي المزودة بلاحقة

يُمكن البروكسي المزود بلاحقة - (Suffix Proxy) المستخدمين من الإطلاع على محتويات شبكة الويب من خلال إلحاق اسم وحدة خدمة البروكسي بعنوان الموقع الخاص بالمحتوى المطلوب الإطلاع عليه (على سبيل المثال، "a.nl6.en.wikipedia.org"). هذا، ويعتبر البروكسي المزود بلاحقة أسهل في الاستخدام من البروكسي العادي. وقد ظهر مفهوم البروكسي المزود بلاحقة عام 2003 في شكل IPv6Gate، وفي عام 2004 في شكل (Coral Content Distribution Network) البروكسي المزود بلاحقة - Suffix Proxy في أكتوبر عام 2008 بواسطة "a.nl6".

14. ملقمات الوكيل المفتوحة (open proxy) هي تلك التي لا تتطلب كلمة مرور لتسجيل الدخول أو الاستخدام وبالتالي يمكن الوصول إليها من قبل أي شخص مستخدم للإنترنت دون معرفة المسؤول عن هذه المزودات للبروكسي.

4-6-3 مزايا مخدّمات البروكسي

من أهم مزايا مزود البروكسي أن زاكرة الكاش المتوفر لديه يمكنه أن يخدم بها كل المستخدمين، فإذا كان الموقع المطلوب، ذا جماهيرية كبيرة، ويطالعه عدد واسع من المستخدمين، خلال فترة زمنية متقاربة، فإن المزود يحتفظ ضمن الكاش بنسخة عن صفحات هذا الموقع، ما يجعل عملية الرد على المستخدم الذي يطلب الصفحة، أسرع، بدون الحاجة لإرسال هذا الطلب إلى الإنترنت مرة أخرى، وهذا بدوره يوفر الوقت على المستخدم، ويؤمن سرعة جيدة في تنفيذ الطلب، كذلك تؤمن تدابير أمنية جيدة للتحكم بعمليات الاتصال بالإنترنت. فمن السهل، باستخدام البروكسي، تعريف الأشخاص المسموح لهم الاتصال بالإنترنت، وتحديد الخدمات التي يمكنهم استخدامها ويمكن لمدير الشبكة أن يحدد أيام أو ساعات يسمح خلالها بالاتصال بالإنترنت، أو أن يمنع الاتصال ببعض المواقع نهائياً.

4-7 مخاطر استخدام الوكيل المفتوح

عند استخدام وكيل مفتوح فإن جهاز الكمبيوتر الخاص بك يجري إجراء اتصال مباشر إلى جهاز كمبيوتر آخر هو في الحقيقة مزود بروكسي أنت لا تعرف من هو المالك أو الذي يملك السيطرة على جهاز الكمبيوتر البعيد هذا أو ربما تم عمله من قبل قرصنة إنترنت، إذا كنت تستخدم ملقمات الوكيل القوائم المفتوحة، هل

يمكن أن تثق بعد ذلك برسائل بريدك الإلكتروني وكلمات المرور أو غيرها من المعلومات الحساسة وتوثقها للشخص الذي يشغل الوكيل المفتوح. شخص ما يمكن أن يشاهد المعلومات التي يتم نقلها عبر الشبكة علاوة على ذلك فإن جهاز الكمبيوتر الخاص بك يصبح أكثر عرضة للأصابة بملفات التروجان و، وذلك عن طريق خفاك للمنافذ المفتوحة، التي تصبح ممرات سهلة المنال لقرصنة الإنترنت والهacker، عبر جهازك عند استخدامك لمزود بروكسي مفتوح ومجهول المصدر والذي من الممكن إنه قد صمم لهذا الغرض أصلاً.

8-4 مخاطر استخدام وحدات خدمة بروكسي مجهولة

من المعروف أنه عند استخدام وحدة خدمة بروكسي (على سبيل المثال، بروكسي HTTP السري) فإن جميع البيانات التي يتم إرسالها إلى وحدة الخدمة (على سبيل المثال، وحدة خدمة HTTP في موقع ويب) يجب أن تمر أولاً عبر وحدة خدمة البروكسي قبل إرسالها إلى الخدمة، دون تشفير في الغالب الأعم. ولذلك، تكون المخاطرة المحتمل حدوثها عند القيام بهذا الأمر هي تسجيل وحدة خدمة البروكسي لكل ما يتم إرساله عبرها، بما في ذلك أسماء المستخدمين وكلمات المرور غير المشفرة. باستخدام سلسلة من وحدات خدمة بروكسي التي لا تكشف عن هوية مرسل الطلب، من الممكن أن يؤدي هذا إلى جعل أنشطة المستخدم غامضة بالنسبة للجهة التي يرسل إليها الطلب. ومع ذلك، قد يكون المستخدم معرضاً لعملية تعقب بياناته التي يتم تركها في البروكسي، وهذا قد يؤدي إلى استخدامها أو تعقب أنشطة المستخدم. وإذا كانت السياسات المستخدمة أو الجهات المسؤولة عن وحدات خدمة البروكسي هذه غير معروفة، فإنه من الممكن أن يقع المستخدم ضحية لهذه الوسائل التي تعطيه شعوراً زائفاً بالأمان فقط لأن تلك التفاصيل تكون في الغالب بعيدة عن أنظار وأذهان المستخدمين. وخلاصة ذلك هي ضرورة توخي الحذر عند استخدام وحدات خدمة بروكسي مجهولة واستخدام الأنواع المعروفة فقط (على سبيل المثال، عندما يكون تكون الجهة المالكة لها معروفة وموثوق فيها وتتبع سياسة واضحة فيما يتعلق بالحفاظ على سرية بيانات العملاء وغير ذلك من العوامل التي تدعم الاستخدام الآمن لمثل هذه المنتجات). أما إذا لم يكن هناك بد من استخدام وحدات خدمة بروكسي مجهولة، فيجب ألا يتم نقل أي معلومات شخصية عبرها (ما لم تكن منقولة عبر قناة اتصال مشفرة). بالإضافة إلى ما سبق، هناك أمر آخر فيما يتعلق بوحدات خدمة البروكسي يعتبر مصدرًا للإزعاج أكثر من كونه خطراً ألا وهو أن المستخدمين يجدون أنفسهم ممنوعين من الدخول على مواقع ويب معينة - حيث يقوم عدد كبير من المنتديات ومواقع الويب بمنع استقبال بعض عناوين بروتوكول الإنترنت التي تخص وحدات خدمة بروكسي قامت في السابق بإرسال رسائل مزعجة (غير مرغوب فيها) إلى هذه المواقع والمنتديات أو رسائل مستنفة غير ذات صلة بما تتم مناقشته.

4-9 طرق الحماية الفيزيائية

1. الدونجل The Dongle

كمثال عليه نذكر D Studio MAX3، والدونجل هو عبارة عن دائرة صغيرة توضع على المدخل التفرعي LPT للحاسب وهو يحمل بداخله دائرة متكاملة صغيرة مبرمجة بحيث تعطي استجابة معينة عند إشارة دخل معينة، ويجب على دائرة الدونجل أن تؤمن توصيل الطابعة إلى منفذها الذي احتله الدونجل وبالتالي يتكون الدونجل من طرفين الأول يدخل في جهاز الكمبيوتر والثاني يسمح لكبل الطابعة بالدخول عبره، وهو نظام حماية فعال جدا وفي بعض الأحيان يتم تخزين بعض الأكواد الضرورية لاستمرار عمل التطبيق المحمي وبالتالي لا يمكن أن يستمر البرنامج بالعمل إلا بوجود الدونجل الخاص به، ومحاسن هذه الطريقة أنه يمكن للمستخدم أن يعمل على جهاز الحاسب الذي يحلو لها بمجرد أن يضع الدونجل على المدخل LPT في الحاسب وبالتالي هو غير مقيد بجهاز معين، أما بالنسبة للشركة فهي تضمن أن نسخة فعالة واحدة فقط تعمل في وقت معين كما تعتبر من مساوئ هذه الطريقة الكلفة الإضافية لإنتاج الدارة الإلكترونية الخاصة بالدونجل وضمان أن هذه الدارة لن تتسبب في أي تعارضات تزعج الطابعة، وكذلك بالنسبة للمستخدم فإن عملية تبديل الدونجل ونزعه ومن ثم إعادة تركيبه هي عملية شاقة وخصوصا إذا كان يمتلك أكثر من برنامج محمي بدونجلات مختلفة.

2. البطاقة التوسعية

وكمثال عليه بعض برامج التصميم المستخدمة في آلات النسيج والتحكم الصناعي، وفي الحقيقة على الأغلب فإن الشركة لن يكون هدفها الأساسي هو الحماية وإنما هو استكمال بناء البرنامج بواسطة تلك البطاقة التي تحتوي على عدة أوامر إلكترونية لقيادة آلة مربوطة بالحاسب، وغالبا يتم تركيب البطاقة على منفذ من منافذ ISA التوسعية، ومن محاسن هذه الطريقة:

غير قابلة للاختراق إطلاقاً، فنسخ البرنامج بحد ذاته لن يفيد ما لم توجد تلك البطاقة التي تعتبر الناطق الرسمي باسم البرنامج وتقوم بتوجيه الأوامر الإلكترونية لآلة معينة ومن مساؤها أنها ذات تكلفة عالية، ولا يمكن تطبيقها عملياً إلا في أنظمة الحاسب المصممة للتحكم الصناعي.

3. إحداث عطب فيزيائي على القرص الليزري Laser lock

وكمثال عليها برامج شركة صخر وشركة بيرسونال كمبيوتر سيستيمز العربية، والليزر لوك هو عبارة عن قطاعات معطوبة على سطح القرص الليزري، محفورة بدقة متناهية من أصل القرص الليزري، حيث تتألف عملية تصنيع الأقراص الليزرية الفضية من ثلاث مراحل:

1. Mastering حيث تبعث أنت بقرص منسوخ عليه البيانات التي تود أن تنسخها على أقراص ليزرية فضية

وبالتالي فإن المعمل يقوم بإعداد شيء يشبه القالب يسمى Master وتكلفة تصنيع الـ Master عالية جداً ولذلك فإن المعامل في المنطقة العربية أغلبها إن لم يكن جميعها لا تستطيع إنتاج Master بل تستند بذلك على الشركات الغربية.

2. Duplication يتم أخذ الـ Master المصنوع من المرحلة السابقة ووضعه في مرحلة ثانية من الإنتاج

وهي آلة لا يتجاوز حجمها الغرفة الصغيرة ومهمتها إنتاج الأقراص الليزرية بالاستناد إلى Master معين وتعمل بسرعة حوالي كل ثلاثة ثوان قرص.

3. Printing & Packaging حيث يتم طباعة الصورة المرغوبة على سطح القرص الليزري المعاكس لسطح

القراءة، ما يهمنا في هذه المراحل هو المرحلة الأولى حيث يتم تحديد أجزاء معينة من سطح القرص الليزري وتوليد القطاعات المعطوبة بدقة متناهية وبما أن المرحلة الثانية وظيفتها فقط إنتاج النسخ بغض النظر عن المنشأ فإنها سوف تنتج أقراصاً معطوبة بعض أجزاءها. وفي النهاية يتم تضمين Software خاص على

القرص الليزري مهمته فحص الحماية وتتم عملية فحص الحماية كما يلي :

-تتم محاولة القراءة من قطاع سليم معين يكون مزروعا بين تلك القطاعات المعطوبة

-إن نجحت عملية القراءة فهذا يعني أن القرص أصلي ويتم فك تشفير الملف وتنفيذه

الليزر لوك يكون غالبا حوالي 3 قطاعات أو 19 قطاع أو 27 قطاع معطوب وطبعا هذه القطاعات تكون

متوضعة على مساحة حوالي 39 قطاع بحيث أن القطاعات المزروعة في أحضانها تكون سليمة وهي التي يتم

فحصها عند تفحص الحماية ،ومن محاسن هذه الطريقة أنها ذات تكلفة منخفضة إذا ما قارناها بالطريقتين

السابقتين ومن مساوئها ،ظهرت بعض البرامج مثل Clone CD ومهمته نسخ مثل تلك الأقراص الليزرية ،

فالمعلوم أن نسخ الأقراص الليزرية يتم بطريقة قراءة سطح المعلومات قطاع قطاع فإن فشلت عملية القراءة عند

قطاع معين فإن نظام التشغيل لن يستطيع الإكمال وسيقوم بإحباط العملية وعدم متابعتها أما Clone CD فهو

مصمم بشكل ذكي جدا بحيث يعطي فرصة لنظام التشغيل مدتها حوالي النصف دقيقة لكل قطاع فإن لم

يستطيع نظام التشغيل قراءة ذلك القطاع فإن ذلك يعني أن هذا القطاع تابع للقطاعات المعطوبة ويتم تجاوزه

إلى القطاع الذي يليه وهكذا حتى يتم قراءة كامل سطح القرص الليزري .

4-10 كيفية اختراق الطرق الفيزيائية

يصعب في كثير من الحالات اختراق الطريقة الأولى والخاصة بالدونجل وخصوصا إذا كان الدونجل من النوع

الذي يخزن بعض التعليمات الضرورية والتي لا توجد ضمن الملف التنفيذي، ولكن في النهاية يستطيع

الكراركز حصر هذه التعليمات وعمل تعليمات برمجية تحاكي تلك التعليمات الموجودة ضمن الدونجل وبذلك

يتم الاستغناء عن الدونجل نهائيا، أما في الحالة الثانية فتصبح مسألة الاختراق مسألة إلكترونية بحتة ويجب

على الكراكز أن يقوموا بصناعة بطاقة مشابهة للبطاقة الأصلية وهذا ما يستحيل عمله في أغلب الأحيان، أما

الطريقة السابقة فيما أنه لا يتم إلا عملية تفحص تلك المناطق المعطوبة فيزيائيا فمسألة اختراق الكود المسؤول

عن الحماية تعتبر سهلة ومحلولة من الناحية النظرية.

كل مهنة أو مهارة من الممكن ان تستغل في الخير او في الشر. نفس الشيء مع الهاكرز وقبل ان نطن ان الهاكر شخص سيئ وهنا لابداء ان نذكر ان هناك فارق بين الهاكر والكرار كما سبق وتحدثنا من قبل وأن الكرار هو الذي يسرق البرامج والمواقع وغيرها لكن الهاكر هو محترف اكتشاف الثغرات في انظمة الحاسب وفي الأصل تستخدم هذه المهنة في تأمين الأنظمة ضد الكرارز. فمثلاً لو كنت تملك شركة وتود ان تتأكد ان نظامك حماية بياناتك أمن ضد الاختراق تستعين بهاكر ليكشف لك ثغرات النظام من ثم تقوم بمعالجتها. والكثير من الشركات الضخمة مثل جوجل وفيسبوك تعرض مبالغ كبيرة للهاكرز اذا قامو باكتشاف ثغرات في أنظمتهم وابلغهم بها.

والآن بعد أن علمنا أن الهاكر مجرد مطور محترف يستغل مهارته لفائدة الاخرين إذاً كيف يمكن ان تستغل هذه المعرفة في الشر؟ حسناً دعنى أخبرك الجانب الأخر السيئ الذي قد يسلكه بعض الهاكرز المحترفين والذي قد يدر عليهم دخل يقدر بعشرات الآلاف من الدولارات شهرياً والمقابل هو "بيع الثغرات الأمنية للهيئات الاستخباراتية

حيث يعتبر الحصول على مكافأة لإيجاد ثغرة هو امر طبيعي ومحمود مهما كان المبلغ كبير لكن الأمر لا صاحب أحد الشركات التي تعمل في مجال الأبحاث الأمنية Chaouki Bekrar يتوقف عند هذا الحد فيذكر أن شركته لا تقوم باخبار جوجل بالطرق المتبعه لإيجاد الثغرات الأمنية ولا حتى مقابل مبلغ ال 60 ألف دولار وأضاف: "لن نقوم بمشاركة جوجل هذه الأسرار ولا حتى مبلغ مليون دولار ولن نخبرهم بالطرق التي تساعدنا على إغلاق الثغرات الأمنية، نريد ابقاء هذا الأمر فقط لعملائنا" هذا يعني انهم سوف يخبرون اشخاص آخرين بالثغرات الأمنية وطرق الوقاية منها لكن لن يخبروا شركة جوجل نفسها، وهذا يعني ان هؤلاء العملاء لا يريدون

جوجل أن تغلق هذه الثغرات وإلا لسمحوا بوصول الثغرة لها. هل تعلم من هم أولئك العملاء؟ “إنهم الجهات الأمنية الحكومية

طبقاً للتقرير فإن الهاكرز من الممكن أن يربح بمتوسط 2000-3000 دولار من الثغرة الأمنية التي يكتشفها في نظام تشغيل أو موقع شركة ما أو حتى برنامج شهير وذلك بأن يبلغ صاحب البرنامج بوجود هذه الثغرة ويحصل على المكافأة التقليدية. لكنه يستطيع أن يربح 10 اضعاف وربما 100 ضعف هذا المبلغ من الشرطة أو الأجهزة الأمنية أو حتى الجواسيس وأعداء صاحب هذا المشروع مقابل أن يجبرهم بهذه الثغرة ويبقيها سراً قالت أن Vupen عن صاحب البرنامج لكي لا يغلقها. أحد المؤسسات المتخصصة في هذا المجال وتدعى عملائها يدفعون مبلغ 100 ألف دولار سنوياً مقابل الاشتراك في خدمة معرفة الثغرات بسرية. أي ان الشركة تقوم بالبحث عن الثغرات وتقوم بعمل باقات “مثل باقات الهاتف” وتقوم جهات مختلفة بالاشتراك بها بمبالغ أن تخبرهم كيف Vupen شركة ضخمة للحصول على الثغرات بسرية ودون الإعلان عنها ولا يطلبون من تحصل على الثغرات ولا حتى من قام أيضاً بشراءها وكل ما يريدونه هو الحصول على الثغرة وعدم نشرها. أما ما هي البرامج التي يجدون بها ثغرات أمنية ويبيعونها لعملائهم فذكروا كمثال تطبيق مايكروسوفت ورد وأخيراً نظام أبل “Google’s Android” و جوجل أندرويد “Adobe Reader” وأدوب ريدر “Word” ويعتبر الأخير هو الأعلى في الأسعار لأنه الأكثر انتشاراً والأصعب اختراقاً. وإليك قائمة iOS الشهير. بأسعار الثغرات طبقاً لكل نظام تشغيل وتطبيق.

بالطبع هناك عوامل كثيرة تتحكم في السعر منها إنتشار نظام التشغيل فهو يعني أن الفئة المستهدفة بالثغرة هي فئة كبيرة، وأيضاً حداثة النظام فاخترق نظام حديث يكلف أكثر لأن الثغرات لاتزال جديده والشركة البائعة له لن تتخيل أن يخترق بهذه السرعة، ونشاهد في القائمة أن سعر ثغرة بنظام تشغيل الماك (الذي أعمل عليه

الآن) تساوي 20-50 ألف دولار مقابل 60-120 لنظام تشغيل الويندوز وهو أمر يبدو غير منطقي للبعض لأن الجميع يظن أن نظام الماك هو الأكثر أمان لذلك ستكون ثغراته هي الأعلى ولكن هناك عامل آخر وهو أن في حالة معرفتك لثغرة قوية بالويندوز فإنك تستهدف أكثر من مليار جهاز حول العالم وهذا العدد اضعاف اضعاف مستخدمى الماك. لكن بالرغم من هذه المبالغ الضخمة التي يحصلون عليها مقابل الثغرات فإن لا تتبع الثغرات حصرياً لمشتري واحد لكنها تبيعها لأكثر من مشتري ولن يعلم أحد منهم أن Vupen مؤسسة هناك من اشترى نفس الثغرة مثله وربما تبيعها لأكثر من جهة حكومية وتعتمد على أن كل مشتري لن يخبر أحد انه يعلم هذه الثغرة ،لكن هناك بعض الهاكرز يفضل أن يحدد مشتري الثغرات الخاصة به وأن يكونوا واعضائها ولا يقومون ببيع الثغرات لأي دولة خارج الناتو NATO مؤسسات كبرى أو تحالفات مثل الناتو وقالوا أنهم يقومون بالتدقيق في طلبات الشراء ويسعون لعدم وصول المعلومات والثغرات التي يحصلون عليها إلى الأنظمة الغير ديمقراطية وذلك لأن الأنظمة الديكتاتورية سوف تستخدم الثغرات ضد شعوبها أما الأنظمة الديمقراطية سوف تستخدمها لحماية شعوبها من الإرهابيين وغيرهم. لكن المشكلة طبقاتاً لقولهم انهم لا يضمنون أن تظل الثغرة في يد المشتري فقط لأن إن قمت ببيع سلاح لشخص ما لا تضمن ألا يقوم هذا الشخص ببيع السلاح لطرف ثالث أو يكون هذا المشتري الجيد والموثوق به مجرد وسيط مثلما حدث طبقاتاً لقولهم أن باعوا أحد الثغرات الأمنية لأحد الدول العربية وفوجئوا بعد ذلك أنها يتم استخدامها لمراقبة النشطاء السياسيين من قبل لا تسأل المستخدم ماذا سيفعل بهذه الثغرة أو بمعنى أدق لا يهتم Vupen النظام السوري. ويقول التقرير أن بأن يعرف لأن كل ما يهمه أن يحصل على المبلغ المتفق عليه في حسابه فقط لا غير أما ان تحسن استخدام الثغرة أو تسيء فهذا أمر لا يهمه ،السؤال الذي يطرح نفسه هو كيف تباع هذه الثغرات؟ ربما تكون أنت محترف في مجال الحاسب الآلي وتكتشف ثغرة ما لكنك لست محترف في التسويق وتقدير سعرها ولا حتى

تستطيع التعامل مع الأجهزة الأمنية كالمخابرات وغيرها لبيع الثغرات لهم. أنت مجرد مبرمج محترف ولا تعرف وهو إسم حركي بالطبع وهو يعيش في العاصمة Grugq's شيء سوى البرمجة هنا يأتي دور الوسطاء ومنهم التايلاندية بانكوك ويعمل بدور الوسيط فيخبره المبرمج بالثغرات الامنية وهو يقدر سعرها ويجري اتصالات بالعملاء والجهات الحكومية ويعرضها عليهم ويجري الصفقة ويحصل في المقابل على نسبة 15% من هذه الصفقات كعمولة. ولا تظن أن هذه النسبة قليلة فطبقاً لقوله فلقد حصل العام الماضي على أكثر من مليون دولار من الصفقات وهذا يجعلك تتخيل ما حجم الصفقات التي يقوم بها؟ ولقد ذاعت شهرته حول العالم مما يجعله الآن لا يتعامل في الثغرات البسيطة ولا يقبل صفقة إن كان سعر الثغرة المستهدف لا يتكون من 5 ارقام على الأقل وقد ذكر انه في ديسمبر الماضي قام ببيع ثغرة لجهة حكومية بسعر ربع مليون دولار.

وحتى بعد انتشار أندرويد لكن iOS وعند سؤالة ما هي أكثر الثغرات ربحاً له والأعلى سعراً اجاب "بالطبع يتطلب اختراق حواجز أبل الأمنية ونظامها المعقد لذلك هي الأصب iOS الأندرويد سهل الاختراق أما والذي كان Jailbreakme الشهير باسم iOS 3 والأعلى" وهذه الثغرات تهم الكثيرين فمثلاً الجيلبريك القديم ل مجرد صفحة إنترنت تقوم بعمل سحب فيحدث الجيلبريك وصل إليه أن هناك منظمات مستعدة لدفع أكثر من ربع مليون دولار مقابل أن تصبح حصريه لهم لانها ستنجح لهم اختراق أي جهاز بسهولة من خلال متصفح سفاري. أما عن أهم عميل لديه فقال إنها الحكومة الأمريكية والتي تعتبر طبقاً لقولة أكبر مشتري للثغرات وأكثر جهة تقوم بدفع مبالغ مرتفعة وهو يحصل على 80% من دخله منها. كما أن هناك أيضاً جهات حكومية أخرى منها الصين والتي يوجد عدد كبير من المطورين يعملون لإيجاد الثغرات وبيعها للحكومة الصينية فقط. لكن الأمر يختلف في الشرق الأوسط حيث يعتبر السوق ضعيف لأسباب كثيرة منها عدم انتشار الاعتماد على التقنية بشكل واسع من قبل الحكومات والشعوب في مختلف اتجاهات حياتهم ، وأحياناً يسعى المخترقون إلى

بنشر فيديو لاختراق Vupen نشر فيديوهات للتعريف بهم وأيضاً تكون دعاية وإثبات قوة ففي مايو 2011 قام جهاز بواسطة ثغرات في الكروم لكنهم لم يعطوا أي معلومات لجوجل عن هذه الثغرة ورفضوا أخبارها كيف يغلقوها. وقامت جوجل بالإعلان أنهم استخدموا ثغره في الفلاش بالمتصفح لاختراقه وليس المتصفح نفسه ردوا على جوجل بأن قالوا أنها تخدم المستخدمين والثغرة Vupen وأصدروا تحديث لإغلاق هذه الثغرة، لكن لازالت موجودة ورفضوا أيضاً مساعدتها وهو الأمر الذي دفع مسؤولي جوجل لوصف المخترقين بأنهم انتهازيين وغير اخلاقيين ويتركون ملايين المستخدمين يتعرضون للخطر من أجل فقط اثبات القوة .



شكل (4-6) يوضح غرفة تامين الثغرات الأمنية بأحد المؤسسات الكبيرة

4- 11 بعض الطرق الوقائية لأففال الشغرات

أن اغلب الشركات والجامعات بدأت بالتوجه إلى استعمال الشبكات، اللاسلكية فان نسبة الخطر في ضلوع أجهزتها بطبيعة الحال ترتفع لأسباب عديدة أولها أن الأجهزة لن تكون في العادة موجودة في مكان ثابت بل تتحرك وربما تخرج من مبنى الشركة نفسها لذا وجب الحذر من اتخاذ كافة الوسائل الممكنة من جعل الشبكة اللاسلكية آمنة قدر المستطاع .

إن الأجهزة المحمولة التي تملك كرت شبكة لاسلكي موصل بمقوي للإرسال، بإمكانها أن تشارك في نقل الملفات والتعامل كما لو كانت في مبنى الجامعة أو الشركة أو الكلية وفي الحقيقة من الممكن أن تبعد كيلومترات عنها! وإذا كانت نقاط الاتصال الموجودة في المؤسسة أو الجامعة لم يتم تضبيط إعداداتها بطريقة سليمة ولم يتم تعديل الإعدادات الافتراضية المعروفة لدى كل باحث، فان أي شخص على بعد أميال (باستخدام مقوي للإرسال) يستطيع الدخول بكل سهولة على الشبكة .

إن أغلب الأمور التي من الممكن أن يتم استغلالها هي الإعدادات الافتراضية لنقاط الاتصال Points Access وفي ما يلي بعض الأمور التي ستساعد في تقليل مخاطر الإعدادات الافتراضية:

انتشر في الآونة الأخيرة الكثير من الشبكات اللاسلكية، خاصة في توزيع خدمة الإنترنت، سواء كانت هذه الشبكات في منزل أو في العمل أو في المطاعم والمقاهي، أو في المؤسسات التعليمية.

وعلى الرغم من امتياز هذه الشبكات بالحصول على خدمة الإنترنت في أي مكان دون الحاجة إلى سلك الشبكة، إلا أنها تحتوي على الكثير من المخاطر.

فما أن تبحث من خلال الجوال أو الجهاز المحمول "الابتوب"، إلا وقد تجد نقطة ساخنة لشبكة لا سلكية، ونضع بين يديكم عدة نصائح أمنية تخص مستخدمي هذا النوع من الشبكات:

1- احذر كل الحذر من النقاط الساخنة المجانية (الشبكات المفتوحة)، خاصة وإن كنت لا تعرف أصحابها، فبالتصاليك بهذه النقاط تكون قد أهديت بياناتك ومعلوماتك إلى المخترقين، وكن على قناعة دائماً أنه لا يوجد في عالم الإنترنت من يهديك خدمة مجانية دون مقابل.

2- قم بالتأكد من استخدام الجدار الناري على جهازك المحمول، والذي يكون عادة مدمجاً في نظام التشغيل مثل ويندوز إكس بي أو ويندوز سفن. (لوحة التحكم / مركز الحماية)، وفي حال عدم وجود البرنامج قم بتنصيب أحد البرامج، لتحمي نفسك من خطر المخترقين.

3- لا تتصل بالشبكة الإنترنت خاصة اللاسلكية دون برامج مكافحة فيروسات، وتأكد من تحديثه، ف 20 ثانية كافية لزراعة جهازك بالفيروسات والديدان، أو حتى السيطرة عليه.

4- قم بإيقاف خاصة مشاركة الملفات على جهازك فبذلك تمنع وصول أي شخص إلى ملفاتك وبياناتك.

5- تبني فكرة حفظ الملفات الخاصة بكلمة مرور معقدة، ويمكنك استخدام برامج التشفير والتي سبق وأن شرحنا أحدها TrueCrypt

6- إن كنت تملك شبكة لاسلكية فتأكد من إعدادات وحدة الإرسال، بحيث تكون البيانات مشفرة وذلك من خلال خاصية VPN والمتوفرة في جميع وحدات الإرسال.

7- عود نفسك على إطفاء كرت الشبكة اللاسلكية على جهازك المحمول بعد قطع اتصالك، من خلال الزر المخصص في المحمول.

8- احذر من إجراء أي مراسلات خاصة أو عمليات مالية كتحويل أموال أو الشراء عبر بطاقة مسبقة الدفع مثل الفيزا كارد، وإن كنت مضطراً لذلك فعليك التأكد من أن موقع الإنترنت يستخدم تشفير SSL وذلك بوجود إشارة قفل صغير أسفل شريط المتصفح.

9- لا تتجاهل العلامة الصفراء التي تظهر على أسفل الشاشة (بالقرب من الساعة)، فظهورها مؤشر على وجود تحديثات لنسخة لويندوز إما لترقيع ثغرات في النظام أو تحذير من مشكلة قد تحدث لنظامك.

خطوات وقائية

1. استخدم التشفير: أكثر الطرق فاعلية لتأمين شبكتك اللاسلكية من المتطفلين هو تشفير الاتصالات أو التشفير على الدخول عليها. ومعظم أجهزة الراوتر اللاسلكية ونقاط الدخول (access points) والمحطات القاعدية (base stations) تتمتع بآليات تشفيرية مصممة بداخلها. فإذا لم يكن جهاز الراوتر الخاص بك متمتعاً بخاصية التشفير، فكر في شراء واحد يتمتع بهذه الخاصية.

وغالبا ما يبيع المصنعون أجهزة الراوتر اللاسلكية وتكون خاصية التشفير فيها غير منشطة. لذا يجب عليك أن تشغل هذه الخاصية. وينبغي أن تشرح لك التعليمات التي تأتي مع جهاز الراوتر اللاسلكي كيفية تشغيل هذه الخاصية. فإذا لم يحدث ذلك، يمكنك زيارة موقع الشركة المصنعة على الإنترنت.

ويوجد نوعان رئيسيان من أنواع التشفير: الدخول المحمي على الإنترنت اللاسلكي (WiFi Protected Access (WPA) والخصوصية المكافئة للإنترنت السلكي (Wired Equivalent Privacy (WEP)). وينبغي أن يستخدم حاسبك الآلي وجهاز الراوتر والمعدات الأخرى نفس نوع التشفير. ويعد النوع الأول هو الأقوى، لذا ينبغي عليك استخدامه لو أمكن. فهو كفيلاً بأن يحميك من معظم القرصنة، وهناك أجهزة راوتر قديمة تستخدم التشفير من نوع (WEP) فقط، وهو خير من عدم وجود تشفير على الإطلاق. والمفترض أن هذا التشفير يحمي شبكتك اللاسلكية من أعمال التطفل العرضية من الجيران أو الهجمات التي يقوم بها القرصنة غير المتمكنين. فإذا كنت تستخدم التشفير من نوع (WEP)، أرفعه لأعلى مستويات الحماية.

2. استخدم برنامج لمكافحة الفيروسات وبرامج التجسس واستخدم حائط ناري: تحتاج الحواسب الآلية الموصلة بشبكة لاسلكية إلى الحماية شأنها في ذلك شأن أي حاسب آلي موصل بالإنترنت. لذا ينبغي عليك تثبيت برنامج لمكافحة الفيروسات وبرنامج لمكافحة التجسس وداوم على تحديثه. وبالنسبة للحائط الناري فلو كان غير منشط احرص على تشغيله.

3. أوقف الإعلان عن اسم التعريف (identifier broadcasting): معظم أجهزة الراوتر اللاسلكية تستخدم آلية تسمى الإعلان عن اسم التعريف، وهذه الآلية ترسل إشارات لأي جهاز في المنطقة لتعلن عن تواجدها. وأنت لا تحتاج لأن تعلن هذه المعلومة إذا كان من يستخدمون الشبكة على علم بوجودها بالفعل. ويستطيع القرصنة أن يستخدموا هذا الإعلان لاقتحام الشبكات غير المحمية. وحرص على تذكر الاسم الخاص بمعرف مجموعة الخدمات (SSID) بحيث يمكنك الاتصال يدوياً. وقم بإيقاف آلية الإعلان عن اسم التعريف إذا كانت تعمل بالفعل في جهاز الراوتر.

4. قم بتغيير اسم التعريف الخاص بجهاز الراوتر من ضبط المصنع: من المحتمل أن يكون اسم التعريف الخاص بجهاز الراوتر اسماً موحداً من ضبط المصنع لجميع الوحدات التي تنتمي لنفس الطراز. حتى وإن لم يكن جهاز الراوتر الخاص بك يقوم بإرسال اسم التعريف للنطاق المحيط به، فإن القراصنة يعلمون أسماء التعريف الموحدة ويمكنهم أن يستخدمونها في محاولة للدخول على شبكتك. قم بتغيير اسم التعريف الخاص بك لشيء تعرفه أنت فقط، وتذكر أن تضبط نفس اسم التعريف على الراوتر اللاسلكي والحاسب الآلي بحيث يتمكننا من الاتصال. واستخدم كلمة مرور تتكون من عشرة أرقام وحروف ورموز (characters) على الأقل. وكلما طالت كلمة المرور كلما تعذر على القراصنة استنتاجها.

5. قم بتغيير كلمة المرور المضبوطة مسبقاً على الراوتر لأغراض التحكم: من المحتمل أن يكون مصنع الراوتر اللاسلكي الخاص بك قد قام بعمل كلمة مرور موحدة تسمح لك بضبطه وتشغيله. ونظراً لأن القراصنة يعرفون كلمات المرور، ينبغي عليك تغييرها إلى شيء تعرفه أنت فقط. وكلما طالت كلمة المرور كلما تعذر استنتاجها.

6. لا تسمح سوى لحواسب آلية معينة بالدخول على شبكتك اللاسلكية: كل حاسب آلي قادر على الاتصال بأي شبكة تخصص له عنوان فريد للتحكم في الدخول على الوسائط (MAC). وعادة ما تتمتع أجهزة الراوتر اللاسلكية بآلية لا تسمح بالدخول على الشبكة إلا للأجهزة التي يكون لها عنوان من هذا النوع. ولكن بعض القراصنة لديهم عناوين مقلدة، لذا ينبغي ألا تعتمد على هذه الخطوة وحدها.

7. أوقف تشغيل شبكتك اللاسلكية إذا كنت تعلم أنك لن تستخدمها: لا يستطيع القرصنة الدخول على جهاز الراوتر اللاسلكي إذا كان مغلقاً. فإذا أغلقت الراوتر في أوقات عدم استخدامه فإنك سوف تقلل الوقت الذي قد يتعرض فيه للقرصنة.

8. لا تفترض أن شبكات الإنترنت اللاسلكي العمومية (hot spots) آمنة: العديد من المقاهي والفنادق وغيرها من المنشآت العامة توفر شبكات لاسلكية كي يستخدمها عملاؤها. وهذه الشبكات تقدم خدمة ملائمة ولكنها قد لا تكون آمنة. ويمكنك أن تسأل مالك المكان عن التدابير الأمنية المطبقة.

9. انتبه للمعلومات التي تطلع عليها أو ترسلها وأنت تستخدم الشبكات العامة اللاسلكية: لكي تظل في أمان، افترض أن المستخدمين الآخرين يستطيعون الإطلاع على المعلومات التي تتطلع عليها وترسلها عبر الشبكات العامة اللاسلكية. فإذا لم تتمكن من التأكد من مستوى الأمان الذي تطبقه الشبكة العامة اللاسلكية، قد يستحسن أن تتجنب إرسال المعلومات الحساسة أو استقبالها عبر تلك الشبكة.

مسرد

التشفير (encryption): تشويش البيانات بشكل سري لا يمكن قراءته إلا باستخدام برنامج لفك شفرة المعلومات.

معرف مجموعة الخدمات الموسع (ESSID): هو الاسم الذي يخصصه المصنع للراوتر. وقد يكون الاسم موحد يخصصه المصنع لكل الأجهزة التي تنتمي لنفس الطراز. ويستطيع المستخدمون أن يحسنوا درجة الأمان بتغيير هذا الاسم إلى اسم فريد يتشابه مع الاسم الخاص بمجموعة الخدمات (SSID).

الحائط الناري: هو البرنامج أو الجهاز المصمم لمنع القرصنة من استخدام حاسبك الآلي لإرسال معلوماتك الشخصية دون إذنك. والحائط الناري يراقب المحاولات الخارجية للنفاذ إلى نظامك ويسد الطريق أمام أي اتصالات مع المصادر التي لا تسمح بها إرسالاً واستقبالاً.

التحكم في الدخول على الوسائط (MAC): هو عبارة عن رقم فريد يخصصه المصنع لكل حاسب آلي أو أي جهاز آخر موصل بالشبكة.

جهاز التوجيه "الراوتر" (router): هو جهاز يوصل شبكتين أو أكثر. ويعمل الراوتر على إيجاد أفضل طريق لإرسال المعلومات عبر الشبكات.

الخصوصية المكافئة للإنترنت السلبي (WEP): هي بروتوكول أمني يشفر البيانات التي يتم إرسالها واستقبالها عبر الأجهزة اللاسلكية ضمن شبكة ما. وهذا البروتوكول أقل في قوته عن التشفير من نوع (WPA).

الدخول المحمي على الإنترنت اللاسلكي (WPA): هو بروتوكول أمني مصمم لمعالجة العيوب الموجودة في بروتوكول (WEP). وهو يشفر البيانات التي يتم إرسالها واستقبالها عبر الأجهزة اللاسلكية اللاسلكية ضمن شبكة ما.

الشبكة اللاسلكية: هي وسيلة للوصول إلى الإنترنت فائقة السرعة دون توصيل الحاسب الآلي بالكابلات

1- استخدم التشفير للتشويش على من يحاولون الدخول على شبكتك. وإذا كان في وسعك الاختيار، فاعلم أن الدخول المحمي على الإنترنت اللاسلكي ((WiFi Protected Access (WPA)) يعد أقوى من الخصوصية المكافئة للإنترنت السلبي ((Wired Equivalent Privacy (WEP)).

2 - استخدم برامج مكافحة الفيروسات وبرامج مكافحة برامج التجسس واستخدم حائط ناري.

3- معظم أجهزة التوجيه (الراوتر) تتمتع بآلية تسمى الإعلان عن اسم التعريف (identifier broadcasting). يمكنك إيقاف هذه الخاصية بحيث لا يرسل حاسبك الآلي إشارات لأي جهاز في المنطقة ليعرفه بوجوده.

4- قم بتغيير اسم التعريف (identifier) في جهاز الراوتر من ضبط المصنع بحيث لا يستطيع القرصنة استخدام اسم التعريف حسب ضبط المصنع للدخول على شبكتك.

5- غير كلمة المرور المضبوطة مسبقاً على الراوتر إلى كلمة مرور تعرفها أنت فقط. وكلما طالت كلمة المرور كلما تعسر استنتاجها.

6 - اسمح لأجهزة معينة فقط بالدخول على شبكتك اللاسلكية.

7- أوقف الشبكة اللاسلكية إذا كنت تعرف أنك لن تستخدمها.

8- يجب ان لا نفترض أن الإنترنت اللاسلكي العمومي (hot spots) آمن، فقد يكون هناك من

يستطيعون الإطلاع على المعلومات التي تطلع عليها أو ترسلها عبر الشبكة اللاسلكية.

9 -يجب حفظ المودمات وأجهزة الربط بعيدا عن الأيدي.

10_ في حالة استخدام الشبكات الخاصة في العمل أو في مكان يمكن للناس الوصول للمودم فهذا سيشكل خطراً.

11- تأمين الاعدادات الخاصة بالمودمات

يجب أن نتعلم كيف ندخل على صفحة الإعدادات الخاصة بالمودم. وغالبا تفتح صفحة الإعدادات بالدخول على المتصفح (كروم أو فايرفوكس أو غيرها) وتكتب في شريط العنوان عنوان المودم وهو غالبا يكون بالشكل هذا "192.168.1.1" أو "10.0.0.137" على حسب نوع المودم، وتدخل اسم المستخدم وكلمة المرور. وتجد هذه المعلومات غالبا على ظهر المودم أو في دليل المستخدم. وبإمكانك البحث في قوقل عن نوع المودم وستجد كل التفاصيل.

12- وضع كلمة المرور على المودم

المودم يأتي باسم مستخدم وكلمة مرور افتراضية (غالبا تكون admin / password) وهذه تكون للإعدادات وليست للاتصال بالشبكة ولذلك قد يستطيع أحد الدخول لصفحة الإعدادات فيجب تغييرها مباشرة من إعدادات المودم إلى كلمة مرور صعبة التخمين (لا تضع رقم جوالك!).

13- تغيير الاسم الافتراضي للشبكة

اسم الشبكة أو SSID غالبا يكون اسم الشركة المنتجة للمودم (مثلا Netgare) ويفضل تغيير اسم الشبكة إلى شيء آخر تميز فيه شبكتك عن غيرها من الشبكات ويجب ألا يكون اسم الشبكة يحتوي معلومات خاصة بك مثل اسمك أو رقم جوالك أو عنوانك. وغالبا يكون تغيير اسم الشبكة في إعدادات الوايرلس wireless settings.

14- تشفير الشبكة / الإشارة (الأكثر أهمية)

أهم إجراء يجب أن نتخذه لحماية الشبكة اللاسلكية هو تشفير الإشارة. ويوجد العديد من طرق التشفير أشهرها WEB وهي ضعيفة جدا ويمكن كسرها بسهولة لكن ميزتها ان أغلب الأجهزة القديمة والحديثة تدعم النوع هذا من التشفير. والأكثر أمانا هو WPA2 لكن مشكلته لا يعمل على الأجهزة القديمة المصنعة قبل عام 2006 .

ولتفعيل التشفير ادخل على صفحة الإعدادات وغالبا ستجد خيار تشفير الإشارة في قسم wireless security settings اختر النوع الذي تريد (ينصح بـ WPA2) واختر كلمة مرور صعبة التخمين ويجب لا أن لا يتم وضع المعلومات البديهية مثل أرقام الهواتف.

15- حدد الـ MAC الخاصة بالشبكة.

لكل جهاز إلكتروني متصل بالشبكة عنوان خاص فيه يأتي مع الجهاز من المصنع يسمى MAC (ليس له علاقة بأبل ماكنتوش) ويمكنك تحديد عناوين أجهزتك المسموح لها الاتصال بالشبكة لإضافة مزيد من الحماية وبالتالي أي جهاز آخر غير مسجل في المودم لا يمكنه الإتصال بالشبكة. ولأنه لا يوجد حماية 100% يستطيع الهاكرز باستخدام بعض الأدوات تغيير عناوين أجهزتهم ويصبح من ضمن القائمة المسموح بها. لكن يجب عليه أولا أن يعرف عنوان أحد أجهزتك لينسبه إلى جهازه.

ولإعداد هذه الخاصية اعمل قائمة بالأجهزة التي تريد أن تسمح لها بالإتصال بالشبكة سواء كانت حاسبات أو جوالات أو غيرها، ثم احصل على عناوينها الخاصة (MAC) وأضفها في اعدادات المودم وغالبا ستجدها في إعدادات الحماية settings security. وبإمكانك معرفة الأجهزة المتصلة بالمودم من صفحة الخيارات. ستجد

جدول يحتوي على عناوين الأجهزة المتصلة بالشبكة وبإمكانك حظر الجهاز الذي لا تعرفه. وبإمكانك استخدام أداة مثل AirSnare لتعرف الأجهزة المتصلة بشبكتك.

16- إغلاق المودم عند الانتهاء من استعماله.

من الجيد أن نقوم بإغلاق المودم عندما لا نستخدمه لفترة طويلة مثل وقت النوم أو خروجك للعمل فهذا يقلل نسبة المخاطرة كثيراً.

17- يجب ان نحرص دائماً على تحديث الـ firmware للحصول على حماية أكبر وكذلك العديد من المميزات الإضافية .

الخاتمة

الحمد لله الذي وفقني على إتمام هذا الكتاب الذي فرضته تحديات أمن المعلومات والاتصالات
لما لها من عظيم أثر في حياة المجتمعات والهيئات والأشخاص الذين يتواجدون ضمن منظومة
واحدة.

تم تناول هذا الموضوع على مستويات عدة شملت مفاهيم أمن المعلومات والاتصالات
والمخاطر والمهددات والثغرات الأمنية وكيفية مراقبتها لمنع أثرها السالبة وماهية الأدوات
والطرق المستخدمة في منعها.

كما تم تناول وتصنيف الشبكات اللاسلكية وطرق تصنيفها ووسائط وأجهزة الربط المستخدمة
فيها ، كما تم تناول بعض السبل والنصائح لحماية الشبكات وذلك باقفال الثغرات الأمنية ، كما
أتمنى ان أجد النصح والتوجيه للمادة العلمية وطرق الاعداد المستخدمة في هذا الكتاب من
الباحثين والعلماء على موقعي الالكتروني www.facebook.com/kamal.yousif.144

أو على بريدي الالكتروني km77_it@yahoo.com

وآخر دعوانا أن الحمد لله رب العالمين

المصادر والمراجع

1.المصادر:

القراءن الكريم ، سورة الفرقان الآيات 61 –67.

2.المراجع العربية:

1.سامي محمد شريف عبدالله، أمن الحواسيب، جامعة السودان المفتوحة،الأولى،2008م

2.أنس الطويلة، أمن الشبكات اللاسلكية،2008م

3.المراجع الأجنبية:

1. Richard Johnson، Wireless Security Vulnerabilities.

2.Chassaing (J-F) L Intent etle droit penal Recueil Dalloz Sirey ,1996.

4.المواقع الإلكترونية:

[1]http://www.streetdirectory.com/travel_guide/2497/computers_and_the_internet/the_security_risks_and_ways_to_decrease_vulnerabilities_in_a_80211b_wireless_environment.html 21/06/2010

[2] [http://www.manageengine.com/wireless-network-management/adhoc-network-in-](http://www.manageengine.com/wireless-network-management/adhoc-network-in-operation.html)

[operation.html](http://www.manageengine.com/wireless-network-management/adhoc-network-in-operation.html) 02/07/2012

[3] <http://www.wireless-center.net/Wi-Fi-Security/1737.html> 13/03/2012

[4]www.itrainonline.org/itrainonline/mmtk 7/04/2012

[5] http://www.wifi.com/how_why.html 11/06/2012

[6] http://ar.wikipedia.org/wiki/Wireless_networks 20/06/2012

[7] <http://www.secure-webz.com/ebooks/Networks-Security.pdf> 15/06/2012

[8] www.kutube.info 09/05/2012



المؤلف في سطور

كمال الدين يوسف يسن محمد.

من مواليد شمال كردفان الحمرة 1977.

درس المراحل الأولية للتعليم بالحمرة.

درس المتوسط والثانوي بحلفاية الملوك.

أكمل تعليمه الجامعي بكل من جامعة أدرمان الإسلامية وجامعة السودان للعلوم والتكنولوجيا (1997-2001).

درس الدبلوم العالي في تقنية المعلومات في جامعة النيلين 2004م.

حصل على درجة الماجستير في علوم الحاسوب من جامعة الجزيرة 2007م.

حصل على درجة الدكتوراة في تقنية المعلومات بدرجة إمتياز من جامعة جون هيفر في بريطانيا 2010م.

عمل مساعد تدريس بجامعة النيلين (2003-2005).

عمل محاضراً لمواد الحاسوب وتقنية ونظم المعلومات بعدد من الجامعات والكليات السودانية (2006-2009).

عمل أستاذ مساعد بعدد من الجامعات السودانية.

يعمل الآن أستاذ مساعد للحاسوب وتقنية المعلومات بسلطنة عمان .

منشورات وأوراق علمية:

- إعداد مشاريع التخرج لطلاب برنامج الحاسوب مشترك مع الدكتور يس بابكر أحمد.
- قام بإعداد منهج تقنية المعلومات لكلية بحري الأهلية .

مؤلفات تحت الطبع:

- ❖ أساسيات الفيچوال بيسك.
- ❖ الفيچوال بيسك للمحترفين.
- ❖ البحث العلمي لطلاب الحاسوب وتقنية المعلومات.
- ❖ الشبكات التخيلية الخاصة.
- ❖ جرائم المعلوماتية (أدوات الجريمة وطرق الإثبات).

الإشراف على الرسائل العلمية:

أشرف على مايقارب 300 رسالة تخرج بكالوريوس ، ساهم في إعداد وتحكيم عدد من أطروحات الماجستير والدكتوراة.

الخبرات والمهارات:

- قام بالإشراف وتركيب عدد من الشبكات، تصميم عدد من مواقع الانترنت وبناء النظم.
- مدرب حاسوب معتمد لبرنامج جامعة كامبردج لتقنية المعلومات.