

العنوان:	مقارنة بين خوارزميات التعمية الحديثة
المؤلف الرئيسي:	المحمد، جمعة علي
مؤلفين آخرين:	شعار، أحمد اديب، الكيالي، علي عادل(مشرف)
التاريخ الميلادي:	2002
موقع:	حلب
الصفحات:	1 - 113
رقم MD:	576280
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة حلب
الكلية:	كلية الهندسة الكهربائية والإلكترونية
الدولة:	سوريا
قواعد المعلومات:	Dissertations
مواضيع:	الهندسة الالكترونية، هندسة الاتصالات، الخوارزميات
رابط:	<a href="http://search.mandumah.com/Record/576280">http://search.mandumah.com/Record/576280</a>

جامعة حلب  
كلية الهندسة الكهربائية والإلكترونية  
قسم هندسة الاتصالات



## مقارنة بين خوارزميات التعمية الحديثة

بحث معد لنيل درجة الماجستير في الهندسة الإلكترونية/هندسة الاتصالات/

إعداد

المهندس جمعة علي المحمد

إشراف

الدكتور أحمد أديب شعار


محاضر في قسم هندسة الاتصالات  
كلية الهندسة الكهربائية والإلكترونية  
جامعة حلب

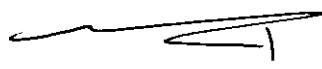
الدكتور علي عادل كيالي

أستاذ في قسم هندسة الاتصالات  
كلية الهندسة الكهربائية والإلكترونية  
جامعة حلب

## شهادة

أشهد أن هذا العمل الموصوف في هذه الرسالة هو نتيجة بحث قام به المرشح المهندس جمعة علي محمد تحت إشراف كل من الأستاذ الدكتور علي عادل كيالي والدكتور أحمد أديب شعار من قسم هندسة الاتصالات كلية الهندسة الكهربائية والإلكترونية بجامعة حلب، وأي رجوع إلى بحث آخر في هذا الموضوع موثق في النص.

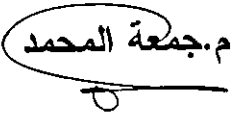
المشرف  
أ.د.م. علي عادل كيالي  


المشرف  
د.م. أحمد أديب شعار  


المرشح  
م. جمعة المحمد  





## تصريح

أصرح بأن هذا البحث "مقارنة بين خوارزميات التعمية الحديثة" لم يسبق أن قبل للحصول على أية شهادة ولا هو مقدم حالياً للحصول على شهادة أخرى.

المرشح  
م. جمعة المحمد  


اعضاء لجنة الحكم

- 1- أ.د. محمد عادل كيالي
- 2- أ.د. محمد أديب شعار
- 3- أ.د. محمد أديب شعار



## كلمة شكر

بعد أن انتهيت من هذا البحث أتقدم بجزيل الشكر إلى الأستاذ الدكتور المهندس علي عادل كيالي والدكتور المهندس أحمد أديب شعار الذين أشرفا على إنجاز هذه الرسالة وقدموا لي العون والمساعدة في ذلك، كما أتوجه بالشكر إلى لجنة التحكيم المؤلفة من السادة: الأستاذ الدكتور المهندس علي عادل كيالي والأستاذ الدكتور المهندس جورج صنيح والأستاذ الدكتور المهندس سامي حاجي علي لقبولهم مناقشة هذه الرسالة.

كما لا يسعني إلا أن أشكر أساتذتي في كلية الهندسة الكهربائية والإلكترونية بجامعة حلب جميعهم، وكل من مدّ لي يد العون لإنجاز هذه الرسالة متمنياً للجميع مزيداً من التقدم والنجاح.

الطالب المهندس

جمعة أحمد

# الإهداء

إلى المخلصين جميعهم في هذا العالم

إلى مثلي الأعلى، الذي رحل قبيل مناقشة هذه الرسالة بأيام قلائل، والذي

الكريم، رحمه الله وأسكنه فسيح جناته.

# المحتويات

I.....	المحتويات
١.....	مقدمة

## الفصل الأول: نظرة شمولية على أمن شبكات المعلومات

٥.	Overview of Information Network Security
٦.....	مقدمة

### ١-١ الهجمات والخدمات والآليات

١٠.....	: ATTACKS, SERVICES, AND MECHANISMS
١٠.....	:SERVICES الخدمات ١-١-١
١٢.....	:CONFIDENTIALITY الكتمان
١٣.....	:AUTHENTICATION التّأصيل
١٣.....	:INTEGRITY السلامة
١٤.....	:NONREPUDIATION عدم التّصل
١٤.....	:ACCESS CONTROL التّحكم بالوصول
١٥.....	:AVAILABILITY الإتاحة

١٥.....	:MECHANISMS الآليات ٢-١-١
---------	---------------------------

١٥.....	:ATTACKS الهجمات ٣-١-١
---------	------------------------

٢٠.....	:PASSIVE ATTACKS الهجمات السلبية ١
---------	------------------------------------

٢١.....	:ACTIVE ATTACKS الهجمات الإيجابية ٢
---------	-------------------------------------

٢٢.....	:A MODEL FOR NETWORK SECURITY نموذج لأمن الشبكات ٢-١
---------	--

## الفصل الثاني: منظومات التعمية التقليدية

### ٢٧..... Conventional Cryptographic Systems

٢٨.....	مقدمة
---------	-------

### ١-٢ منظومات التعمية المتماثلة الكلاسيكية CONVENTIONAL

٢٩.....	:CRYPTOGRAPHY ( CLASSICAL TECHNIQUES)
---------	---------------------------------------

٢٩.....	:TRANSPOSITION CIPHERS معميات إبدال الموقع ١-١-٢
---------	--

٣٠.....	:SUBSTITUTION CIPHERS معميات الإعاضة ٢-١-٢
---------	--

### ٢-٢ منظومات التعمية المتماثلة الحديثة

٣٤.....	:CONVENTIONAL CRYPTOGRAPHY (MODERN TECHNIQUES)
---------	--

٣٤.....	:DATA ENCRYPTION STANDARD (DES) معيار تعمية المعطيات ١-٢-٢
---------	--

٢-٢-٢ الخوارزمية العالمية لتعمية المعطيات

٣٦.....:International Data Encryption Algorithm (IDE A)

٣٧.....:TRIPLE -DES معيار تعمية المعطيات الثلاثي

## الفصل الثالث: تعمية المفتاح العمومي والتعمية التقليدية

٣٩.. Public-Key Cryptography & Conventional Cryptography

٤٠.....مقدمة

٤١.....١-٣ مبادئ منظومات تعمية المفتاح العمومي:

٤٢.....٢-٣ منظومات تعمية المفتاح العمومي والتعمية التقليدية:

٤٩.....٣-٣ تطبيقات منظومات تعمية المفتاح العمومي

٥٠.....٤-٣ متطلبات تعمية المفتاح العمومي:

٥٢.....٥-٣ تحليل تعمية المفتاح العمومي:

## الفصل الرابع: منظومات تعمية المفتاح العمومي

٥٤..... Public-Key Cryptographic Systems

٥٥.....مقدمة

٥٦.....١-٤ منظومات العوامل الصحيحة:

٥٦..... خوارزمية (Rivest, Shamir and Adleman) R.S.A

٦٣.....٢-٤ منظومات اللوغاريتم المنقطع DISCRETE LOGARITHM SYSTEMS:

٦٣.....١-٢-٤ خوارزمية الجمل ELGAMAL ALGORITHM:

٦٥.....٢-٢-٤ معيار التوقيع الرقمي (DIGITAL SIGNATURE STANDARD) DSS:

٣-٤ منظومة تعمية المنحني الإهليلجي

٦٦..... THE ELLIPTIC CURVE CRYPTO SYSTEM

٦٨.....٤-٤ مقارنات COMPARISONS:

٦٨.....١-٤-٤ مقارنة سويات الأمن COMPARISON OF SECURITY LEVELS:

٦٩.....٢-٤-٤ مقارنة حجم المفتاح COMPARISON OF KEY SIZE:

٦٩.....٣-٣-٤ مقارنة عرض الحزمة COMPARISON OF BAND WIDTH:

## الفصل الخامس: نظرية المنحني الإهليلجي

٧١..... The Elliptic Curve theory

٧٢.....١-٥ المنحني الإهليلجي على الأعداد الحقيقية:

٧٢.....تعريف:

٧٣.....١-١-٥ الجمع في المنحني الإهليلجي بالطريقة الهندسية:

٧٤	..... جمع نقطتين متميزتين $P, Q$ : .....
٧٥	..... جمع النقطتين $P, -P$ : .....
٧٦	..... مضاعفة النقطة $P$ : .....
٧٨	..... مضاعفة النقطة $P$ إذا كان $YP=0$ : .....
٧٨	..... ٢-١-٥ الجمع في المنحني الإهليلجي بالطريقة الجبرية: .....
٧٩	..... جمع نقطتين متميزتين $P, Q$ : .....
٨٠	..... مضاعفة النقطة $P$ : .....
٨١	..... ٢-٥ المنحني الإهليلجي على الحقول المحدودة: .....
٨١	..... ١-٢-٥ مجموعة المنحني الإهليلجي على الحقل $F(P)$ : .....
٨٤	..... مضاعفة النقطة $P$ : .....
٨٥	..... ٢-٢-٥ مجموعات المنحني الإهليلجي في الحقل $F2^M$ : .....
٨٧	..... الحسابات في مجموعة المنحني الإهليلجي وفق الحقل $F2^M$ : .....

## الفصل السادس: استخدام المنحني الإهليلجي في التعمية

### ٩٤ ..... Elliptic Curve in Cryptography

٩٥	..... مقدمة .....
٩٥	..... ١-٦ ايجاد اللوغاريتم المنفصل DISCRETE LOGARITHM : .....
٩٨	..... ٢-٦ تنفيذ عملية تبادل المفاتيح (KEY EXCHANGE) باستخدام المنحنيات الإهليلجية: .....
٩٩	..... ٣-٦ التعمية باستخدام المنحني الإهليلجي: .....
١٠٧	..... ٤-٦ تطبيقات الـ ECC (ELLIPTIC CURVE CRYPTOGRAPHY): .....
	..... ١-٤-٦ التطبيقات التي تحتاج تشغيل مفتاح عمومي بشكل مركز
١٠٧	..... : APPLICATIONS REQUIRING INTERSIVE PUBLIC- KEY OPERATIONS .....
	..... ٢-٤-٦ التطبيقات المتلازمة مع قنوات مقيدة
١٠٧	..... : APPLICATIONS INVOLVING CONSTRAINED CHANNELS .....
١٠٨	..... ٣-٤-٦ استخدام البطاقات الذكية Use of smart cards : .....
١٠٩	..... ٥-٦ معايير الـ ECC STANDARDS: ECC : .....

## ١١٠ ..... الفصل السابع: النتائج والمناقشة

١١١	..... ١-٧ أداء النواة البرمجية المقترحة: .....
١١١	..... ١-١-٧ خوارزمية ايجاد اللوغاريتم المنفصل: .....
١١١	..... ٢-١-٧ خوارزمية التعمية: .....
١١٢	..... ٢-٧ الخلاصة: .....
١١٣	..... ٣-٧ المقترحات: .....



i .....	المصطلحات
viii.....	المراجع

## مقدمة

يعرف علم التعمية (Cryptography) بأنه علم دراسة الكتابة المعماة (السرية). حيث تستخدم طريقة سرية للكتابة Cipher من أجل تحويل نص صريح (Plaintext) إلى نص معمي Ciphertext، والذي يدعى في بعض الأحيان Cryptogram، وتدعى عملية تحويل النص الصريح إلى نص التعمية بعملية التعمية Encyption (أو Encipherment)، بينما تدعى العملية العكسية الهادفة إلى تحويل النص المعمي إلى نص صريح بعملية الإظهار Decryption (أو Decipherment). ويتم التحكم بكلتا عمليتي التعمية والإظهار بواسطة مفاتيح تعمية (Cryptographic Keys) [22].

لقد أصبح أمن المعلومات information security في غاية الأهمية لاسيما بعد دخول الحاسوب واستخدام الشبكات ووسائل الاتصالات لنقل المعطيات وقد استخدمت آليات متعددة لتقديم الخدمات الأمنية ولكن الأساس لمعظم هذه الآليات هو تقنيات التعمية. إننا نعيش اليوم عصر الإنترنت والتجارة الإلكترونية التي تعتمد بشكل أساسي على أمن شبكات المعلومات والتعمية والتوقيعات الرقمية حيث ظهرت تطورات هائلة في تكنولوجيا أمن اتصالات الحواسيب و لاسيما خوارزميات التعمية.

إلا أنه هناك خطورة بالغة في البرمجيات الأمنية المستوردة التي تنفذ عملية التعمية والتوقيع الرقمي، لأنهم عندما يصدرونها إلينا يكونون قد ابتدعوا طريقة كسر هذه المعميات وصنعوا برمجيات التعمية الأفضل والأصعب كسراً.

وقبل الخوض في علم الاتصالات المعماة لابد لنا من كلمة نعطي فيها للتاريخ

بعض حقه المهضوم في هذا المجال.

فمن الناحية التاريخية، يمكننا القول: إن تقنيات أمن الاتصال قديمة قدم التاريخ، فمن المعروف أن يوليوس قيصر استخدم إحدى طرق التعمية وذلك بإزاحة موقع كل حرف من أحرف الرسالة المراد تعميئها إلى الأمام بمقدار  $k$  موقعاً حيث تتم الإزاحة بشكل حلقي، بيد أن علم الاتصالات المعماة Cryptography تبلور بشكل موثق لأول مرة على يد العرب، ومن ضمن مصطلحات الرياضيات العربية انتقلت كلمة صفر Cipher إلى الغرب.

وفيه استخدمت لتعني مشفر (مُعَمِّي) نظراً لعدم احتوائها على معلومات للطرف غير المخول. وقد أشارت دراسة ديفيد كان إلى أن أول دراسة كاملة عن علم الاتصال المعمي مكتوبة كجزء من موسوعة "صبح الأعشى" التي ألفها العالم العربي شهاب الدين أبي العباس أحمد بن علي بن أحمد بن عبد الله القلقشندي، الذي اعتمد في كتابه ذلك الجزء على مؤلفات العلامة العربي تاج الدين علي بن محمد بن عبد العزيز الثعالبي الموصللي الملقب بابن الدريهم وأهمها "مفاتيح الكنوز في إيضاح المرموز" الذي عاش بين العام ١٣١٢ و١٣٦١ للميلاد.

وقد أثبتت الدراسات الحديثة أن علم الاتصالات المعماة قد ظهر قبل ابن الدريهم بخمسة قرون وذلك على يد العلامة العربي يعقوب ابن إسحاق الكندي (٧٣٠م) وأشهر أعماله "رسالة في استخراج المعمي" [22].

يهدف هذا البحث إلى كتابة نواة لبرمجيات تقوم بالتعمية باستخدام الخوارزميات الجديدة المسماة بـ Elliptic Curve Cryptography (ECC) التي تعتبر حالياً أحدث طرق التعمية بالمفتاح العمومي في العالم، وتمتاز عن غيرها بالسرعة الأكبر وحجم المفاتيح الأصغر والذاكرة الأقل مع تقديم مستوى أمني مساو لما تقدمه سواها.

يقدم هذا البحث نواة برمجية تعتمد على خوارزمية تعمية المنحني الإهليلجي Elliptic Curve Cryptography (ECC)، لأن هذه الخوارزمية أصبحت معيارية

واعتمدت من قبل الـ IEEE في شهر شباط من عام ٢٠٠٠، وتعد اليوم الخوارزمية الأسرع والأفضل أداءً من بين خوارزميات التعمية المفتاح العمومي (public-key cryptographic algorithms) المعروفة. ويبين هذا البحث أنه يمكننا إنشاء صناعة برمجية أمنية وطنية وتلافي الخطورة التي تكمن في البرمجيات المستوردة.

ونظراً لأن تعمية المنحني الإهليلجي تعتمد على رياضيات المنحني الإهليلجي، لذلك فقد دراسنا تطبيق هذه الرياضيات على الأعداد الحقيقية وفي الحقول المحدودة.

تعد صناعة برمجيات أمن المعلومات إحدى التحديات الكبرى التي تواجه البلدان النامية ومن بينها بلدنا، نظراً للخطورة البالغة التي تكمن في الاعتماد على البرمجيات الأمنية المستوردة، لأن الأمن الوطني لأي بلد مرتبط بمدى تطوره في مجال تكنولوجيا أمن المعلومات والاتصالات. ويبين الباحث أنه يمكننا إنشاء صناعة برمجية أمنية وطنية وتلافي الخطورة الكامنة في البرمجيات المستوردة. وإن هذا العمل يحتاج إلى فريق متكامل من المتخصصين في رياضيات أمن المعلومات ومن المبرمجين المحترفين، وهو بعمله هذا يضع اللبنة الأولى لهذا البنيان.

قام الباحث بتنفيذ البحث من خلال محورين رئيسيين:

١. المحور الأول: دراسة تحليلية لخوارزميات التعمية الحديثة وإجراء مقارنة بينها، ثم اختيار الأجود.

٢. المحور الثاني: كتابة نواة برمجية أمنية وفق الخوارزمية الأفضل، تقوم بعملية التعمية.

يتألف البحث من مقدمة وسبعة فصول، في الفصل الأول تم إلقاء نظرة شمولية على أمن شبكات المعلومات Information network security واستعراض المظاهر الرئيسة لها، أما في الفصل الثاني فتم استعراض التعمية المتماثلة Symmetric بنوعيتها:

▪ التعمية التقليدية (التقنيات الكلاسيكية)

Conventional cryptography (Classical techniques)

▪ التعمية التقليدية (التقنيات الحديثة)

.Conventional cryptography ( Modern techniques)

والفصل الثالث يقارن بين تعمية المفتاح العمومي public-key cryptography والتعمية التقليدية conventional cryptography. أما الفصل الخامس فيتضمن دراسة خوارزميات تعمية المفتاح العمومي public-key cryptographic algorithms مع إجراء مقارنة بينها وتحديد الأجود.

الفصل الخامس يلقي الضوء على نظرية المنحني الإهليلجي Elliptic Curve theory، أما في الفصل السادس فتم التعرض إلى استخدام خوارزمية المنحني الإهليلجي في التعمية، وكذلك التطبيقات العملية للـECC، وأخيرا الفصل السابع يتضمن تقييما لأداء النواة البرمجية المقترحة من وجهة نظر السرعة، كما يقدم اختبارات تؤكد وثوقية عملية التعمية، وكذلك خلاصة البحث والمقترحات لمن أراد إتمام ما توصل إليه وتطويره وكذلك يبين أسباب اختيار لغة Visual Basic.

## الفصل الأول

### نظرة شمولية على أمن شبكات المعلومات

#### Overview Of Information Network Security

٥٦٣٤٧٦

في هذا الفصل:

١-١	الهجمات Attacks والخدمات Services والآليات Mechanisms
١-١-١	الخدمات Services
٢-١-١	الآليات Mechanisms
٣-١-١	الهجمات Attacks
٢-١	نموذج لأمن الشبكات A Model for Network Security

## مقدمة:

تطلب أمن المعلومات Information Security في أية منظمة سواء كانت عسكرية أو مدنية، تغييرين رئيسيين في العقود الأخيرة الماضية. فأهمية معلومات منظمة ما وعلى سبيل المثال تلك التي تستخدم وسائل أمنية فيزيائية ووسائل أمنية إدارية تنظيمية أصبح ضرورياً بعد الاستخدام الواسع لجهاز معالجة المعطيات. من الأمثلة على الوسائل الفيزيائية استخدام خزائن ملفات عديدة ذات أقفال مركبة لتخزين الوثائق الحساسة. ومن الأمثلة على الوسائل الإدارية التنظيمية، القيام بإجراءات تفتيش على الموظفين.

أمن الحواسيب Computer Security هو الاسم العام لمجموعة الأدوات المصممة لحماية المعطيات ولإعاقة الخراقين Hackers. فبعد انتشار الحاسوب، برزت الحاجة إلى أدوات مؤتمتة لحماية الملفات والمعلومات الأخرى المخزنة في الحاسوب، خصوصاً في حالة المنظومة المتقاسمة، كما في حالة المنظومة المتقاسمة زمنياً. كما تكون الحاجة أكثر إلحاحاً من أجل المنظومات التي يمكن دخولها عبر الهاتف العام وشبكة المعطيات [1].

التغير الأساسي الثاني الذي أثر على أمن المعلومات، هو إدخال المنظومات الموزعة واستخدام الشبكات ووسائل الاتصالات لنقل المعطيات بين المستخدم الطرفي والحاسوب وبين الحاسوب وحاسوب آخر [6]. فهناك حاجة لإجراءات أمن الشبكات Network Security لحماية المعطيات أثناء إرسالها. ومن البديهي أن مصطلح "أمن الشبكات" يعتبر مضملاً إلى حد ما لأن جميع المنظمات التجارية والحكومية والأكاديمية،

تربط أجهزة معالجة معطياتها، بشكل عملي مع عدد من الشبكات الموصولة مع بعضها البعض. وبشكل عام تدعى هذه المجموعة شبكة متداخلة internet (\*) [1].

في الواقع ليس هناك حدود واضحة بين هذين الشكلين من أشكال الأمن، أمن الحواسيب وأمن الشبكات المتداخلة. فمثلا: يعد فيروس الحاسوب أحد أهم النماذج العامة التي تهاجم منظومات المعلومات. فالفيروس يمكنه اختراق أية منظومة فيزيائيا على القرص Diskette وتلقائيا يجد مكانه في الحاسوب أو أن تدخل الفيروسات عبر الشبكة المتداخلة internet. في كلتا الحالتين يكون الفيروس مقيما في منظومة الحاسوب وعندئذ فنحن بحاجة إلى أدوات أمن الحاسوب الداخلية لكشف الفيروس والتخلص منه [1].

عند دراسة أمن الشبكات المتداخلة internet Security يتم التركيز على الإجراءات لإعاقه ومنع والتقاط وتصحيح مخالفات الأمن المتعلقة بإرسال المعلومات. وبناء على هذا فإن أمن الشبكات يشمل مجالا فسيحا من العمليات، ولناخذ الأمثلة التالية على مخالفات الأمن بعين الاعتبار [1]:

١. يرسل المستخدم A ملفا إلى المستخدم B. يحتوي الملف على معلومات حساسة (مثل سجلات دفع payroll records) والتي يجب أن تكون محمية من الافتضاح. بالنسبة للمستخدم C غير المخول بقراءة هذا الملف، بيد أنه قادر على مراقبة الإرسال والتقاط نسخة من الملف خلال عملية إرساله.
٢. يرسل مدير الشبكة، D رسالة إلى الحاسوب E الذي يتحكم بإدارته والتي بموجبها يتم تحديث ملف التحويل للحاسوب E. تأمر الرسالة الحاسوب E بتحديث ملف التحويل وذلك ليتضمن هويات عدد من المستخدمين الجدد الذين سيعطون حق الوصول إلى ذلك الحاسوب. ولكن يعترض المستخدم F سبيل الرسالة ويقوم بتبديل محتوياتها ليضيف أو يحذف بنودا منها،

\*- لقد استخدمنا مصطلح internet بـ "i" صغيرة تمييزا له عن الـ "Internet".



وعندئذ يوجه الرسالة إلى E الذي يتقبل الرسالة كما لو أنها أتت من المدير D ويقوم بتحديث ملف التخويل وفقا لذلك.

٣. وعلاوة على ذلك فلا يكتفي المستخدم F باعتراض الرسالة بل يقوم بإنشاء رسالته الخاصة بالبنود التي يرغبها ويقوم بإرسال تلك الرسالة إلى المستخدم E كما لو أنها أتت من المدير D. ويتقبل الحاسوب E الرسالة كما لو أنها أتت من المدير D مباشرة ويحدث ملف تخويله وفقا لذلك.

٤. عندما يتم تسريح موظف ما دون إنذار فإن مدير شؤون الموظفين يرسل رسالة إلى منظومة المخدم Server ليعطل حساب الموظف. عندما ينهي التعطيل يرسل المخدم ملاحظة إلى ملف الموظف على شكل تأكيد للتعطيل. ولكن الموظف يكون قادرا وللمرة الأخيرة على اعتراض الرسالة وتأخيرها لكي يتمكن من الدخول إلى المخدم لحذف المعلومات الحساسة، ثم إعادة توجيه الرسالة إلى المخدم. وإن عمل هذا الموظف قد لا يكشف إلا بعد مرور فترة ليست بالقصيرة.

٥. عند قيام زبون ما بإرسال الرسالة إلى سمسار البورصة بأوامر معينة من أجل إجراءات مختلفة. وبعد خسارة تلك الاستثمارات ينفي الزبون إرسال تلك الرسالة.

رغم أن هذه القائمة لا تتضمن كل النماذج الممكنة للمخالفات الأمنية إلا أنها

توضح مدى أهمية أمن الشبكات المتداخلة internet security.

أمن الشبكات المتداخلة موضوع ساهر ومعقد في آن واحد. وسنورد فيما يلي

بعض هذه الأسباب [1]:

١. إن موضوع الأمن الخاص بالاتصالات والشبكات ليس بالموضوع البسيط

كما يبدو لأول وهلة للقارئ العادي. وقد تبدو المتطلبات مباشرة، ولكن بالواقع إن معظم المتطلبات الأساسية من أجل خدمات الأمن يمكن أن تقدم لافقات (عناوين) مؤلفة من كلمة واحدة تفسر نفسها بنفسها: الكتمان

confidentiality والتأصيل authentication وعدم التنصل nonrepudiation والسلامة integrity. لكن الآليات mechanisms التي استخدمت لتواجه تلك المتطلبات معقدة تماما لا وبل يحتاج فهمها إلى تعليل عقلي حاذق.

٢. إننا أثناء تطوير آلية أو خوارزمية أمن معينة نعلم إلى إجراءات مضادة counter measures دائما ونستغل نقاط الضعف غير المتوقعة في الآلية. فقد وضعت إجراءات مضادة في كثير من الحالات عن طريق تفحص المشكلة بطريقة مختلفة.

٣. بسبب النقطة (٢)، عادة ما تكون الإجراءات الهادفة إلى تقديم خدمات محددة، من النوع المضاد للحدس counterintuitive: قد لا يكون واضحا من نص متطلب وحيد محدد، الحاجة إلى إجراءات متقنة محكمة. عندما تأخذ الإجراءات المضادة مجراها بعين الاعتبار عندئذ تصبح الإجراءات ذات معنى.

٤. من الضروري أن نقرر أين نستخدم آليات الأمن المختلفة بعد تصميمها، وهذا ينطبق على مجال مصطلحات التوضع الفيزيائي (مثلا: عند أية نقطة من نقاط الشبكة نحتاج إلى آليات أمن محددة) وعلى مجال الحس المنطقي (مثلا: عند أي طبقة أو طبقات من بناء ما مثل TCP/IP، يجب أن توضع الآليات).

٥. إن آليات الأمن تنطوي على أكثر من خوارزمية محددة أو بروتوكول محدد. وعادة تتطلب من المشاركين أيضا بعض المعلومات السرية (مثل مفتاح التعمية encryption key)، التي تثير جوا من التساؤلات حول توليد وتوزيع وحماية تلك المعلومات السرية. وبالاعتماد على بروتوكولات الاتصالات التي يعقد سلوكها عملية تطوير آلية الأمن [1]. وإحدى هذه التعقيدات على سبيل المثال إنها تفرض قيودا زمنية على فترة العبور للرسالة من المرسل إلى المستقبل، وإن أي بروتوكول أو شبكة، تتسبب

بتأخيرات زمنية غير متوقعة يمكنها تحويل هذه القيود الزمنية إلى قيود عديمة النفع.

سنبدأ بمناقشة نماذج الهجمات attacks التي تولد الحاجة إلى خدمات وآليات أمن الشبكات. ثم سنقوم بتطوير نموذج عام وشامل جدا يمكن من خلاله رؤية ومعالجة خدمات وآليات الأمن.

## ١-١ الهجمات Attacks والخدمات Services والآليات Mechanisms:

يحتاج المدير المسؤول عن الأمن إلى طريقة نظامية لتحديد المتطلبات والطرق اللازمة لتحقيق هذه المتطلبات هناك ثلاثة مظاهر لأمن المعلومات [1]:

- مهاجمة الأمن security attack: إن المعلومات الخاصة بمنظمة ما قد تتعرض لخطر مهاجمتها بسبب أي عمل غير مدروس.
- آلية الأمن security mechanism: إن آلية الأمن قد صممت لكشف أو لمنع أو تصحيح الهجمات على الأمن.
- الخدمة الأمنية security service: إن الخدمات الأمنية قد تم تصميمها لمنع الهجمات الأمنية وذلك باستخدام آلية أو أكثر من الآليات الأمنية فهي خدمات تعزيزية لأمن منظومات معالجة المعطيات ولعملية نقل المعلومات لمنظمة ما لا على التعيين.

### ١-١-١ الخدمات Services:

من الممكن النظر إلى خدمات أمن المعلومات على أنها عملية نسخ من نماذج الوظائف الأمنية المترافقة عادة مع الوثائق الفيزيائية. فالكثير من أنشطة البشر في عدد من المجالات المتنوعة، كالتجارة، والسياسة الخارجية، وعمل الجيش، والتفاعلات البشرية، تعتمد على استخدام الوثائق وعلى ثقة كلا الفريقين المتعاقدين بسلامة تلك الوثائق. وتتمتع هذه الوثائق بتواقيع وتواريخ، وقد تحتاج للحماية من الافتضاح أو

التلاعب أو التخريب، كما قد تراقب وتشهد (يشهد عليها شهود)، وقد تسجل أو ترخص،..الخ.

لعبت المعلومات الإلكترونية عدة أدوار بعد أن أصبحت منظومات المعلومات أكثر انتشارا وأصبحنا نعتمد عليها أكثر في إنجاز أعمالنا في حين كانت تنفذ تقليديا بوثائق ورقية [1]. تبعا لذلك يجب أن تتجز الوظائف المقرونة تقليديا بالوثائق الورقية، على وثائق ذات شكل إلكتروني. هنالك مظاهر متعددة للوثائق الإلكترونية تجعل تأمين هذه الوظائف أو الخدمات تحديا كبيرا. نذكر من تلك المظاهر:

١. من الممكن التمييز بين وثيقة الورق الأصلية ونسخ الورق المصورة Xerographic. بينما تكون الوثيقة الإلكترونية على شكل تتابع من البتات bits ولا يوجد أي اختلاف البتة بين الأصل أو أي عدد من النسخ.

٢. إن أي تعديل على الوثيقة الورقية يترك دليلا فيزيائيا على ذلك التعديل. فعلى سبيل المثال، قد يتسبب المحو في تشكيل بقعة رقيقة أو خشونة في السطح. بينما البتات bits المعدلة في ذاكرة الحاسوب لا تترك أي أثر فيزيائي أو أية إشارة.

٣. إن عملية التصديق على سلامة وثيقة فيزيائية تعتمد على المميزات الفيزيائية لتلك الوثيقة (مثلا: شكل توقيع الكتابة اليدوية أو ختم كاتب عدل). فعلمية التصديق على أصالة authenticity الوثيقة الإلكترونية يجب أن يعتمد على دليل داخلي موجود في المعلومات ذاتها.

ركزت فعاليات بحث وتطوير أمن الشبكات والحاسوب على عدة خدمات أمن عامة وهي تشمل الوظائف المتنوعة المطلوبة من ميزات أمن المعلومات. فإحدى التصنيفات المفيدة لخدمات الأمن هي [1]:

▪ الكتمان confidentiality: الذي يؤكد على أن المعلومات في منظومة الحاسوب والمعلومات المرسله قابلة للوصول accessible فقط من أجل القراءة من قبل الأطراف المخولة. هذا النموذج من الوصول يتضمن طباعة

وإظهار أشكال أخرى لكشف المحتوى وبكل بساطة يمكننا الكشف عن موضوع ما.

- التأصيل authentication: الذي يؤكد على أن يكون أصل الرسالة أو المستند الإلكتروني معرفا بشكل صحيح، وأن تكون هوية الوثيقة أصلية غير زائفة.
- السلامة integrity: تضمن أن تكون موجودات منظومة الحاسوب والمعلومات المرسله قابلة للتعديل من قبل الأطراف المخولة فقط. يتضمن التعديل modification كتابة وتغيير حالة وحذف وإنشاء وتأخير أو إعادة replay الرسائل المرسله.
- عدم التوصل nonrepudiation: يتطلب أن لا يكون مرسل الرسالة ولا المستقبل قادرا على نكران (deny) الإرسال [1].
- التحكم بالوصول control access : يتطلب القدرة على التحكم بالوصول إلى مصادر المعلومات عن طريق منظومة الهدف target system.
- الإتاحة availability: تتطلب أن تكون موجودات منظومة الحاسوب متوفرة (متاحة) للأطراف المخولة عند الحاجة إليها.

الآن لنلق المزيد من الضوء على هذه الخدمات:

### الكتمان Confidentiality:

الكتمان هو حماية المعطيات المرسله من الهجمات السلبية [1]. فيما يخص فضح محتويات الرسائل، فمن الممكن استخدام عدة مستويات للحماية. الخدمة الأعرض تحمي جميع المعطيات المرسله بين مستخدمين اثنين خلال برهة من الزمن. مثلا إذا تم تركيب دارة افتراضية (virtual) بين منظومتين، فإن هذه الحماية العريضة ستقوم بمنع فضح أي معطيات عبر الدارة الافتراضية. ومن الأشكال الأضيق لهذه الخدمة يمكن أن يشار إليها على أنها حماية رسالة ما أو حتى حقول خاصة ضمن الرسالة. يمكن أن

تكون هذه التحسينات refinements أقل فائدة من المقاربة الواسعة وقد تكون أكثر تعقيدا وغالية التنفيذ.

المظهر الآخر للكتمان هو حماية حركة المرور من التحليل. وهذا ما يتطلب أن يحرم المهاجم من قدرته على مراقبة المصدر والهدف والتردد وطول الرسائل أو حرمانه من المميزات الأخرى لحركة المرور على أداة الاتصالات.

### التأصيل Authentication:

تهتم خدمة التأصيل بالتثبت من أن الاتصال أصيل Authentic [7]. في حالة رسالة واحدة كحالة إشارة التحذير أو إشارة المنبه، تكون وظيفة خدمة التأصيل هي التأكيد للمستلم بأن الرسالة هي من المصدر الذي يدعي بأنها تكون مرسله من قبله. في حالة التفاعل الآني، كحالة وصل طرفية ما إلى الحاسوب المضيف يكون هنالك مظهران. أولا: في حين بدء الربط تؤكد خدمة التأصيل بأن الكائنين أصيلين، أي أن كل كائن صادق بما يدعي عن هويته. ثانيا: يجب أن تؤكد الخدمة أن الوصلة ليست متداخلة بطرف ثالث يمكن أن يتكرر كواحد من الطرفين الشرعيين بهدف القيام بإرسال أو استقبال غير مخول.

### السلامة Integrity:

كما في حالة الكتمان، يمكن تطبيق خدمة السلامة على سلسلة من الرسائل أو رسالة واحدة أو حقول مختارة من الرسالة. ومرة أخرى تكون المقاربة الأكثر نفعاً والمباشرة، هي حماية سلسلة الرسائل بكاملها [1].

يمكننا الآن تعريف خدمة السلامة الموجهة توصيلياً (a connection\_oriented integrity service)، على أنها الخدمة التي تتعامل مع سلسلة من الرسائل وتؤكد بأن الرسائل قد استقبلت كما أرسلت، دون نسخ، أو حشر، أو تعديل، أو إعادة ترتيب reordering، أو إعادة replay. تدمير المعطيات هو أيضا مشمول تحت هذه الخدمة.

لذا تتعامل خدمة السلامة الموجهة توصيليا مع كل من تعديل سلسلة الرسالة ورفض الخدمة. من ناحية أخرى تعرف خدمة السلامة اللاتوصيلية ( connectionless integrity service)، على أنها تلك الخدمة التي تتعامل مع مختلف الرسائل والتي تؤمن حماية من تعديل الرسائل فقط. يشير الباحث Kent إلى إمكانية تقديم خدمة هجينة من أجل التطبيقات التي تتطلب بعض الحماية من الإعادة replay وإعادة الترتيب .reordering

يمكننا التمييز بين الخدمة التي تؤمن الاسترداد والخدمة التي لا تؤمن ذلك. لأن خدمة السلامة ترتبط بالهجمات الإيجابية، فكل اهتمامنا ينصب على الكشف أكثر من المنع. إذا ما تم الكشف عن مخالفة Violation للسلامة، عندئذ تقوم الخدمة بالإبلاغ عن هذه المخالفة، ولتصحيح هذه المخالفة يجب إدخال أجزاء برمجيات أخرى أو تدخل الأفراد. وكبديل يوجد آليات تصحيح نقص سلامة المعطيات. ويعتبر إدخال آليات الاسترداد المؤتمتة أمرا عموما بديلا ذا جاذبية كبيرة.

#### عدم التنصل Nonrepudiation:

تمنع خدمة عدم التنصل كلا من المرسل والمستقبل من نكران رسالة مرسلة. وهكذا عندما ترسل رسالة ما يمكن للمستقبل إثبات أن الرسالة كانت في الحقيقة قد أرسلت من قبل المرسل المزعوم [1]. وعلى غرار ذلك عندما تستقبل الرسالة يمكن للمرسل إثبات أن الرسالة كانت في الواقع قد استقبلت من قبل المستقبل المزعوم.

#### التحكم بالوصول Access Control:

وبمجرى الحديث عن سلامة الشبكة فإن التحكم بالوصول هو القدرة على الحد من والتحكم بالوصول إلى منظومات المضيف (host) وتطبيقاته عن طريق وصلات الاتصالات [1]. لتحقيق هذا التحكم يجب أولا أن يتم تعريف أو تأصيل كل كائن entity يحاول كسب وصول، بحيث يتم تفصيل حقوق الوصول لكل شخص على حدة.

## الإتاحة Availability:

يمكن أن ينتج عن أنواع مختلفة من الهجمات فقداناً أو نقصاً في الإتاحة [1]. وقد تكون بعض هذه الهجمات سهلة الانقياد لإجراءات معاكسة مؤتمتة، مثل التأسيس authentication والتعمية encryption، في حين يكون البعض الآخر يحتاج لعمل فيزيائي ما لمنع أو لتصحيح فقدان إتاحة عناصر المنظومة المهاجمة.

### ١-١-٢ الآليات Mechanisms:

لا يوجد آلية واحدة بإمكانها تقديم جميع الخدمات أو إنجاز جميع الوظائف. هنالك تنوعاً من الآليات قيد التداول [1]. بيد أنه يمكننا ملاحظة نقطة واحدة تشكل الأساس لمعظم آليات الأمن التي قيد الاستخدام ألا وهي تقنيات التعمية Cryptographic techniques. التعمية encryption أو التحويلات الشبيهة بالتعمية encryption-like transformations للمعلومات فهي أكثر الوسائل شيوعاً لضمان الأمن. لذا يركز هذا البحث على تطوير واستخدام وإدارة هذه التقنيات.

### ١-١-٣ الهجمات Attacks:

عرف سايمونز G. J. Simmons بشكل حدسي أمن المعلومات على أنه طريقة لمنع الخداع أو إفشاله وذلك بكشف الخداع ضمن المنظومات القائمة على المعلومات حيثما لا يكون للمعلومات نفسها بحد ذاتها وجود فيزيائي.

يورد الجدول ١-١ بعض الأمثلة الأكثر وضوحاً على الخداع فكل واحد منها برز مرات عديدة في الحياة العملية [1]. وهذه الأمثلة على بعض الهجمات المحددة التي يجب أن تعاكسها المنظمات أو الأفراد بالنيابة عن المنظمات. وقد تختلف الاستجابة نحو هجمة ما من منظمة إلى أخرى طبقاً للظروف المحيطة. ولحسن الحظ يمكننا مقارنة



المسألة من زاوية مختلفة وذلك بالنظر إلى النماذج العامة للهجوم كما هو موضح في المقطع اللاحق.

### الجدول ١-١ أسباب الخداع Reasons for cheating

١. اكتساب وصول غير مخول إلى المعلومات (مثل: التعدي على السرية secrecy أو الخصوصية privacy).
٢. انتحال شخصية مستخدم آخر لإلقاء المسؤولية على شخص آخر أو لاستخدام رخص الآخرين بهدف:
  - إنشاء معلومات مزورة.
  - تحوير معلومات شرعية.
  - استخدام هوية مزورة لكسب وصول غير مخول.
  - تأصيل فعاليات مزورة أو تصديقها.
٣. التوصل من المسؤولية أو الاستحقاقية Liability للمعلومات التي ولدها المخادع.
٤. ادعاء المخادع بأنه استقبل من مستخدم آخر معلومات هي في الواقع من إنتاجه.
٥. الادعاء بأنه قد أرسل إلى مستقبل (في زمن محدد) معلومات لم ترسل في الحقيقة (أو أنها قد أرسلت في وقت مختلف).
٦. التوصل من استلام المعلومات التي كان قد استلمها مسبقاً، أو الادعاء باستلامها في وقت مخالف عن موعد استلامها.
٧. توسيع الرخصة الشرعية للمخادع (من أجل الوصول والتوليد والتوزيع والخ...)
٨. التعديل (بدون إذن لفعل ذلك) رخصة الآخرين (إدراج الآخرين احتيالياً، تقييد أو توسيع إنشاء الرخص، الخ...)