أمن بروتوكول الإنترنت
(IP Security)

المحتويات

ـ مقدمة:

بعد التقدم والتطور الذي حصل في عالم أمن المعلومات، وبعد تطور أساليب المخترقين في عملياتهم وتنوعها مثل:(Man-IN-The-Middle , Sniffing , Relaying) والكثير غيرها، كان لا بد من إيجاد طريقة آمنة لتخطي هذه الأمور وخصوصاً في التعاملات المالية كالتجارة الإلكترونية وعمليات كشف الحسابات عن طريق الإنترنت وغيرها، فكان لابد من طريقه لتأمين ذلك، فتم تطوير تقنية الSSL : Secure Socket Layer وامنت هذه الطريقة قيام اتصال آمن مشفر Encrypted ضمن تعقيدات متفاوتة فمنها الBit40 ومنها bit128 فتم استخدام الSSL لتشفير وحماية قنوات الاتصال التي تنتقل عبرها البيانات مثل SMTP او الDatabase Communications.

وتم استخدام ما يعرف بSSL over HTTP في المواقع التجارية ومواقع البريد الالكتروني فأصبحت تسمى HTTPS : Secure Hyper Text Transfer Protocol واستخدم بورت 443 بدلاً من 80 الخاص بـHTTP ـ، وانتشر واشتهر بشكل كبير.

ثم ظهرت تقنية مشابه له ولاستخدامه وهي الTLS : Transport Layer Security وهي تقنية محسنة من الSSL ولكنهما يختلفان في طريقة أداء العملية ، والطريقتان تحتاجان للشهادات الالكترونية Certificates أو بالأحرى Web-based Certificates .

وظهرت تقنية أخرى داخل الشبكة نفسها وليس على شبكة عالمية كالانترنت ، وهي SMB Signing ، الجميع يعلم أن الSMB : Server Message Block هي الpackets الي يتم إرسالها بين السيرفر والأجهزه في عملية المشاركة في الملفات وغيره Sharing ، وللحماية من طريقة سرقة المعلومات أثناء مرورها في الأسلاك Man In The Middle MITM وهذه الطريقه تدعى SMB Signing ، يتم بواسطتها إضافة الHash (وهي طريقة يتم من خلالها استخلاص رمز معين تم حسابه باستخدام عمليات رياضية من الرسالة ، ومن الامثلة عليه SHA-1 , MD5 , MD4 ويتم تشفير هذا الHash واضافته للرسالة وبذلك نحافظ على صحة الرسالة Message or Packet Integrity .

لكن ظهرت المشكلة الكبرى بكون جميع هذه التقنيات تعمل على طبقة التطبيقات المسماة بـ(Application) Layer في النموذج المعياري لربط النُظم المفتوحة المسمى بـ(OSI Model) أي أن وظائف هذه التقنيات السابقة محدودة جدًا، فهي لا تستطيع تشفير الا ما بنيت لأجله، ولذلك كان لا بد من ابتكار طريقة تمكننا من تشفير كل حزمة (Packet) تصدر من أي جهاز ،، فتم ابتكار تقنيه الSecurity IP وهي تقنيه تعمل على طبقة الشبكة المسماة بـ(Network Layer) في الOSI Model بمعنى انه يقوم بتشفير كل شيء يصدر عن الجهاز ويرسله على الشبكه Network بما ان الـ(Network Layer) هي الجهة التي من خلالها يمرر كل شيء للشبكة.IPSec تقنية توفر الموثوقية والصحة والتشفير لكل شيء يمر من خلالها على مستوى الIP Packet. وفي هذه الورقة ستتناول كل مايتعلق بالIP من أنواعه وأقسامه وفوائده وكيفية عمله إن شاء الله تعالى.

Application	S/MIME	PGP		
Presentation				
Session	Kerberos	HTTP	UDP	SSL
Transport	TCP			
Network	IP			**IPsec**
Data Link				
Physical				

شكل 1: توضح الصورة موقع الIPSec في الOSI Model

- ما هي ال IPSec؟

IPSec: هي مجموعة معايير من البروتوكولات والخوارزميات طورت بواسطة اللجنة الخاصة لنظام الإنترنت Internet Engineering Task Force (IETF) واعتمدت كمعايير الإنترنتِ لتوفر التحقق من سلامة وسرية المعلومات التي أرسلت عبر شبكات الIP، وذلك بجعلها تعمل في طبقة الIP بحيث تتمكن من حماية أي نوع من نقل البيانات من خلال الIP.

عادةً يعبر عن الIPSec بأنها Transparent Security Protocol لأن المستخدم و التطبيقات لايشعرون بوجودها لأنها تعمل على طبقة الشبكة (Network Layer)، ويعمل ال IPSec في البيئات التي تكون سرعة الاتصال بها سريعة.

- بروتوكولات الIPSec

ينقسم ال IPSec الى ثلاث بروتوكولات:

أولاً: AH : Authentication Header

يستخدم الAH في توقيع Sign الرسائل والبيانات ولا يعمل على تشفيرها Encryption ، حيث يحافظ على:

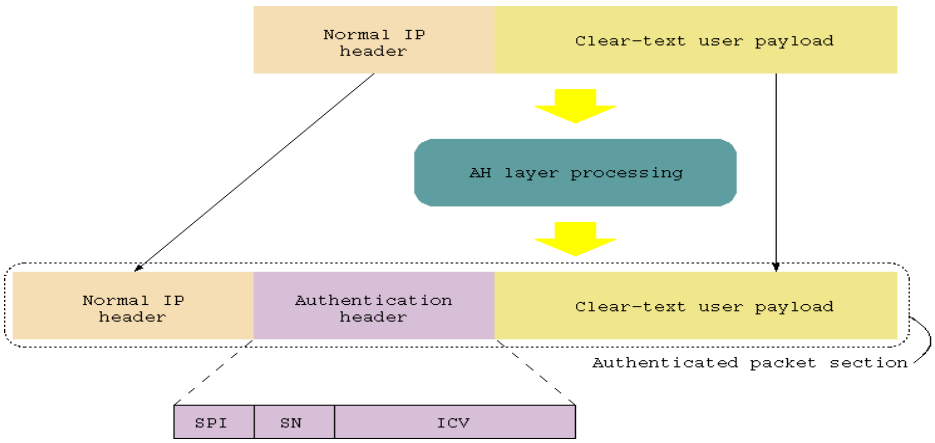
1.موثوقية البيانات **Data authenticity**: أي أن البيانات المرسلة من هذا المستخدم هي منه وليست مزورة أو مدسوسة.

2.صحة البيانات **Data Integrity** : أي أن البيانات المرسلة لم يتم تعديلها على الطريق (أثناء مرورها على الأسلاك)
.

3.عدم إعادة الإرسال **Anti-Replay** : وهذه الطريقة التي يستخدمها المخترقون حيث يقومون بسرقة كلمة المرور وهي مشفرة ويقومون بإعادة إرسالها في وقت آخر للسيرفر وهي مشفرة وبالطبع يفك السيرفر التشفير ويدخل اسم المستخدم على أنه شخص آخر، فالIPSec يقدم حلولاً لمنع هذه العملية من الحدوث.

4.الحماية ضد الخداع **Anti-Spoofing protection** : ويوفر أيضاً الIPSec حماية ضد الخداع من قبل المستخدمين ، مثلاً يمكن ان يحدد مدير الشبكه انه لا يسمح لغير المستخدمين على الsubnet 192.168.0.X بينما لا يسمح لحاملي الهويه x.192.168.1 من دخول السيرفر ، فيمكن للمستخدم ان يغير الIP Address الخاص به ، لكن الIPSec يمنع ذلك .(وايضا يمكنك القياس على ذلك من خارج الشبكه الى داخلها) يكون لكل حزمة Packet موقعها Digitally signed.

هذا هو الشكل العام لحزمة البيانات Packet التي تمر في بروتوكول AH .



ثانياً: Encapsulating Security Payload : ESP

يوفر هذا البروتوكول التشفير والتوقيع للبيانات معا Encryption and Signing ، و يستخدم هذا البروتوكول في كون المعلومات سرية Confidential او Secret ، أو عند إرسال المعلومات عن طريق Public Network مثل الانترنت.

يوفر الESP المزايا التالية:

1. **Source authentication** : وهي مصداقية المرسل ، حيث كما وضحنا في مثال الSpoofing أنه لا يمكن لأي شخص يستخدم الIPSec تزوير هويته (هوية المرسل).

2. التشفير للبيانات **Data Encryption** : حيث يوفر التشفير للبيانات لحمايتها من التعديل أو التغيير أو القراءة.

3. **Anti-Replay** : موضحة في الAH .

4. **Anti-Spoofing Protection** : موضحة في ال AH.

ثالثاً : Internet Key Exchange : IKE

الوظيفة الاساسيه لهذا البروتوكول هي ضمان الكيفية وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي الIPSec ، فهو بروتوكول الnegotiation أي النقاش في نظام الIPSec كما أنه يعمل على تأكيد طريقة الموثوقية Authentication والمفاتيح الواجب استخدامها ونوعها (حيث ان الIPSec يستخدم التشفير DES3 وهو عبارة عن زوج من المفاتيح ذاتها يتولد عشوائياً بطرق حسابية معقدة ويتم إعطاءه فقط للجهة الثانية ويمنع توزيعه وهو من نوع Symmetric Encryption أي التشفير المتوازي ويستخدم تقنية الPrivate Key .

- أقسام الIPSec

أو انواع الIPSec التي يستخدمها في الشبكة، وينقسم الIPSec الى نظامين او نوعين وهما :

1. نظام النقل Transport Mode

2. نظام النفق Mode Tunnel .

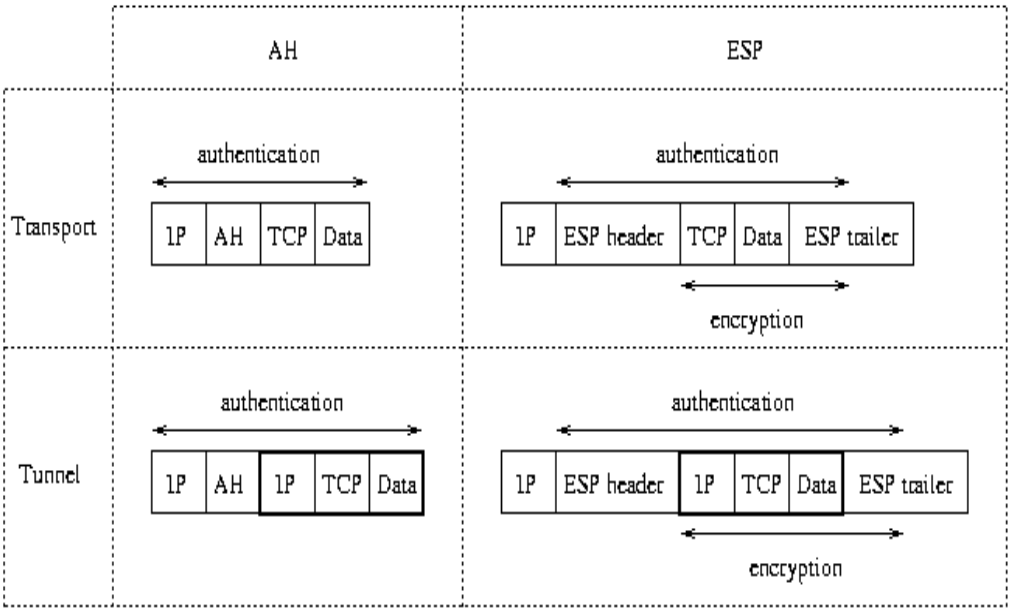
نظام النقل: يستخدم هذا النظام عادة داخل الشبكة المحلية Local Area Network : LAN حيث يقدم خدمات التشفير للبيانات التي تتطابق والسياسة المتبعة في الIPSec بين أي جهازين في الشبكه أي يوفر Endpoint-Encryption to-Endpoint فمثلاً اذا قمت بضبط سياسة الIPSec على تشفير جميع الحركة التي تتم على بورت 23 وهو بورت الTelnet (حيث ان الTelnet ترسل كل شيء مثلما هو دون تشفير Text Plain) فإذا تمت محادثه بين السيرفر والمستخدم على هذا البورت فان الIPSec يقوم بتشفير كل البيانات المرسلة من لحظت خروجها من جهاز المستخدم الى لحظة وصولها الى السيرفر. يتم تطبيق هذا النظام في الحالات التالية:

أولاً: المحادثة تتم بين الأجهزة في داخل أو نفس الشبكة الداخلية الخاصة Private LAN.

ثانياً: المحادثة تتم بين جهازين ولا يقطع بينهما Firewall حائط ناري يعمل عمل NAT : Network Address Translation (نظام يمكن الFirewall من استبدال جميع عناوين الIPs في الشبكه الداخليه من حزمة البيانات Packet واستبدالها في عنوان Public IP اخر ، ونستفيد من ذلك هو أننا لن نحتاج سوى الى عنوان IP واحد One Public IP ، وأيضاً أنه يقوم بإخفاء عناوين الأجهزه عن شبكة الانترنت للحماية من الاختراق الخارجي) .

نظام النفق: يتم استخدام هذا النظام لتطبيق الIPSec بين نقطتين تكون بالعادة بين Routers 2 ، إذاً يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافياً أي سيتم قطع الانترنت في طريقها الى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعده جغرافيا Network WAN : Wide Area ، يستخدم هذا النظام فقط عند الحاجه لتأمين البيانات فقط اثناء مرورها من مناطق غير آمنة كالانترنت ، فمثلاً إذا أراد فرعين لشركة أن يقوم بتشفير جميع البيانات التي يتم إرسالها فيما بينهم على بروتوكول FTP : File Transfer Protocol فيتم إعداد الIPSec على أساس الTunnelling Mode .

وهذه صوره مخطط لكل من الPackets في الAH , ESP في كلتا النظامين Tunnel and Transport Modes .



- فوائده IPSec Benefits

لقد ظهر ضعف كبير في عملية الEncryption العادية التي تتم بين الأجهزه في الشبكات ، وهذا الضعف تمثل في صعوبة تطبيق هذا الموضوع ، وايضا استهلاكه للوقت أي بطئه الشديد في القيام بعملية التشفير وفكه Encryption and decryption ،فالفائده الكبرى التي ظهرت في الIPSec هي أنه يوفر حماية كاملة وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالث Layer 3 of the OSI Model وما بعدها.

من مميزات الIPSec أيضا هو أنه موجود أصلا Built-in في داخل حزمة الIP Packet ، فلذلك هو لا يحتاج لأي إعدادت لانتقاله عبر الشبكة ولا يحتاج لأي أجهزة إضافية لذلك .

- كيف يحمي الIPSec من الهجوم على الشبكة؟

إن الشبكة والبيانات التي تمر فيها يمكن ان تتعرض للعديد من أنواع الهجمات المختلفة ، بعض الهجمات تكون غير فعاله Passive مثل مراقبة الشبكة Network Monitoring ، ومنها ما هو الفعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر أسلاك الشبكة. و سوف نستعرض بعض انواع الهجمات على الشبكات.

أولاً: التقاط حزم البيانات snooping Eavesdropping, sniffing or:حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكه بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ، ويعالجها الIPSec عن طريق تشفير حزمة البيانات، عندها حتى لو التقطت الحزمة فإن الفاعل لن يستطيع قراءتها أو العبث بها، لأن الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل.

ثانيا: تعديل البيانات Data modification:حيث يتم بذلك سرقة حزم البيانات من الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل، ويقوم الIPSec بمنع ذلك عن طريق استخدام الهاش Hash ووضعه مع البيانات ثم تشفيرها معاً ، وعندما تصل الحزمة إلى الطرف المستقبل فإن الجهاز يفحص Checksum التابع للحزمة إذا تمت مطابقته أم لا، فإذا تمت المطابقة مع الهاش الأصلي المشفر تبين أن الحزمة لم تعدل، لكن إذا تغير الهاش فإن حزمة البيانات قد تم تغييرها على الطريق.

ثالثاً: انتحال الشخصية spoofing Identity: بحيث يتم استخدام حزم البيانات على الشبكة والتقاطها وتعديلها لتبين هوية مزورة للمرسل، أي خداع المستقبل بهوية المرسل، ويمنع ذلك عن طريق الطرق الثلاثه التي يستخدمها الIPSec وهي: بروتوكول الكيربرس (Protocol Kerberos)، والشهادات الالكترونية Digital Certificates ، ومشاركة مفتاح معين (Preshared Key).

حيث لا تتم عملية بدأ المحادثة وإرسال البيانات قبل التأكد من صحة الطرف الثاني عن طريق احدى الطرق المذكورة.

رابعاً: Service DoS -Denial of رفض الخدمة أو حجبها: حيث تعمل هذه الهجمة على تعطيل خدمة من خدمات الشبكه للمستخدمين والمستفيدين منها ، مثلاً كاشغال السيرفر في الشبكة بعمل عليه Flood مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين. ويعمل الIPSec على منع ذلك عن طريق إمكانية غلقه أو وضع قواعد للمنافذ المفتوحة Ports.

خامساً: Middle MITM -Man In The: من أشهر الهجمات في الشبكات، وهي أن يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسلة من طرف لآخر وإمكانية العمل على تعديلها أو العمل على عدم إيصالها للجانب الاخر، ويعمل الIPSec على منعه بواسطة طرق التحقق من الموثوقية Authentication methods .

سادساً: الهجمات على طبقة التطبيقات Application Layer Attacks : حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في أجهزة الشبكة وأيضاً تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الأمثله عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى اخطاء المستخدمين. يعمل الIPSec على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أي حزمة بيانات لا تتطابق مع الشروط الموضوعة لذلك ، لذا فتعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج.

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

طريقة التشفير المستخدمة في الIPSec عبارة عن دمج لعدة Algorithms ومفاتيح، وحيث

Algorithm: عباره عن العملية الحسابية التي تمر فيها البيانات لكي تشفر.
Key: وهو عباره عن رقم (كود) سري يتم من خلاله قراءه أو تعديل أو حذف أو التحكم في البيانات المشفرة بشرط مطابقته للطرف الثاني الذي قام بعملية التشفير.

المراجع والمصادر:

الأوراق:

[1] Sheila, Frankel, "AN INTRODUCTION TO IPSec*", Computer Security Division/Information Technology Laboratory/National Institute of Standards and Technology.*

[2] Cary, Hayward, "The Internet Protocol Security (IPSec) Standard: Clearing up the Confusion", *Product Marketing Manager/RedCreek Communications.*

الكتب:

[3] Eric, Cole, *"Network security bible"*, 1St Edition, Indianapolis, Wiley Publishing, 2005.

مواقع الإنترنت:

[4] www.microsoft.com/technet/itsolutions/network/ipsec/default.mspx
[5] www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.mspx
[6] searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214037,00.html
[7] www.windowsecurity.com/whitepapers/Linux_Administrators_Security_Guide__IP_Security_IPSec.html
[8] searchsecurity.techtarget.com/generic/0,295582,sid14_gci1147334_tax299834,00.html?adg=299807&bucket=REF
[9] www.intranetjournal.com/articles/200206/se_06_13_02a.html
[10] www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm
[11] www.ceenet.org/workshops/lectures2000/Richard_Perlman/ipsec/sld009.htm
[12] www.microsoft.com/technet/itsolutions/network/security/ipsecarc.mspx
[13] certcities.com/editorial/features/story.asp?EditorialsID=50
[14] www.ceenet.org/workshops/lectures2000/Richard_Perlman/ipsec.ppt
[15] www.intel.com/network/connectivity/resources/doc_library/white_papers/products/ipsecurity/index.htm