Technical Paper

Enhancing Enterprise Security

An Overview of Network Security Issues and Technologies

Enhancing Enterprise Security
An Overview of Network Security Issues and Technologies

Contents

Enhancing Enterprise Security

An Overview of Network Security Issues and Technologies

Acronyms and Abbreviations

3DES
Triple Data Encryption Standard

AH
Authentication Header

BITS
bump in the stack

BITW
bump in the wire

CA
certificate authority

CPU
central processing unit

DES
Data Encryption Standard

ESP
Encapsulating Security Payload

HMAC
Hashed Message Authentication Code

IDEA
Internet Development and Exchange Association

IETF
Internet Engineering Task Force

IPSec
Internet Protocol Security

ISP
Internet service provider

KMAC
Keyed Message Authentication Code

Organizations large and small have increased the use of networked computers every year since networks were invented. Where once only electronic mail was exchanged within or between companies, now intellectual property, product information, invoices, purchase orders, human resources data, credit card numbers, and more travel over these networks. The computer network has become critical to the success of the enterprise.

With the expansion of the Internet and the increasing use of Internet technology inside the organization, more and more computing resources have become connected to networks that can potentially be reached from outside the enterprise and from inside the enterprise as well. As connectivity increases, so does the risk of attack on the network. In this environment, two factors drive the need for a network security system: the need to maintain the integrity of data communications and the need to protect intellectual property and information assets. This paper presents an overview of the systems and strategies available to protect today's computer networks.

Security Requirements

Maintaining security is a never-ending struggle. Just when you think you have an airtight system in place, a new hacker technology or an especially diabolical adversary enters the picture. In addition, it's important to note that threats aren't necessarily external. In fact, the FBI Computer Crime Unit reports that more than 80 percent of all network security breaches are inside jobs—disgruntled or dishonest employees with their own particular agendas.

Regardless of the type or location of perceived threat, an effective system for securing the integrity of information while maintaining availability of information assets must:

- Allow access to information by authorized parties
- Implement policies determining who is authorized for what access to which information
- Employ a strong user authentication system
- Deny malicious or destructive access to any information asset
- Protect data from end to end

Threats to Enterprise Security

A computer networking system can be attacked in a number of ways, resulting in differing degrees of damage. These attacks can take several forms:

- Denial of service. The attacker disrupts the smooth flow of information by crashing or overloading a critical device such as a server, router, or firewall. This is an attack on the availability of information.
- Theft of information. The attacker acquires information that is proprietary to the organization. This can be done by eavesdropping, by masquerading as an authorized entity, or by a brute-force attack such as the use of a computer program that guesses passwords. This is an attack on the ownership of information and intellectual property.
- Corruption of data. The attacker either destroys or corrupts data stored on disk or corrupts data as it is transmitted across the network. This is an attack on the integrity of information.

Threats to the availability, ownership, and integrity of information assets can arise at any of these locations (Figure 1):

- The people who use the system (divulging passwords, losing token cards, etc.)
- Internal network connections such as routers and switches
- Interconnection points such as gateways between corporate intranets and the Internet
- Third-party network carriers such as long-distance carriers and ISPs
- Application-level imposters, eavesdroppers, and attackers

Establishing adequate or even impenetrable security at one point of attack while leaving one or more of these other points uncovered is like posting a guard at the front desk and leaving the company's doors and windows wide open. An employee seeking revenge or a serious thief will try every avenue of entry, particularly if the value of the information is great and the access is relatively easy.

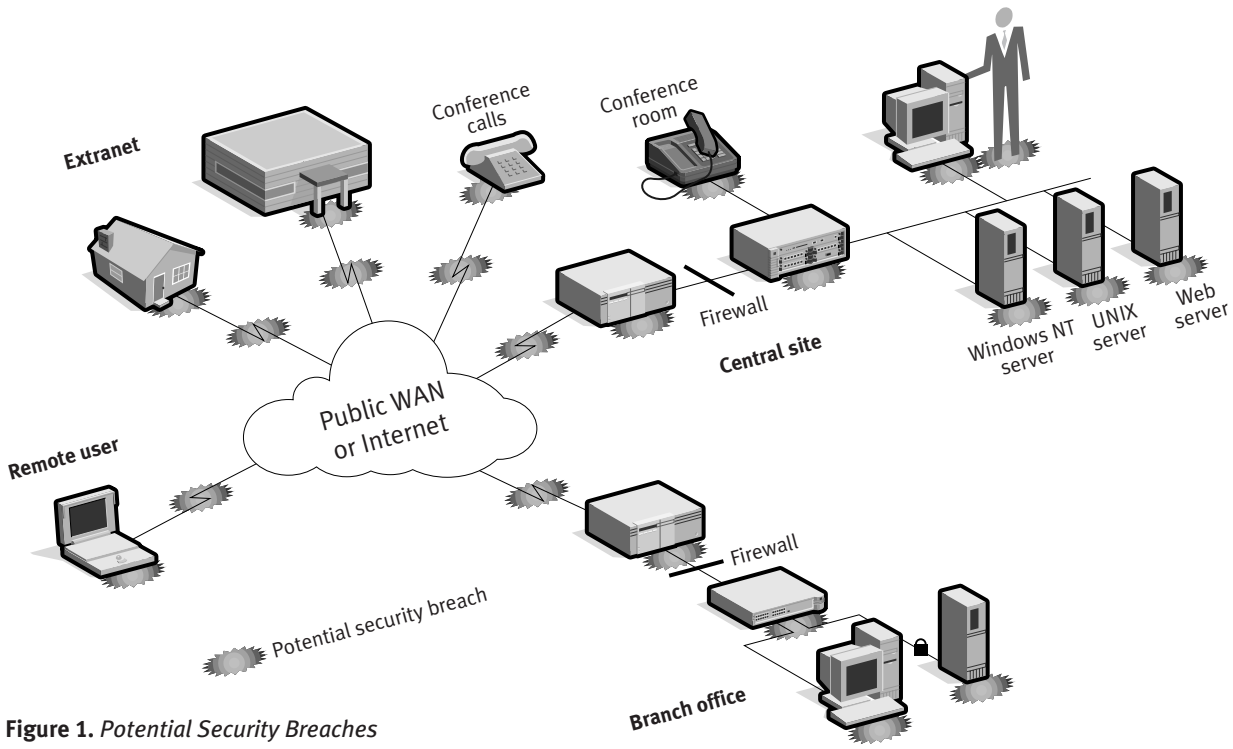

Figure 1. *Potential Security Breaches*

Elements of a Comprehensive Security Solution

A complete security solution that maximizes the benefits of networked data communications must contain these elements:

- Physical protection—where are you?
- User authentication—who are you?
- Access control—what asset are you allowed to use?
- Encryption—what information should be hidden?
- Management—what is going on within the network?

An enterprise may employ any or all of these elements to achieve integrity and access control. The best strategy depends on the risk involved, the cost of the deployment, and the cost of a security breach or lost data. The following sections look more closely at each element in a total security solution.

Physical Security

Physical risks most often involve access to machines or people. A number of strategies can be used to enhance physical security:

- Place computers in a secure environment. The degree to which the console, keyboard, and monitor of a computer can be physically accessed to a large extent determines the level of system security. This is a common "back door" opening to an intruder. To implement physical security, organizations often use receptionists, security guards, physical keys, combination or electronic door locks, and other access controls. Something else not to be overlooked: modem pools and all Internet connections should be firewalled.
- Destroy sensitive documents, including disks, when no longer used. Sophisticated tools can reconstruct files supposedly erased from a disk. Only destroying the disk itself guarantees the destruction of the data it once contained.
- Store digital keys on smart cards, not on disks. Disks can be duplicated; smart cards are more difficult to copy.
- Keep passwords secure. Avoid writing passwords down, then sending them through electronic mail or placing them in messages

Acronyms and Abbreviations

MAC
Message Authentication Code

NIC
network interface card

PKI
public key infrastructure

SA
Security Association

SPD
Security Policy Database

TCP/IP
Transmission Control Protocol/Internet Protocol

VPN
virtual private network

that are archived or incorporated in group discussion systems.
- Do not write PINs on ID cards. Writing a PIN number on an ID card is similar to hiding the front door key under the welcome mat. Security training can help make employees aware of their part in maintaining network security.
- Lock down portable equipment. The laptop computer represents one of the greatest physical threats to a security system, because it contains a great deal of information and can so easily be carried off. The same is true of other devices such as external disk drives, tape backup systems, and the like. These devices must be locked away or bolted to the desk to guard against theft.

User Authentication

Proof of identity is an essential component of any security system. It's the only way to differentiate authorized users from intruders. User authentication to the network is a necessity for any enterprise that is serious about protecting information assets and knowing who is attempting to gain access to the network. Authentication becomes particularly important when some of the more sophisticated communication methods are used.

In addition to proving identity, authentication systems are used to determine what information the requestor can access—for example, a human resources database or corporate financial database. True authentication generally incorporates two or three of the following elements:

- What the user has or possesses (smart card, certificate)
- What the user knows (password)
- A physical attribute (fingerprint or other biometric information)

Authentication is most often achieved through challenge and response, digital certificates, or message digests and digital signatures.

Challenge and response. In this authentication method, a software agent within a database system or a workgroup server presents the person requesting access to a resource with a challenge, most often requesting a username and password. This is the most common form of security and one that is easily broken when passwords are not carefully chosen and maintained.

Digital certificates. One of the earliest uses of digital certificate technology was Privacy Enhanced Mail, the predecessor to S/MIME (Secure/Multipurpose Internet Mail Extensions), a widely used specification that brought a higher level of security to e-mail through encryption and digital signature-based authentication. Since their introduction, the use of digital certificates has continued to grow steadily.

Digital certificates are essential components of a public key infrastructure (PKI), which can be generally defined as a security system that consists of protocols, services, and standards that support applications of public-key cryptography. Public key cryptography is used to validate messages that have been digitally signed. Such messages can be simple e-mail or part of a protocol for establishing a secure communications session. The sender of the message to be authenticated digitally signs the message using a private key. The signature can be validated using the sender's corresponding public key, which is contained in the sender's certificate and can either be sent along with the message or retrieved from a certificate repository.

The association between the sender's identity and the sender's public key can be authenticated through a digital certificate issued by a trusted certificate authority (CA). The CA certificate is issued in advance to all parties, and its public key can be used to authenticate the public key in the sender's certificate. When the sender's public key has been validated, it can be used to authenticate the digital signature of the message itself. Since the CA certificate is already available to both the sender and receiver, this method can be used to authenticate messages in either direction without contacting a third party.

To implement a secure certificate or signature system (Figure 2), the following conditions must be met:

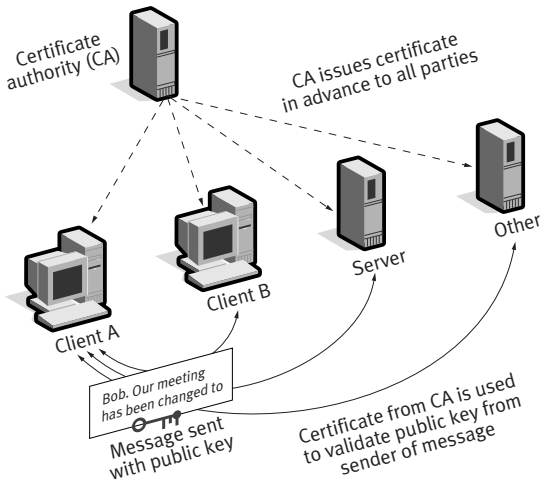

Figure 2. *Deploying Digital Certificates*

- A certificate authority service provider or software package must issue a certificate to all potential senders and receivers.
- The receiver must be able to use the CA certificate to verify the sender's public key.
- The sender's authenticated public key must then be used to verify the digitial signature of the message itself.

Although a digital certificate system can affect the performance of heavily used servers, this is usually not the case. Typically, the certificate itself is provided by the client, in which case the authenticator does not need to perform any server access. Moreover, the value of preventing a security breach often far outweighs the inconvenience of slightly delayed access.

Message digests and digital signatures. Message digests are created by applying a one-way hash function such as MD5 or SHA-1 to a message. "One-way" means that the original message cannot be recreated from the digest. A digital signature uses the private key of an individual (see "Alice" in Figure 3) to encrypt the message digest. At the receiving end, the digest is recreated from the message text, the public key is used to decrypt the digest from the digital signature, and the two message digests are compared. If they match, the messages are in all probability the same. Comparison of the message digests provides both a means of authenticating the signature and a check of message integrity.

Access Control

Access control governs a user's ability to make a connection to a particular network, computer or application, or to a specific kind of

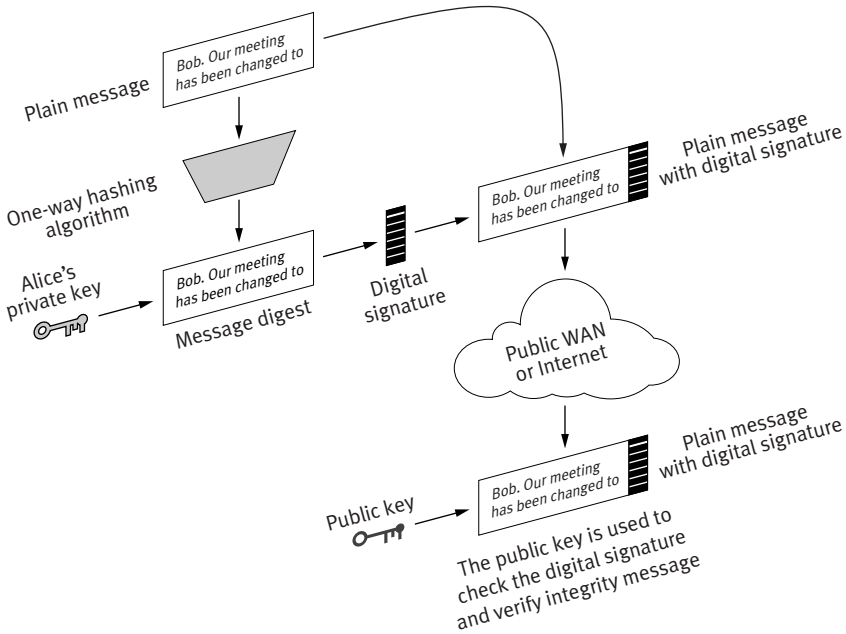

Figure 3. *Authentication with Digital Signature*

data traffic. Access control systems are generally implemented using firewalls, which provide a centralized point from which to permit or deny access.

Firewalls. These physical devices or software agents filter packets heading into or out of an organization based on a set of policy rules. They can allow access to an enterprise network by username/password, type of service requested (ftp, http, telnet), location of destination (network or computer), or location of requestor (network address). A firewall can request authentication before allowing any traffic to pass at all, and in so doing can take advantage of the various authentication schemes available. There are two distinct types of firewalls as well as some hybrids that don't fit neatly into any category. The difference between firewall types is primarily related to how they handle external traffic.

- Packet-filtering firewalls. This type of firewall controls access and data into and out of the network. Packet-filtering firewalls can simply be routers or switches that are configured with access lists. They can permit or deny access based on the protocol, source or destination port, and source and destination of IP addresses. Moreover, for a higher level of security, they can be configured to allow TCP communications only when initiated from the internal network. Packet-filtering firewalls typically do not employ any kind of user authentication, because the environments in which they are usually deployed handle levels of traffic that are too high to allow for it.
- Application/proxy firewalls. These devices or software agents handle requests in place of the network application or server they are safeguarding. They provide network resources inside the firewall with a layer of protection, ensuring that secure resources are never accessed directly. Application/proxy firewalls typically support local caching of Web content and address translation, thereby hiding internal IP addresses from Internet surfers. Proxy firewalls can allow access based on source address, destination address, or an identity (authentication).

There are many firewall products offered by numerous vendors at a wide range of prices. In many cases these products also include a Web server, thus creating a turnkey system. Any organization that has an open connection to the Internet should deploy one or more of these devices to ensure adequate security.

In addition to firewalls, an enterprise may implement a network-level security protocol, such as Internet Protocol Security (IPSec), to protect information as it moves through a network. IPSec works at the packet level. Every packet is protected to provide authentication, integrity, and (optionally) confidentiality. Any of the firewall devices described above, as well as each of the individual computers or servers on a network, can implement IPSec. IPSec is discussed in greater detail later in this paper.

Encryption

Even if both access control and authentication security systems are completely effective, the enterprise can still be at risk when data communications travel over a third-party network such as the Internet. Indeed, the low cost and ease of connecting to the Internet have made it an extremely attractive medium for communication within and between enterprises.

Encryption is used to protect against eavesdropping. It renders information private by making it unreadable to all except those who have the key needed to decrypt the data. It does not matter whether a third party intercepts packets over the Internet; the data still cannot be read. This approach can be used throughout the enterprise network, including within the enterprise (intranet), between enterprises (extranet) or over the public Internet to carry private data in a virtual private network (VPN).

The degree of protection afforded by encryption depends upon the strength of the encryption algorithm. Against brute-force attacks, that strength is determined by the number of possible keys, which in turn is defined by the key size, as shown in Table 1.

A recent brute-force attack was able to try 245 billion keys per second. With this type of computing power, an intruder could try all possible 56-bit keys in 81 hours, finding the

Table 1. *Number of Possible Encryption Keys Is a Function of Key Size*

Key Size	Number of Keys
32 bits = 2^{32}	4.3×10^9 keys
56 bits = 2^{56}	7.2×10^{16} keys
112 bits = 2^{112}	5.2×10^{33} keys
128 bits = 2^{128}	3.4×10^{38} keys
168 bits = 2^{168}	3.7×10^{50} keys

key in an average of 40 hours. However, with 112-bit key and the ability to try 245 billion keys per second, it would take an average of 336 trillion years to discover the key. A Triple Data Encryption Standard system (3DES) uses either 112-bit or 168-bit keys.

Encryption systems in common use today include the following:

- Shared key encryption. Both or all parties possess a previously distributed key that locks and unlocks the data (Figure 4). The sender provides the key to a shared symmetrical encryption algorithm to encode the data before placing it in a packet bound for the remote site; the remote site then provides the key to the same encryption algorithm to decode the data. Shared key encryption systems use DES, 3DES, RC5, IDEA, and other algorithms that are extremely fast. Their strength lies in the length of the key and their resistance to analyzing encrypted data. Their weakness is that if the key becomes known, anyone can decrypt the cipher text.
- Public key encryption. One party possesses a private unlocking key and makes a public locking key (Figure 5 on page 8). Any sender can use the public key to encrypt the communication; the receiver then uses its corresponding private key to decrypt the data. Directory servers from Novell, Netscape, and others can store a digital certificate that contains a user's public key. This system can also be combined with data exchanged at the time of communication to arrive at a shared, session-specific secret key.

  The public key/private key system can also be used to create a digital signature, which is a digest of a plain message encrypted using a key and appended to the plain message. This digest makes it possible to authenticate the sender of the message and verify that the message has not been altered since being sent by the author.

  Public key encryption is very CPU-intensive. It is typically used for small amounts of data where strong security is required.
- Secure key exchange. Both parties first authenticate themselves (often using digital certificates) during a session-specific encryption key distribution process. The session key is created based on data generated by both parties at the time of communication (Figure 6 on page 8). This key can then be used to encrypt and decrypt all other communications.

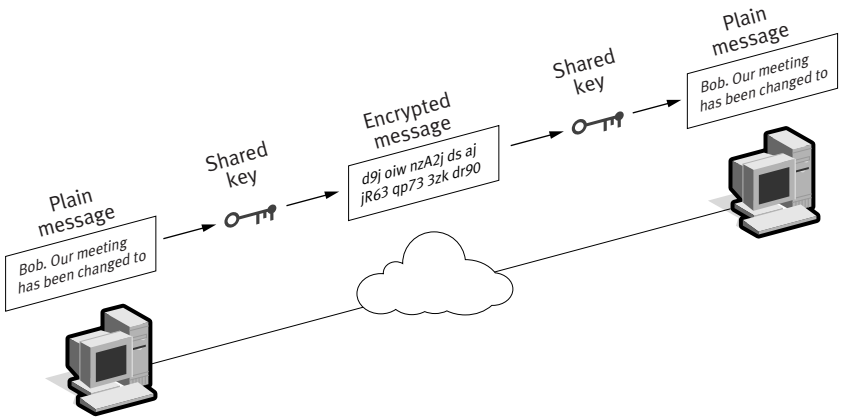

Figure 4. *Shared Key Encryption System*

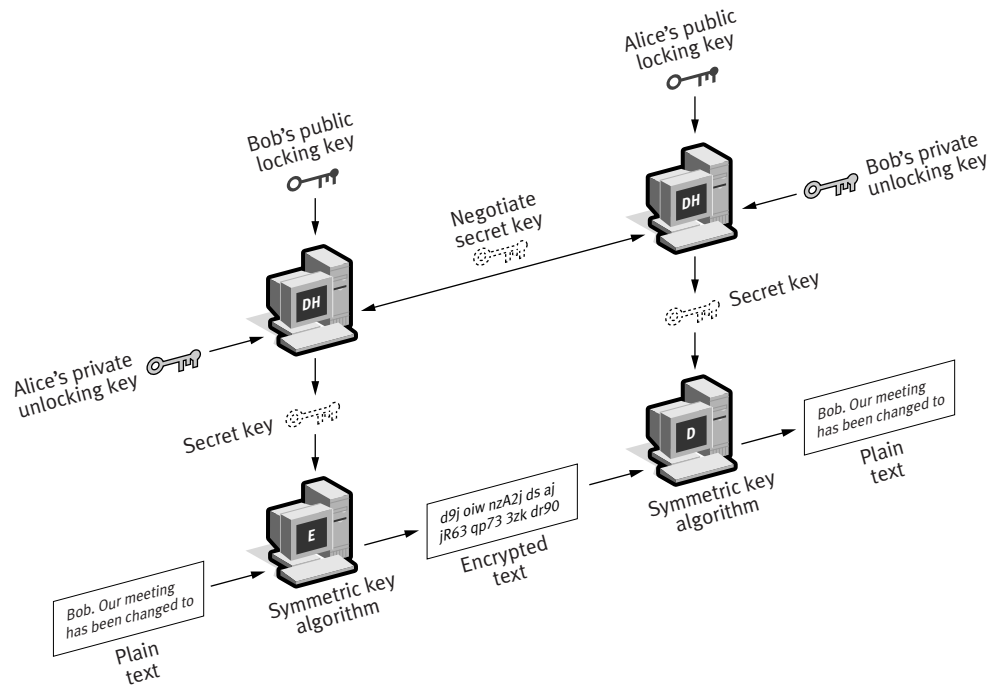

Figure 5. *A Public Key Distribution System*

All encryption systems place an additional load on the network because one or more round trips are needed to authenticate the parties. The machines involved in the communication must also perform large mathematical operations to encrypt and decrypt data, and this can amount to a noticeable increase of CPU cycles on systems that pass many packets. To free the CPU from this task, the conventional burden of encryption systems can be moved to firmware or hardware, such as a coprocessor on the network interface card (NIC) or elsewhere in an embedded system.

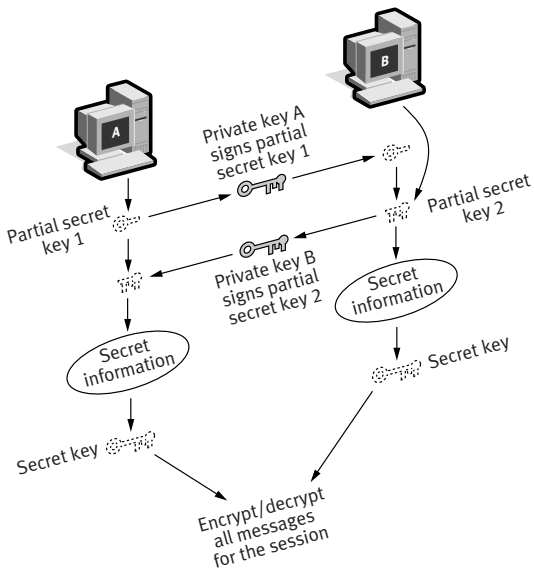

Figure 6. *Secure Key Exchange*

Security Management

A security system should allow for oversight and control by a human authority. Any system that uses authentication requires some central authority to verify those identities, whether it be the /etc/password file on a UNIX host, a Windows NT domain controller, or a Novell Directory Services (NDS) server. The ability to see histories, such as repeated failed attempts to breach a firewall, can provide invaluable information to those charged with protecting information assets. Some of the more recent security specifications, such as IPSec, require the presence of a database containing policy rules. All these elements must be managed for the system to work correctly. However, management consoles or functions themselves represent another potential point of failure of a security system. It is therefore important to ensure that these systems are physically secured and that authentication is in place for any logon to a management console.

Internet Protocol Security

As the Internet becomes more critical to organizations and enterprises of all sizes, the need to protect intellectual property and at the same time conduct business has grown. To promote security for business communications, the Internet Engineering Task Force (IETF) developed Internet Protocol Security. IPSec offers standards-based, consistent security for IP networks.

In an IPSec communication, the two communicating entities (which can be individual hosts or intervening devices, such as routers or firewalls) first establish a Security Association (SA). During negotiation of the SA, the two entities agree on what kind of security will be employed.

The Internet Security Architecture document (RFC 2401) specifies two major traffic security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP).

- Authentication Header (Figure 7). Every IP packet sent during the life of the SA contains an Authentication Header in addition to standard IP headers. This AH verifies that the packet received is identical to the one the sender sent. It contains a Message Authentication Code (MAC), which authenticates the sender of the packet and ensures that the contents of the packet have not been altered. Two techniques are used to create the MAC, both involving message digests and a shared secret (established in a separate security session): (1) Keyed MAC (KMAC): the sender encrypts the digest with the shared secret, and the receiver decrypts it to check for validity; or (2) Hashed MAC (HMAC): the sender creates the digest over the combination of the shared secret and the message text; the receiver does the same and compares the two digests for validity.
- Encapsulating Security Payload (ESP). In the ESP method, the actual payload data of a packet is encrypted using a session key. This key is often derived for the session itself using a public key encryption system. First, the entity on the other end of the key exchange is authenticated, then a key derived from the agreed-upon parameters is transmitted. In addition to encrypting the data portion of the message, ESP can also be used to provide authentication and integrity—features provided by AH. However, ESP security is less comprehensive than that provided by AH. The AH header protects entire messages, whereas ESP only covers the portion of the message after the ESP header.

A single SA specifies one of the two types: AH or ESP. A single communication may employ both AH and ESP by creating two SAs. The calculations required of the computers

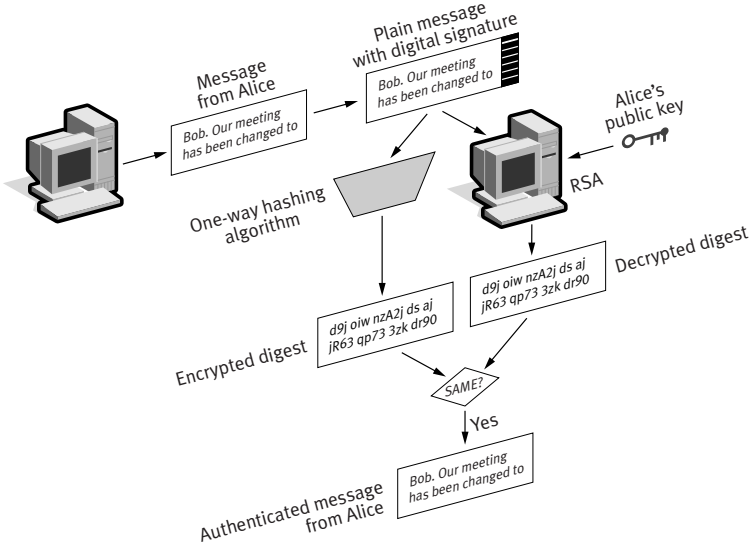

Figure 7. *IPSec Authentication*

involved in an IPSec communication depend on the system of security and the level of encryption employed.

A Security Policy Database (SPD) keeps track of the kinds of security, encryption, and authentication that a particular enterprise can implement, and also keeps track of the active Security Associations. This makes it possible to monitor IPSec activity across the network, and to manage the security systems employed at any given site.

IPSec offers a complete and integrated system for securing data networks. IPSec can be used within the organization or on the Internet because it is based on a set of open specifications including the entire TCP/IP protocol suite. Also, like TCP/IP (and unlike proprietary schemes), IPSec is designed for interoperability between enterprise systems.

Network system designers can integrate IPSec into an existing system in three ways:

- By integrating IPSec processing into the TCP/IP network stack of the host or other device. This requires the host CPU to do security processing.
- By performing IPSec processing in software before the data packets are processed by the existing TCP/IP networking stack (known as a bump in the stack, or BITS). This approach also requires the host CPU to do security processing.
- By performing IPSec processing before the data packets are processed by the host computer (known as bump in the wire, or BITW). This system offloads security processing to a processor on a network component, such as a NIC with an on-board encryption chip, and leaves the CPU free.

The use of an additional processor (or BITW) to handle IPSec security tasks promises the greatest throughput while still delivering the full benefit of a comprehensive security system.

Conclusion

Recent studies by the *Boston Globe* and others indicate that businesses that do not use the Internet for daily communication will suffer in the marketplace within the next five years. As enterprise resources are connected to a larger global network, the implementation of an effective security system becomes imperative.

The security system should provide the following functionality:

- Authenticate users and messages
- Control access to resources based on identity
- Provide protection at all points of entry
- Protect the integrity of data and intellectual property
- Employ encryption systems that cannot easily be broken
- Impose the least possible burden on existing systems
- Interoperate with business partner systems

The IPSec security system offers all of these protections in one integrated, standards-based package. By using coprocessors or other firmware solutions to process security information, the IPSec system can leave existing systems unburdened while still protected.

With an appropriate security system in place, it is possible to use the Internet safely for nearly all facets of today's business, including electronic commerce, Electronic Data Interchange transactions, and electronic banking. Clearly, IPSec is an emerging standard that is enabling the Internet to become a mainstream business tool. ◘

About 3Com Corporation

With more than 200 million customers worldwide, 3Com Corporation connects more people in more ways to information than any other networking company. 3Com delivers innovative information access products and network system solutions to large, medium, and small enterprises; carriers and network service providers; PC OEMs; and consumers. 3Com—More connected.™

3Com Corporation
P.O. Box 58145
5400 Bayfront Plaza
Santa Clara, CA
95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 408 326 5001
World Wide Web:
www.3com.com

3Com Americas International
U.S. Headquarters (serving Canada and Latin America)
Phone: 1 408 326 2093 or
1 408 326 6075
Fax: 1 408 326 5730 or
1 408 326 8914
Miami
Phone: 1 305 461 8400
Fax: 1 305 461 8401/02

3Com Canada
Burlington
Phone: 905 336 8168
Fax: 905 336 7380
Calgary
Phone: 403 265 3266
Fax: 403 265 3268
Edmonton
Phone: 403 423 3266
Fax: 403 423 2368
Montreal
Phone: 514 683 3266
Fax: 514 683 5122
Ottawa
Phone: 613 566 7055
Fax: 613 233 9527
Toronto
Phone: 416 498 3266
Fax: 416 498 1262
Vancouver
Phone: 604 434 3266
Fax: 604 434 3264

3Com Latin America
Argentina (serving Argentina, Paraguay, and Uruguay)
Phone: 541 312 3266
Fax: 541 314 3329
Brazil
Phone: 55 11 246 5001
Fax: 55 11 246 3444
Chile (serving Bolivia, Chile, and Peru)
Phone: 562 240 6200
Fax: 562 240 6231
Colombia
Phone: 57 1 629 4110
Fax: 57 1 629 4503
Mexico
Phone: 52 5 520 7841
Fax: 52 5 520 7837
Peru
Phone: 51 1 221 5399
Fax: 51 1 221 5499
Venezuela
Phone: 582 267 5550
Fax: 582 267 3373

Asia Pacific Rim
Melbourne, Australia
Phone: 61 3 9934 8888
Fax: 61 3 9934 8880
Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247
Beijing, China
Phone: 8610 68492568
Fax: 8610 68492789
Shanghai, China
Phone: 86 21 6350 1581
Fax: 86 21 6350 1531
Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149
India
Phone: 91 11 644 3974
Fax: 91 11 623 3192
Indonesia
Phone: 62 21 572 2088
Fax: 62 21 572 2089
Osaka, Japan
Phone: 81 6 536 3303
Fax: 81 6 536 3304
Tokyo, Japan
Phone: 0120 31 3266
(toll free from Japan)
Phone: 81 3 5977 3266
Fax: 81 3 5977 3370
Korea
Phone: 82 2 3455 6300
Fax: 82 2 319 4710
Malaysia
Phone: 60 3 715 1333
Fax: 60 3 715 2333
New Zealand
Phone: 64 9 366 9138
Fax: 64 9 366 9139
Phillippines
Phone: 632 892 4476
Fax: 632 811 5493
Singapore
Phone: 65 538 9368
Fax: 65 538 9369
Taiwan
Phone: 886 2 2 377 5850
Fax: 886 2 2 377 5860
Thailand
Phone: 662 231 8151 5
Fax: 662 231 8158

3Com Austria
Phone: 43 1 580 17 0
Fax: 43 1 580 17 20

3Com Benelux B.V.
Belgium
Phone: 32 2 725 0202
Fax: 32 2 720 1211
Netherlands
Phone: 31 346 58 62 11
Fax: 31 346 58 62 22

3Com Eastern Europe/CIS
Bulgaria
Phone: 359 2 962 5222
Fax: 359 2 962 4322
Czech Republic
Phone: 420 2 21845 800
Fax: 420 2 21845 811
Hungary
Phone: 36 1 250 83 41
Fax: 36 1 250 83 47
Poland
Phone: 48 22 6451351
Fax: 48 22 6451352
Russia
Phone: 7 095 258 09 40
Fax: 7 095 258 09 41
Slovak Republic
Phone: 421 7 317 850
Fax: 421 7 317 849

3Com France
Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54

3Com GmbH
Munich, Germany
Phone: 49 89 627320
Fax: 49 89 627 32 233

3Com Iberia
Portugal
Phone: 351 1 3404505
Fax: 351 1 3404575
Spain
Phone: 34 1 509 69 00
Fax: 34 1 307 79 82

3Com Italia S.p.A.
Milan, Italy
Phone: 39 2 253011
Fax: 39 2 27304244
Rome, Italy
Phone: 39 6 5279941
Fax: 39 6 52799423

3Com Middle East
Phone: 971 4 319533
Fax: 971 4 316766

3Com Nordic AB
Denmark
Phone: 45 48 10 50 00
Fax: 45 48 10 50 50
Finland
Phone: 358 9 435 420 67
Fax: 358 9 455 51 66
Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01
Sweden
Phone: 46 8 587 05 600
Fax: 46 8 587 05 601

3Com Southern Africa
Phone: 27 11 807 4397
Fax: 27 11 803 7405

3Com Switzerland
Phone: 41 844 833 933
Fax: 41 844 833 934

3Com UK Ltd.
Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903
Ireland
Phone: 353 1 823 5000
Fax: 353 1 823 5001
Manchester
Phone: 44 161 873 7717
Fax: 44 161 873 8053
Winnersh
Phone: 44 1189 27 8200
Fax: 44 1189 695555

To learn more about 3Com products and services, visit our Web site at www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

Printed in U.S.A. on recycled paper

503023-001 4/98