Extranet Security:
A Technical Overview from a Business Perspective

Jennifer Jordan

University of Maryland
Graduate School of Business

May 1, 1997

Abstract

Linking an Intranet to the Internet to enable electronic commerce is the focal point of activity at thousands of companies. Only a handful of organizations provide Intranet access to their business partners, according to various surveys, but close to half are moving in that direction.[1] While an Intranet allows employees access to proprietary information, an Extranet uses the same technology to allow access by trading partners. Extranets will increase revenues, reduce time to market, improve customer service, and otherwise fulfill every CEO's income-statement dreams, according to proponents. A host of equally compelling internal opportunities also awaits Intranet managers and users with vision. [2] Success at reducing costs and improving customer service has made these applications indispensable, but the systems haven't been managed that way. The emerging wave of applications require features, such as daily backup, increased reliability, and robust security that business units are not equipped to deliver.[3] This paper will analyze the security and business issues involved in the movement from Intranets to Extranets from a technological perspective. Also, current technologies will be examined and needs outlined. Finally, final conclusions will be drawn about the future of security in the Intranet/Extranet arena.

[1]Winkler, Opportunities Knock

[2]Winkler, Opportunities Knock

[3]Korzeniowski, Intranet 100

Description of Technology

An Intranet is a private Web site that only allows access by the internal members of an organization. It is built on Internet technology, using the TCP/IP protocol. The content of an Intranet ranges from static pages to a highly interactive site that provides a Web browser front end to legacy applications. Empowering employees by providing them access to the vast databases within an organization is a high-priority opportunity for many companies. Web browsers, HTML editors, and other Intranet tools are the ideal front end to defuse the complexities of multiple incompatible data sources that comprise most data warehouses, reports Thomas Murray, integrated solutions marketing manager at the King of Prussia offices of Lockheed Martin Corp. in Pennsylvania. As many as 20 front-end data-warehouse projects are under way at the aerospace giant, Murray says.[4] In its most basic form, an Intranet is made up of just three pieces of software: a Web server, Web browser, and firewall to keep unwanted visitors out.

Servers

Web servers are the system software that usually reside either on Windows NT or Unix boxes. To deal with today's much more open Internet environment, such security features as IP address and domain-name restriction, secure transaction capabilities, and firewall proxies are available in commercial Web servers. Various forms of encryption are also available, such as public key, MD2 and MD5. Aside from the main Web and Internet services, servers must also support a number of ancillary capabilities, including support for SMTP, POP3, MIME file types, FTP, gopher, newsgroups, and chat rooms.[5]

Web Browsers

Web browsers, which provide the user interface for all Intranets and Extranets, are applications that translate the HTML code to graphical Web pages. Web browsers are rapidly becoming commodities, with the two main suppliers, Microsoft in Redmond, Wash., and Netscape in Mountain View, Calif., giving them away for free, or nearly so.[6]

Firewalls

"A firewall is a process that filters all traffic between a protected 'inside' network and a less trustworthy or 'outside' network."[7] There are three types of firewalls that perform different functions: screening routers, proxy gateways, and guards. Screening routers examine the addressing information contained in the packet header to determine if the packet is allowed onto the network. Data is split into packets for transmission. Each packet has a few bits for the purposes of addressing information. Proxy gateways, on the other hand, look at the data inside the packets. A proxy is a type of software that resides on a server and controls the entry and exit of data to and from the network. A proxy gateway accepts incoming packets as if it was the

---

[4]Winkler, Opportunities Knock

[5]Bharadway and Rodriguez, untitled

[6]Orzech, Software: The Dream Team

[7]Pfleeger, Security in Computing

intended application in order to determine if the packet can continue onto the actual intended application. A guard is a sophisticated proxy firewall in that it contains more complex code than a proxy does. The guard makes security decisions based on "some quality of the data of the communication."[8]

The biggest problem with firewalls, according to consultants and users, is that they're too hard to manage. "Lots of users shoot themselves in the foot trying to administer their firewall," says Michael Zboray, VP for network security at Gartner Group Inc., an IT advisory firm in Stamford, Conn. What's needed, he contends, is foolproof firewalls that require practically no administration. Given the pace of product development, he believes, improved packages should be available by late 1997. [9]

Reacting to this threat, an increasing number of network administrators are installing state-of-the-art proxy-servers, or application-level firewalls as barriers against outside attacks. These gateways provide a choke point at which control and audit can be imposed. They allow access to resources on the Internet from within the organization while providing controlled access from the Internet to hosts inside the private network.[10]

Security Functions in Intranets and Extranets

Before the widespread interest in the Internet, most network administrators were concerned about internal attacks on their networks from disgruntled workers. But with most organizations now connecting to the Internet, the motive for mischief from outside is growing rapidly and creating a major security risk to enterprise networks. According to the Gartner Group, "Given the greater perceived risk of using the public Internet, private networks or Intranets will be the dominant approach to using Internet technology to access confidential information for the next two years (0.8 probability)".[11] Traditionally, security in computer systems is based on three areas: secrecy, integrity, and availability. This section will explain their relevance to Intranet and Extranet technologies.

Secrecy

Secrecy is especially crucial in Intranet/Extranet applications because a company (the host) will have many different parties entering their system to obtain data. Secrecy is the prevention of unauthorized access. In order to prevent unintended access, the host company must create security plans for access control. Access control determines what data, applications and other resources an authenticated user can reach. Companies must identify and classify the types of users that will be accessing their system and assign roles based on those classifications. Therefore, controls can be set up through role-based security enforced through the application and database. Describing this idea in reference to Netscape server products, Andreessen, VP of that company, says:

---

[8]Pfleeger, Security in Computing

[9]Orzech, Software: The Dream Team

[10]EDGE Publishing, NEC's Internet Business Unit Now Shipping PrivateNet 2.0

[11]Gartner Group, Electronic Commerce Infrastructure

> "You can have a global directory that gets replicated to all the different servers that you are running. You can say 'Here are all the directory entries and access control info for people in my company and here is a separate section of the directory for people who are at one of my suppliers.' Those people literally come into your network and they literally log into your directory. They authenticate themselves to your directory so they are just like your internal users and they have access to only a subset of resources."[12]

Also, audit trails should be used to help track user activity.

Where secrecy is the hiding of data from unauthorized users, data confidentiality is the prevention of in-transit security breaches. This type of security is typically provided by encrypting the data, particularly when transmitting it across a network. Web technology can support encryption of transmitted data through the use of SSL or S-HTTP.[13] These issues will be highlighted in the discussion of transport security.

Integrity

Data integrity guarantees that data has not been changed since its last official update. Encryption techniques use a hash function to develop a digest, which functions like a check digit. A hash function uses a hash algorithm, which protects data against modification. "If you want to protect the data against undetected modification, you would compute the hash algorithm result" of the data before it is sent and again after it is sent.[14] Comparing the two will let you know if the data was altered. Given the potential for tampering by hackers, the use of a hashing algorithm should be strongly considered.[15]

Once the data's integrity is assured, proof of the identity of the sender and receiver should be maintained. This function is especially important in Extranets, since proprietary data is transmitted between parties. Because business decisions and relationships rely on this data, it is crucial to identify the parties. Nonrepudiation is handled by a set of protocols that either prohibits the recipient of a message from denying having received it, or prohibits the sender from denying having sent it.[16] Nonrepudiation is accomplished through the use of digital signatures and certification authorities.

Availability

Availability describes the time, in percentage form, that the system is actually accessible to the intended users. Guaranteeing reliability is usually a numbers game. One way to increase availability is to maintain a backup system that will operate if the main system is breached or

---

[12]Kanellos, Interview with Marc Andreessen

[13]Gartner Group, Electronic Commerce Infrastructure

[14]Pfleeger, Security in Computing

[15]Gartner Group, Electronic Commerce Infrastructure

[16]Gartner Group, Electronic Commerce Infrastructure

fails. Also, If the number of servers is reduced, the chances of failure decrease. This fact highlights the need for a central data security plan that includes hardware, software, and data management issues.

Discussion of Security Issues

Remote vs. Local Users

The geographic dispersion of a company's employees has security implications due to methods of access to an Intranet. A company with an employee population residing at one site can be networked by a highly secure LAN, whose main point of vulnerability would be a connection to the Internet. Companies with a dispersed employee population must use remote access methods. An employee can connect either through leased lines or dial-up to one of two network types. First, the Internet provides a low cost solution to companies that wish to transmit data, but involves high security risks. Second, Value-added network (VAN) providers offer a highly secure, but costly means of transmission. A value-added network provider is a company that owns its own cables, routers, and gateways, adds services, such as security measures, and sells network time to its clients. In a WEBWEEK poll, 58% of the respondents reported that their non-headquarter employees access their Intranet via private WAN or VPN lines, while 21% access through direct dial-up.[17] A WAN is a 'wide area network', which means it is a system of cables, routers, and gateways that covers an area larger than that within a single building, or section of a building. A VPN, or 'virtual private network', is made by applying high security to the Internet, so that it seems as though the company using it has its own private network.

Extranets involve tying together the Intranets of two companies for the reason of exchanging competitive information. Therefore, they involve the same security issues as those of an Intranet with remote users. Andreessen, Netscape Corp.'s Senior Vice President, says: "There are a couple ways we see people doing basic configurations for Extranets. One of them is to have a direct lease line where you actually have full control, full physical control, over the line from intranet to intranet. Another way people do it is with a secure link over the Internet where they use the Internet as a universal private number. Having servers outside the firewall that communicate with other servers inside the firewall, it makes a lot of sense. Some 50 percent of Intranets already have partners in them."[18]

Two Layers of Security

When one refers to the layers of a network, often the individual is referring to the OSI Seven Layer Model. This model describes the layers by which network communication occurs. Each layer serves a different function in the transmission of the message. Please refer to the glossary for a more complete description of the OSI Seven Layer model.

Transport Security

Transport security assures that the communications session between the client software and the server software is secure. For example, the Secure Sockets Layer (SSL), after an encryption key exchange authentication process, ensures a secure communications session. Transport security provides "channel security," which allows client/server applications to

---

[17]Gardner, Survey Reveals Scope of Intranet Use

[18]Kanellos, Interview with Marc Andreessen

communicate in a way that cannot be eavesdropped upon. This security, however, only exists between applications, and does not address the security of data after it has been communicated.[19]

SSL's object is to "provide and maintain a secure communications link between a browser and a WWW server." The steps below outline how the SSL protocol actually functions.

- There is a handshake sequence between the client and the server that negotiates an encryption algorithm and a session key, as well as authenticating the server to the client.
- Once complete, all transmitted data is encrypted using the negotiated session key. To ensure integrity of the data, the protocol creates a message authentication code, or digital signature.
- In the current version of SSL, the server can optionally authenticate the client.[20]

Data Security

Data security protocols provide additional security of data within the message being transmitted. Because transport security protocols are application independent, they can be layered on top of applications. Also, because the transport security protocol does not address the security of the data after the communications session has ended, data protection is needed for end-to-end security. The choice of the data to be secured, and to what extent that data is secured, is a decision made by the applications developer.

The common thread through most of the protocols is the reliance on a digital signature. The signature is created using a pair of keys, private and public, which are generated using RSA data security technology. This technology, however, usually requires that there be a trusted third party, known as a Certification Authority (CA), to certify the key pair as being owned by a particular person.[21] Recently, some cutting-edge companies have begun to act as their own CA. These companies have placed certificate servers, directory servers, and key management devices behind their firewalls. This simplistic, yet effective setup allows them to keep user registration and management functions in-house.

Hardware vs. Software

Currently, there is a debate among the vendors as to whether security measures should reside on hardware or software. When asked if moving security functions to software can save on the larger hardware costs, Marc Andreessen of Netscape, replied:

> "Absolutely. That this stuff can be done in the software means that it cannot only be done more cheaply, but it can be done more easily. Instead of having to get the network engineers to spend three months trying to get the network configuration to work, you can do it overnight because you just make additional directory entries."[22]

---

[19]INPUT, Electronic Commerce Over the Internet

[20]INPUT, Electronic Commerce Over the Internet

[21]INPUT, Electronic Commerce Over the Internet

[22]Kanellos, Interview with Marc Andreessen

The network configuration that Andreessen is referring to describes the hardware components of the network, which is the traditional idea of hardware. However, recently newer hardware security technologies, which provide both high levels of security and lower cost, have entered the market.

Two similar types of hardware security tools are smartcards and security tokens. "Smart cards are just one form of what specialists in the field call "hardware implementations" of security. These individuals like hardware because it is harder to compromise than computer software and, as typified by smart cards, it is portable: Its possessor can use it in any compatible piece of equipment, be it a personal computer or point of sale terminal."[23] Thomas E. Honey, director of the certification and public key infrastructure program at International Business Machines Corp., said portability is crucial. "As prices come down, (hardware implementations) will be more generally accepted. People will be carrying tokens in their back pockets." A former Visa International executive who helped IBM take part in recent proving of the MasterCard-Visa Secure Electronic Transactions (SET) protocol for Internet credit card payments, Mr. Honey said the United States is behind Europe in smart card acceptance. SET will become important in Intranets and Extranets as companies may wish to get internal employees and trading partners to actually make purchases from the private Web pages.

As it gets off the ground, SET is largely a software phenomenon, existing in computer hard drives, though not for long if a recent RSA show is any indication. "A hardware token is safer and can be accepted at more places," Mr. Honey said. "We have to get smart card readers out on terminals." A simple diskette could serve the purpose, at least for the time being. Fischer International, a Naples, Fla., cryptography innovator, offers to solve the software vulnerability problem by essentially putting the power of a smart card on a diskette called Crypto SmartDisk. It was designed with tamper-proof storage for encryption keys, preventing the illicit copying to which software methods are prone. Fischer recently took that a step further, modifying the standard diskette with a sleeve for a smart card. The resulting product, Smarty, allows a PC through its disk drive to read a smart card. Users don't have to wait for smart card readers to be incorporated with PCS, as has been advocated by a consortium called the PC/SC Work group.[24]

Bundled vs. Unbundled Firewalls

In addition to the debate between hardware and software security tools, other vendors are engaged in the issue of bundling security features into the Web and firewall servers. Some Intranet server vendors offer firewall software. Dennis Tsu, director of Internet product marketing at Sun Microsystems, says Sun bundles firewall software with its Netra line of Web servers because companies want complete systems that don't need to be integrated. Others vehemently disagree with the bundled approach. Digital Equipment, Hewlett-Packard, and IBM recommend that companies place firewall software on a separate computer running in front of a Web server. Some customers agree. "We have general Internet access with firewalls, but we need to control them better," says Gary Ellis, manager of corporate engineering information

---

[23]Kutler, untitled

[24]Kutler, untitled

technology for Westinghouse Electric Corp. in Pittsburgh. "More than just a firewall is required--we're interested in a firewall server."[25]

Firewalls that are not integrated into the Web servers cause performance flaws. Ideally, all Web servers will have firewalls integrated and enabled. Firewall software is implemented as a separate user process (called the firewall proxy) that filters incoming packets. That causes a huge performance penalty because of the time taken to context-switch into the user process and copy the data back and forth between the firewall proxy and the kernel. Several vendors have attempted to put the code into the kernel, but that has substantially increased the size of the kernel. To resolve those limitations, future Web-server systems will have to incorporate a number of additional features, including support for large-address-space applications, such as integrated search engines, audit trails and enterprise-wide decision support.[26]

Current State

It has been said by Internet pundits that an Internet "year" is equivalent to three calendar months due to the fast pace of change in this market. In order to understand the future of Intranet and Extranet security, we must first comprehend the current state. This section will examine the "cutting edge" of current technologies, including the most advanced vendor offerings.

Encryption

Encryption is used to ensure that, even if data is intercepted during transmission, it cannot be read by an unintended party. It is usually accomplished through the use of a pair of keys. The message is first encrypted with the recipient's public key. When the intended party receives the message, it uses its private key to decrypt it. SecureFile(TM), a personal information security tool, provides a one-click operation to protect sensitive documents for personal use as well as for secure sharing of information amongst a group of users. SecureFile also integrates with existing email packages allowing users to communicate securely over the Internet. Querisoft's SecureFile is completely integrated with the Microsoft Windows 95(R) and Windows NT(R) 4.0.[27] Therefore, with this new product, protecting any document is as simple as a right click to encrypt/decrypt or sign/verify.

Digital Signature

When two companies are transmitting data between them over their shared Extranet, digital signatures are important to ensure non-repudiation, which is proof that a transaction occurred. SecureFile, as mentioned in the previous section, makes signing a transmitted message extremely simple. Similar to encryption, the digital signature is accomplished by encrypting the entire message, or an embedded part of it, with the sender's private key. The recipient decrypts it with the sender's public key. A decrypted message will guarantee that the stated sender was the actual transmitter. "A digital certificate uses public and private keys to ensure confidentiality, guarantees that a user is who he or she claims to be, and offers non-repudiation. Many experts

---

[25]Korzeniowski, Intranet 100

[26]Bharadway and Rodriguez, untitled

[27]Hudda, untitled

believe digital certificates offer much stronger security than traditional passwords and IDs."[28] Digital certificate software and services have been pouring into the market. But despite the rollouts, corporate America is unlikely to quickly embrace the validation and security technology due to a lack of standards and interoperability.[29]

Verisign, the digital certification specialist that RSA spun off a few years ago, demonstrated what it called the first on-line issuance of its Class 1 Digital IDs on smart cards. That demo combined Cryptoflex cards from Schlumberger with other technology from Litronic and Microsoft Corp. Verisign termed it "a major step forward in portable digital identification." President Stratton Sclavos said it showed how "smart cards will become the digital wallet of the future, securely holding and transporting information about our most important relationships."[30]

Certification Authorities

Although digital signatures are accepted in the market, the lack of key certification authorities inhibit businesses from engaging in Web trade. While companies can manage their own creation, storage , and distribution of keys, this process is time-consuming and difficult. Certification authorities not only manage that process, but also provide the key checking function for verification. VeriSign, Inc. is the world's leading Internet Certification Authority, the trusted third party that authenticates, issues and manages digital certificates on the Internet. VeriSign Digital IDs enable trusted electronic commerce by authenticating the individuals, organizations and content involved in an electronic transaction. VeriSign offers its certification services through the company's online Digital ID Center(SM), which operates 24 hours a day, seven days a week from VeriSign's secure operations center located in Mountain View, California. VeriSign's Public Digital IDs are available to all Internet consumers and businesses in ascending levels of assurance designated as Class 1, 2, 3, or 4. They are enabled in more than 50 Internet applications including market leading products and services from AOL, Netscape, Microsoft, and Oracle. VeriSign also offers Private Label Digital ID services built around customized versions of the Digital ID Center for Fortune 500 companies in the financial services, publishing, healthcare, and transportation industries.[31]

With similar technologies, some software vendors are providing packages that automate key management. Entrust is an encryption and certificate management technology from the Secure Networks division of Northern Telecom Limited (Nortel), one of the worlds leading manufacturers of telecommunications equipment. Being Entrust-compliant allows companies to communicate with existing Certificate Authorities on the Internet today, eliminating the need for manual key distribution.[32]

---

[28]Davis, Security Check

[29]Davis, Security Check

[30]Kutler, untitled

[31]PRNewswire, untitled, January 27, 1997

[32]Two Ten Communications, untitled, November 12, 1996

Smartcards

A smart card looks similar to a credit card, but contains an integrated circuit with electronic information. The smart card industry is a 400 million dollar a year market worldwide, growing at 30 percent a year, predominantly in Europe and Asia where the technology has been used to secure banking transactions, telephone and health care payments and medical records. The principal driving applications in North America are banking, digital cellular phones, university campuses, and Internet and Intranet security. Inherently portable and tamper-resistant, smart card technology is well-suited for secure computing requirements.[33]

Smartcards are poised for growth because they will provide a solution to carrying a digital ID. They are portable, which translates to ease of use for employees and trading partners alike. They can be encoded with other identifying information as well as a digital ID.

Firewalls

Conventional firewalls are designed specifically for use on the Internet with the ability to filter the Internet Protocol (IP) traffic only and thereby seemingly protect the network from outside Internet-based hacker threats. Yet computer experts, like the National Computer Security Association (NCSA) and the FBI, indicate that eight out of ten breaches in network security originate within the organizations themselves, where hundreds of non-IP protocols are in common use.[34] An application-level firewall with a proven operating system is more secure than other approaches that merely packet-filter out unauthorized Internet addresses. FireWall/Plus for Windows NT is such a product. The product uses stateful inspection technology that operates at the application, circuit, frame (LAN), and packet levels. It achieves security above and beyond other firewalls by simultaneously filtering traffic at any layer of the communications architecture for any protocol or application. It is the first multi-protocol network security firewall in the industry that ensures the safety and integrity of a corporate Intranet by securing all of the protocols used internally.[35] Most firewalls only monitor addressing of IP packets. Multi-protocol security ensures a network security solution that can support the entire corporate network. In the NT environment, multi-protocol is the norm, so a firewall should secure all protocols to solve security problems correctly - not just the most popular.

Proxy Caching

Filtering and IP network address translation are offered at the packet level for systems and applications not using proxy caching. Proxy caching allows users faster access to HTML pages by storing frequently used pages in a local area proxy cache. Pages will be stored and updated based on frequency of use, file size and time-to-live dates. By delivering faster web access, proxy caching reduces the time users spend waiting to view the information they need, increasing system availability and reliability. Because proxy caching avoids constantly reloading frequently used pages from the Internet, it can lessen the risk of incoming security problems. In addition, the proxy cache includes SSL bind-session support to enable secure transactions with

---

[33]PRNewswire, untitled, January 27, 1997

[34]INPUT, Electronic Commerce Over the Internet

[35]Business Wire, December 3, 1996

SSL web servers.[36]

Security Solutions

As IS takes charge of the Intranet-server explosion, systems-management features come to the fore. A need for backup, performance monitoring, and server management is driving many IS managers to full-service server vendors because they can provide hardware and software packages that prevent intranet collapses. Especially important in the new products is the ability to "tunnel" through the Internet. In other words, through security measures, these products turn the Internet into a virtual private network(VPN). This section will explain the features of recently-announced full-service products from six key vendors.

Milkyway SecurIT SUITE is the first one-stop network security solution incorporating the integrated functionality of four security functions into one package - a firewall, ultra-secure mobile remote access, network security auditing, and security policy designs. At the core of the Milkyway SecurIT SUITE is Milkyway's Black Hole, a full-service firewall product. Black Hole is the only firewall that is Entrust-aware, allowing users to interconnect multiple networks via encrypted tunnels creating VPNs using the industry-leading key management technology from Entrust. Entrust is an encryption, digital signature, and automated key-management product from Entrust Technologies.

The Gauntlet Internet Firewall is an application gateway firewall that is based on minimalism. In other words, "that which is not expressly permitted is prohibited"[37]. Although Milkyway's Black Hole is purported to be the first completely integrated security solution, Gauntlet from Trusted Information Systems was proven to be the fastest by the National Computer Security Association [38]. Furthermore, Gauntlet's Commercial Key Recovery (CKR) capability provides strong cryptographic protection that qualifies for export under US Government regulations. Thus, "users can extend their private networks beyond national borders, without relying on weak encryption methods and without having to give their cryptographic keys to any government agency"[39]. Additionally, Gauntlet extends these features to remote corporate users via its Gauntlet PC Extender.

In addition to virtual private networking, the option to add unlimited nodes, or trading partners, to a company's Extranet is extremely valuable. NEC Technologies Inc.'s Internet Business Unit (IBU) is now shipping its PrivateNet Firewall, which includes a new graphical user interface (GUI), tunneling, and multiple authentication support. It also incorporates IBU's recently announced TCP/IP software enhancement that protects networks against denial-of-service (SYN flooding) attacks from hackers."[40]

---

[36]M2 Presswire, untitled, December 13, 1996

[37] Baker, Extranets: The Complete Sourcebook

[38] Firewall Product Functionality Summary, July 22, 1996

[39] Baker, Extranets: The Complete Sourcebook

[40]EDGE Publishing, NEC's Internet Business Now Shipping PrivateNet 2.0

The Fujitsu Software Corp. has introduced the TeamWare Intranet Security Server. According to the company, the new software "provides remote and mobile users with a secure connection to corporate Intranets." The company says that the product enables users to establish authenticated and encrypted connections across the Internet or any other public network. Features include user and client/server authentication, access control, data sealing, and data encryption. The product is based on Internet Protocol (IP) tunneling between security clients and a security server, and works with any standard TCP (Transmission Control Protocol)

Digital Secured Networks Technology, Inc. (DSN) has added some key automated firewall capabilities to its new Intranet security solution, the NetFortress. It automatically seals off all unwanted communications to a corporate LAN while encrypting and authenticating all authorized communications to other NetFortress protected hosts. Scrambled streams of data are generated with complete transparency to users and administrators, and with no cost to network performance.[41]

IBM's SecureWay Cryptographic Infrastructure divides security into four areas-applications, services and subsystems, APIs and tool kits, and cryptographic engines-and gives developers common specifications for creating and integrating encryption and security technologies into mainstream applications.[42]

Future Issues

Market trends suggest that Intranets and Extranets are here to stay and not just a passing technological fad. The "Wave II" study, performed by executives at Info World in October 1996, revealed that 63 percent of the respondents have or plan to implement an Intranet, up over 54 percent from the April study. Wally Palmer, Info World's director of research, said, "The implementation of Intranets means that over time many corporate applications will only have to be written to TCP/IP, rather than a machine or network operating system."[43] WEBWEEK reported in their January 6, 1997 issue that in a survey of 57 Intranet deployers, that 39% already allow non-employees to enter their Intranet. Furthermore, 42% of the respondents said that they are considering allowing access to outside parties.[44] As this trend continues, CIOs will be forced to face the issues involved in setting up their own Intranet and then tying it to those of their trading partners.

In order for Intranets and Extranets to proliferate, certain security issues must be resolved in the future. Both transport and data security must be increased in order to increase the level of confidence in Internet technologies in the business community. The key to achieving this in the near future is certification authorities. They authenticate, issue and manage digital certificates on the Internet. However, CA s alone will not provide enough incentive for companies to engage in the widespread use of digital signatures. Software that automates key distribution and collection

---

[41]Business Wire, untitled, December, 11, 1996

[42]PC Week, October 10, 1996

[43]Stamates, Study Shows Intranets Growing

[44]Gardner, Survey Reveals Scope of Intranet Use

is needed to manage the process. Finally, even if CA s and automated key distributors exist, companies will still find the management of these keys cumbersome. “That's because until now, certificate software has taken a hierarchical approach. That means that a certificate can be authenticated only by the authority that issued it. It also means users can end up with a pile of digital IDs.”[45] Therefore, a central key authority is needed. Currently, there are a few certification authorities including VeriSign, GTE’s CyberTrust, Nortel, and IBM.[46] However, it is clear that without a single governing body over the key authenticating process, exchanging information for trade over the Internet will continue in its infancy stage.

In addition to the importance of key management, systems management is also an area that must be improved. The six security system vendors mentioned above have realized this need and released products before a large demand exists for them. They realize that being first to market with these technologies will be important in building trust in the future. Firewall software that is bundled with the Web server itself will be crucial, as it will be fully integrated into the system. This feature, along with graphical system management interfaces will allow system administrators to manage the many levels of access and encryption issues that will be present.

Currently, digital ID s are the answer to encryption and authentication in transport security, but future technologies may provide more secure solutions. Tokens and smartcards can provide the storage capacity for biometric information that cannot be duplicated. In addition to digital certificates, the chip cards or other tokens could potentially hold a photograph or other more sophisticated means of biometric identification, such as a fingerprint, voiceprint, or eye pattern. PCMcIA cards, the standard input devices for laptop computers, are an already popular alternative. One example, the Luna token from Chrysalis-ITS Inc. of Ottawa, Canada, gained momentum this week with several alliance announcements. In perhaps the most prominent, Luna will be available for encryption with two Netscape Communications Corp. products, Communicator and Enterprise Server." Especially in the financial and government communities, we see the need for higher-level security that is tamper-proof and allows for the storage of certificates," said Tim J. Hember, president of TimeStep Corp., a Canada-based Newbridge Network subsidiary that is providing encryption technology and tokens to Chrysalis-ITS.[47]

Final Conclusions

Intranets and Extranets are technologically feasible, but currently only the early adopters are investing in them. Security fears are the number one reason that CIOs gave for not allowing trading partners into their Intranet in a survey by Gartner Group.[48] The emergence of certification authorities, automated key distributors, and smartcards have brought Intranets and Extranets to the edge of acceptance and proliferation, but issues remain. Through the issuance of keys by a

---

[45]Davis, Security Check

[46]Roberts, Where Trust is Like A Spy Movie

[47]Kutler, untitled

[48]Gartner Group, Electronic Commerce Issues

central authority, key management will be facilitated. Also, smartcards may provide a solution to the portability of digital ID s, but biometrics will provide a non-duplicable way to identify users. When these issues are solved, the incredible benefits of Intranets and Extranets can be fully realized.

Glossary

Availability - Availability describes the time, in percentage form, that the system is actually accessible to the intended users.

Certification Authority (CA) - A CA certifies that the key pair is owned by a particular person. Also, the CA authenticates, issues and manages digital certificates on the Internet.

Digital signature - Similar to encryption, the digital signature is accomplished by encrypting the entire message, or an embedded part of it, with the sender's private key. The recipient decrypts it with the sender's public key. A decrypted message will guarantee that the stated sender was the actual transmitter. " A digital certificate uses public and private keys to ensure confidentiality, guarantee that a user is who he or she claims to be, and offer "non-repudiation" - proof that a transaction occurred.

Encryption - Encryption is used to ensure that, even if data is intercepted during transmission, it cannot be read by an unintended party.

Firewall - A firewall is a process that filters all traffic between a protected 'inside' network and a less trustworthy or 'outside' network. There are three types of firewalls that perform different functions: screening routers, proxy gateways, and guards.

Integrity - Data integrity guarantees that data has not been changed since its last official update.

Non-repudiation – Non-repudiation is handled by a set of protocols that either prohibits the recipient of a message from denying having received it, or prohibits the sender from denying having sent it.

OSI Seven Layer Model - This model describes the layers by which network communication occurs. Each layer serves a different function in the transmission of the message.

The table below describes each layer:

Layer	Name	Activity
7	Application	User program; initiates and processes messages
6	Presentation	System utilities; standardize data appearance. text compression
5	Session	Operating system; establish user-level session and manage existing sessions
4	Transport	Network manager; end-to-end error detection and correction
3	Network	Network manager; manage connection, routing
2	Data Link	Hardware; reliable data delivery over physical medium, packet framing
1	Physical	Hardware; individual bit communication of data

Packet headers - Data is split into packets for transmission. Each packet has a few bits for the purposes of addressing information.

Proxy server - A proxy is a type software that resides on a server and controls the entry and exit of data to and from the network.

Secrecy - Secrecy is the prevention of unauthorized access.

SSL - SSL's object is to "provide and maintain a secure communications link between a browser and a WWW server."

VAN - value added network - A value-added network provider is a company that owns its own cables, routers, and gateways, adds services, such as security measures, and sells network time to its clients.

VPN (virtual private network) - VPN, or 'virtual private network', is made by applying high security to the Internet, so that it seems as though the company using it has its own private network.

Web server - Web servers are the system software that resides either on Windows NT or Unix boxes usually.

[49]Pfleeger, Security in Computing

Bibliography

Baker, Extranets: The Complete Sourcebook, McGraw-Hill, 1997.

Bharadwayand and Rodriguez, PRNewswire, December 2, 1996.

Business Wire, untitled, December 11, 1996.

Business Wire, December 3, 1996.

Davis, Beth "Security Check." *InformationWeek*, February 10, 1997.

EDGE Publishing, "NEC's Internet Business Unit Now Shipping PrivateNet 2.0." December 13, 1996.

Gardner, Elizabeth, "Survey Reveals Scope of Intranet Use." *WebWeek*, January 6, 1997.

Gartner Group, "Electronic Commerce Infrastructure." December, 1996.

Gartner Group, "Electronic Commerce Issues." February, 1997.

Hudda, untitled, Business Wire, January 28, 1997.

INPUT, "Electronic Commerce Over the Internet." January, 1997.

Kanellos, Michael, "Interview With Marc Andreesen." *Computer Reseller News*, March 10, 1997.

Korzeniowski, Paul, "Intranet 100." *InformationWeek*, November 18, 1996.

Kutler, untitled, *American Banker*, November 1996.

M2 Presswire, untitled, December 13, 1996.

Nash, Kim S. "Extranet: Best of Both 'Nets." *ComputerWorld*, August 12, 1996.

National Computer Security Association, "Firewall Product Functional Summary." July 22, 1996.

Orzech, Dan, “Software: The Dream Team.” *InformationWeek*, November 18, 1996.

PC Week, “Intranet Security.” October 10, 1996.

Pfleeger, Security in Computing. Upper Saddle River, NJ: Prentice Hall, 1997.

PRNewswire, untitled, January 27, 1997.

Roberts, Bill, “Where Trust is Like a Spy Movie.” *WebWeek*, January 6, 1997.

Stamates, David, “Study Shows Intranets Growing.” *WebWeek*, January 6, 1997.

Two Ten Communications, untitled, November 12, 1996.

Winkler, Connie, “Opportunities Knock.” *InformationWeek*, November 18, 1996.