

Everything You Wanted to Know About B2B Security*

(* But were afraid to ask.)

Ralph Berwanger
Ambassador to Standards, bTrade
rberwanger@btrade.com
972-580-3970

January 2003

Everything You Wanted to Know About B2B Security*:
*(*But Were Afraid to Ask)*

[This page left intentionally blank.]

Introduction

Depending on your point of view, security is either magic or mathematics. Both perceptions are correct. The totality of security functions is performed within black boxes—either in hardware or software form. Security functions (composed of a series of complex computations) are hidden from inspection by all; therefore, they are often seem as high-tech slight-of-hand.

Governments protect strategic information from exposure to potential adversaries—it has been that way from the dawn of time. We often associate the protected information with military secrets. However, the 'classified' material includes information from a variety of areas, to include: political, economic, medical, and scientific. Information requiring the highest degree of protection was labeled 'TOP SECRET' information. The belief was that compromise of 'TOP SECRET' would cause irreparable damage to the security of a nation. Exposure of this information could result in the total destruction of a nation. There is a direct corollary between national and business information. Enterprises that do not protect their proprietary information risk irreparable damage.

bTrade is at the heart of the world's greatest trading networks. Since 1990, bTrade has been delivering B2B infrastructure solutions to the Fortune 500 and over 100,000 of their most important business partners. Our expertise in leading migrations on behalf of many large companies such as American Airlines, FedEx and Honda, coupled with our experience with assisting hundreds of Wal-Mart and Meijer suppliers gives bTrade the ability to identify and act on the most common issues in implementing B2B over the Internet.

Examine your data

Data security must be understood within the context of business requirements and business processes. Before trying to understand the science of digital signatures and encryption, assess the value of the institution's information to the information's owner and external parties. It is not surprising that enterprises discount the importance of some of its most valuable information. They lock up the formulas for their products but expose the names and addresses of their customers.

After establishing the information's value, analyze the data's risk of exposure. Some highly sensitive information may require little protection beyond that already provided. Other information categorized as having only moderate value may require an entirely new security regimen to protect it. Information owners should select security services based on the information's value and the potential risk of exposure. While a comprehensive risk analysis will benefit most organizations, a set of common sense questions that can identify a fundamental need for some level of security are:

- Do non-trusted individuals have access to your information?
- Can competitors leverage your information to weaken your position within the market place?
- Can non-trusted individuals access information that obligates organizational resources?
- Can non-trusted individuals access information about strategic plans or partnerships of your organization?
- Is private information about your clients exposed to non-trusted individuals?

Everything You Wanted to Know About B2B Security*: (*But Were Afraid to Ask)

Understand the threats

Threats to the security and integrity of digital information come from both internal and external sources. Attacks are considered internal because of who initiates the attack, not where they are conducted. Internal attacks comprise the vast majority of attacks. These attacks permit employees to steal, alter, or destroy information belonging to the enterprise. Attacks that come from individuals who do not belong to an organization are classified as external.

Attacks against digital information take multiple forms. The attacks can allow competitors to examine and use an enterprise's proprietary information, they can limit an enterprise's ability to communicate, or they can misrepresent an enterprise's information to another party. There is a stark reality associated with these attacks—they are seldom detected at their first occurrence. The enterprise that discovers a security breach may never know how much of their data has been exposed to unauthorized individuals.

Passive attacks

Passive attacks are the most insidious and most difficult to detect. These attacks permit unauthorized parties to monitor an enterprise's digital exchanges without any indication that the monitoring is taking place. Sometimes, individuals conducting passive attacks cause no damage to the enterprise—the attackers simply make a game out of accessing information — other times these attacks can be very damaging.

Attackers can use information obtained through these clandestine means to recast product offerings or beat a competitor's product to market. Entire marketing programs can be neutralized by these attacks. Computer hackers capturing unsuspecting consumers' credit card numbers are frequently associated with this class of threat.

Active attacks

In 1999, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Ku Klux Klan were attacked by political activists protesting the site's politic¹.

On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of Jörg Haider and his party into a coalition government.²

Active attacks can be categorized in two types — denial of service and information manipulation. Denials of service attacks are intended to restrict an organization's ability to communicate. There are numerous examples of denial of service attacks against government and commercial Internet sites. These attacks bombard information servers with more messages than they are able to process. The end result is that the attacked server collapses under the weight of the message traffic. Other times, the servers are inundated with fabricated service requests. The attacked server stays busy servicing these requests and is not available to perform valid requests.

In either case, the organization that owns the Internet server is not receiving value for their

¹ See Flashback Sweden <http://www.flashback.se/hack/1999/>.

² To view a copy of the hacked web site, see <http://www.flashback.se/hack/2000/02/07/1/>

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

investment. The impact of these attacks can range from moderate annoyance to loss of revenue. Either way, the significant byproduct of these attacks is a loss in confidence in an enterprise's communications infrastructure.

Information manipulation attacks take a variety of forms. All can be very painful to the enterprise under attack. Attackers intercept information - then the mischief begins.

In the first attack scenario, information can be *misdirected*—forwarded to a party other than the intended party. Sensitive information can suddenly be projected into the public domain. Sometimes the information simply embarrasses the data's owner; however, at other times the information becomes the property of individuals with criminal designs.

Attackers can also *reply* information. Multiple copies of a single message are forwarded to the intended receiver of the information. If the information is a notice regarding an upcoming event, it is a nuisance: if the information is a purchase order, the attack could have tragic implications; failed deliveries, incorrect inventories, and lost customers.

Data modification attacks are also information manipulation attacks. As the name implies, these attacks change the content of the information exchanged between parties. The impact of these attacks is evident. Identities within the information are incorrect, dates and schedules are wrong, quantities are invalid. The residual effect of these attacks is they cause all subsequent information to be suspect.

Dealing with security threats

Mature security services have been devised to deal with potential threats to digital information. They range in complexity and cost from almost no cost to multi-million dollar systems. It will be the decision of business managers to select the security services that best meet the perceived security threats within a defined budget.

Security controls are much more than pass phrases, they include physical security policy for your computer equipment and data access policies. This paper discusses security features that protect the integrity and confidentiality of information exchanged between business partners; however, a moment must be spent speaking about protection of the information within the confines of the originating organization. All security analysts reveal that the greatest risk of attacks against business information occur within the organization owning the information.³

According to a study conducted in 1999 by Michael G. Kessler & Associates Ltd., disgruntled employees are the greatest threat to a computer's security.⁴

Employees that steal confidential information and trade secrets account for thirty-five percent of the theft of proprietary information.⁵

³ Sinrod, Eric J. and Reilly, William P., "Hacking Your Way To Hard Time: Application Of Computer Crime Laws To Specific Types Of Hacking Attack," *Journal Of Internet Law*, (1999).

⁴ David Noack, *Employees, Not Hackers, Greatest Computer Threat*
http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html.

⁵ *ibid.*

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

In fact, data suggests that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to outside hackers with modems.⁶

Internet Security Systems' Chris Klaus estimates that over eighty percent of the attacks on computer systems are committed by employees.⁷

If information is of critical value to an organization, access to the information should be limited to only those who require access to the information.

Methods for limiting access are widely available. They range from storing the information on removable, magnetic media to password protecting directories and files on mass storage devices to encrypting data maintained on computer systems. The problem is not selecting a method for protecting the information; the problem is identifying what information must be protected and then implementing a policy to ensure that proper security is maintained.

Protecting data integrity

Data has integrity when the data received is exactly what was sent. Most business processes desire assurance of data integrity. Integrity is normally achieved by producing a hash value⁸ for the data. There are several computer algorithms that use complex mathematical processes to generate the *hash* value. Examples of these algorithms would be MD5 or SHA1. Both of these examples are in wide use today.

The hash value is computed by the sending party and forwarded to the receiving party along with the data. The receiving party computes a hash value for the received data and compares the value with the value provided by the sender. If the values match, the data is understood to have integrity.

Hashing does not assure the receiver of the authenticity of the data. The receiver of a message cannot be guaranteed that the originator of the message applied the hash value in a message. An active attack on the data could have intercepted the data, changed the data, added a new hash value, and then forwarded the data. This means that the hash is only intended to detect changes that have occurred to the data while it was in transit.

Additional security services are required to provide data authenticity.

⁶ Richard C. Hollinger & Lon Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116 (1988).

⁷ Matthew Nelson, *Internet Security Systems' Chris Klaus says companies should close back doors to be secure*, INFO WORLD, Jan. 10, 2000, at 40a. According to a recent survey of 643 computer security practitioners in the U.S., 71% reported unauthorized access by insiders. Computer Security Institute, *Ninety percent of survey respondents detect cyber attacks, 273 organizations report \$265,589,940 in financial losses* (Mar. 22, 2000) http://www.gocsi.com/prelea_000321.htm.

⁸ The Open Group, Technical Standard Common Security: CDS and CSSM, Version 2; (May 2000). A cryptographic algorithm used to compress a variable-size input stream into a unique, fixed-size output value. The function is one-way, meaning the input value cannot be derived from the output value. A cryptographically strong hash algorithm is collision-free, meaning unique input values produce unique output values. Hashing is typically used in digital signing algorithms.

Protecting data authenticity

Paper documents historically use hand-written signatures to authenticate the information in a document. The signature implied that the information contained in the document was the information intended for delivery to the receiver. The signature, bound to the document when the ink permeated the paper, provided 'non-repudiation of origin'. The sender of the document could not claim that the document did not originate with the sender. There was always the possibility of forgery, so notary services were employed to provide real 'non-repudiation of origin'. The electronic information realm actually supports data authenticity in two areas: it assures the receiver of the identity of the sender and assures the receiver that the information received is exactly what the originator sent.

Authentication is achieved by using a *digital signature*.

The digital signature is actually a numeric value, the result of a sophisticated mathematical calculation. A digital signature should not be confused with digitized signatures. Digitized signatures are graphical representations of a physical signature. They are clever additions to electronic documents but are not useable in any security service. They can be easily copied and reused by any person with access to the signature graphic. It is currently unknown how many false documents have been signed using signatures extracted from the Internet.

Digital signatures employ asymmetric cryptographic techniques. This means that a pair of keys, versus a single shared key, is used to create and validate a digital signature. The technique uses a *private* key value to create the digital signature value. This private key is protected by the owner of the key and never shared.

The second key, the *public* key, is provided to anyone who needs to verify the digital signature. Digital signatures are created through a two-step process. The first step in creating a digital signature is to hash the information to be signed. This is the hash process previously discussed in this document. The hash value serves two purposes: it is an important input to the digital signing algorithm and it will permit the receiving site to verify the integrity of the information.

Passing the hash value along with the private key value into the signing algorithm produces the actual digital signature value. This digital signature value is passed to the receiver, along with the information that was signed. Data authentication reverses the signing process. First, the receiver presents the digital signature value and the information sender's public key value into a signature validation algorithm.

There are two byproducts of the signature validation algorithm. First, the algorithm will indicate whether the signature value is valid. Second, the algorithm produces a hash value. This hash value is equal to the hash value that was used to create the digital signature.

As a last step, the received information is hashed. The hash value of that process is compared to the hash value created by the signature validation process. If the two are equal, then the information can be assumed to be exactly what the originator signed.

Protecting data confidentiality

Imagine a context where there is a large body of information that exists for a very specific audience. Only those belonging to the intended audience should have access to the information.

There are a variety of encryption methods and cryptographic algorithms used to provide confidentiality for this category of information. Widely used encryption techniques are classified as either symmetric or asymmetric.

Symmetric encryption

Symmetric encryption techniques employ a single encryption key that is shared with all who have access to the information. The information owner uses the symmetric key to encrypt the information. Anyone desiring to use the data in its original form must use the symmetric key to decrypt the information.

Asymmetric encryption

Asymmetric encryption techniques confuse many people; however, when the process is examined, minus the intimidating formulas, it is a very understandable transformation method. Asymmetric encryption techniques are similar to the digital signature techniques since each uses key pairs to perform the cryptographic transformation of the data. The difference is that each party (sending and receiving) will use two keys to perform the cryptographic operation.

The sending party will use the sender's private key and the receiver's public key to encrypt the symmetric key value. The receiving party will use the receiver's private key and the sender's public key—the reciprocal key values—to decrypt the symmetric key value.

Asymmetric techniques are slow in comparison to symmetric techniques. Most implementations actually use a symmetric process to encrypt plain text information; for example the Digital Encryption Standard, also known as DES. Then an asymmetric technique is used to encrypt the symmetric key that was used to encrypt the plain text.

A long list of potential cryptographic solutions can be produced supporting an organization's confidentiality requirements. Each algorithm identified will provide varying degrees of cryptographic strength. It is possible to increase the strength of a candidate algorithm by modifying some of the parameters used by the individual cryptographic process.

For instance, an order of magnitude of strength may be achieved by increasing the length of the cryptographic key. It is also possible to degrade the efficiency of a specific security solution by incorrectly implementing the cryptographic algorithm. This is often the result of conflicts within the complex mathematical transformations that are applied to the plain text information. Simply stated, if you shuffle cards enough, you can return them to a state close to the one they were originally in.

It is critical that individuals knowledgeable of the interdependencies of the security environment examine a specific security implementation. The goal of the examination is to ensure that the cryptographic parameters used by a security process are properly guarded and that the process is implemented according to approved standards.

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

Persistent versus non-persistent security services

The analysis of a specific user's security requirements must determine how long the specific security features will remain with the information being protected. Many times, there are no requirements to maintain the information in an encrypted form - only to protect the information while it is in the communications channel. In addition, the operational environment may require digital signatures to be maintained for many years.

Therefore, the security implementation must select the correct security protocols and processes to support the persistence requirements of a specific business environment. Security techniques are applied to data using a variety of methods. Some techniques are tied directly to the method used to communicate the information; some methods are based on the syntax used to represent the data.

All security services supplied via the transport system are identified as *non-persistent*—they expire with the delivery of the information. Other security services applied through a defined data syntax that is independent of the transport method used to exchange the information are identified as *persistent* security services.

Transport security

Transport security is designed to protect information while it is in transit between the sender and receiver. It is point-to-point. When information is forwarded to an intermediate point for delivery to the final destination, the sender can only be assured of the security services between the point of origin and the intermediate point. It is the responsibility of the intermediate point to apply the security services between itself and the next intermediate point or the final destination.

This technique can be achieved using either hardware or software devices. Early security solutions relied on the use of hardware devices; this was a fairly expensive solution. Newer technology permits less expensive software to perform the encryption functions heretofore performed by hardware.

Secure Socket Layer (SSL)⁹ technology is one software technique that provides confidentiality. There are multiple versions of SSL in use; the most recent is version 3.0. Additionally, a new standard *Transport Layer Security*¹⁰ (TLS)—an improved version of SSL—is the more current security standard. A benefit of using SSL or TLS is that it is relatively low cost to implement and is fairly ubiquitous. SSL and TLS do not explicitly provide message authentication. There is an implicit authentication capability provided when the SSL or TLS communications session is established. Depending on the version of the protocol used, single or dual party authentication is provided. This authentication is not discrete to the information being passed; rather, it is discrete to the parties participating in the communications session. SSL 3.0 and TLS support a data hashing process that reports the integrity of the information; so combining the user authentication with the integrity checks provides a quasi-authentication capability.

⁹ Frier Alan O, Karlton Philip, and Kocher, Paul C.; The SSL Protocol Version 3.0 (Internet Draft), Internet Engineering Task Force, March 1996.

¹⁰ Dierks, T and Allen, C. , Internet Engineering Task Force RFC 2246: The TLS Protocol Version 1.0, January 1999.

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

Syntax Security

Syntax-based security provides varying degrees of persistence. In all cases, the security continues only as long as the information secured remains in the syntax where the security services were applied. Once the information is transformed into another format or protocol, the security features from the previous protocol are lost. There are many different protocols that contain security features. The Secure/Multipart Internet Mail Extensions (S/MIME)¹¹ protocol is the method used largely in electronic mail exchanges and for protecting Electronic Data over the Internet.¹²

This protocol provides digital signatures and confidentiality. Information secured using this protocol has a level of security similar to SSL without the secure channel. The security services do not persist beyond the mail agent that processes the mail message. It is possible to archive the original S/MIME communications to provide some persistence of the security for the information if the requirement exists. S/MIME employs the RSA encryption¹³ algorithm. There is a similar secure MIME technique that uses *Pretty Good Privacy* (PGP) encryption.¹⁴ It is referred to as PGP/MIME. The only difference between these two mail-privacy techniques is the underlying cryptography.

Other syntax security schemes, like the ASC X12¹⁵, UN/EDIFACT¹⁶, and eXtensible Markup Language (XML) Digital Signature¹⁷ standards provide stricter definition of specific data structures to secure the data. The syntax security schemes are constructed to ensure that the security features can exist without considering the transport mechanism that is used to communicate the information. For example, a secured ANSI ASC X12 transaction set can be communicated using commercial value-added networks (VANs), the Internet, or on a diskette.

The security infrastructure

Asymmetric encryption techniques are in wide use for personal and business applications. This demands the use of asymmetric keys to support these security processes. The major issue surrounding the use of the asymmetric keys is their trustworthiness.

Software applications are available to permit any computer user to create a set of cryptographic keys that can be freely exchanged. For data exchanges that do not risk financial or legal commitments, these keys may be adequate. The problem arises when the receiver of secured information must trust the identity of the reported sender. Could someone have misrepresented the key? Was the key valid when it was used?

¹¹ Ramsdell, B.; Internet Engineering Task Force RFC 2633: S/MIME Version 3 Message Specification, June 1999.

¹² Internet Engineering Task Force, RFC 1767, MIME Encapsulation of EDI Objects, June 1992

¹³ RSA Laboratories, PKCS #1 v2.1: RSA Cryptography Standard, September 17, 1999

¹⁴ For more information, see <http://www.counterfactual.org/crypt/index.php3> .

¹⁵ American National Standards Institute Accredited Sub-Committee X12 Electronic Data Interchange, www.X12.org

¹⁶ United Nations/Electronic Data Interchange for the Facilitation of Administration, Commerce, and Transport is defined in the International Standards Organization (ISO) Standard 9735. Security components are specified in Parts 5,6,7, and 9. www.un-edifact.org .

¹⁷ Internet Engineering Task Force and Worldwide Web Consortium, XML–Signature Syntax and Processing Specification, June 2000. www.w3c.org .

Everything You Wanted to Know About B2B Security*: ***(*But Were Afraid to Ask)***

A formal *public key infrastructure* (PKI) establishes the integrity and validity of asymmetric keys. The PKI has two major functions: authenticate the identity of individuals or organizations who are issued asymmetric key values and generate public key values in a form that will permit them to be validated prior to use. The PKI normally generates and signs a digital certificate containing identification information about the certificate owner and the public key value of the asymmetric key pair. Presently, digital certificates are formed according to structures defined in the X.509, version 3 format.¹⁸

A PKI is built on a very specific trust model. The model assumes that anyone who uses a certificate generated by a PKI possess a high degree of confidence in the PKI. An identity that is authenticated by a PKI is not questioned within the context of the security policy used by the PKI to prove the identity of the certificate owner. The PKI security policy may require that two forms of photo identification be presented to the PKI prior to issuance of a digital certificate or may require a less stringent criteria such as having certificate requesters sign statements attesting to their true identity. All digital certificates are treated as valid unless the PKI reports the contrary. Any party using a digital certificate can verify the certificate's validity based on the certificate issuer's digital signature stored in the certificate.

Remember the trust model— if you trust the PKI and the certificate is signed by the PKI, the certificate is valid. Checking the issuer's digital signature does not prove that the certificate is STILL valid, only that it was created by the PKI and that it has not been altered. The certificate must also be checked to ensure that the issuer has not revoked it. Passing this test, the certificate is determined fit for use.

The structure of the PKI can be tailored to the specific requirements of an organization. The PKI could exist external to the organization; a third-party vendor could generate certificates as a commercial service. The PKI could also be an organic component of an enterprise. The benefits to these options need to be carefully examined before deploying a PKI strategy. The cost models and benefits widely vary between the two options.

¹⁸ International Telecommunication Union, Data Networks and Open System Communications - Directory (ITU-T Recommendation X.509), June 1997.

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

Conclusion

Data security techniques are not rocket science, yet they must be expertly introduced to a business environment to ensure consistent results. An improperly configured security system is more dangerous than no system at all, so enterprises must take time to do it right. Bulletproof vests are great, but they will not protect against airborne chemical agents. Security solutions, either hardware- or software-based, must match the actual security threats of the enterprise. One must determine what information must be protected and from whom it must be secured. Spend time correctly assessing your security risks and planning solutions that adequately mitigate the risk. Correctly implement the security solution to ensure that it does what it was intended to do. These steps are all standard components of the planning of security solutions. Prudent managers would never allow a system to operate within their enterprise without having considered these issues.

About the author

Ralph Berwanger is the Ambassador to Standards and has 20 years experience designing and implementing electronic commerce solutions for business and government. In 2002, Mr. Berwanger was elected chair of the Trade Facilitation and Business Process Group of UN/CEFACT Forum, which plays a leading role in defining eBusiness standards. In 1999, he was elected as Vice Chair of the ASC X12 Committee where he had been an active contributor since 1991, including service as the chair of the Data Security Work Group. Mr. Berwanger holds a BS in Education from the University of the State of New York and a BS in Computer Science from the University of Maryland. He earned a Master's degree in Strategic Intelligence from the Defense Intelligence College while on active duty in the United States Air Force. bTrade is at the heart of the world's greatest trading networks.

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Glossary

AES	<p>Advanced Encryption Standard</p> <p>A new Federal Information Processing Standard (FIPS) that specifies an encryption algorithm(s) capable of protecting sensitive government information well into the twentyfirst century. The U.S. Government will use this algorithm and the private sector will use it on a voluntary basis.</p>
Algorithm (cryptographic)	A clearly specified mathematical computation process; a set of rules that gives a prescribed result.
ANSI X.509 Public key cryptography	The ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.
Asymmetric encryption	An algorithm that uses two mathematically related, yet different key values to encrypt and decrypt data. One value is designated as the private key and is kept secret by the owner. The other value is designated as the public key and is shared with the owner's trading partners. The two keys are related such that when one key is used to encrypt data, the other key must be used for decryption. See <i>public key</i> and <i>private key</i> .
Authentication	The verification of the source (identity), uniqueness, and integrity (unaltered contents) of a message.
CA	<p>Certifying Authority or Certification Authority.</p> <p>Secure server that signs end-user certificates and publishes revocation data. Before issuing a certificate, the CA follows published policies to verify the identity of the trading partner that submitted the certificate request. Once issued, other trading partners can trust the certificate based upon the trust placed in the CA and its published verification policy. See <i>certificate</i>.</p>
Certificate	A public key certificate. Certificates are issued by a certification authority (CA), which includes adding the CA's distinguished name, a serial number and starting and ending validity dates to the original request. The CA then adds its digital signature to complete the certificate. See <i>CA</i> and <i>digital signature</i> .
Certificate request	An uncertified public key created by a trading partner as part of the Rivest Shamir Adleman (RSA) key-pair generation. The certificate request must be approved by a certification authority (CA), which issues a certificate, before it can be used to secure data. See <i>CA</i> , <i>public key</i> , <i>RSA</i> , <i>trading partner</i> , and <i>uncertified public key</i> .

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Common key	Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, "common key" refers to this last share. It is not assumed secure, as it is not continually in an individual's possession.
Cryptography Public Key Cryptography	The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.
Data authentication	Refers either to data integrity alone or to both integrity and origin authentication (although data origin authentication is dependent upon data integrity.)
Data integrity	Verify that data has not been altered. One of two data authentication components.
Decryption	The process of transforming ciphertext into plaintext.
DES Digital Encryption Standard.	A standard, U.S. Government symmetric encryption algorithm that is endorsed by the U.S. military for encrypting "unclassified, yet sensitive" information. The Data Encryption Standard is a block cipher, symmetrical algorithm (extremely fast) that uses the same private 64-bit key for encryption and decrypting. This is a 56-bit DES-CBC with an Explicit Initialization Vector (IV). Cipher Block Chaining (CBC) requires an initialization vector to start encryption. The IV is explicitly given in the IPsec packet. See <i>triple DES</i> , and <i>symmetric algorithm</i> .
Digital signature	An electronic signature that can be applied to any electronic document. An asymmetric encryption algorithm, such as the Rivest Shamir Adleman (RSA) algorithm, is required to produce a digital signature. The signature involves hashing the document and then encrypting the result with the sender's private key. Any trading partner can verify the signature by decrypting it with the sender's public key, recomputing the hash of the document, and comparing the two hash values for equality. See <i>hash function</i> , <i>private key</i> , <i>public key</i> , and <i>RSA</i> .
Distinguished name	A set of data that identifies a real-world entity, such as a person in a computer-based context.
Encryption	The process of transforming plaintext into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decrypting process (two-way encryption).

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Extended security option	Public/private key creation software that allows only the public key to be sent to the certifying authority.
Hash function	An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that: (1) a message yields the same result every time the algorithm is executed using the same message as input, (2) it is computationally infeasible for a message to be derived, or reconstituted, from the result produced by the algorithm, and (3) it is computationally infeasible to find two different messages that produce the same hash result using the same algorithm. The kind of hash function needed for security applications is called a "cryptographic hash function", an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the "one-way" property) or (b) two data objects that map to the same hash result (the "collision-free" property). See: MD2, MD4, MD5, SHA-1.
HMAC	Hash Message Authentication Code. A keyed hash that can be based on any iterated cryptographic hash (that is, MD5 or SHA-1), so that the cryptographic strength of HMAC depends on the properties of the selected cryptographic hash. See MD5 and SHA-1.
IA	Issuing Authority. An entity that issues, suspends, or revokes a certificate.
Key (cryptographic)	A parameter that determines the transformation from plaintext to ciphertext or vice versa. For example, a
DES	Digital Encryption Standard (DES) key is a 64-bit parameter consisting of 56 key bits and 8 bits, which may be used for odd parity. See DES and odd parity.
Key generation	The trustworthy process of creating a private key/public key pair. The public key is supplied to an issuing authority during the certificate application process.
Key generator	(1) An algorithm that uses mathematical or heuristic rules to deterministically produce a pseudo-random sequence of cryptographic key values. (2) An encryption device that incorporates a key generation mechanism and applies the key to plaintext (for example, by Boolean exclusive ORing the key bit string with the plain text bit string) to produce ciphertext.
Key interval	The period for which a cryptographic key remains active.

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Key pair	A private key and its corresponding public key. The public key can verify a digital signature created by using the corresponding private key. See <i>private key</i> and <i>public key</i> .
MIME	M ultipurpose Internet M ail E xtension is an extension to the original Internet e-mail protocol that lets people exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII handled in the original protocol, the Simple Mail Transport Protocol (SMTP). Servers insert the MIME header at the beginning of any Web transmission. Clients use this header to select an appropriate "player" application for the type of data the header indicates. Some of these players are built into the Web client or browser (for example, all browser come with GIF and JPEG image players as well as the ability to handle HTML files); other players may need to be downloaded. New MIME data types are registered with the Internet Assigned Numbers Authority MIME as specified in detail in Internet RFC-1521 and RFC-1522.
Non-repudiation	Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.
PGP	P retty G ood P rivacy. A security system used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route.
PKI	P ublic K ey I nfrasturcture. A system of CAs, RAs, directories, client applications, and servers that model trust. The Internet Engineering FT (IEFT)'s X.509 standard is the de-facto standard by which public keys can be managed on a secure basis. See <i>CA</i> and <i>RA</i> .
Plaintext	Unencrypted data; intelligible data that can be directly acted upon without decryption.
Private key	The mathematical value of an asymmetric key pair that is not shared with trading partners. The private key works in conjunction with the public key to encrypt and decrypt data. For example, when the private key is used to encrypt data, only the public key can successfully decrypt that data. See <i>secret-key</i> .

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Public key	The mathematical value of an asymmetric key pair that is shared with trading partners. The public key works in conjunction with the private key to encrypt and decrypt data. For example, when the public key is used to encrypt data, only the private key can successfully decrypt that data.
Public key encryption	Encryption that uses a key pair of mathematically related encryption keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature. This permits users to verify each other's messages without having to securely exchange secret keys.
Repudiation	The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.
S/MIME	Secure/Multipurpose Internet Mail Extensions. An Internet protocol [R2633, June 1999] to provide encryption and digital signatures for Internet mail messages.
Secret key	The value used in a symmetric encryption algorithm to encrypt and decrypt data. Only the trading partners authorized to access the encrypted data must know secret keys.
Security	A set of three technologies that include (1) access control to guarantee the network connections, (2) encryption to protect data privacy, and (3) authentication to verify the user's identity and the integrity of the data. Session key A random, one-time secret key.
SHA-1	Secure Hash Algorithm is a hash algorithm. HMAC is a keyed hash variant used to authenticate data. See <i>hash function</i> .
SSL	Secure Sockets Layer. A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The SSL upper layer provides asymmetric cryptography for server authentication (verifying the server's identity to the client) and optional client authentication (verifying the client's identity to the server), and enables them to negotiate a symmetric encryption algorithm and secret session key (to use for data confidentiality) before the application protocol transmits or receives data. A keyed hash provides data integrity service for encapsulated data.

Everything You Wanted to Know About B2B Security*:
 (*But Were Afraid to Ask)

Symmetric algorithm	An encryption algorithm that uses the same key for encryption and decryption.
TLS	Transport Layer Security. SSL has been endorsed and included in the Transport Layer Security protocol promoted with the Internet Engineering Task Force (IETF) by several major data communications technology corporations, such as IBM.
Triple DES	A security enhancement to Digital Encryption Standard (DES) encryption that employs three-successive single- DES block operations. Using two or three unique DES keys, this increases resistance to known cryptographic attacks by increasing the effective key length. See <i>DES</i> .
VAN	Value Added Network. The source or service that resolves the issues resulting from communicating with a number of different trading partners. They provide EDI communication skills, expertise, and equipment necessary to communicate electronically.
Verify (digital signature)	In relation to a given digital signature, message, and public key, to determine accurately that (1) the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key contained in the certificate and (2) the associated message has not been altered since the digital signature was created.
X12	An international standard for EDI messages, developed by the Accredited Standards Committee (ASC) for the American National Standards Institute (ANSI).
X12.58	An ANSI security structures standard that defines data formats required for authentication and encryption to provide integrity, confidentiality, and verification of the security originator to the security recipient for the exchange of Electronic Data Interchange (EDI) data defined by Accredited Standards Committee (ASC) X12. See <i>X12</i> .
X.509	The International Telecommunications Union-T (ITU-T) specification that describes the format for hierarchical maintenance and storage of public keys for public-key systems.

Everything You Wanted to Know About B2B Security*: *(*But Were Afraid to Ask)*

Bibliography

American National Standards Institute Accredited Subcommittee X12 Electronic Data Interchange, www.X12.org.

Dierks, T. and Allen, C. Internet Engineering Task Force RFC 2246: The TLS Protocol Version 1.0, January 1999.

Flashback Sweden <http://www.flashback.se/hack/1999/>. To view a copy of the hacked web site, see <http://www.flashback.se/hack/2000/02/07/1/>.

Frier, Alan O, Karlton Philip, and Kocher, Paul C. The SSL Protocol Version 3.0 (Internet Draft), Internet Engineering Task Force, March 1996.

Hollinger, Richard C. & Lanza-Kaduce, Lon, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116 (1988).

Internet Engineering Task Force and Worldwide Web Consortium, XML—Signature Syntax and Processing Specification, June 2000. www.w3c.org.

International Telecommunication Union, Data Networks and Open System Communications - Directory (ITU-T Recommendation X.509), June 1997.

Internet Engineering Task Force, RFC 1767, MIME Encapsulation of EDI Objects, June 1992.

Nelson, Matthew. *Internet Security Systems' Chris Klaus says companies should close back doors to be secure*, INFOWORLD, Jan. 10, 2000, at 40a. According to a recent survey of 643 computer security practitioners in the U.S., 71% reported unauthorized access by insiders. Computer Security Institute, *Ninety percent of survey respondents detect cyber attacks, 273 organizations report \$265,589,940 in financial losses* (Mar. 22, 2000) http://www.gocsi.com/prelea_000321.htm.

Noack, David. *Employees, Not Hackers, Greatest Computer Threat* (Jan. 4, 2000) http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html.

Ramsdell, B.; Internet Engineering Task Force RFC 2633: S/MIME Version 3 Message Specification, June 1999.

RSA Laboratories, PKCS #1 v2.1:RSA Cryptography Standard, September 17, 1999.

Sinrod, Eric J. and Reilly, William P. "Hacking Your Way To Hard Time: Application Of Computer Crime Laws To Specific Types Of Hacking Attack," *Journal Of Internet Law*, (1999).

The Open Group, Technical Standard Common Security: CDS and CSSM, Version 2; (May 2000). A cryptographic algorithm used to compress a variable-size input stream into a unique, fixed-size output value. The function is one-way, so the input value cannot be derived from the output. A cryptographically strong hash algorithm is collision-free, meaning unique input values produce unique output values. Hashing is typically used in digital signing algorithms.

United Nations/Electronic Data Interchange for the Facilitation of Administration, Commerce, and Transport is defined in the International Standards Organization (ISO) Standard 9735. Security components are specified in Parts 5,6,7, and www.un-cefact.org.