TriStrata: Breakthrough in Enterprise Security

By Dorothy E. Denning
Georgetown University
December 19, 1999 [1]

In today's information rich and networked economy, information security is crucial to organizations and global enterprises. It is also complex, encompassing access controls, network security, encryption, authentication, intrusion detection, auditing, malicious code protection, operational security, and security administration, among other things. There are numerous products to assist, but few offer a comprehensive enterprise-wide approach to secure information management. Moreover, most require expert staff to manage the security-critical components that handle authorizations, key management, and auditing.

This is where TriStrata comes in. Founded by John Atalla, developer of automatic teller machine security and the PIN, the Redwood Shores, California company has taken a broad approach to information security. Their philosophy:

- *All information must be secured, whether it is in storage or transit.*
- *Access to information must be enforced based on rules, which can be dynamically changed.*
- *All security operations must be controlled by a network-centric management system that keeps a real-time audit of all processes.*

What they came up with is a Management System for Information Security that offers comprehensive information management and security services for organizations and their extended enterprises. An enterprise can include customers, partners, suppliers, shareholders, consultants, and others. Design and development were driven by what major corporations said they needed to manage their people and information.

TriStrata also developed a business model wherein Application Service Providers and a new class of Security Service Providers (SSPs) can maintain and administer the security system for an enterprise. This can simplify the integration of security into an enterprise, while introducing a new business opportunity for SSPs. A company can internally manage its own security services, but TriStrata envisions that security system maintenance and administration will be predominantly an outsourced business made available by trusted network service providers and applications service providers. They anticipate a multi-billion dollar market within three years.

What they came up with is a Management System for Information Security that offers comprehensive information management and security services for organizations and their extended enterprises

The TriStrata Management System for Information Security addresses the information security policy requirements across all industry sectors. It supports a rich set of access control policies, incorporating the concepts of roles, groups, departments, classifications and clearances, and personalized sharing within a single framework. The access capabilities of users are centrally managed but locally applied. They are dynamic and can be altered or fully revoked in real time. The system provides auditability and accountability for all security operations. Critical components are replicated and backed up.

Encryption is used to enforce policy and protect information in storage and in transit. It can be end-to-end for maximum security and performance. It is centrally managed so that an organization never loses control over its sensitive information. Encrypted information is fully protected and recoverable.

The TriStrata approach to secure information management addresses both the insider and outsider threat. Encrypted information is accessible only to persons who have been explicitly granted authorization to access the information. Further, no information can be encrypted or decrypted without leaving an audit trail, so it is easy to track access to sensitive information. If an insider is suspected or found guilty of wrongdoing, the person's access capabilities, and ability to decrypt documents, can be instantly revoked.

Many companies have been reluctant to give their employees encryption tools out of concern over lost keys. They need

[1] *This is a revision of the January 1999 report. It incorporates TriStrata's new business model and features added in Version 2.5 and follow-up extensions.*

security systems that ensure they will never be locked out. The TriStrata system does just that. Because encryption keys are centrally managed, there is no risk of them being lost or held hostage by a rogue employee.

The TriStrata infrastructure supports security at both the application and network layer. It offers utilities for file and disk security, electronic mail security, and virtual private networks. It supports and will interoperate with PKI systems. The system is modular and based on open industry standards, so that it can readily accommodate new applications and encryption methods. The security infrastructure runs on TCP/IP, making it suitable for protecting information on corporate intranets and extranets, as well as the Internet. Employees can telecommute from home or access sensitive corporate data while on travel without introducing vulnerabilities that could be exploited by hackers. Sensitive information can be placed on database and Web servers without jeopardizing its security, while access to such data can be systematically audited.

The TriStrata system is a turnkey, fully integrated, centrally managed system. It provides a high-performance framework for electronic business and commerce. The centralized approach to security management does not introduce a bottleneck or single point of failure. The current implementation can support an enterprise with thousands of organizations and up to one million users. The client software currently runs on Windows 95/98/2000/NT4 workstations. Server (or entity) software runs on the same plus Solaris 6/7. TESS runs on Windows NT 4.0 and is being tested against pre-release versions of Windows 2000.

The system is inherently recoverable by the owners of the information and as such, has been approved for worldwide export by the U.S. government, making it well suited to protecting the information assets of a global enterprise. The U.S. government does not hold any keys and cannot access protected information without the knowledge and cooperation of the enterprise.

The TriStrata approach to secure information management addresses both the insider and outsider threat.

This report reviews the functionality and security offered by Version 2.5 of the TriStrata system. The next section gives an overview of the system, describing its security architecture and access control. This is followed by a section describing the TriStrata utilities, which provide application and network security. The third section gives a more detailed review of the encryption and authentication functions. Finally, security administration is discussed.

SYSTEM OVERVIEW

Security Architecture

The TriStrata system has three main components: the TriStrata Extended Enterprise Security Server (TESS), TriStrata Client Modules (TCMs), and TriStrata Entity Modules (TEMs). The TESS is logically a single machine, but physically a collection of between one and 32 pairs of replica machines which track each other as peers. A TCM is typically a user's personal workstation and a TEM a shared machine such as a file, database, or Web server. TCMs and TEMs are both clients to TESS within a client/server architecture.

The TESS oversees all security operations and enforces the enterprise-wide security policy. Users and entities must be enrolled in TESS before they can perform security-related operations. At the time of enrollment, each user is given a unique Security Registration Number (SRN) and assigned to an organization. Various security agents perform enrollment and other security management functions.

Users must receive authorization from TESS before they can encrypt or decrypt data. Without authorization, they will not have the information (keys) needed to perform the operation. The security policy is stored in a database on TESS and is accessible only to TESS.

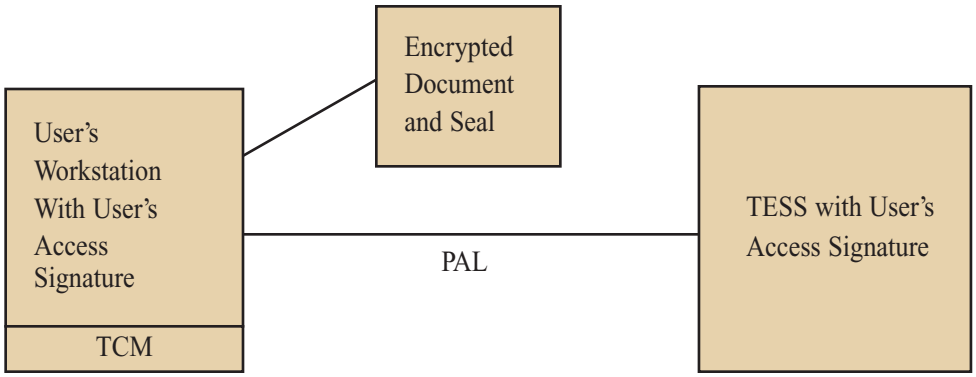
If TESS approves a request to encrypt information, it gives the user's client a "permit" to perform the operation. The permit contains a dynamically generated encryption key. TESS also places the key in a "seal" that is given to the client to store with the cipher text. In addition to the key, the seal contains information about the method of encryption and policy information indicating who is allowed to decrypt the information. TESS encrypts the seal under a private key. Only TESS can decrypt the seal. TESS does not retain its own copies of the data encryption keys.

When a user wants to decrypt information, the user's client presents the seal stored with the cipher text to TESS. TESS breaks the seal (decrypts it) and checks the policy to see if the user is authorized to perform the decryption. If so, it gives the client a permit with the decryption key.

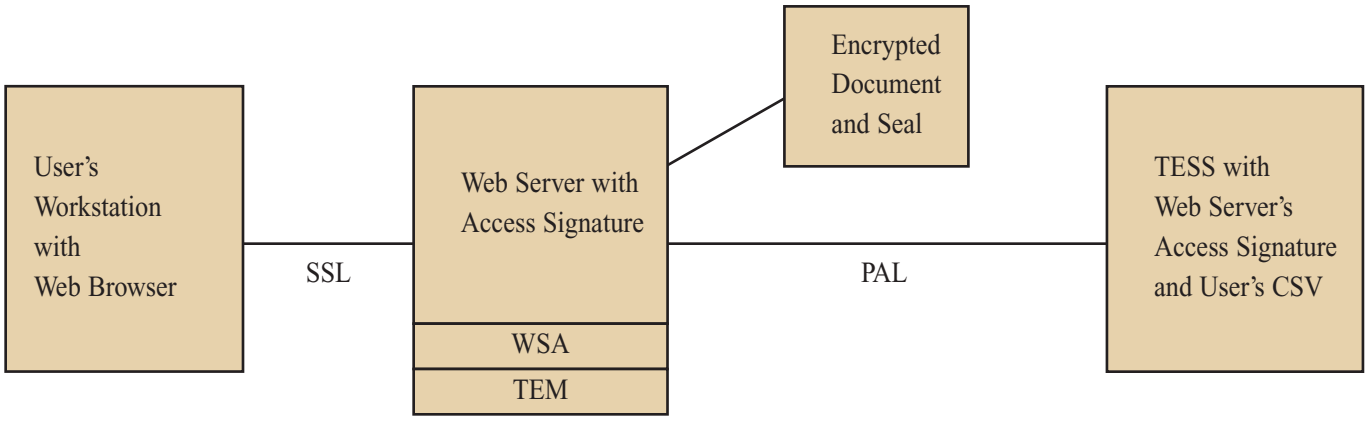
Users must receive authorization from TESS before they can encrypt or decrypt data.

All communication with TESS is performed with the Private Access Line (PAL) protocol. PAL provides mutual identification and authentication, privacy (encryption), and data integrity between the client and TESS.

To interact with TESS, a user must have an Access Signature. The Access Signature, which is known only to the user and TESS, is used to establish a private, authenticated communication channel with TESS under the PAL pro-



(a) Operation when user has an Access Signature



(b) Operation when user is authenticated through a CSV

Figure 1. TriStrata Modes of Operation

tocol. It is created and assigned at the time of enrollment, and stored on the user's workstation encrypted under a pass-phrase known only to the user.

The TriStrata system supports users who do not have Access Signatures and the software needed to perform PAL and other TriStrata functions. These users interact with the system through a standard SSL-enabled Web browser. The browser connects to a TriStrata-enabled web server that operates as a proxy client to TESS and communicates with TESS using PAL like any other client. A Web Server Agent (WSA) decrypts documents on behalf of the user (assuming the user is authorized) and then re-encrypts them under SSL before transmitting to the user. The user is authenticated to TESS using a Client Stored Value (CSV) derived from a pass-phrase. TriStrata calls this their "zero footprint solution" because the user does not need any special software beyond an SSL-enabled Web browser.

Figure 1 illustrates the two modes of user operation. Because Access Signatures confer a higher level of assurance than CSVs, they are required to access department "classified" information and to perform security management functions. CSVs might be used with customers, suppliers, and others who are physically remote and have no need to access a company's most sensitive information. Every user with an Access Signature also has a CSV, which is a hash of the pass-phrase used to protect their signature. The CSV could be used when working from a computer without the signature or TriStrata software.

The TriStrata system provides security for files, disks (volumes), electronic mail, and corporate networks. It will provide public-key infrastructure (PKI) capabilities so that users can interoperate with public-key systems and communicate with persons outside the TriStrata environment. The PKI capabilities will support digital signatures, SSL-secured Web servers and browsers, S/MIME-based secure e-mail, and inter-TESS communications.

All TESS transactions are logged on disk or tape. In addition, applications can generate arbitrary audit records, which are sent to TESS and recorded in the log. The log provides accountability for all accesses to encrypted data and other security-related operations. The system provides real-time audit reduction tools to prepare the audit informa-

tion for use in analysis and reporting tools.

While a company can operate and manage its own TESS, TriStrata believes that most will outsource that security management function to a trusted security service provider or applications service provider. A company offering such services can support up to 32,000 organizations on a single TESS. Each organization can be totally partitioned off from the others (i.e., be its own independent enterprise) or share visibility with a selection of other organizations (i.e., be part of a larger enterprise).

Access Control Policy

The TriStrata system uses encryption to enforce an enterprise-wide access control policy. The framework for setting policy supports three forms of protection: personal, person-to-person (individual and group-based), and departmental (classification-based). These three types of security offer companies a comprehensive and rich set of options for managing information. They reflect the type of sharing that actually takes place in business as well as in other types of organizations.

With personal security, information encrypted by the user is not accessible to other users. Except under limited conditions (discussed later under data recovery), nobody else will be given a permit with the key needed to decrypt the information.

With person-to-person security, users make encrypted information available to others, either individually or through their associations in dynamic membership groups (DMGs). They select the individuals and groups that are to receive access. DMGs can be defined for arbitrary functional units, work groups and affiliations. They can be used to bring together individuals who play a common role within an organization, for example, all sales representatives or the members of a product development team. They can also be used to create affiliations that span multiple organizations within the enterprise, for example the chief information officers or a multi-organization project team.

When person-to-person security is used, the seal attached to cipher text data will specify the individuals and groups who are permitted access. TESS will not give a user a permit with the key unless the user is included in the set of authorized persons.

With departmental security, users make encrypted information available to all persons who are cleared to access the information within an organization. Clearance is determined by two attrib-

DR. DOROTHY E. DENNING

Dorothy E. Denning is professor of Computer Science at Georgetown University. She is also professor and member of the advisory board of the Communication, Culture and Technology program and a faculty mentor in the Science and Technology in International Affairs program. Her current work encompasses the areas of information warfare and assurance, encryption policy and technology, and the impact of technology on law enforcement and society.

Before coming to Georgetown in 1991, Dr. Denning was a member of the research staff at Digital Equipment Corporation, a senior staff scientist at SRI International, and an associate professor at Purdue University. She has served as president of the International Association for Cryptologic Research, chair of the International Cryptography Institute, chair of the National Research Council Forum on Rights and Responsibilities of Participants in Networked Communities, co-chair of the ACM Conference on Computer and Communications Security, member of the National Institute of Standards and Technology Review Panel on Information Technology, member of the ACM cryptography policy study group, and member of the board of directors of the Computing Research Association. She is presently a member of the President's Export Council Subcommittee on Encryption Policy and co-chair of Georgetown's Technology Oversight Committee.

Dr. Denning is author of Information Warfare and Security (Addison Wesley, 1999), Cryptography and Data Security (Addison Wesley, 1982) and over 100 articles. She is co-editor of Internet Besieged: Countering Cyberspace Scofflaws (Addison Wesley, 1998). She has testified before the U.S. Senate and House of Representatives, is a frequent lecturer at conferences and symposia, and has appeared on TV and radio programs throughout the world. She is an ACM Fellow and has received the National Computer Systems Security Award and the Distinguished Lecture in Computer Security Award.

In April 2000, she was named the TechnoSecurity Professional of the Year. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University.

utes: department and authorization level. Departments represent an organization's broad functional divisions, for example, human resources, manufacturing, accounting, marketing, and engineering. Authorization levels reflect the roles of people within an organization and the classifications of information. For example, from lowest to highest they might be contractor, staff, management, executive, proprietary, and restricted. An organization can have up to 20 departments and 7 authorization levels. The same levels apply to all departments. However, each of the up to 32,000 organizations in an enterprise can have a different set of departments and levels.

When information is encrypted with departmental security, the encrypted data will be assigned a list of departments and authorization levels. This information will be stored in the seal along with the encryption key. TESS will give a user a permit with the key to decrypt the data only if the user is cleared into one of the departments at a level at least as great as that specified. Users can be cleared into multiple departments with different authorization levels for each.

All information about users (including their Access Signatures), groups, departments, and authorization levels is stored in a database maintained by TESS. It is not accessible to any client. The TESS database is kept in main memory for optimal performance. Access decisions can be made instantly.

With all three types of security, it is possible to revoke some or all of a user's authorizations at any time, for example, when an employee changes positions or is terminated. Revocation is instant. With discretionary security, removing a user from a group has the immediate effect of denying that user access to information encrypted to the group. Similarly, with departmental security, revoking a user's clearances has the immediate effect of denying access to information encrypted at that level. In all cases, it is not necessary to revoke or change any encryption keys. The policy changes are recorded in the TESS database and used by TESS to determine whether to grant a user a permit to encrypt or decrypt information. This approach to authorization and revocation is a potent weapon against insider threats. Systems which put encryption entirely in the hands of users are much more vulnerable to misuse.

Similarly, if a user is added to a group or assigned new clearances, the user will be able to access encrypted information that is confined to the group or clearance level. No keys need to be changed to make this happen and documents do not have to be re-encrypted.

Security agents, who specify the organizational structure, departments, authorization levels, and groups, administer the access control policy for an enterprise. They enroll users and add and revoke authorizations.

APPLICATION AND NETWORK SECURITY

The TriStrata framework can support a variety of applications for electronic business and commerce. The company currently offers software for file, disk, and e-mail encryption and for secure networking. They also provide an application developer's toolkit for integrating security into client applications. The toolkit provides encryption, privacy, and assurance operations. Additionally, it allows the developer to create arbitrary secure, auditable events in the client application. Such events generate audit records, which are sent to TESS and recorded on the log. This section discusses file, disk, and e-mail security; secure virtual private networks, real-time video and teleconferencing, and PKI interoperability.

File Security

The TriStrata Explorer Extension allows users to protect sensitive files quickly and easily. Encryption and decryption are implemented as an extension to the Windows or Windows NT Explorer. A user can select one file or a group of files for individual encryption. If a folder is selected, the system will recursively encrypt each file in the folder and all subfolders. The user can also define a collection of files and folders to be encrypted or decrypted whenever the user clicks a button on the TriStrata tool bar. This makes it easy to lock files at the end of a work session and unlock them again when work resumes.

The protection assigned to a file or collection can be personal, person-to-person, or departmental. For departmental security, the user selects a department and authorization level from a list. The user must be cleared into the department at the selected level. For person-to-person security, the user is given a list of visible users and groups from which to make a selection.

The TriStrata Explorer Extension allows users to protect sensitive files quickly and easily.

When a file is encrypted, the system assigns a default name to the cipher text file which is the same as the original, but with the added extension of ".tss". The user can select a different name if desired. There are four options for handling the original plaintext file: retain on disk, automatically delete, delete if confirmed (the user is asked), or wipe (delete and overwrite the bits on disk). An organization's security policy determines the default. Of course, if plaintext files are retained, the encryption is essentially useless against an adversary who gains access to the disk. The option would be useful, however, if a file were encrypted for the purpose of transporting it over an insecure channel or on a floppy disk.

File encryption and decryption are fast. I have observed practically no delay encrypting and decrypting complete folders on my computer at Georgetown University in Washington, DC, even though the operations are controlled by the TriStrata TESS in

Redwood Shores, California.

Disk Security

The TriStrata application TSDisk gives users the capability to create one or more secure disks (volumes). Files are automatically encrypted when they are saved or copied to a secure disk from any application. Similarly, they are automatically decrypted when opened or copied to another location from any application. Application software does not have to be TriStrata-aware.

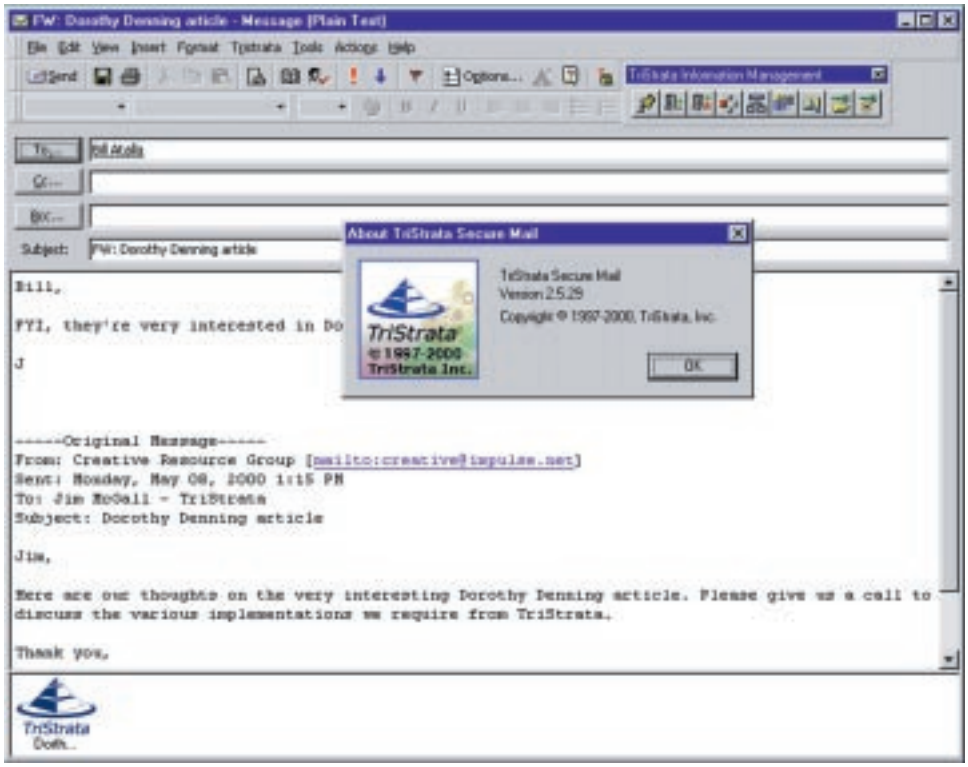
To create a secure disk, the user specifies a name for the disk, the disk's size, and whether the disk is expandable. The user also specifies the access policy, which can be personal, person-to-person, or departmental, as for file security. In addition, the user specifies a drive onto which the disk is to be mapped. For example, a disk might be labeled "Secure" and mapped to the S: drive on the user's personal computer. The secure disk is displayed as a "removable disk" in Windows Explorer. The files on the drive are listed without any extensions such as ".tss."

When a secure disk is first created, the user must be connected to TESS. TESS will create a seal for the disk and give the client software a permit with the key. Later, the user will be able to access the disk by connecting to TESS in much the same manner as for accessing an encrypted file. The client software will send the seal to TESS, and TESS will return a permit with the key.

With a secure disk, it is also possible for the user to access the disk offline, that is, without being connected to TESS. This would be especially useful when the user is traveling or working at home in an offline environment where it is not possible or convenient to make the connection. It would enable the user to protect files that otherwise could not be encrypted because of the need for access.

For offline access, the user must first create an Offline Key Ring file. This file, which contains the key, is stored in the Windows file directory encrypted under a pass-phrase chosen by the user (the pass-phrase is hashed to a key using SHA-1). The pass-phrase must be at least 8 characters. While this is perhaps adequate in many environments, for a high level of security, users should pick longer pass-phrases as discussed earlier.

Offline disks are fully recoverable even when the Key Ring file is lost or destroyed, or the user forgets the pass-phrase. This is because the key is stored in the seal, which TESS can unlock on behalf of a Recovery Agent.



TriStrata's secure mail interface.

The TSDisk application uses the Blowfish algorithm with 448-bit keys to protect a secure disk. The encryption/decryption rate is 8 MB/sec. The data are encrypted at the block level rather than on a file basis.

Electronic Mail Security

TriStrata offers extensions to Microsoft Exchange and Microsoft Outlook for encrypting electronic mail. A user-friendly point-and-click interface is integrated into the e-mail application. When a message is encrypted, all attachments are automatically encrypted along with the message body.

For ease-of-use, all e-mail encryption is person-to-person, with users identified by their e-mail addresses. A user can still use the desktop encryption capabilities to encrypt attachments under organization or group policies before dropping them into an e-mail document. In that case, the attachments will be double encrypted.

E-mail in release 2.5 can be used off-line when connection to a TESS is impossible. When the off-line capability is enabled, the mail client will create a secure disk using the technology described above. All decrypted incoming messages and outgoing drafts will be automatically saved on the secure disk. This capability responds to input received from large enterprise users who piloted the TriStrata system.

Proxy-enabled Web Servers

TriStrata offers software that can be installed on any SSL-enabled Web server. The software, called a Web Server

Agent (WSA), allows users to access encrypted documents through an SSL-enabled Web browser such as Netscape or Internet Explorer. The WSA operates as a proxy on the user's behalf. The user does not need to install any TriStrata software or have an Access Signature for this mode of operation.

The user is authenticated through a Client Stored Value (CSV). The user types in a pass-phrase, which is transmitted to the server using SSL encryption. The server computes the CSV from the pass-phrase (by hashing it with SHA-1) or retrieves it from secure storage. It also fetches the requested document. It then transmits the CSV, along with the document's seal, to TESS in the encrypted payload of the PAL protocol. After determining that the user is allowed access to the document, TESS returns a permit with the key. The server decrypts the document and then re-encrypts it under standard SSL encryption for transmission to the user's browser.

Secure Virtual Private Networks

The TriStrata SVPN, also called TriStrata Secure Sockets (TS3), offers secure virtual private networks (VPNs). TS3 provides a secure channel at the Winsock layer for all TCP/IP and UDP/IP applications. It requires no modification to application software.

TS3 uses the TriStrata encryption and access control services to provide message confidentiality and integrity, server access control, auditing at TESS, and identification and authentication of clients and servers at the Winsock level. The software can be used to protect corporate intranets and extranets, and to protect all communications to and from users who telecommute from home and hotel rooms. An employee, at home or on travel, could dial into a company network through a local Internet service provider that is not part of a TriStrata enterprise. Because TS3 provides end-to-end security from the user's workstation to a secure server, the ISP need not be trusted and the communications can safely travel over the dial-up line and the Internet. Unauthorized persons would be unable to connect to the internal network because they would not be enrolled in the system. Even if they had a copy of all the software and shared data, they would not have an Access Signature. Without that, they would be unable to pass an authentication check with TESS or get encryption keys from TESS.

TS3 uses RC4 with 128 or 256-bit keys. This provides a data rate of over 7 MB per second, which is adequate for real-time video and other streaming applications for the foreseeable future. Transmission speed is limited only by the bus, not by the security system.

Real-Time Video and Teleconferencing

The TriStrata technology is particularly well suited to real-time video. Encrypting video on a 400 MHz Pentium processor uses less than 1% of the CPU and produces no transmission delay.

The method of encryption (cipher block chaining) allows users to tap into a cipher text stream at any point. They need not be there at the beginning. This makes the technology ideal for applications such as paid television and teleconferencing. The encrypted video could be broadcast over a satellite or cable network, or it could be multicast over the Internet. The seal in the cipher text stream would carry with it the name of a subscriber group. The subscriber's machine would transmit the seal to a TESS server, which would authenticate the user and check whether the user belongs to a group of subscribers who paid for the channel or conference. If so, the user would be given the key to decrypt the stream. All of this can happen without any noticeable delay.

Existing satellite TV systems are vulnerable to piracy. Thieves acquire the keys and program them onto their own access cards, effectively cloning the cards. The channel keys are posted on the Web, where they may be picked up by thousands of pirates.

The TriStrata system would make such pirating virtually impossible. Even if it did occur, it would be detectable through an audit of the TESS log. Two people would be using the same Access Signature from different physical locations. Indeed, the signature might be used by thousand of people. This type of activity could be detected with methods similar to those used by cell phone companies to detect cellular fraud. In both cases, detection is possible because the subscriber interacts with a centralized system, which records the transaction. The technology currently used by the TV industry cannot detect piracy because it requires no interaction with the subscriber. Hence, there is no way of knowing when and where keys are used.

Once fraud is detected, the subscriber can be deleted from the system. At that point, the subscriber's card and any cloned cards will be useless. If the subscriber is a victim of the operation, the person can be issued a new card and Access Signature before the deletion is performed so that there is no loss of service.

PKI Capabilities

When public-key cryptography was first invented, it was seen as a solution to the key management problems of conventional cryptosystems. Two users could communicate privately and digitally sign messages without the need for a trusted third party. They could post their own public keys in a public directory and obtain the keys of others from the directory. No other entity would need to know their private keys. Soon, however, the need for a trusted party became apparent, particularly if public-key cryptography was to be used to authenticate transactions and support electronic commerce. The trusted entity

The TriStrata system would make such pirating virtually impossible.

was needed to authenticate public keys, handle compromises and revocations of keys, and keep track of which keys were current. This gave rise to certificate authorities and digital certificates.

Public-key cryptography has another limitation. It does not integrate readily with authorization and access control policies. To illustrate, suppose a file, video, or some other data object is to be made available to a group of users. With public-key, one could encrypt the data with a conventional system, say DES or Triple-DES, and then encrypt the DES key separately under the public keys of each group member. The individually encrypted keys would be attached to the data and the entire package transmitted to group members (or the keys could be shipped individually). There are two problems. First, it would be costly to encrypt information for large groups because of the high overhead of public-key methods. Second, there would be no convenient and instantaneous way of revoking a user's group access to any encrypted object. The overhead could be reduced by encrypting the data under a shared group key, but managing such keys would be a nightmare. If someone is removed from the group, a new group key must be distributed to all remaining members. Also, the larger the group, the more likely the key will be compromised.

The situation is even worse with departmental security. Here, the user would need to encrypt the DES key under the public key of each cleared person — a set that is continually being revised. Of course, public-key algorithms could be integrated into a security framework similar to that of TriStrata's, but they would not perform as well as the TriStrata encryption algorithms.

Another drawback of public-key systems is that it is necessary to retain users' old keys and certificates so that previously encrypted data can be decrypted and previously signed messages verified. Yet care must be taken to discontinue use of the keys, especially if they were compromised. This leads to a cumbersome system for key revocation and a potential nightmare for organizations concerned about losing access to encrypted data. By contrast, with the TriStrata system, a user's Access Signature can be replaced at any time without the need to retain the old one. There is nothing a user can do, deliberately or accidentally, that impairs the ability of the organization to decrypt data.

The TriStrata system has an open crypto architecture, making it possible to readily introduce new encryption algorithms.

For these reasons plus the performance advantages of conventional methods, the TriStrata system is based on single-key cryptography rather than public-key. The system will, however, provide public-key infrastructure (PKI) capabilities in support of global communications and e-commerce. Users will be able to communicate with others outside an enterprise and digitally sign transactions and messages using public-key cryptography. This enhancement to the 2.5 system is under development and will be released to customers at no cost when development and testing are completed.

The PKI capabilities will support S/MIME-based secure e-mail, SSL-secured Web servers and browsers, and public-key digital signatures. In addition, they will support inter-TESS communications, allowing secure information sharing between users in different TESS-enabled enterprises. For inter-TESS communications, a seal is transmitted from one TESS to another. The key used to encrypt the seal is encrypted under the public key of the receiving TESS and sent with the seal.

To use the PKI, a user must be given PKI privileges. These are granted by the user's Agent, say at the time of enrollment. The privileges allow a user to have personal public-private key pairs. When a pair is generated, it is encrypted and stored in a file. Like any other encrypted file, it is given a seal with the file encryption key. The seal can be unlocked only by TESS.

To use the private key of a key pair, the user's client must get a permit from TESS to decrypt the key pair. This means the user's PKI privileges can be revoked at any time. TriStrata is considering allowing offline access to key pairs, although this would preclude immediate revocation.

The TriStrata PKI distinguishes between two types of public-private key pairs: key-encrypting keys and signature keys. Key-encrypting keys are used to encrypt and decrypt the session key used to encrypt the data (even in a public-key system, the data is encrypted with a single-key method). Signature keys are used to create and validate digital signatures. This separation allows an enterprise to establish key recovery only for encryption keys and not signature keys, thereby protecting the non-repudiation properties of signature keys. To enable recovery, all session keys encrypted with destination public keys are also encrypted with a TESS Recovery Team Public Key so that Recovery Agents are able to retrieve session keys necessary for decryption.

TriStrata's PKI will provide certificate management services. Specifically, it will support certificate enrollment through a TriStrata protected Registration Authority (RA), application validation, issuance, distribution, renewal, and revocation. Certificates will be x.509 compliant and stored in an LDAP directory, not TESS, although TESS will keep a record of certificate serial ID numbers.

ENCRYPTION AND AUTHENTICATION

The TriStrata system has an open

crypto architecture, making it possible to readily introduce new encryption algorithms. The current release supports Triple-DES with 168-bit keys, RC4 with 128-bit and 256-bit keys, CAST5 with 128-bit keys, and Blowfish with 256-bit and 448-bit keys. Triple-DES, CAST5 and Blowfish are used in Cipher Block Chaining (CBC) mode. All of these methods are believed to offer strong security. The key sizes are sufficiently long that they cannot be broken by brute force. TriStrata also plans to support the Advanced Encryption Standard (AES), and has already been granted export approval for all candidates in preparation for when it is adopted.

For hashing, TriStrata uses the SHA-1 algorithm, which produces a 160-bit hash. Message authentication codes are computing using SHA-1 with the HMAC algorithm. HMAC uses keyed hashing to compute a message authentication code (MAC). Again, these methods are believed to offer strong security.

This section describes how the TriStrata system uses encryption in the PAL protocol and for data security. The proxy Web server and PKI interoperability are discussed later.

All TriStrata keys are derived from 610 Megabytes of hardware-generated random data. The data are produced with a Spyrus EES-Links Card, which has an NSA-certified hardware random number generator. They are generated at TriStrata under two-person control and written to CD. The process takes about six days. The CD is delivered to the customer in an intrusion evident envelope. Check sums are also used to detect tampering of the data. Customers can generate their own random source data if desired.

TriStrata Private Access Line (PAL) Protocol

All communication between a client and the TESS is performed under the PAL protocol. PAL requires that the client have a private Access Signature, which is shared with the TESS. This signature is 256 KB and is derived from the 610 MB of hardware-generated data. Because the Access Signature is known only to the client and TESS, it allows the two parties to mutually authenticate each other and the contents of the messages. The Access Signature is also used to derive session keys for encrypting communications between the client and TESS. All PAL encryption uses Triple-DES in CBC mode.

In today's economy, information security is crucial to global enterprises.

PAL supports two types of transactions. The first is a standard transaction, where the client sends a request in the clear and TESS responds with an encrypted reply. The request message contains 4 pseudo-random numbers, each 32 bits, which are indexes into the Access Signature (modulo 256 KB). It also includes a 20-byte message authentication code. The MAC is computed over the entire message (including the random indexes) using HMAC-SHA-1 with a key derived from the contents of the signature at the indexed locations. The response message from TESS similarly contains 4 random indexes into the Access Signature, which are used to compute a MAC for the reply. In this case, however, the indexes are hardware-generated (Spyrus Card) real random numbers. The payload of the reply is encrypted with Triple-DES using a session key derived from the contents of the signature at all 8 of the indexed locations. Because 4 of the indexes are true random numbers and the key itself is derived from true random numbers, it is extremely unlikely that a session key could be cracked or that the same session key would be generated more than once.

With the second type of transaction, the encrypted response from TESS includes a permit and seal. The permit contains a key, which the client uses to send an encrypted message back to TESS. The seal, which includes the key and a time-stamp, is returned to TESS in the encrypted message. When TESS receives the encrypted response, it decrypts the seal and checks the time-stamp. If more than 60 seconds has elapsed, it rejects the request and sends an error message back to the client. This protects against replay attacks, limiting them to a 60 second window.

Signature Protection

A user's Access Signature is extremely sensitive. If someone could capture it, the person could take actions on behalf of the user, including encrypting and decrypting data.

The TriStrata system minimizes the risk of signature exposure. When a user is enrolled, the Access Signature is generated by TESS and transmitted to the enrolling agent's workstation encrypted under that agent's signature (using the PAL protocol). It is decrypted on the agent's workstation and immediately re-encrypted (using Triple-DES) under a

pass-phrase. The ciphertext signature is then transmitted to floppy disk. Both the plaintext signature and pass-phrase are immediately erased from memory, so there is little danger of compromise on the agent's workstation.

If the user is present during enrollment, the user types in the pass-phrase. Even the agent does not know it. If the user is not present, the agent supplies a pass-phrase and sends the encrypted signature to the user. The pass-phrase is distributed over the phone. If it has been set for one-time use, the user will be prompted for a new one.

In order to encrypt and decrypt data, the user's Access Signature must be loaded into memory and decrypted. The user is prompted for the pass-phrase, which is then used to decrypt the signature. The pass-phrase is immediately erased from memory; however, the plaintext signature is retained in memory to enable high-speed transactions with TESS. It is erased from memory if there has been no TESS activity for a period of time specified by the Security Officers. When TESS operations resume, the user must re-authenticate by typing in the pass-phrase. This feature will be integrated with a screen saver.

An Access Signature could potentially be acquired by compromising a client workstation. If malicious software can be loaded onto the workstation, it might attempt to locate the plaintext Access Signature and transmit it to an adversary. Alternatively, the malicious code could capture a user's pass-phrase while it is being typed in and transmit the pass-phrase and cipher text Access Signature.

The TriStrata system does not specifically prevent the introduction of viruses and Trojan horses, which could enter a client's machine via an e-mail attachment or from a Web page. This potential vulnerability exists on all PCs and needs to be addressed by other means. It is a limitation of all encryption systems and illustrates why cryptography is not a 100% solution to security problems.

If an adversary can gain physical access to a user's machine, for example, by stealing a laptop, the person might be able to locate the plaintext signature on disk in swap space. One would need the full 256 KB signature, however. If any parts were missing or rearranged, it would be useless. The chances of a signature being compromised in this manner are probably quite small, but there is some risk.

Although the TriStrata system does not prevent these scenarios, it offers an advantage over other systems in terms of its ability to detect and respond to such attacks. If an adversary succeeds in compromising a user's Access Signature, no damage occurs until the signature is actually used to decrypt information or perform some other operation with it. Nothing can be done, however, without the cooperation of TESS. The signature by itself does not allow access to any encrypted data; TESS must break the seal that is attached to the data and return the key. Because TESS records all security operations on its log, the unauthorized activity can be uncovered with an intrusion/misuse detection system that processes the audit data. The unauthorized operations most likely would take place at unusual hours or otherwise deviate from the user's normal behavior. At that point, the Access Signature can be discontinued and the user issued a new one. Additionally, whenever users change their pass-phrases, they are issued new access signatures, further limiting an attackers window of opportunity. Decentralized encryption systems do not provide this type of protection because users can decrypt information without the cooperation of a central server that audits such operations.

TriStrata's system addresses security requirements across all industry and government sectors.

As already noted, a user's Access Signature is stored on disk encrypted under a pass-phrase chosen by the user using Triple-DES. The Secure Hash Algorithm (SHA-1) is used to hash the pass-phrase into the Triple-DES. The system requires that a pass-phrase be at least 14 characters long and can be configured to require even more characters. It does not require, but encourages, the use of both upper and lower case letters, digits, spaces and punctuation characters.

In general, if a pass-phrase is a random sequence of printable characters (95 possibilities per character), then a 14-character pass-phrase is comparable to a 92-bit key in terms of brute-force breakage. If it is random string of lowercase letters (26 possibilities per character), it provides 66-bit security. At that length, it is potentially breakable; though doing so would require a substantial commitment of resources over an extended period of time. However, if it is lowercase and also drawn from English (or some other natural language), its security diminishes to about 32 bits because of the redundancies in the language.[2] An English pass-phrase must be about 24 characters long in order to provide security comparable to

[2] This is assuming a bit rate of 2.3 bits per letter (compared with 4.7 bits per character when all 26 letters are equally likely). For details see Dorothy E. Denning, Information Warfare and Security, Addison-Wesley, 1999, pp. 326-327.

DES (55-bit security). At 30 characters, if offers approximately 69-bit security.

This potential vulnerability is not unique to the TriStrata system. All cryptosystems rely on passwords (including pass-phrases and PINs) to protect users' private keys. Users cannot be expected to memorize or type in these long random bit sequences, which for public-key cryptography can be several thousand bits, so systems use secret passwords to control access to a user's keys, which are stored on disk or a medium such as a smart card. Many systems place no restrictions at all on the length or characters set of a password.

Extremely long or random pass-phrases do not necessarily offer stronger security. If users cannot easily remember their secret phrases, they will write them down in a place that might offer less security than the phrases themselves. Ultimately, the security of any system relies in part on the practices of users. This is unavoidable and the TriStrata system is no exception. TriStrata does, however, attempt to mitigate these risks through appropriate security controls. For example, extremely sensitive operations cannot be performed by a single individual acting alone (see later discussion). All security operations are audited, so any attempts to use a stolen pass-phrase to encrypt or decrypt data will show up in the log. The system also can be configured to force users to change their pass-phrases (and access signatures) after a period of time. When they change their pass phrase a new access signature is created and delivered to them and the old access signature is invalidated.

In the TriStrata system, the pass-phrases used to protect signatures are used only on a local workstation. They are never transmitted over the network, so they cannot be acquired with a packet sniffer. Remote authentication is always through the Access Signature and PAL protocol.

All security operations are audited, so any attempts to use a stolen pass-phrase to encrypt or decrypt data will show up in the log.

Biometrics (finger, face, and iris prints, for example) offer a stronger form of authentication than pass-phrases and do not rely on users' memories. This technology potentially can enhance the security of any system, including TriStrata's.

Data Encryption Through Permits and Seals

In order to encrypt data, a client needs a permit and an encrypted seal, both of which are created by TESS. The permit contains the encryption key. The seal also contains the key, but in addition, it contains information specifying the encryption algorithm, the identity of the client, policy information indicating who is allowed to access (decrypt) the data, and a hashed digest of the data. Except for the key, this information is provided by the client in the request message for the permit and seal. Both the request to TESS and the response from TESS with the permit and seal are transmitted in the encrypted payload of the PAL protocol. The client attaches the seal to the data at the time of encryption.

When TESS creates the seal, it encrypts it using triple-DES in CBC. The 168-bit DES key and 64-bit CBC initialization vector are private to TESS and unique to each object. They are extracted from a 128 KB pool of hardware-generated random numbers. The method of extraction produces over 1055 unique combinations. It is almost certain that each seal will be encrypted with a different key.

To decrypt data, a client first sends TESS the seal that was attached to the data. TESS decrypts the seal and determines, from the policy information, whether the client is authorized to access the data. If so, TESS returns a permit with the key to the client. This is transmitted in the encrypted payload of the PAL response. The client then decrypts the data and computes a hashed digest using the SHA-1 hashing algorithm. If the 160-bit computed digest matches the digest stored in the seal, the client concludes that the data have not been altered. The combination of identity of the originator of the seal and validation of the integrity using the digest returned from the seal provides for arbitrated non-repudiation of the event.

The only way of decrypting data without the cooperation of TESS is by compromising the Triple-DES key (and initialization block) used to encrypt the seal. At 168 bits per key (plus 64 bits for the secret initialization vector), breaking one of these keys is impossible. One would need to compromise TESS. TESS security is discussed later.

SECURITY ADMINISTRATION

Security administration for the TriStrata system involves policy administration and TESS administration. These services, particularly TESS administration, can be managed by security service providers and application service providers, who in turn offer them to customer organizations on a monthly fee based on the number of users. By outsourcing the services, a company can concentrate on its security policies instead of TESS operations and other high-level administrative func-

By outsourcing the services, a company can concentrate on its security policies instead of TESS operations and other high-level administrative functions...

tions, including those performed by the Administration Security Officers.

This section describes the administration functions independent of where they are performed.

Policy Administration

The security policy of an enterprise is defined and administered by two Administration Security Officers and a variable number of agents. There are six types of agents: System Group Agents, System Recovery Agents, Organization Agents, Organization Recovery Agents, Super Agents, and Agents. Except for System Group Agents and System Recovery Agents, who are affiliated with the extended enterprise, agents are affiliated with a particular organization in the enterprise and operate on behalf of that organization. Table 1 summarizes the various roles.

The two Administration Security Officers create the organizations in the enterprise, establish and maintain a security policy for each organization, and enroll all other administrators except for Agents, who are enrolled by Super Agents. For the zero-footprint solution, one or more of these organizations are designated "Web organizations." These organizations are flat structures with a single department and authorization level. The reason is that Users enrolled in these organizations can be authenticated through a Client Stored Value, essentially a pass-phrase, rather than through an Access Signature, which offers greater assurance.

Roles	Scope	Enrolled by	Duties
Administration	enterprise		create organizations and specify whether public or private; create departments & authorization levels for each organization; enroll and manage various agents; create system-level DMGs; select encryption methods
System Group Agents	enterprise	Security Officers	manage system-level DMGs
System Recovery Agents	enterprise	Security Officers	participate in data recovery
Organization Agents	organization	Security Officers	participate with Security Officers when super agents are enrolled or policy is updated
Organization Recovery Agents	organization	Security Officers	participate in data recovery
Super Agents	organization	Security Officers	enroll and manage Agents; assign clearances and list of visible organization
Agents	organization	Super Agents	enroll and manage Users and Entities; assign clearances and list of visible organizations to Users; specify whether Users are listed and have PKI Privileges; create and manage agent-level DMGs
Users	organization	Agents	run applications that encrypt and decrypt data

Table 1. TriStrata Security Management Roles.

The policy for an organization can be set to require the participation of an Organization Agent in subsequent administrative functions (enrolling super agents and updating policy) and the participation of an Organization Recovery Agent in recovery operations (discussed later). Policy settings also determine whether the organization is public, in which case it is potentially visible to users in other organizations, or private, in which case it is not. They determine the default algorithms to be used for data encryption on an organization and group basis.

Both Security Officers must be present for the initial configuration and for any updates. Their authority to perform these operations is established by two Authentication Disks, which are created by TESS during system installation. Both floppies must be inserted in order to proceed with security administration. For maximum security, the pair of disks must be physically protected in such manner that they are not accessible to others or to a single Security Officer. For example, each officer could store a disk in a private safe, or the pair could be stored in a double-locked safe. Backup disks, similarly protected but stored in a separate physical location, are also needed to protect against disk failures.

More than two people can be assigned the role of Security Officer to ensure the availability of at least two. For example, two persons could be given a copy of the first disk and two others a copy of the second disk. TriStrata uses this approach to administer their own system.

When the Security Officers enroll a Super Agent, the agent is assigned to a specific organization. The Super Agent is also assigned a set of public organizations that are visible to the agent.

Super Agents enroll and manage Agents within their organizations. The Agents are given a set of visible organizations, which must be a subset of those visible to the Super Agent enrolling them. For non-Web organizations, the Agents are also assigned clearances, which are specified as authorization levels within particular departments in the organization.

> One of the dangers of using encryption is that an organization can find itself locked out of its own information.

Agents enroll and manage Users and Entities such as file and database servers. In non-Web organizations, the Agents assign Users clearances, which must be at or below their own clearance, and a subset of their visible organizations. They also specify whether a User is to be listed or unlisted and, in an enhancement currently being developed, whether the user has public-key infrastructure (PKI) privileges.

When a User is enrolled in an organization, the User is assigned a unique Security Registration Number (SRN). For non-Web organizations, the User is also given an Access Signature, which serves to authenticate the User to TESS and establish a mechanism whereby the User and TESS can communicate securely. For a Web organization, the User is enrolled with a Client Stored Value (CSV). Instead of communicating with TESS directly, the Web Server operates as a proxy on behalf of the User. If the User also has an Access Signature, the User is given the option of using the signature for direct communication with TESS or of using the proxy Web Server.

> TriStrata addresses this requirement by allowing persons enrolled as Recovery Agents to decrypt any information that has been encrypted within the enterprise.

Users can enroll themselves into a Web organization if so permitted by the organization's policy. This might be done by visiting the organization's Web site. Users can also be enrolled automatically from LDAP-compliant directories. This allows enrollments of people who are already known and registered with the organization's Web.

The TriStrata management framework supports two types of dynamic membership groups: agent-level DMGs and system-level DMGs. Agent-level DMGs are created by Agents and restricted to the users within a particular organization who were enrolled by the Agent. They are not visible to other users. System-level DMGs are created by the Security Officers. They can be made visible, in which case the group and its membership (including unlisted users) is visible to all users, or they can be made invisible, in which case they are visible only to group members. In addition, they can be restricted to a particular organization or they can be open to all users enrolled in any of the public organizations. The Security Officers also decide whether a Systems Group Agent is required to add or remove users to the group, or whether users can be added and removed by the Agents who enrolled them.

In general, policy parameters can be changed. Agents and users can be removed. Clearances can be increased or decreased. Group memberships can change. Visibility settings can be altered. However, it is not possible to delete departments or authorization levels. This ensures that the seal attached to information encrypted at the departmental level can always be interpreted by TESS. The drawback is that if an organization is restructured or the framework

for clearances is found to be inappropriate, it may be necessary to create a new organization and re-enroll users into the new organization.

The employees of an organization can perform more than one role. For example, someone might be enrolled as a Super Agent, Agent, and User. Each role has a separate identity in the system, with a unique Security Registration Number and Access Signature or CSV. In order to perform the duties associated with a particular role, a user must operate from the SRN for that role.

Data Recovery

One of the dangers of using encryption is that an organization can find itself locked out of its own information. For example, an employee might die, quit, or be fired, leaving behind encrypted files. Alternatively, the organization might suspect an employee of wrongdoing, for example, engaging in fraud or selling company secrets, and want to review information stored on the person's computer (assuming company policy does not give employees an expectation of privacy). As a third possible scenario, a law enforcement agency might serve the organization with a court order to search an employee's computer for evidence of criminal activity. In all three scenarios, a mechanism is needed whereby someone other than the user with normal access to the data can decrypt it.

TriStrata addresses this requirement by allowing persons enrolled as Recovery Agents to decrypt any information that has been encrypted within the enterprise. There are two types of agents, System Recovery Agents, who operate on behalf of the enterprise, and Organization Recovery Agents, who belong to particular organizations. At least two recovery agents must be present for decryption to proceed, but an organization can require more than that and it can require that at least one of its own agents be present during decryption. TriStrata recommends that two to three times as many persons be enrolled as Recovery Agents than needed so that enough can be gathered together on short notice. An organization can also establish a position of Key Recovery Official. That person would have the legal authority to authorize recovery and be the only one with the software needed to perform the decryption. The complete recovery process is designed to ensure that an organization retains control over its information.

The hardening and limited functionality offered by TESS protect it from network intruders. The system has so far withstood penetration testing and analysis.

Each encrypted message must be recovered separately. The Recovery Agents transmit the seal in a message to TESS. TESS decrypts the seal and returns the encryption keys for the message. Like other transactions with TESS, recovery operations are logged.

TESS Operation and Security

The TriStrata Enterprise Security Server (TESS) forms the heart of the system. Obviously, TESS security is crucial to the overall security of an enterprise. If it can be compromised, someone could get all of the secret information needed to read sensitive data, alter a user's authorizations, or reprogram TESS to bypass some or all of the TriStrata security measures.

TriStrata controls physical access to their own TESS by keeping it in a double deadbolt-locked room with motion and sound alarms, a self-auditing access-controlled electronic lock, and a glass wall. Two persons (the Administration Security Officers) are needed to open the locks and enter the room. Thus, assuming the locks cannot be picked or stolen and the electronic lock and the monitored alarm system cannot be bypassed, a single person cannot compromise physical security. Even if someone got in, others might notice the breach of security through the glass wall.

The TESS software runs on Windows NT4, which is potentially vulnerable to attack. To protect against software attacks, the TriStrata Installation Guide gives instructions on how to harden TESS. These changes are to be made by a knowledgeable Windows NT Systems Administrator. They include disabling network server, workstation, and browser services and marking various other services for manual startup only. All network ports are disabled except for the port used by TESS to communicate with clients and with its replicas. Other changes include renaming the Administrator account, disabling the Guest account, disallowing network access, requiring at least 8 characters in passwords, turning on auditing, and numerous other measures designed to protect Windows NT machines. The TriStrata hardening procedures are a TESS-specific and expanded version of those written by Russ Cooper at Lucent Technologies.

The only communications supported by TESS are PAL transactions with clients and interactions with its replicas. All communications are private and authenticated, precluding spoofing attacks. It is not possible for someone to Telnet to TESS, FTP files from TESS, or perform any of the other operations used by hackers to invade systems. The PAL protocol includes a length field, so TESS is not vulnerable to buffer overflow attacks from client machines.

The hardening and limited functionality offered by TESS protect it from network intruders. The system has so far withstood penetration testing and analysis.

TESS is potentially vulnerable to a remote denial-of-service flooding attacks. However, because it is replicated across multiple machines, an adversary would have to bring them all down

in order to shut down services. If there are enough replicas, the network will become clogged with traffic before every TESS machine is stopped. To prevent these attacks, the TCP/IP stacks can be replaced with ones that have counter measures. TriStrata also aborts empty or invalid socket requests on a configurable time-out to make this type of attack even more difficult.

The Windows NT TESS Administrator is the only person with an account on TESS. The Administrator could potentially compromise TESS, but not by acting alone. Because the system cannot be accessed remotely and is kept in a double-locked room, the Administrator cannot access the machine without the cooperation of the two Administration Security Officers with keys to the room. TriStrata requires that at least one of those persons be present during system maintenance operations on their own TESS machines. The TriStrata security administration functions, which are used to initialize the TESS databases, create organizations, specify policy, and enroll users, require the presence of two Administration Security Officers. The administration software will not proceed until both Security Officers have loaded their Authentication Disks.

The TESS security administration functions can be installed on a TESS server or on a separate machine running Windows NT. If the latter option is used, TriStrata recommends that the machine be given the same physical security as the TESS machines. TriStrata performs its own security administration directly on its primary TESS. If administration is performed on a remote workstation that is used to run other applications, for example, e-mail and Web browsing, there is the possibility of malicious code entering the workstation. That code could not, however, migrate to TESS or compromise TESS. Even if it succeeded in taking over the workstation, any security-related operations would show up in the TESS log and so be detectable.

The TESS databases are critical to system operation. If certain data is destroyed or becomes unusable, it could become impossible to decrypt data or know who is authorized to access it. The TriStrata system protects against such data loss through backups and two-person control. After one TESS (the primary) is initialized, the database of random numbers which are used to generate keys is backed up onto two CDs. Both CDs are needed to reconstitute the database (the database is the XOR of their contents). Similarly, the database of information about the organizations, users, clearances, authorizations, and so forth is backed up onto two CDs (it is also backed up following major changes). The four CDs are then used to initialize a second (backup) TESS. This is done by performing a TESS recovery operation from the CDs, in the process testing their integrity in case they are ever needed to restore the primary TESS. The CDs protect against possible sabotage of TESS.

A single TESS can handle 2,000 transactions per second in its current configuration. With up to 32 replicas, a collection could handle 64,000 transactions per second, or about 23 million an hour. This is more than adequate to support a community of 1 million users. The main limitation is writing the log. Next is bandwidth on the network. The total amount of data exchanged in the PAL transaction (request plus response) is typically around 500 bytes, about half of which are for the seal.

A single TESS can handle 2,000 transactions per second in its current configuration.

CONCLUSIONS

The TriStrata system represents a breakthrough in secure information management for organizations and their extended enterprises. Its infrastructure offers a comprehensive approach to security, from policy definition and administration to enforcement and detection of security violations. Encryption is an integral feature, but it is coupled with access control, authentication, and auditing. It is centrally managed so that an organization retains control over its information assets. Access capabilities can be revoked at any time. All encrypted information is fully recoverable.

The TriStrata product provides a high-security, high-performance framework for electronic business and commerce. The centralized component, TESS, does not introduce a bottleneck or single point of failure. The system addresses both insider and outsider threats. It is exportable world-wide. The TriStrata system is well suited to enterprise security, better than PKI while maintaining the capability to transparently interoperate with PKI. It would be an excellent choice for any enterprise, whether a single organization or an international affiliation of thousands.

The TriStrata system represents a breakthrough in secure information management for organizations and their extended enterprises. Its infrastructure offers a comprehensive approach to security...

The TriStrata business model allows Application Service Providers and Security Service Providers to maintain and administer the security system for an enterprise, including its TESS. This can simplify the integration of security into an enterprise, while introducing a new business opportunity for SSPs.

For more information
about the TriStrata Management
System for Information Security,
contact:

3 Lagoon Drive
Redwood Shores, CA 94065
TEL: 650.596.1757 FAX: 650.596.1750
www.tristrata.com