Electronic Business without Fear: The Tristrata Security Architecture

Nearly 80% of global CEOs surveyed believe Internet enabled electronic business will reshape competition in their industries, according to a recent Price Waterhouse/World Economic Forum Survey. Computer data security is fundamental to companies and individuals conducting electronic business over the Internet. Yet, in spite of the enormous potential of electronic business, companies, their customers, and their business partners are often reluctant to adopt new market and technology strategies. This is partly because of concern about computer network security and confusion about the many layers and aspects of current and planned security systems. A welter of largely incompatible intra-company and inter-company security approaches exacerbates the confusion. Technologies added over the years to systems designed for a now obsolete computing world still burden many business and government enterprises.

The TriStrata architecture is a "clean sheet" approach with high security, low overhead, no export restrictions, and general applicability to any enterprise computing environment. In this paper we describe this new approach and its implications for Price Waterhouse clients engaged in electronic business.

Data security: linchpin of electronic business

Electronic business depends upon secure data communications. Electronic business applications support hundreds of activities such as displaying advertising, sending e-mail messages, browsing a catalog, placing an order, checking on the status of the order, and communicating with customers. None of these activities can or should happen without the assurance that data being transmitted between computers will be private. Electronic commerce enterprises, their customers and their business partners must know that data will not be tampered with, that data will not be lost in transit, and that data will not be accidentally deleted.

Yesterday's challenge was to manage a company's own internal network users and data security across a worldwide network. Today's challenge is to manage numerous individuals and business partners outside the company, each with a different security environment, and each with permission to access specific data within that network. Tomorrow's challenge will be to ensure that data security policy and procedures will be sufficiently flexible to give organizations a competitive edge in a constantly changing electronic marketplace, yet to do so efficiently without ever compromising security standards.

Since 1997, Price Waterhouse has been working with Tristrata Security to perfect a data security architecture that addresses these issues. Tristrata was founded by electronic commerce pioneer Dr. John Atalla, the former CEO of Atalla Corporation. Atalla invented the Atalla Box—a hardware encryption device that is used to protect over 90% of all ATM networks in operation today. Along with the Atalla Box, Dr. Atalla also invented the PIN PAD technology that each of us uses daily with our ATM cards.

The Tristrata architecture is a response to the electronic commerce needs of business enterprises, their partners and their customers. To fully understand the importance of the Tristrata architecture and its implications, it is helpful to understand how data security requirements and systems have evolved in today's electronic business environment.

Challenges of protecting data in the networked era

Data protection has been a challenge and a priority since the earliest days of computing. Like so many other 20th century technologies—Scuba, Radar, Jet engines, the Internet—scientists developed them for military applications and later adapted them for commercial use. At first, security was aimed at physically controlling the actual storage and transmission media. This included guarding the data center with its computers under lock and key and keeping storage media such as magnetic disks in a separate, remote location. Meanwhile, data transmitted over telecommunications links was scrambled to make it incomprehensible to eavesdroppers. Scrambling data this way is called encryption. Encryption combines digital "keys" (sequences of bits) with the "plain text" data using mathematical functions that transform the data into "cipher text." The cipher text appears to the outside observer to be almost a random sequence of gibberish. However, a recipient with a corresponding digital key can undo the function to turn the cipher text back into the original plain text. Even though encryption does provide data protection, additional challenges remain. For example, users must exchange the keys privately and protect them with secret passwords. This, in turn, leads to challenges such as granting individuals access to keys, granting access only to certain data, tracking who is using the keys, and revoking their access when the keys are stolen or compromised.

These new considerations and new mechanisms for computer security have been introduced incrementally over time. Approaches to security in a networked environment are often incremental adaptations of outdated communication security methods spawned before data transmitted over networks even emerged from the four walls of the data center. In the world of electronic commerce we cannot simply lock up the data center for the night and go home.

For example, physical control over a private network can be relied upon when both end points of a circuit are controlled and the circuit is used only for transmitting secure data. At first, most networks were private, and simple security mechanisms were sufficient. However, transmitting data over a public network, such as the telephone system, is a potentially less secure process and therefore required the computers to identify each other by secret codes before beginning a data transmission. Later, communication became even less secure in "packet switched" networks, which break up a data transmission into small packets for which there is scant control over their individual routes from source to destination.

The Internet is a public packet switched network in which physical control by sender or recipient is impractical. The response has been to introduce technology that establishes a "virtual" private network (VPN). In a VPN, computers identify each other and authenticate users by the exchange of secret keys and then communicate with each other by exchanging only encrypted data packets. Today there are already several different security standards for virtual private networks: IP security (IPsec), SOCKS, Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP). Each of these has its own supporting vendors and is incompatible with the others, which limits their usefulness for exchanging information between business partners. Other mechanisms include "firewalls" that block certain types of messages entirely, and "proxies" that hide the details of an internal corporate network from the external Internet. There are hundreds of these incremental adaptations of basic Internet protocols.

Electronic business opportunities—and threats

Computer networks have long enabled individuals to exchange information within companies, but electronic business really began when electronic data interchange (EDI) and electronic messaging technologies began to facilitate the exchange of information between businesses. This information exchange has since broadened to encompass not only data exchange, but also business-to-business and business-to-consumer transactions conducted over the Internet and the World Wide Web.

In response to changing security needs many companies developed multiple security mechanisms to provide different degrees of protection from different types or threats. It is tempting to believe that each of these different mechanisms acts as a ring of protection, each one providing a strong and complete layer of security. Unfortunately, this is not the case. Different network security mechanisms provide different degrees of protection from different types of threats, have different strengths and weaknesses, and are complementary, not complete. Penetration of any one mechanism can compromise the entire system.

As will happen in any complex system that has evolved and been engineered in an undirected, incremental way, the systems that provide data security using these techniques have become increasingly complex, cumbersome and costly. The cost and complexity arises not only in the technical systems within a business unit, but reaches farther. The cost is paid by IT departments everywhere working to provide authentication, confidentiality and availability across security domains even within a single company. The cost is paid in corporate boardrooms where a multitude of inconsistent security technologies hinder rather than promote communication with business partners. The cost is paid in public life where government and international policy debates ensue over issues such as key escrow, recovery, export restrictions, and privacy.

Meanwhile the opportunities for companies engaged in electronic commerce are unprecedented. IDC, for example, estimates that Internet commerce will explode from $8 Billion in 1997 to $333 Billion in 2002. It is difficult to identify any industry—financial services, manufacturing, health care, education, travel—that is not being transformed by the changes wrought by the Internet.

Commerce conducted over the Internet or any future public data network has the potential to wreak profound change on the pace and cost of doing business for every enterprise, no matter its size. The Internet is creating new service opportunities at every point along every supply chain and new efficiencies at every distribution and retail outlet. It also creates new threats to every existing communication, broadcast and publication medium. That is because the Internet and its successors enable the transmission of data from anyone to anyone—between companies and their employees, suppliers, and customers. In part, this is due to the open nature of the network, with features that make disparate computers and organizations able to exchange information according to simple, standard, open data formats and network protocols. Moreover, the exchange of data is not only relatively simple, but also fast and getting faster. Improvements in the physical network will allow the transmission of data from anywhere to anywhere at hundreds of times current modem speeds. For example, the wireless communications company Teledesic is building a global, broadband "Internet-in-the-Sky” using satellites that will support millions of simultaneous voice, data and multimedia communications at speeds up to 2,000 times faster than today's standard analog modems.

Yet, against the tide of hyperbole about such sweeping implications, skepticism is understandable: one naturally seeks the fatal flaw in the vision. One does not need to look far to discover that flaw: data transmitted over a network so open stands vulnerable to interception, redirection, tampering, and outright loss. Malicious hackers can gain access to data that allows them to impersonate other individuals and initiate fraudulent transactions. As Richard Power of the prestigious Computer Security Institute recently noted, “In cyberspace, the doorknobs get rattled every day.”

Today, those responsible for the networks and the applications that use the networks must find ways to ensure the privacy of communications. They must:

- ensure positive identification of the senders and recipients of data;
- ensure that the information being transmitted is not lost or modified in transit, and
- implement security policies in an environment of unprecedented technological and organizational disruption.

There seems to be no escaping it: anxiety over complex security issues and confusion over what security mechanisms to adopt has been, and remains, a key blocking factor in electronic commerce initiatives large and small.

A clean sheet approach

Tristrata offers a fundamental shift of perspective: a “clean sheet” approach to data security architecture encompassing an end-to-end security solution. The design starts with the premise that although any computing device and its data storage can be physically secured from tampering, the device is also a connection point into a fast, global, public, packet switched network. As with any engineering design challenge, Tristrata began by defining fundamental data security requirements and then designing a system to meet them. The requirements met by the Tristrata design include:

- strong but fast encryption;
- minimal communication overhead;
- minimal key management;
- freedom from government restrictions or dependencies;
- built in audit trails;
- fine grained, user-to-user authentication;
- security for all existing software and data.

The main features of the Tristrata data architecture ensure that:

- *all* data throughout a distributed computer system can be economically encrypted and sealed;
- an enterprise wide security architecture using a server-based approach to granting and data accesses by specific individuals and groups';
- a log of all accesses to the encrypted data is recorded in files that cannot be tampered with;
- accesses are restricted to named individuals no matter where the data is read;
- the control over which individuals are allowed to read any data is centralized, secured, and can be revoked globally with a single step.
- self managed key recovery that can be performed on the authority of any defined number of participants;
- export approval already granted by the US government.

The underlying security architecture ensures that data is encrypted, signed, and contains its own access control information. Hence, it dramatically reduces reliance on a Babel of other Internet security mechanisms. The simplification offered to enterprises doing business on the Internet is revolutionary—providing competitive advantages such as:

- secure access to corporate data for employees with mobile computers without any need for dedicated remote access computers;
- secure communication over inexpensive Internet connections between computers at any number of corporate sites in any country;
- simplified enrollment to grant secure network access to any business partners needing real-time access to corporate information;
- tight control over every data access: efficient, centralized, secured, and able to be revoked globally with a single step;
- restriction of access to any data to any named individuals no matter where the data is read.

The Tristrata security architecture is patent pending and a full description for a technical audience is forthcoming in a peer reviewed cryptography journal. In the following paragraphs we offer an executive summary of how the Tristrata architecture meets the fundamental security requirements of organizations engaged in electronic commerce.

Strong but fast encryption

Encryption is the only practical means to provide data confidentiality. The main goal of an encryption algorithm is to ensure that a computer can encrypt and decrypt data efficiently when the keys are known. It is also vital to ensure that the keys are the only economically feasible decryption method. Moore's Law, attributed to Gordon Moore of Intel—says that the number of transistors on a chip of a given size doubles every 18 months. This means that the amount of computing power available at a given price also doubles every 18 months (or, equivalently, increases by a factor of 10 every five years). Just as the ability to record data increases exponentially, so does the need to protect it. Thus, enterprises need to be able to encrypt efficiently and make an attack economically infeasible in a technology environment in which the production and storage of data accelerates constantly.

A tutorial on encryption technology and cryptography is well beyond the scope of this article. However, it is important to understand that for any sensible encryption scheme, the longer the keys are, the greater effort it takes to compute the mathematical function. This, in turn, makes it that much more difficult for an attacker to find the key. Furthermore, as computers get more powerful in accordance with Moore's Law, the advantage needs to accrue to the encryptor and not to the attacker.

For example, suppose that a dozen bits to the key means it takes twice as much computing effort to encrypt some data. It should then far more than double the size of the problem from the attacker's point of view. All encryption schemes in wide use today have this desirable property. However, they vary enormously in how much computation they require and how resistant they are to attack relative to that computational effort. For example, the US Government's Data Encryption Standard (DES) is currently around 100 times faster when implemented in software than the RSA encryption scheme. Yet, breaking RSA keys is believed to be far more than 100 times as difficult as breaking DES keys. Both algorithms have their appropriate uses; the point is that different schemes differ in the protection they provide relative to their cost.

An ideal encryption scheme from this point of view, then, would provide strong protection against attack but require very little computation—just a few simple arithmetic operations worth of computation for each byte of data. Although cryptography is one of the most active areas of research in computing today, the need for strong encryption that satisfies this property does not necessarily imply a need for new or more complex approaches. In particular, the Vernam system and its refinement by Lyman Morehouse at AT&T can, with long enough keys, provide sufficient levels of confidentiality—even though it was invented in 1917. The Morehouse cipher, as it is called, draws its keys from an arbitrarily large (say, a Megabyte—8 million bits) block of random data, and needs only a few of the most primitive mathematical operations called the "exclusive or" to encrypt or decrypt data. The Tristrata system bases its encryption on the Morehouse cipher and as a consequence can encrypt and decrypt large amounts of data almost as fast as it can be moved.

Minimal communication overhead

Transmitting data from point to point over a computer network takes time. The total elapsed time consists of various kinds of delays. Like a commuter going into town from the suburbs, there is the time spent in the car driving at a given speed, but also time spent getting into and out of parking lots, waiting at stop lights, and taking detours around traffic jams. In computer networks, these delays comprise the communication overhead (also called latency).

For example, in principle a message consisting of a thousand bits of data can be sent at a million bits per second over a wire and will only take one tenth of a second to arrive. In reality, it will take longer. That is because the message incurs latency at each point along its path where the data is stored, routed, and repackaged into different forms. Additional delays occur during the round trip time in which the receiving end acknowledges receipt of data from the sender.

When the data sent is small relative to the available bandwidth, the user spends far more time waiting on the latency in the network than on the actual transmission. Therefore, it is undesirable to design computer programs that use complicated cycles of sending and acknowledgment in order to get things done. As the Teledesic example cited above shows, there will soon be a great deal of bandwidth available. Therefore it is important to design new computer systems to minimize latency, even if that means sending additional data in bigger chunks.

This challenge is particularly relevant for virtual private networks (VPNs). VPNs encrypt all their data before sending it in packets over the public Internet. One of the crucial steps for the programs that implement virtual private networks is a setup stage, in which one computer contacts another to exchange encryption keys. Some schemes generate and exchange keys before each new transfer. Under current schemes, the sender and the receiver must both send and acknowledge messages to each other and to a trusted third computer before the data transfer can begin. From the user's point of view, all of this incurs latency and slows communication.

The Tristrata architecture minimizes the communication overhead in a VPN. It achieves this by sending encrypted data with an "access signature" already embedded in it. The signature lies within a seal created by a secure server—indeed, the only server that can actually open the seal. To send data, the sender sends a single message to the TESS (Tristrata Enterprise Security Server) and TESS returns a seal, which the sender uses to encrypt the data going to the recipient. Upon receiving the sealed data, the recipient need only send and receive a single message to the same TESS to unlock the encrypted data that remains. The keys are therefore hidden in the data being sent, and TESS will only unlock the seal for the intended recipient. Having fewer steps in the process improves overall efficiency.

Minimal key management

Key management is one of the most important aspects of security architecture. This process consists of creating new keys, distributing them to users, and ensuring that lost or otherwise compromised keys can be revoked, updated or replaced. In some cases, it may also be desirable to archive keys, possibly with a third party who holds the keys in escrow.

Any cryptographic scheme needs these key management functions. For many applications in which individual users are accessing a central facility of some kind, a shared private key infrastructure is appropriate. For example, in the case of automated teller machines, each card has a private key, the owner has a password, and these are used to support private communications with the bank. For other applications in which any user may wish to communicate privately with any other party, a public key infrastructure is more appropriate. In a public key architecture, the mathematical functions used for encryption and decryption uses a pair of keys:

- an individual's secret key, which is not shared with anyone, and
- the individual's public key that is published to the world so that anyone can send an encrypted message to its owner.

While a public key scheme makes user-to-user private communications possible, it also requires the establishment of a public key infrastructure. A public key infrastructure must include certification authorities that maintain directories of users and their public keys. A certification authority is a legal or business entity, not a technology, so that a public key infrastructure involves more than just complex technology. It also requires a legal and operating framework that is not necessarily compatible from company to company—or country to country. For example, the groupware system Lotus Notes assigns public keys to each user. As a result, they can send private messages to each other. However, secure e-mail between companies generally required other mechanisms, because until recently those keys were incompatible with the keys used for other Internet based secure messaging schemes.

Even with a public key infrastructure in place, a fundamental issue remains: once you assign a key, it's hard to revoke it. Consider the position of relying party Robert, who receives an encrypted message that purports to be from sender Susan along with her public key, which has been certified by the issuing authority Imperium. Robert (the relying party) needs to ensure that the key really belongs to Susan. As it stands today, the relying party must exchange an electronic message with the issuing authority Imperium every time he uses a key. Otherwise, Susan's private key may have been stolen and the message forged. Even if Susan had notified Imperium, she would not have been able to tell everyone who might possibly receive a forged message from the thief.

Tristrata has developed a simpler approach to solve the revocation challenge, based on a change in perspective. Since the relying party must exchange an electronic message with some issuing authority to use a public key, TESS simply provides the same certifying function without involving a third party. In the Tristrata architecture, TESS maintains a directory of users and their access signatures. The sender of a message to a given user obtains from TESS a set of one-time keys which it uses to encrypt and seal its message. The recipient of the message then exchanges messages with TESS to unlock the sealed message. In this way, the exchange of certification messages is combined with the act of encrypting or decrypting the data. Hence, there is only one place in the system—TESS—where the signature can be revoked. Revoking the key via TESS instantly prevents anyone from either sending or receiving messages intended for that user.

Freedom from government restrictions or dependencies

Because electronic business is global, ideally there would be uniform applications across different government jurisdictions. Unfortunately, this is not the case and current data security implementations fail this uniformity criterion. United States government policy classifies strong encryption technology as weapon and imposes restrictions on its export. This restriction is often debated in the context of exporting commercial systems like RSA, but the US State Department rarely approves export even of DES—the government's own standard. Strong encryption products are available from outside of the US but interoperability is not guaranteed. By contrast, the Tristrata architecture uses cryptographic algorithms that are not subject to export restrictions, have already been approved for export by the US government, and are implemented identically worldwide.

Some security technologies also rely on proprietary cryptography covered by US patents. Generally, the standards that govern Internet communications are not adopted when they depend on proprietary algorithms. This is because the owner of the algorithm would have an effective monopoly requiring all users to license the algorithms from them. For example, even though the recognition of US intellectual property is not uniform worldwide, international standards bodies are reluctant to adopt standards such as S/MIME, a secure electronic messaging standard for the Internet, because it depends on proprietary RSA technology. By contrast, although the Tristrata architecture is patent pending, its cryptographic algorithms have long been in the public domain and present no obstacle to interoperability.

Finally, establishment of a public key infrastructure depends on a combination of enabling legislation and government policy. For example, there are no internationally accepted procedures for the establishment or licensing of certification authorities. Different governments take different positions with respect to whether private keys can or should be archived or held in escrow. These differences create significant uncertainty and risk for both key holders and relying parties.

A better approach places the responsibility for key management back in the hands of the private sector. In the Tristrata approach, the TESS is the repository of a closed system in which:

- users are granted keys under a defined security policy,
- the keys are archived or made recoverable under control of the issuing company, and
- the authentication of legitimate users and their access to all data is controlled from a single point.

Built-in audit trails

Maintaining data security in any organization is a serious responsibility. It is also increasingly difficult, especially in the Internet environment where technologies for ensuring secure communication are changing rapidly and becoming increasingly complex. There are many different technologies for security strategies such as virtual private networks, cryptography, key management, and so on. It is rare to find an organization that has *all* of the necessary technical staff, skills, policies, and procedures in place to cope with many different types and points of attack. Technical attacks are not the only threat. For example, in an electronic business setting, it is important to be able to provide proof of message delivery, which current Internet messaging standards do not achieve and which requires yet another layer of complex security software. Moreover, responsibility for data security is increasingly shared outside the company, with the Internet service provider, with public key certificate authorities, with an increasing number of software vendors, and with business partners having access to internal networks. The combination of increasing complexity and shared responsibility for the safety of the enterprise rightly is a major challenge for today's CEOs and IT executives.

In the midst of all this complexity it is worth re-examining some fundamental issues.

The most basic of security procedures is the monitoring activity that detects evidence of: (1) attempted intrusion; (2) changes in user activity and privileges; (3) unauthorized accesses or other unauthorized events. Those procedures require the existence of logs (audit trails) of security related events. Yet, the responsibility for ensuring the creation, integrity and maintenance of these logs is diffuse, with different software products generating logs in such different ways that often, additional third-party software tools are needed just to summarize and analyze them. Ironically, the most fundamental event in a secure data network—a given user using a key to unlock data at a given moment in time—is usually not logged at all.

The Tristrata architecture reverses these trends toward greater complexity, diffusion of responsibility, and disappearance of crucial information. Each time data is encrypted, TESS creates a new seal on behalf of the sender, and later unlocks that seal for the recipient. TESS is thus able to log both the sending and the receipt of the data without penalizing either user. From an engineering perspective, the amount of information recorded is small. As a result, it is highly cost-effective to ensure the server can write the logs fast enough to keep up with network speed and usage. This is especially true when one considers the costs of the alternative strategy: reconstructing evidence of unauthorized usage from a variety of sources. Disk space is cheap; proof is priceless.

User-to-user authentication

Authorization is the process of determining how an authenticated user is permitted to use computing resources, or, more specifically, determining what data an individual user is allowed to access. Authorization rules in most computer systems are normally specified by Access Control Lists (ACLs) that consist of names of specific individual users and may include other ACLs. One of the desirable features of a comprehensive security architecture is a fine grained level of authorization control for every user. In principle, any individual user should be able to grant and revoke access to their data to any other authenticated user and to no others. Secure e-mail is a simple example: a user should be able to send an encrypted message that only its intended recipient can decode.

More generally, it should be possible for a user to create an ACL for any data and to change the ACL independently so as to flexibly grant and deny access to any named individuals. Current mechanisms for doing the latter are relatively primitive. For example, a user might send an encrypted file to a number of individuals, and distribute the password separately to specific individuals. Once revealed, however, the password cannot be taken back. Current groupware systems typically reserve to system administrators the privilege of creating an ACL, and then only for relatively large units of data such as an entire document collection.

Tristrata seals data for transmission along with its ACL. The ACL may already be a named group stored on the TESS, or could be constructed specially for any specific data set by simply listing the individuals or group recipients who should have access. When any recipient requests TESS to open the sealed data, TESS checks the ACL to ensure that the recipient is currently authorized to do so. The implications are profound: sealed data can be made available to any number of individuals, their ability to access it enabled from a single point, and in combination with mechanisms for logging access and revoking authorization, the originator can exercise an unprecedented degree of control.

Security for all data and application programs

The architecture of any complex system is composed of many layers of design, with the upper layers depending on the operation of the lower levels. In the case of a computer system, the lower layers are the physical hardware, the subroutines (drivers) that control individual devices such as disks and network interfaces, and the operating system. Upper layers include the applications that handle functions like e-mail and databases, and personal productivity applications like spreadsheets. It stands to reason that in the case of data security, the fewer layers it depends upon, the more secure it will be against attack from within the system itself. Indeed, data security is so fundamental that it needs to be built into the lowest possible layer—the operating system. Furthermore, this integration should be transparent, so that all the higher layers of design that depend on the operating system can benefit from the strong security without requiring any upgrade, re-configuration, re-installation or replacement.

Tristrata has achieved this integration through two main components, the Tristrata server (TESS) and the client software that establishes network connections between computers. The Tristrata server uses a fault tolerant pair of Intel-compatible servers running a security hardened version of the Microsoft Windows NT operating system. In this configuration, the server remains available 24 hours a day and supports hundreds of security transactions per second. The client software runs on any computer running the Windows operating system and is tightly integrated into “Winsock,” the portion of the operating system responsible for communicating with other computers using Internet protocols. In this way, all existing applications continue to work just as before—better, in fact, because users will not need to sign on and provide passwords separately to access different computers, networks, applications, or protected files.

The benefits are manifold and accrue to the organization both internally and externally. The Tristrata architecture creates an exceptionally secure virtual private network. One of the ways this is used is to allow employees with mobile computers to connect to the Internet using any low cost local service provider, yet still connect to any data resources that they could normally access in the enterprise. This eliminates the need to purchase and monitor the security threats arising from one or more dedicated corporate remote access points. Similarly, any pair of users enrolled and authenticated by a TESS can exchange information over the Internet whether both, one or neither are physically located in the same facility as the TESS. Over the long term, applications with their own, redundant security mechanisms can be simplified. Programs downloaded from the Internet, such as Java applets, no longer need to be separately authenticated and can easily be given controlled and limited access to specific data. Database programs need no longer require users to identify themselves separately upon connecting. Users are not burdened by significant computing overhead thanks to the efficient encryption and communication design, yet corporate data security is vastly increased.

Business implications of secure networking

The cumulative impact of applying simple, reliable, effective technology to complex network applications is often astonishing.

The success of the World Wide Web, for example, can be attributed in large measure to the simplicity and transparency of hypertext Markup Language (HTML). HTML is the language used to “mark up” Web documents with fonts, formatting, and hypertext links. Computer scientist Tim Berners-Lee designed HTML to make it easy for users without extensive programming background to publish documents on the World Wide Web. He achieved this by ensuring that even minimally marked up text would be presented readably on any computer. Berners-Lee also designed HTML to help both Web publishers and readers to create links and navigate between the documents. The complexities of achieving this were hidden in the web server and web browser software programs, invisible to the users who only needed to point and click. Today, the quantities of information published and consumed in this way have succeeded beyond anyone's expectations, thanks to the compounding effect of easily used technology propagated across a global network.

Effective use of Internet technologies in an "Extranet"—a virtual private Internet accessible to trading partners—requires more security and control than the open publishing model of the World Wide Web. Atalla, like Berners-Lee, expects that the reliable, and effective network security technology he has designed will have compounding benefits—in this case for electronic business companies, their partners and their customers. Consider the following illustrations from the fields of finance and engineering.

Financial information exchange

Until recently, securities broker/dealers and institutional investors communicated via telephone, fax and other person-to-person technologies. First, broker/dealers would contact institutional investors concerning trading opportunities. Then, institutional investors would respond with requests for a quote. The ensuing quotes, acceptances, allocations, confirmations and other specialized types of communications involved in executing the trade were communicated and transcribed in a variety of ways ranging from now obsolete ticker tape and hand signals between pages on the trading room floor to the telephone and the fax.

Now that broker/dealers and institutional investors have the ability to exchange this information securely over the Internet, there have been radical changes in the way they communicate. Today, information is distributed more rapidly and simultaneously to a global audience of potential trading partners, accelerating the pace and efficiency of the market. The Financial Information eXchange (FIX) communications protocol, developed in 1993 and first appearing in products in 1996, was an important innovation that enables securities firms and institutional investors to interact electronically. FIX uses DES encryption to achieve privacy. The majority of FIX traffic is currently transmitted over the Internet because of the low cost compared to either private networks that charge by the message, or dedicated lines with their high fixed costs.

However, FIX traffic still represents only a fraction of trades and is rarely used for larger trades (over 10,000 shares). Such trades require a complex pattern of communication: information about market conditions and individual traders' strategies should only be shared with selected trading partners at selected times; messages may be sent and then updated; senders must know and later be able to prove when messages are sent and read. Current Internet protocols for secure communication make for an awkward channel for these types of communication. This is because they fail to support efficient message update, message receipt records, flexible control over the timing of release and retraction of information, and flexible control over which individuals can see which information. The Tristrata architecture offers a sound infrastructure for each of these areas, with its more efficient encryption, flexible access control list management, improved control over shared data, and access log capabilities.

Concurrent engineering and product data management

One of the distinguishing features of the products created by the world's largest companies is their complexity: automobiles, aircraft, chemicals, computers, copiers. These products undergo endless cycles of research, development, refinement and evolution, involves hundreds to thousands of components or processing steps in production, dozens or hundreds of suppliers, and require extensive distribution and maintenance organizations. The amount of product data created, used and changed at every stage of these complex product life cycles is staggering. Not only would the documentation relating to a jumbo jet far outweigh the plane itself, but its hundreds of seats would hold only a fraction of the number of people from the manufacturer, subcontractors, suppliers and depot operators who created it.

As a result, it is critical that manufacturing organizations be able to share information and foster collaboration across functional and organizational boundaries. "Concurrent engineering" methods strive to ensure communication of design changes to downstream manufacturing, production, and maintenance organizations so that they can plan their activities and anticipate potential conflicts. When a product is ready for manufacturing, the data that is exchanged includes catalogues of standard parts, production and maintenance schedules, order completion status, test results, and quality statistics. In concurrent engineering the data that is exchanged includes more complex data such as CAD (Computer Aided Design) models of parts and subassemblies, specifications, and documentation, and even the software that is present in products such as toys that include computer chips. Internet technology employed in this setting enables individuals to access the information they need to make design and other decisions directly. When this is done between companies that are business partners, the design and manufacturing collaboration fosters shorter time-to-market, while customer self-service provides cost efficient support and frees customer service representatives to add value in other ways.

One of the most important effects of Extranet extensions of internal systems is to encourage customer and partner loyalty. Yet, the set of customers and partners with access to design and manufacturing information can change rapidly. In sectors such as the semiconductor industry, small design companies often contract with two or more companies who are themselves are rivals, so the need for extremely good control over information is paramount. Thus, there is a paramount need for finely tuned and efficient information control even within the Extranet itself. If the default behavior of the system does not ensure strict control, companies could face more technical drawbacks than advantages in their business partnerships. Moreover, the volume of CAD, simulation, visualizations and other data is so large that solutions requiring expensive encryption schemes are impractical. Finally, the software applications used in engineering design are often custom software or extremely specialized packages: it is impractical to expect modification of these programs to accommodate a new security scheme. Security must be embedded into the operating system and environment transparently so that existing applications benefit from security without additional overhead. The Tristrata approach has all of these features, making it a robust environment for these complex environments.

Status of the Tristrata solution

Can network data security, a Gordian knot of many complex technical facets, really yield to the sword of the simpler Tristrata architecture? Price Waterhouse and Tristrata have worked together since 1997 under a joint arrangement to perform an in-depth evaluation. With the participation of over thirty Price Waterhouse IT security professionals and several world renowned security experts, the evaluation results to date have shown that the architecture meets all expectations. The multifaceted evaluation included setting up a demonstration laboratory, exhaustive penetration attacks, stress tests on performance, and development of a live prototype application for Price Waterhouse users and eight key business partners.

The success of the evaluations to date indicate that the Tristrata architecture is ready for full scale applications and is superior to other approaches now available. We believe that Tristrata technology will become the *de facto* standard enterprise wide security solution. Price Waterhouse's Enterprise Security Solutions group will offer its clients a range of services: design and installation of the Tristrata architecture, servers, and services, as well as outsourcing of Tristrata based security solutions and services.

References

- RSA Labs Cryptography FAQ, http://www.rsa.com/rsalabs/faq.htm, March 1998.
- Price Waterhouse Global CEO Survey, February 1998.

- Andrew Grove, Only the Paranoid Survive: How to exploit the crisis points that challenge every company and career. Doubleday, New York: 1996.
- Tower Group, Trade Order Routing Networks: Redefining Institutional Trading Practices, October 1997.
- Tower Group, FIXing Securities Trading Connectivity Among Broker/Dealers and Institutional Investors, October 1997.
- Gartner Group, Extranets: Planning the Border crossing, Electronic Commerce & Extranet Applications, November 1997.

Acknowledgments

This article was prepared with substantial technical and editorial assistance from Matthew Haines of Price Waterhouse Enterprise Services and Solutions, and Lauren John, Terry Retter, and Paul Turner of the PW Global Technology Centre.

About the author

Walter Hamscher is Director of Strategic Architectures at the Global Technology Centre and a doctoral graduate of MIT in Electrical Engineering and Computer Science.