Securing

Conducting business electronically...
... whilst minimising the risks!

Securing e-business

Conducting business electronically… .
… ..whilst minimising the risks!

"Ray White Real Estate have reduced their information delivery costs by 90%, by implementing a secure Intranet"

"Trac Logistics Group have improved customer satisfaction and lowered inventory levels by securely tracking their customers 'freight details between international branches over their Extranet"

"Carat Crystal have enabled clients to remotely manage their portfolios of advertising slots on a common web server, whilst maintaining secure client separation"

About the author

Peter Brookes is a Chartered Engineer, who has specialised in voice and data communications for over 20 years, with clients that have included AT&T and one of the top five global consultancy firms.

With the recent emphasis on e-business, projects have included: a major study on 'securing remote access 'for the Information Security Forum; and leading a full day workshop on 'remote access security 'at Secure Computing Magazine's International Conference on Network Security.

Frequently Asked Questions

- How can we use the Internet for e-business, without compromising the security of our whole corporate network?
- What are the risks we should really be looking out for?
- I know that static passwords are easily compromised but aren't 'strong' methods of user authentication expensive?
- We have our corporate firewall in place – isn't that enough?
- How can we stop our business partners from seeing their competitors' confidential data?
- Can we implement security without becoming security experts ourselves?

About this Paper

This white paper sets out to answer the questions that are frequently asked in relation to the securing of web based technologies, for conducting business electronically. This includes the use of Intranets and Extranets, as well as the Internet, for the purpose of remote data access and electronic trading (e-business).

The paper examines the risks involved in allowing remote access to corporate resources and why the traditional methods of securing corporate networks are insufficient. The importance of an enterprise security architecture is outlined, along with specific security controls that can be employed to minimise the risks. Too much security, apart from unnecessarily reducing profits, can encourage employees to find creative ways of circumventing it. Hence, this paper promotes the concepts of 'appropriate 'security, relative to the sensitivity of information.

Technologies are beginning to evolve that are aimed specifically at securing e-business. This paper describes what is available, together with the advantages and disadvantages of each approach. Finally, there is an independent evaluation of a new e-business security product, which has been designed specifically for e-business.. We hope you find it valuable.

What is e-business?

The history of e-business

Electronic commerce (e-business) has been around for a long time, in many different guises. In fact, any telecommunications link between two parties' computer systems, in order to facilitate business transactions, is e-business. Common examples are travel agency bookings of flights or holidays, and credit card authorisation by shopkeepers. The problem has been that each one is a proprietary system which has to be specially set up in advance, often with dedicated hardware.

The reason why e-business remained as only isolated cases was the lack of standards. Many attempts were made at establishing a consistent way of communicating electronically between systems but the only ones that had a limited success were some of the Electronic Data Interchange (EDI) standards. Even the predominant computer manufacturer, IBM, had only limited success in promoting its Systems Network Architecture (SNA) as a de facto 'standard', although many telecommunications carriers did offer SNA network services.

It has only been with the advent of the World Wide Web (www), invented in 1990 by Tim Berners-Lee at the European Laboratory for Particle Physics (CERN), that e-business has become universally viable. The Internet had been around for a long time but, for many years, was the preserve of the academic community. Suddenly, business saw the opportunity that the Internet provided, through universal connectivity, and 'browsers' emerged (the most common examples of which are Netscape and Microsoft's Internet Explorer).

The benefits of secure e-business

The commercial benefits of conducting business electronically are well documented (three examples of which are given on the first page) but, whilst most companies recognise the potential, many are concerned about the risks. E-business security is about protecting the *confidentiality*, *integrity* and *availability* of information that is exchanged between remote locations.

Only if all three aspects of security can be achieved, can the following benefits of e-business be realised:

- *Access to reliable information, anytime, anywhere*
- *Protection of the organisation's competitive advantage*
- *Increased customer satisfaction through rapid response*
- *Enhancement of the organisation's image in the marketplace*
- *Ability to conduct business in the most cost-effective location*
- *Increased employee satisfaction, through flexible/home working*

The elements of e-business

We have described the background to e-business, and the benefits it can bring, but what is it? Figure 1 is a typical e-business structure, showing the elements required for conducting business electronically.

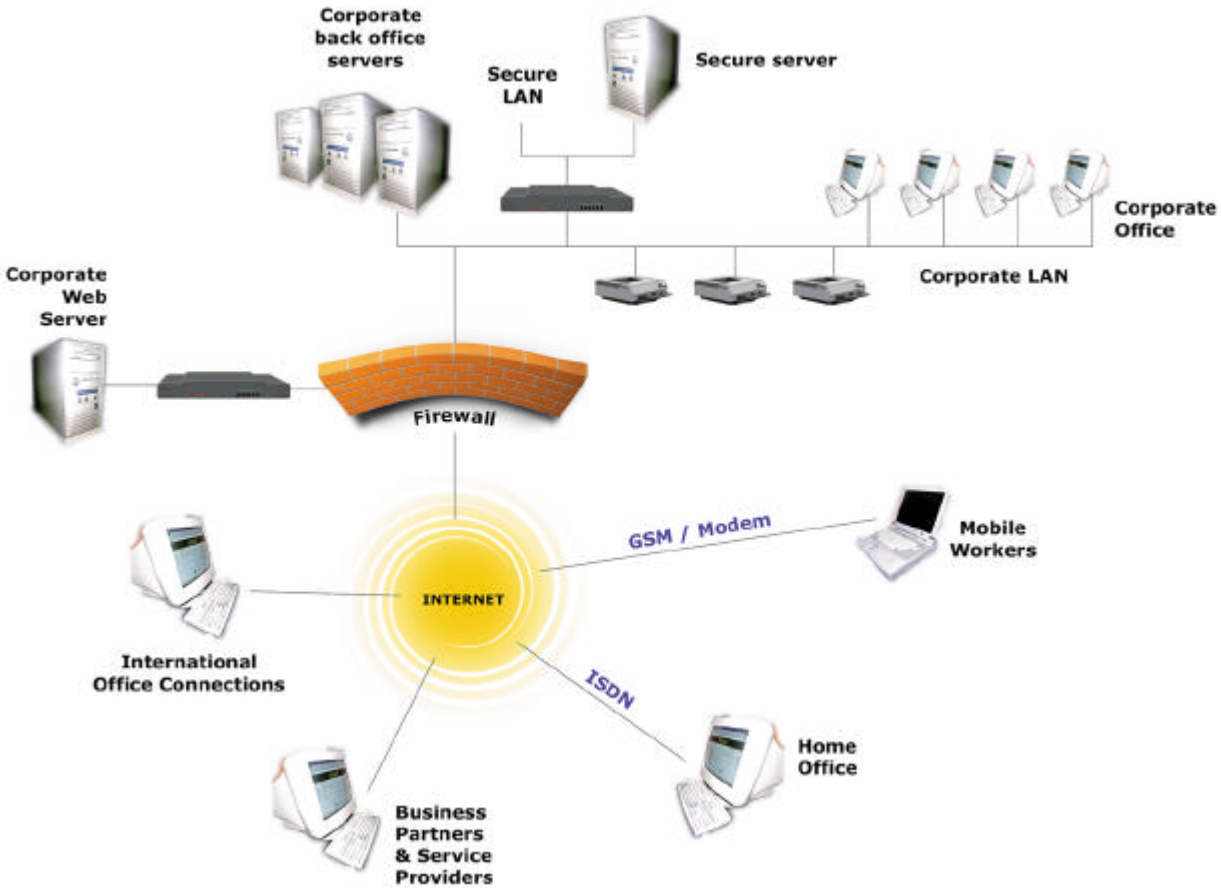

Figure 1. Typical e-business structure

A remote user, such as a business partner or employee, makes a remote connection to a Wide Area Network (WAN), using a web browser installed on a network enabled computer. The WAN is a telecommunications service that could be a private network, a 'Managed' network service or the Internet (as shown). A corporate connection links the WAN to the web server, enabling the remote user to access any software application installed on it.

The corporate web server is normally connected to the back office servers, which contain the more sensitive corporate information, through a firewall. However, if the web server itself contains sensitive information and is accessed only by trusted employees, it may be located inside the firewall.

If this infrastructure is exclusively for internal use, it is known as an 'Intranet' but, if it is extended to include external business partners, it is known as an 'Extranet'. Either way, it is based on web technologies and the Internet Protocol (IP), which routes traffic across the network, enabling the exchange of information between computers without prior set-up. The integrity of information and acknowledgement that it arrived is usually enabled by the Transmission Control Protocol (TCP). The two are referred to as TCP/IP.

What is holding e-business back?

The two main factors that are limiting an otherwise explosive growth in e-business are: limited bandwidth on the Internet; and concerns about security. The first issue is one that no single organisation can control and, although many telecommunications carriers and Internet Service Providers (ISPs) are adding huge amounts of bandwidth, the demand for it is rising dramatically. The decision that has to be made is whether or not the performance of the Internet is 'adequate' for the business need. If it is, the Internet is a convenient and 'free' resource (apart from access charges).

Alternatively, there are many types of Managed Network service, whereby a company leases a Virtual Private Network (VPN) on a wholly owned, private backbone. These are available from most telecommunications carriers and other commercial organisations. The cost is normally significant (although less than a private network of leased lines) but may be justified in terms of improved business performance. Whatever type of network is chosen, one of the most important factors is the availability of local Points of Presence (PoPs), wherever electronic business is likely to be carried out. This not only keeps access charges to a minimum, but improves ease and reliability of connection (availability).

The security issues are similar, irrespective of the type of network chosen, but the degree of risk is different. The Internet has to be considered 'inherently unsafe' and adequate protective measures taken. Fortunately, there are many solutions, which are explored later in this document.

What are the risks?

Business exposures and risk analysis

As with the implementation of any new IT system, a risk analysis should be conducted, as risks are present within each of the elements shown in Figure 1. However, it is impossible to assess risks if the resulting *business exposures* are not understood first. The most common of these are:

- *Information may be used for personal gain*
- *Information may be used for malicious purposes*
- *Information may be lost or modified*
- *Systems may not be accessible when required*
- *False information may be used for deception*
- *Denial of information transmitted may occur*

The risk analysis starts with the question: What would happen if any of the situations listed were to occur? Examples of the type of impact are: a new product launch strategy could be obtained and sold to a competitor; or funds diverted from the intended recipient to another account.

Unfortunately, a lot of security breaches are perpetrated by people with a grudge of some sort. These may be people who have been laid off from a company or overlooked for promotion (it is estimated that over 70% of attacks are internal). Even if there are no specific causes, some people feel they have to 'get their own back on the world' or show how 'clever' they are. This is a lot of the motivation behind virus authors and 'hackers'.

Perhaps the most difficult malicious attack to prevent is the 'denial of service' attack. This is where an organisation's web site is bombarded with requests for service, swamping the access points and preventing legitimate users from gaining access. In a recent occurrence, 50 computers, in different locations on the Internet, were simultaneously used to target the web site of a well known Internet Service Provider.

Having determined the impact of an exposure occurring, a cost can be estimated, not just in financial terms, but in loss of reputation and image, which gives an idea of the level of security required and contingency measures to be considered.

Categories of risk

Many different types of risk exist throughout the 'end-to-end' e-business structure, making them difficult to identify and eliminate, unless they can be grouped together and categorised. Fortunately, they fall into three main areas:

- *Unauthorised access to computer systems*
- *Loss or modification of data in transit*
- *Lack of 'trust' in a commercial relationship*

These are explored in more detail, in the following sections, along with some popular misconceptions.

Unauthorised access to computer systems

If an unauthorised user gains access to the corporate network, the systems themselves, or the information contained therein, can be used to benefit the user or to harm the organisation. Internal attacks tend to be for personal gain or malicious purposes, whereas external attacks may also include the 'denial of service' type, where a web server is disabled in some way.

WARNING!

Firewalls are not enough!

It is essential to fit a firewall between the corporate network and any external network, especially the Internet. However, firewalls can only deny access to data 'packets', dependent on network source / destination addresses and type. They do not:

- *authenticate individual users*
- *authorise system resources based on user profiles*
- *protect data in transit*
- *monitor content*

Remote access highlights these limitations, especially if an organisation provides access to employees, or contractors, as if they were in the office. This can be particularly dangerous, as access can be made from home, out of normal office hours, with no-one else looking at what is displayed on the screen. The most common risk is that the corporate facilities may be used to access 'unsuitable' web sites on the Internet, exposing the organisation to possible prosecution, adverse publicity and virus attack.

As firewalls have to be programmed to allow data from network source / destination addresses that are specifically permitted, it can be a difficult management task in the sort of environment shown in Figure 1. Firewalls can be relatively complex and have to be actively managed to be effective - they are not 'fit and forget' devices!

WARNING!

Static passwords are easily compromised!

Most organisations use a combination of User ID and static password to verify the identity of the user (authentication) and to enable access only to that which the user is permitted (authorisation). Whilst this may be considered adequate for some internal systems, it is a high risk for e-business. Single factor 'authentication (based only on what someone knows) is weak, especially as most people are careless with passwords. People frequently choose a password that can be easily guessed, write it down where it can be easily seen or share it with others.

Attempts at forcing users to change passwords frequently or to use a random sequence of characters can make matters worse, as they usually have to write the password down! In addition, a password can often be gained by so-called 'social engineering', where someone takes on a false identity (such as a bogus maintenance technician), pretends to have a legitimate request and asks the user to divulge it.

WARNING!

Security devices that transmit PINs can be 'sniffed'!

One of the ways in which companies can help prevent unauthorised access is to use a security device in combination with a password or Personal Identification Number (PIN). However, many of the leading devices on the market require the user to transmit the PIN 'in the clear' (i.e. not encrypted) leaving it susceptible to 'sniffing' by anyone with access to the network.

Loss or modification of data in transit

Sensitive data may be accessed more easily when it is in transit between systems, than when it is contained within a corporate system. Electronic eavesdropping can be accomplished in a variety of ways but is relatively easy on the Internet. Sending sensitive information or financial data across the Internet, if it is not encrypted, constitutes a particularly high risk. The risk is much lower across most public telecommunications systems or 'Managed' network services (such as Frame Relay or ATM), as both are owned and managed by reputable organisations, with known security standards.

'Data in transit' also applies to information stored on a laptop or handheld computer. In well publicised accounts, some of the battle plans for the Gulf War, and the entire personnel database of an international clothing company, have been made public through the loss and theft, respectively, of laptop computers. Organised theft of laptop computers, for the information they contain and not the hardware value, has significantly increased in recent years, particularly at airports. Even if the laptop does not change hands, it is amazing how much sensitive information can be read on other peoples' laptops in airport lounges and on the train!

Lack of 'trust' in a commercial relationship

Any electronic commerce that is set up without a contractual relationship between all the parties is a high risk. Such a contract should not only set out expected behaviour but, in the event of a problem, can be used to seek redress, either commercially or in the courts.

However, 'trust' is not just about personal or legal relationships. It is also about being confident that someone really is who they say they are, that the information they sent really came from them and, if they change their mind, they cannot deny sending it (non-repudiation).

WARNING!

authentication may not be sufficient for establishing trust

If users are properly authenticated, the organisation can be confident that they are who they say they are. However, authentication alone does not provide confidence about the content of transactions, such as a quantity of products ordered or the value of electronic payments.

In order to establish an adequate level of trust for commercial transactions, they should be verified by the inclusion of electronic signatures. These can be generated in several ways but rely on the use of encryption to calculate a numeric value that can only have been derived from the original transaction content.

How to secure e-business

The importance of a security culture

Security is not something that can be 'bolted on' to an IT system, but needs to form an integral part of the organisation's IT strategy. This is especially true in relation to e-business, which is reliant on adequate 'trust' between parties. It is also imperative that a security culture is implemented to prevent trust being compromised through lack of user awareness.

In the same way that individuals automatically lock all windows and doors before leaving their houses, protecting the organisation's business, including its reputation, has to become a habit with every employee and partner. This will only happen if there is strong, active support from the CEO / Managing Director and a continuous education process. A security policy, endorsed by the head of the organisation, and acceptance of it (in writing) in everyone's personnel file is a starting point. Constant reminders, through newsletters, promotion materials and, especially during the logging-on process, reinforce the need to maintain vigilance.

The security policy has to embrace all parties. The importance of legally binding contracts between business partners and between employees and employers cannot be over stressed. They should extend to 'standards of business conduct' for employees and cover the use of any electronic equipment, such as a laptop computer or hardware token, for company business.

Building a security architecture

There are many publications about building an enterprise security architecture but one of the most useful is the British Standards BS7799 document. This 'Code of Practice for Information Security Management' is founded in common sense and acts as a useful 'check-list' of points that need to be considered. For instance, in the section on remote users, it describes authentication requirements and how they can be met by a variety of means, including Challenge / Response systems.

The most important factors in building a security architecture are: classifying information and protecting it with appropriate security controls; providing resilience for critical components (including the security systems) and documenting the entire infrastructure, especially external network connections.

Conscious decisions can only be made about protecting data, if the sensitivity of information contained within the systems is established. Data segmentation is analogous to the layers of an onion, as shown in Figure 2. Not only should sensitive data be protected by additional layers of security but redundancy should be built in to mission-critical systems. The two most common exposures in the corporate network are unauthorised modems and unknown telecommunications links. However, it is not just physical connections that should be documented but configurations of networking components, such as routers and firewalls.

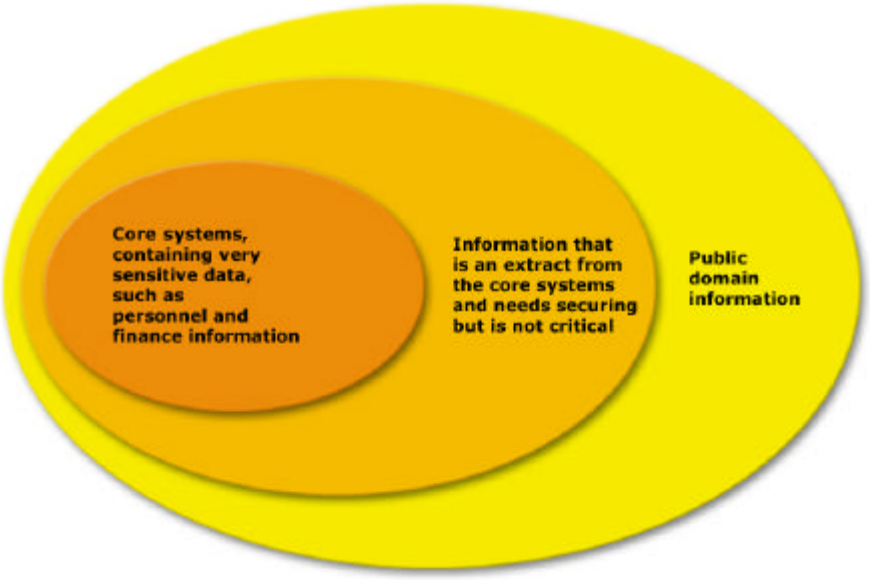

Figure 2. Layers of data classification

Where to locate information

Referring to Figure 1, the corporate web server usually contains information in the public domain but may also be required for secure partner access. The corporate back office servers are protected behind the firewall and may contain pricing and stock level information. The web server, if it is to be used for e-business, will need to frequently communicate with the back office servers, resulting in data being transmitted through the firewall. It is therefore essential that the right type of firewall is chosen or it may be possible for a 'hacker' to gain access to the back office servers, should the web server be compromised.

A typical firewall designed for e-business, is shown in Figure 3. This uses Network Address Translation (NAT) to ensure that the real network addresses of servers inside the firewall cannot be seen from the outside world. The web server can be located on the semi-secure 'partner LAN' whilst a 'De-Militarised Zone' (DMZ) enables the installation of traffic analysers, which can provide warning of attempted attacks.

Core systems, containing very sensitive information, should be contained in a 'secure server', and located on a separate LAN, as shown in Figure 1. Information on this server can be protected by additional user authentication and/or by encrypting files. In any case, the router that links the secure LAN to the corporate LAN should be programmed to block any data packets from the outside world, in case the firewall is breached.

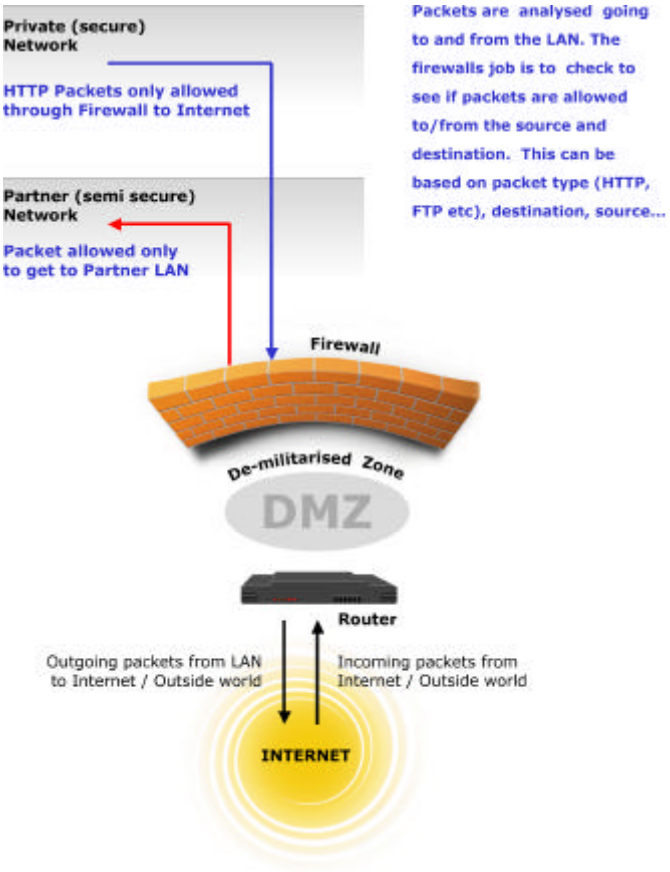

Figure 3. A firewall used for e-business

The importance of AAA

'AAA' is the acronym used to describe the process of: *Authenticating* users; *Authorising* resources to which they are permitted access; and *Accounting* for who had access to which resources and when. To ensure adequate security, all three functions must be carried out. Although these can be performed by separate systems, the co-ordination and administration is very difficult and they should, therefore, be accomplished by a single system.

Authentication – to confirm the identity of an unknown party, based on one or more of the following factors:

- *Something you know, e.g. a PIN number*
- *Something you have – a security device, e.g. a card or token*
- *Something you are, e.g. a fingerprint*

A single factor is weak authentication. A combination of two of these methods, however, increases the level of security achieved exponentially and is known as '2-factor' or 'strong' authentication.

Security devices vary enormously in cost, effectiveness and useful life and great care should be exercised in choosing which ones to use. For example, smart cards can be used for multiple purposes but require expensive card readers. Biometric devices, which measure a unique attribute of the body (such as the retina of the eye, fingerprint or voice pattern) are also expensive and as yet not sufficiently reliable.

It is imperative that deployment, ongoing management and support costs are considered in conjunction with the initial outlay. This is referred to as the Total Cost of Ownership and is particularly relevant to organisations which neither have nor wish to have, the relevant knowledge or resources.

Tokens, in combination with a PIN, are a relatively inexpensive and reliable method of 'strong authentication'. They come in hardware and software versions and require authentication software, resident on a corporate server.

Software tokens have to be loaded onto client machines and properly maintained. Should a laptop be stolen, the secret key can relatively easily be cracked. Hardware tokens must be designed to be 'tamper proof'. It should be noted that hardware tokens which use a 'challenge/response' protocol are more secure than those that are 'response' only. Finally, the cost of the authentication software, the features it provides and the type of machine on which it has to be run are significant factors that have to be evaluated carefully.

Authorisation – the process of allowing a specific user access to certain resources, based on a pre-determined set of rules called a user profile.

Traditional access control has been based on a simple 'access' or 'no access' approach to a particular IP address and port number of an internal server.

The problem with this approach for e-business is that a common resource, e.g. a customer database, may contain confidential information for multiple clients. The *authorisation* process, therefore, needs to be able to differentiate between users, so that they are only able to access their own specific information. The level of detail to which a user can be granted or denied access is a concept called *'granularity'*.

Accounting – the ability to keep complete records for each user, detailing connection times and resources used. These records are sometimes used to bill individual departments, based on usage, but the most important purpose is to be able to identify unusual patterns of access that may indicate a security breach.

Before purchasing a AAA system, the ease of management and clarity of reports should be evaluated. This is because the purchase cost of the system is usually small compared with the on-going management costs.

AAA standards

The integration of a AAA system will be much easier if it will interface to one of the common AAA standards. The two main ones in use today are RADIUS (Remote Authentication Dial-In User Services) from Livingston (now part of Lucent Technologies) and TACACS+ (Enhanced Terminal Access Controller Access Control System) from Cisco Systems.

One of the reasons why integration of authentication systems is important, is because most organisations have found that they can only keep track of changes to users and profiles if the records are centralised. It is quite common for an organisation to have a centralised RADIUS server (which may enable, for instance, Calling Line Identity authentication) linked to other authentication systems. With the advent of powerful directory services, such as Novell's NDS, X.500 or Microsoft's Active Directory, integration with these systems will become increasingly important.

Protecting data in transit

The risks of data being lost or modified whilst in transit have also been covered and that it is another area of security not solved by a firewall. A private or 'Managed' network service is normally considered sufficiently secure for most of the data that is transmitted over it, except for critical information. However, the Internet has to be considered totally insecure and even diary information can sometimes be useful to a competitor. For this reason, there are a large number of schemes for protecting data on the Internet, all based on cryptography.

One of the first schemes, and still in wide spread use today, is Secure Sockets Layer (SSL), developed by Netscape for secure credit card transactions. In fact, it has been adopted by the Internet Engineering Task Force (IETF) as the basis for its Transport Layer Security (TLS) standard. It is now universally available, having been included in Microsoft's Internet Explorer, as well as the Netscape browser. However, there are some organisations who feel that the 'US export' version, which limits the RSA key to 512 bits (rather than1024 bits) and has a maximum secret key length of 40 bits (rather than 128 bits), is not adequate.

Many organisations have chosen to purchase equipment that creates a Virtual Private Network (VPN) across the Internet, by creating encrypted 'tunnels' between remote locations. VPN servers may be based on another IETF standard, IPsec. However, they can also use much stronger encryption, including DES (Data Encryption Standard), a block cipher that uses a 56-bit key or triple-DES, which uses the encryption algorithm three times with three different keys. The downside of VPN equipment, however, is the reduction in throughput caused by the time taken to execute the encryption algorithm and the cost of management.

Information contained on laptop computers can also be protected by encryption. However, care must be taken by travelling personnel not to take encryption devices into countries where it is prohibited, unless previously authorised. Finally, other devices that should be considered when transmitting data electronically are:

- *Virus scanners*
- *E-mail content screeners*
- *Internet URL screeners*
- *Proxy servers for Internet access*

Public Key Infrastructures and digital certificates

A Public Key Infrastructure (PKI) is an encryption system that uses a public / private key pair. Its main advantage (over a private key crypto-system) is that the transmission of encrypted data can be carried out without having to transmit a secret key. A sender's public key (which enables the data to be decrypted by the receiver) is contained in a digital certificate, which is used to 'sign' the data. This is one of the 'enablers' of the SSL system but requires an independent Certificate Authority (CA) to vouch for the identity of a device or person, through the issuing of an X.509 certificate. It certifies that a public key was signed by a particular CA, sealed through the use of a digital signature. Digital certificates, therefore, give people, organisations and businesses on the Internet ways to verify each other's identity. There are four main types of certificate, which contain the appropriate public key and the following information:

- *Certification Authority (CA)* - either the name of the CA or the service being certified
- *SSL Server* - the names of the organisation and Internet host
- *SSL Client* – individual's name and other information such as e-mail and postal address
- *Software publisher* – used to sign distributed software

In addition to the *types* of certificates, there are four main *classes* of certificate, (classes 1 – 3 and 'secure server'). These have differing levels of validation and liability levels. A 'class 1' certificate merely assures that the user can receive e-mail at the given address and that no other certificate has been issued for that address. At the other end of the range, the CA validates the entity, using background checks and investigation services, before issuing a 'secure server' certificate.

There are now many CAs, whose certificates are built into Netscape and/or Internet Explorer. This is the reason why SSL is a universally recognised protocol for e-business. When a browser connects to a web server using the SSL protocol, the server sends the browser the public key in an X.509 certificate. This is used to authenticate the identity of the server and to distribute the server's key. Client certificates have a similar function to server certificates, but are linked to personal information.

SSL is used much more in the US than in the rest of the world, because the US domestic version has much stronger encryption. There are other PKI standards that have been developed specifically for e-business payments, such as the Secure Electronic Transaction (SET) protocol and CyberCash. Note that Kerberos, a network security system developed at MIT, is not a PKI.

Many organisations have investigated the possible deployment of a PKI and it may be appropriate for some businesses. However, there are very few organisations that have implemented one, due to the difficulties of groups sharing a digital ID and the complexity and costs associated with obtaining digital certificates and key management.

Digital signatures

Digital signatures, like digital certificates, can be used to verify the identity of an individual or organisation and also use a private/public key pair. They have another function, however, that of non-repudiation. A cryptographic 'receipt' can be created so that the author of a message cannot falsely deny sending it or, even more importantly, falsely claim that the content was different.

E-business is increasingly dependent on the use of digital signatures, which are, at last, being recognised by the legal profession. As an example, there is now a proposed *Electronic Communications Bill* before the UK Parliament, to give electronic signatures explicit legal recognition.

Digital signatures can be generated from a private key stored in many different types of devices. These include computer hard disks, removable magnetic media, smart cards or tokens. Whilst there are advantages and disadvantages of each, tokens have the following advantages:

- *Low cost*
- *Require no additional hardware*
- *Ease of use*
- *Ease of carrying*
- *Ease of deployment and support*
- *Robust*
- *Tamper proof*
- *Proven technology*

For the purposes of conducting business electronically, perhaps the greatest advantage of hardware tokens is that the same device can be used for user authentication and to generate digital signatures.

The introduction of Windows 2000

Microsoft's latest operating system, Windows 2000, is based on Windows NT but has many of the more user friendly advantages of the Windows 95/98 operating system. There are major improvements in terms of security features, which include:

- *Active Directory*
- *Encrypting File System*
- *Virtual Private Networking*
- *PKI and X.509 certificate support*
- *Kerberos support*
- *Single Sign-on.*

These should simplify the implementation of some of the required security controls and reduce the need for purchasing other equipment. However, there are some serious issues with migrating to Windows 2000. A senior Microsoft spokesman is quoted as saying that the only 'sure-fire' way to get good performance out of Windows 2000 is to buy it pre-installed on new hardware, rather than installing it on existing PCs. There is also no laptop version currently available. As a result, the consensus view from within the UK Back Office User Group is "caution!"

Evaluating

as an e-business security provider

How Identikey™ addresses a new market requirement

Identikey™ was originally developed to secure web pages using a single hardware token as the authentication device. The token selected for the task had already been in wide spread use in the banking market and contained unique features suitable for web based authentication. The original version of the product was released in October 1998 and immediately established itself as an innovative product, winning multiple awards for its leading edge design.

The emergence of the e-business market place saw Identikey™ selected as the authentication engine of choice by a number of leading organisations, because of its unique capabilities. The ability to easily combine user authentication into a web based program together with a digital signature capability for non-repudiation of electronic transactions, placed Identikey™ in a unique position with respect to the e-business market.

The R2 version of Identikey™ (released in January 2000) was designed to specifically address the following requirements:

- *Operating system independence*
- *Web server independence*
- *Mixed environment compatibility*
- *Complete remote management*
- *Ease of integration into external systems*
- *Open interface for extensibility*

What differentiates Identikey™ from other token based schemes?

The advantages of hardware token based user authentication schemes have been described in the previous section of this paper. However, some of the products on the market have been around for a long time, and were designed when the only requirement was to authenticate users to a corporate network, as if they were in the office. This has been shown to be extremely dangerous and entirely unsuitable for e-business. A product that *authorises* users to see only their own resources on a web site serving multiple customers, as well as *authenticating* them, is essential.

Because Identikey™ was designed specifically for e-business, it is the only product that provides all of the following essential requirements:

- *Full authentication, authorisation and accounting capability*
- *No client-side software required*
- *Challenge/Response protocol*
- *User selectable PIN which is not transmitted*
- *Generation of digital signatures*
- *Generation of one-time password*
- *Support for DES and triple-DES based tokens*
- *Seamless integration with IIS, Apache and Domino R5*
- *Replication across multiple servers for resilience*
- *Proxy to RADIUS server*

How does Identikey™ work?

This section describes how the Identikey™ software provides the authentication, authorisation and accounting functions.

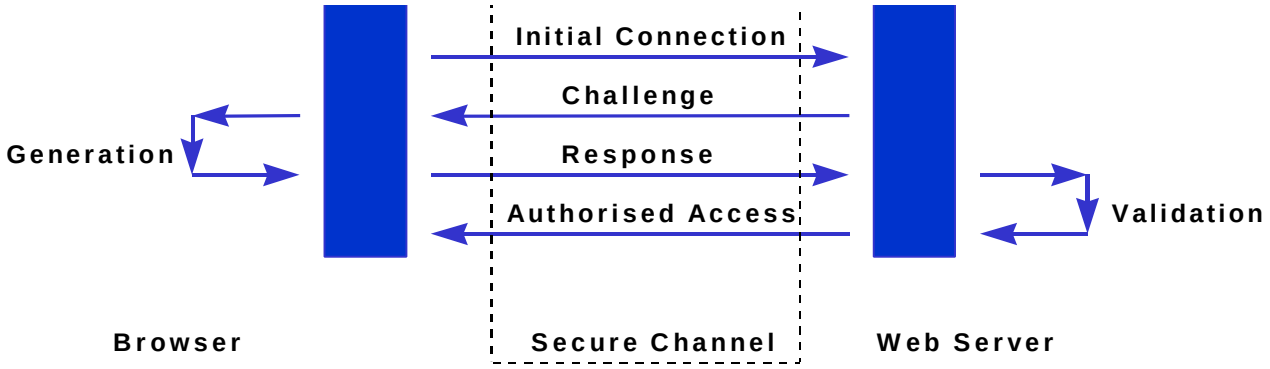

Figure 4. Authentication process

Authentication - the asynchronous authentication process between a client (token) and an Identikey™ authentication server is illustrated in Figure 4. The sequence is as follows:

1. The Identikey™ server generates a random and unique external challenge, which is displayed within a standard browser as a flashing pattern. It is used as one factor in the encryption process on both server and client sides of authentication.
2. The elapsed time (in seconds) from the seed date is calculated
3. Both server and client encrypt this random challenge together with the time variable, using the DES algorithm and the specific DES secret key assigned to that token. This key remains constant.
4. The encryption process yields a unique, one time password (OTP), in both the client and server. The server compares the passwords in order to confirm (authenticate) the identity of the user to the server.

Authorisation - uses three profiles stored in the Identikey™ database. The *site profile* memory map stores all configurations and site related details associated with a particular site on the Web Server. The site that the client is attempting to access is then checked to see if it is located in memory. The resources available to a user are assigned in the *resource pool profile* memory map, as the access indicator. After a user is authenticated to a site and the *user profile* has been loaded, a search is performed to see if the resource pool profile for that user exists in memory. The user profile memory map contains the records of the users that are authenticated for use on the web server.

In this way, the user profile is matched to the site and resource pool profile, so that the user can only access those resources to which he is expressly permitted. This enables an e-business web site to serve multiple customers or partners and allow them to see only their own information.

Accounting - the Identikey™ Manager keeps a record of who accessed which resource over what period of time, as well as providing the administration of the software. Installed as its own web site, the Identikey™ Manager provides a web service to administer the Identikey™ system. The web site may run on any IP address or port number and may therefore be protected by a firewall or be available for remote administration of the Identikey™ service anywhere in the world.

All administration actions are available via the Identikey™ Manager, including user, site and token management. There are two administration features that keep management overheads to a minimum. The first is that, because the PIN is user selectable and stored on the token, PINs do not have to be administered on the server. If a user enters an incorrect PIN three times, the token will lock. However, the token can be unlocked remotely, provided the authorised identity of the user can be established.

Identikey™ resilience

The Identikey™ software is built around a number of individual components that perform separate functions and combine to produce a robust, distributed authentication system. The three main components, the authentication engine, the database and the logger are designed to be replicated across multiple servers, providing built in redundancy. This enables the provision of a resilient user authentication system, in order to increase the availability of information to clients and business partners.

Identikey™ open authentication

The Identikey™ Authentication engine has been created to support any authentication device or methodology, hardware or software, which has the appropriate software libraries available. The Identikey™ database records what type of authentication method, or methods, each user has available. Any attempt to authenticate will cause the server to test the attempt against each registered method until a match is found. If no match is found then authentication will fail.

As new methods of authentication, either devices or software, are released, they can be incorporated within the capabilities of the Identikey™ server module. The open authentication capability allows an organisation to utilise populations of existing devices so that the full value of any existing investment is realised. Identikey™ currently supports the Vasco range of Digipass Tokens and has plans to incorporate support for hardware tokens from other leading manufacturers.

Identikey™ currently incorporates a RADIUS client, so that it can authenticate users and then confirm the authentication with the external RADIUS server or other user database. Identikey™ will be enhanced to include a fully functional RADIUS server. This will enable an organisation to use Identikey™ as a total authentication solution and drive existing legacy applications through their RADIUS connections.

The addition of the RADIUS server will allow Identikey™ to authenticate users via existing RADIUS enabled applications, such as modem pools, mainframe applications and Remote Access Servers. Identikey™ will be the single point of Authentication, easing administration and co-ordination of access control.

Identikey™ is currently adding strong authentication to a range of Operating Systems. The initial work has been undertaken to modify the standard Microsoft® MS-GINA to require Identikey™ authentication when logging onto the NT server.

With the Identikey™ authentication, and resulting audit trail, every access to the server can be monitored and traced. By removing the fixed password, greater confidence can be achieved in who is accessing the server. The use of Identikey™ eliminates the ability for a third party to access the server using a found or guessed password.

Identikey™ support for digital signatures

Identikey™ supports the banking industry's standard Message Authentication Code algorithm, ANSI X9.9. This algorithm has been in use for many years by banks, financial institutions and other organisations with a requirement for an effective, readily available signing solution.

The Identikey™ implementation of the ANSI X9.9 algorithm generates an electronic signature, based on a predetermined number of fixed length values (default is 3 values comprised of 5 digits). This can then be used to 'sign' a document or transaction, providing full non-repudiation.

The equivalent international standards for ANSI X9.9 are ISO 8730 and ISO 8731. The ISO standards differ slightly in that they do not limit themselves to DES to obtain the message authentication code, but allow the use of other message authentication codes and block ciphers.

Conclusion

Identikey™ is a new generation of e-business security product. It has been specifically designed to enable 'strong' authentication from any location, using a hardware token, without the need for client software. It is a true AAA product that allows multiple third parties to access only their own resources on a common web server. As such, it is suitable for a range of organisations and business applications, including:

- *Geographically dispersed organisations*
- *Travelling employees*
- *GroupWare*
- *Customised web sites for key clients*
- *Internet subscription services*
- *Strategic partnerships*
- *Internet banking*
- *Government On-line*

Head Office – Brisbane, Australia

Identikey Pty Ltd
Ground Floor
143 Coronation Drive
PO Box 1606
Milton QLD 4064

Phone : +61 7 3236 5050 (Australia: 1-800-INTERNET)
Fax : + 61 7 3236 5850

European Offices

Identikey Europe
Gebouw De Veldert
Gelderlandplein 75 L
1082 LV Amsterdam
Postbus 71082
1008 BB Amsterdam

Phone : +31 20 504 56 24

Identikey UK
ASMEC Centre
Eagle House
The Ring, Bracknell
Berkshire RG12 1HB
United Kingdom

Phone : +44 1344 382 062
Fax : +44 1344 303192