eBusiness and Security

a European perspective

White Paper Number: 01/99
Author: Bruno Beloff
Published: January 1999

Introduction

Security is indispensable to eBusiness. The use of the Internet for both the exchange of information across virtual enterprises and the execution of transactional operations - now widely referred to as eCommerce - requires a host of new security functions and services. These security functions must act as surrogates for the familiar procedures of finance, commerce, health care and other sectors.

Across almost every conceivable commercial, industrial and governmental sector, the potential advantages of eBusiness, and particularly e-commerce, are no longer in dispute. IT vendors have responded with products which address many of the technological issues, and have entered into a powerful learning cycle with customers. The resulting products offer the strengths of the best conventional IT environments, but with the promise of extended reach.

Throughout this process, the development and uptake of security systems has frequently been limited by misunderstanding and suspicion, both amongst customers and their national governments. The phenomenon is recognisable in North America, but has been much more evident in Europe. This is unfortunate not least because, in almost all other respects, the European experience is the same as that of the rest of the developed world. Given that eBusiness opens a global market, that similarity should not be surprising.

There are reasons why an understanding of security systems have lagged behind that of other core functions, and reasons why this is now changing. Consider the definition of security according to the Oxford English Dictionary:

> **Security... 1.** The condition of being protected from or not exposed to danger; safety. **2.** Freedom from doubt. **3.** Freedom from care, anxiety or apprehension; a feeling of safety.

This is a solid foundation. It is so important, that it is worth taking apart a counter definition, in this case from the writer and philosopher Germaine Greer: “Security is when everything is settled, when nothing can happen to you; security is the denial of life.” Therein lies an important confusion: security systems act in order to disable certain operations, yet their function is to enable a heap of others.

Security is an enabler - eBusiness cannot develop without it. However, security systems raise issues which are quite different from other aspects of application development and management. Added to this, the function and behaviour of Internet-based security systems is different from those in either the glass house or the desktop. Only a few technology vendors are in a position to properly address these issues. In Europe, those issues are trans-national; the only suitable vendors are necessarily trans-national too. Amongst them, IBM is in a privileged position. This report examines matters which are both universal and specific to Europe, and outlines IBM’s response.

Background

The rise of the Internet has allowed businesses to extend the range of interactions available to new classes of customers, to business partners, and employees. A technical infrastructure can now be put in place to allow this to happen - based on databases, application servers, and distributed applications - all acting over common protocols. For the most part, the technologies required to make this happen are extensions of existing technologies. Thus, although application servers represent a relatively new technology, the concept predates the Internet.

In contrast, many of the required security functions are a product of Internet experience. The purpose of these functions has itself changed: in a host-terminal or protected local area network environment, the chief security function is access restriction. Unfortunately, access restriction is something of an anathema to Internet activities. Although access remains an issue, eBusiness focusses on four aspects of security, otherwise known as the PAIN conditions:

- **Privacy** - The network and its contents must be resistant to eavesdropping and intrusion.
- **Authentication** - There must be a way to confirm the identity of the individual with whom one is conducting business.
- **Integrity** - The content or data must be resistant to tampering and unauthorised access. Alternatively, any tampering must be immediately identifiable.
- **Non-Repudiation** - Transactions, once concluded, must be binding; neither party involved can unilaterally disavow the transaction.

The value of eBusiness is such that it is often no longer practical to build applications which are not Internet-ready, even if their initial use is wholly within an organisation's protected network. Thus, the issues surrounding eBusiness security may actually apply to all application development. It should also be remembered that organisations are most vulnerable to attack from within: estimates suggest that between 60 and 80 percent of all attacks on IT systems originate from within the organisation. Added to this, the problems of securing a corporate network are not so different from those of an extended network.

Security Infrastructure

The state of eBusiness security across the European Union differs from the rest of the world primarily in its experience of legislation. In general, variation in law across Europe impacts on such things as accounting procedures, business practices, currency and - decreasingly - customs regulations. Viewed from an IT perspective, Europe looks like a region undergoing political transition: companies and regulatory bodies frequently act across national boundaries, and are subject to both local and Union-wide legislation.

All of these phenomena impact on the way in which IT systems of European trans-nationals are constructed. Security is a special case, though, because here the law is specifically directed at IT products. This is also true in North America, but in the European Union each member state has historically taken its own approach.

Neither the US Federal Government nor the European Union has yet been able to resolve some of the outstanding issues. In the mean time, there is clear evidence that Europe is catching up in its ability to deploy effective eBusiness security systems is a consistent way. The ways in which this is happening must be reflected in the architecture of eBusiness solutions in general, and the design of their security infrastructures in particular.

Cryptography and Law

It is unusual to turn to legislation in order to evaluate a general-purpose IT solution, but these are unusual circumstances. For some time, a raft of laws in Europe have governed the movement, deployment and use of cryptographic systems, for similar reasons as have been put forward in North America. The difference is that local variation in Europe has actually thwarted past efforts in deploying actual systems.

One example illustrates the scale of the problem: in April 1996, the European Information Exchange Service for the Communication between Harbour Areas (EIES) publicly reported on its attempts to build a secure, trans-national extranet. It concluded that:

> ... any EIES service offering encryption must assure that any email traffic from and to partners in France is not encrypted, unless in the rare case that an encryption permission exists. In Germany the use of cryptography is legal, but some politicians are talking about new laws to change this to a situation similar to France. This obviously opens some security holes in EIES. On the other hand it is pretty obvious that confidential data, may it be between police authorities or business partners should not be sent through the Internet without some sort of protection. The only way out, apart from cryptography, would be to build up a closed Corporate Network... for this part of the EIES service.

As in the US, governments had turned their attention to the encryption systems at the foundation of a Public Key Infrastructure (PKI). The PKI, in turn, serves to provide the PAIN criteria. In other words,

governments focussed on the privacy of communications and, as a result, the ability for users to gain authentication, integrity and non-repudiation was curtailed.

The legal situation across Europe has now changed, and is continuing to evolve. In particular, the application of encryption is now more-or-less unrestricted. However, questions remain over the import and export of software which supports strong encryption. During 1998, US Federal law was revised, allowing the controlled export of strong encryption systems to customers in specific countries and specific commercial sectors. This solved the problem for some customers and vendors. Others have taken a more pragmatic approach.

The Wassenaar Arrangement

The Wassenaar Arrangement was formed in 1995 and now has thirty three members again including the main European nations, the United Kingdom, the United States, Canada, Australia, New Zealand, the Russian Federation and the Slovak Republic. Although it represents a marked shift towards European consistency, there is still room for European confusion here.

The Arrangement controls the export of weapons and of dual use goods - goods that can be used for both military and for a civil purpose. Cryptography falls into this category. Its General Software Note excepted mass market and public domain cryptographic software from the controls. Some countries, notably Australia, France, New Zealand, Russia and the US deviate from General Software Note, and continue to control the export of mass market and public domain cryptographic software. (However, export via the Internet does not seem to be covered by the regulations.) There is a personal use exemption which allows export of products accompanying their user for the user's personal use, for example on a laptop.

The Wassenaar Arrangement was revised in the meeting in Vienna in December 1998, and this resulted in restrictions on the General Software Note. These changes effectively amount to a further restriction, as the Wassenaar Arrangement has now been extended to include mass market encryption tools using keys greater than 64 bits. However, the Wassenaar provisions are not directly applicable - each member state has to implement them in national legislation for them to have effect.

The movement - as opposed to the application - of cryptographic systems is not relevant to all users, but does impact on organisations attempting to build trans-national extranets. In general, any restrictions on the uptake of strong cryptographic systems have a restraining influence on the development and growth of eBusiness.

The Future in the European Union

In 1997, the European Commission presented a Communication "Ensuring Security and Trust in Electronic Communication - Towards a European framework for Digital Signatures and Encryption", underlining the need for a coherent approach in this field. The Communication identified the lack of security on electronic networks as being one of the major bottlenecks impeding the rapid development of electronic commerce.

In May 1998, the Commission adopted a proposal for the European Parliament on electronic signatures: "A Common Framework for Electronic Signatures." This stresses the economic importance of cryptography, and the Commission does seem to be concerned that restrictions on encryption affect a right to privacy, its effective exercise and the harmonisation of data protection laws in the internal market.

By way of compromise, European Ministers of Justice and Home Affairs apparently agreed at a meeting in January 1998 that law enforcement agencies must have access to keys and plain text, and a policy paper was prepared stating that it may be necessary for law enforcement to have access in certain circumstances, which may be either overt (explicitly demanding decryption) or covert (probably through key recovery).

Solutions

Just prior to the 1998 US Federal decision to relax the export restrictions on 56-bit public key encryption, it became clear that 56-bit encryption is not all that much more secure than its 40-bit alternative. In July, San Francisco's Electronic Frontier Foundation (EFF) cracked a Data Encryption Standard (DES) encrypted message in 56 hours using purpose-built hardware. It was no great trick, either. The EFF undertook the task more as proof of concept than because the project held any particular technical challenge. The American government is now working on replacing DES with an Advanced Encryption Standard (AES), for its own use.

The US Government's position on exporting encryption has provided a small windfall for software vendors based outside the US. This situation helps American vendors indirectly: the availability of strong encryption technology outside of North America will have a positive impact on the uptake of eBusiness solutions overall. In any case, regulations covering cryptography will be simplified and liberalised over time.

In the meantime, selling strong encryption systems anywhere still remains a slightly awkward process. Thus, Europe's legal position has generated a new type of software industry, in which local developers replicate encryption functionality in order to circumvent import or export restrictions. In order to gain credibility and access to markets, the process favours alliances with the established vendors. One such initiative has seen an acquisition of the Swiss-based R3 Security Engineering by Network Associates, giving Network Associates access to development labs in both Switzerland and Germany.

Projects such as these may eventually be recognised as within both American and European law. In the mean time locally-available strong encryption systems might seem to give the vendor a strategic competitive advantage. However, a security infrastructure must be approached as a whole in order to be effective.

For the customer, the ability to select a specific low-level service component such as an encryption algorithm is useful. But as we shall see, the co-ordination and integration of all security functions remains the decisive factor. That factor does not favour the part-solution vendors.

Elements of a Secure Platform

The secure platform must uphold the PAIN criteria in a manner which is both consistent and complete. Where this is achieved, the security of the overall system should be invisible to applications and users who are acting properly, and be invincible to attack.

Achieving this is not a trivial exercise. Consistency and completeness are both challenged by the heterogeneity of IT system in question. Particularly in an eBusiness environment, there may be many operating systems, databases, and application types employed. Added to this, the security infrastructure must not damage the performance of the system. This last issue is of major concern because the Public Key Infrastructure in particular generates a very high volume of directory activity. The PKI, however, is only one of five major components of the secure platform.

The Public Key Infrastructure (PKI)

The PKI includes all the services that enable the use of public key cryptography and certificates in a distributed computing system. PKI services allow organisations to establish security domains in which they issue keys and certificates. Within these domains, the PKI enables the use of both encryption keys and certificates. PKI products also allow organisations to establish trusted relationships with other security domains, either in a certification hierarchy or through direct cross-certification. Services enabled by the PKI include:

- **Key management** - This includes key update, recovery and escrow (for key recovery).
- **Certificate management** - Including generation and revocation of keys.

Certificates augment public-key cryptography by providing the means to validate the public key. As defined by the x.509 standard, a certificate binds a public key to the identity or another attribute of its the entity which it identifies. These entities can be people or application code.

The certificate can also contain policy information, such as the authorised uses of the key. A Certificate Authority (CA) creates and signs the certificate with its own private signature key, vouching for the authenticity of the key and the identity of its owner.

PKI services are becoming important tools for authorisation in a variety of applications and protocols. These include Secure Sockets layer (SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Electronic Transactions (SET), and code-signing services for both Java and ActiveX components. However, PKI will not displace Kerberos and other access control systems for bounded networks. Kerberos will most likely remain as the primary authentication and security system for the Distributed Computing Environment (DCE) and Windows NT, and will work alongside the PKI.

Some protocol is required to allow open access to public keys and certificates within the security domain. One convention stands out as the most effective in this situation: the Lightweight Directory

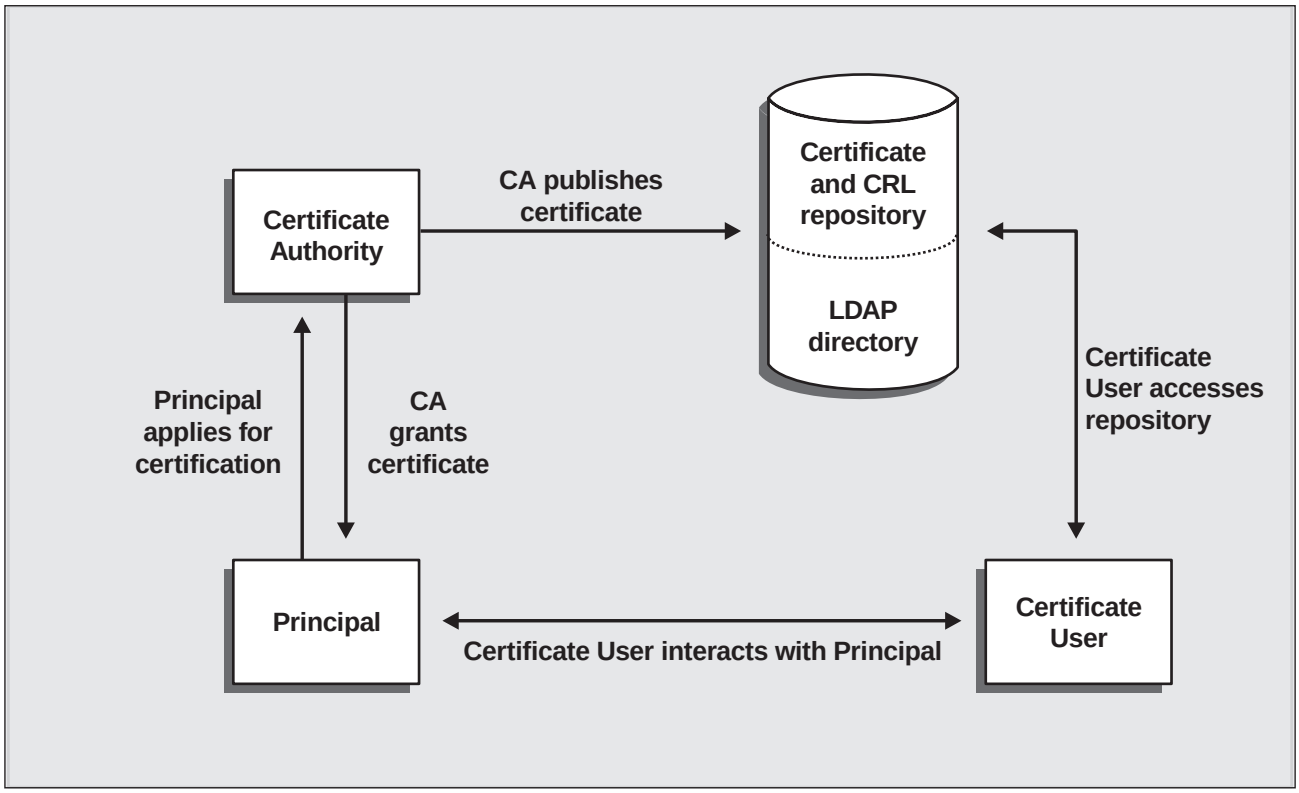

Fig. 1: PKI Certificate Operations

Access Protocol (LDAP). LDAP represents an established, general-purpose Internet Engineering Task Force (IETF) standard. Network systems have historically generated large numbers of incompatible directories for email, system management and application component interaction. In many situations, those incompatibilities have proved cumbersome and awkward. For the security platform, incompatibilities of this type would be disastrous, given the range of applications and resources which require access. To-date, not all security vendors have learned this lesson.

Aside from the access protocol, the PKI's Certificate and Certificate Revocation List (CRL) must be supported by a highly scalable database. All interactions between certificate users and principals (the entities identified by the certificate) must commence with a query to the certificate repository, in order to ascertain whether the certificate is valid.

Access to public keys is required on a similar basis to certificates: the certificate is used to authenticate the key, then the public part of the Principal's public-private key pair is used to authenticate incoming messages and encrypt outgoing messages. Certificates are normally updated only when the status of a principal changes, for example when an employee leaves the organisation. However keys - and their certificates - may be updated more rapidly: on a regular, staggered basis in order to maintain security, or when a private key is believed to be compromised.

Private keys may also be subject to an escrow regime. In this case, a Message Recovery Key is held by a central authority, and this key, like the private key, can be used to decrypt or impersonate the principal. Key escrow is controversial for both technical and political reasons. Technically, it represents a potential weak link in the security regime; certainly, the MRK repository must be established, populated and managed with extreme care.

Politically - more in the United States of America than in Europe - key escrow has become associated with civil liberties issues, as governments equivocate over the issue of legally enforced access to MRKs. In practice, an escrow regime provides a useful failsafe mechanism in the case of lost private keys. Most PKI vendors offer the option of corporate escrow, which can be implemented at the customer's discretion.

Cryptography Control

Cryptography control implements the administration functions applicable to the PKI - it provides a framework for key management, certificate management, policy management and repository access. Functions in this area include:

- **Automated certificate validity checks** - It should be possible to check automatically that a user's certificate has not been modified since it was issued.

- **Revocation of user certificates** - It should always be impossible to encrypt or sign messages using revoked keys.

- **Automatic CRL checks** - The CRL should always be checked automatically to ensure certificates being used have not been revoked.

- **Automatic key update** - Users are issued new keys automatically prior to the expiry of existing keys, allowing an uninterrupted security service.

- **Management of key histories** - In many cases, an encrypted document will persist longer than the currency of the key which was used to encrypt it. In such a case, the cryptography control service should select automatically the appropriate decryption key to decipher the document.

A range of cryptography policy issues are to be included here too. Chief amongst the operational issues is the control of who is issued a certificate, how long it will be valid for, and for what purposes the certificate may be used.

Firewalls

Firewalls provide "perimeter protection" for Local Area Networks and Intranets. Firewall systems provide access control by monitoring and filtering the traffic of data at the boundaries between different zones of a network. In doing so, they are able to guard against unwanted accesses and to provide an audit of network traffic.

Firewall products vary in the techniques used to filter data traffic and in the sophistication of attack which they are able to identify. A packet filter firewall has the same system architecture as a conventional router, and, like a conventional router, acts on information only at the network level. A firewall of this type therefore introduces minimal latency to network traffic, and most of it can be implemented in hardware. Unfortunately, not all types of unwanted access can be identified by examining packets and hardware-level network connections. The solution to this is to use an application-level firewall, which carries out a stateful monitor and control regime over the a specific application traffic. The most sophisticated firewall solutions provide for both forms of control.

Achieving both invisibility and invincibility (within its area of responsibility) in a firewall is a complex and ongoing task. Some tradeoff may have to be made in specificity of control, swapping the freedom for legitimate users' data to cross the firewall, and vulnerability to attack. Since the tradeoff will continually alter, the firewall must be securely accessible to a central administrator.

Virus Protection

Virus protection represents the penultimate level of security protection for a networked system. For a foreign virus to become the subject of a virus protection system, it would have to have defeated the firewall, the PKI's application validity check, and the data validity check of the cryptography control. Only the resource's access control follows this, and the virus's activity may be intercepted here too. In practice, many viruses are imported into the organisation via digital media such as CDs, and have not uncommonly been found on media from reputable software publishers. Virus protection is therefore a crucial part of an end-to-end security regime.

Like the firewall, the virus protection system must be amended rapidly as circumstances require. The solution here is the same: distributed anti-virus software should be under the control of a secure central administrator.

Access Control

Only fully identified and authenticated clients should be able to access enterprise networks, systems, and applications. Access control lists and data protection methods, such as encryption, maintain confidentiality and protect information technology.

In many important respects, access control issues remain unchanged in the transit from the conventional computing environment to eBusiness: a user-oriented or resource-oriented scheme is required, and this acts under the control of a policy management directive. For an eBusiness system, access to resources such as databases would normally be granted to resources such as middle-tier application components.

Methodology

Methodology in this case refers to the way in which resources are specified and implemented. The experience of security systems shows us that methodology is crucial to the effective deployment and

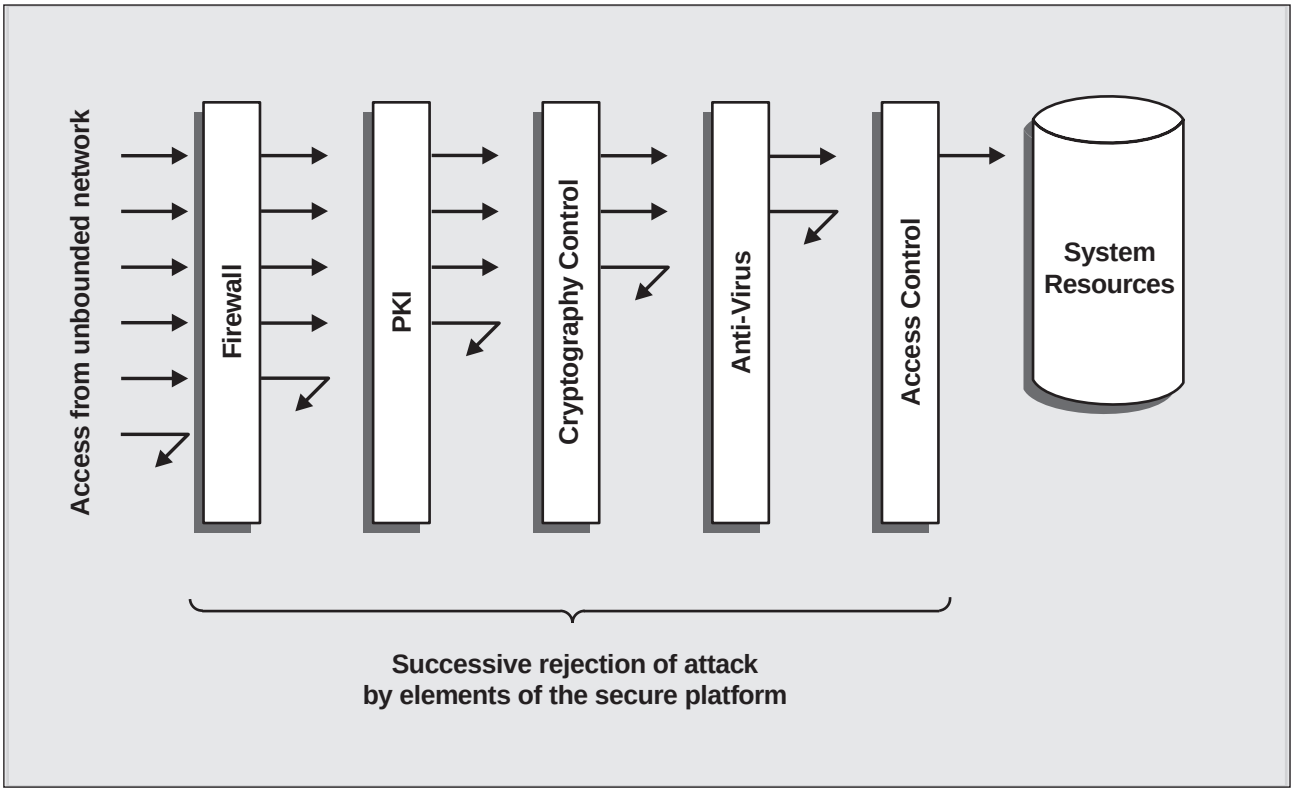

Fig. 2: The Secure Platform

use of the security platform - no amount of strong encryption algorithms or sophisticated virus detection techniques can overcome weak systems design.

A simple comparison between a security and an application system illustrates this: poor applications development methodologies tend to cause relatively linear degradation in applications performance; poor security methodologies tend to defeat the entire security system. Against this stark warning, current industry experience tells of complexity arising from migration to PKI, the absence of consistent policy implementation tools, and multi-vendor systems incompatibilities. As a result, limitation of eBusiness development is taking place for purely technical reasons.

Whilst not the only vendor of an integrated PKI system, IBM stands out in addressing the problems and complexities associated with implementing an effective security methodology. The company's response is in the form of the IBM SecureWay FirstSecure solution. The Foundation gathers together five groups of related resources. A clear, open and secure relationship exists between these groups with, in time, each group presented as a product. These groups cover:

- **Intrusion Immunity** - Functions include network intrusion detection, system intrusion detection, vulnerability checking, anti-virus and attack containment.

- **Secure Business Server** - Components and functions include firewall, network service access control, Web single sign-on, support for virtual private networks, client file encryption, Smart Card access to IBM Hosts, and a Secure Java Virtual Machine.

- **Public Key Infrastructure** - This includes the IBM Vault Registry, with PKI support.

- **Tools and Libraries** - These include APIs for building and deploying secure applications and managing the security environment. Reusable security objects will be provided for IDE environments such as VisualAge.

- **Security Policy Director** - This provides a centralised Policy Director supporting adaptive intrusion response, audit control, fine-grained access control for all components of the security platform.

The Security Foundation components are able to provide a consistent view of the complete security environment across multiple operating systems. It therefore provides an expressive environment through which a security methodology may be followed.

Implementation

Prior to its recent security initiatives, IBM had already assembled most of the components of its Security Foundation: its eNetwork Software security and directory integration products provided security directory functions; IBM Global Sign-On and Security Dynamics SecurID enhanced logon capabilities; IBM LDAP Directory, Tivoli, and IBM DCE enabled policy administration; and IBM DCE, VPN, and SSL capabilities allowed the secure communication required in bounded networks. IBM eNetwork Firewall, AntiVirus, Content Technologies MlMEsweeper, and Network Security Auditor provided availability for unbounded networks.

The integrated security offerings form one part of the newly-completed eBusiness Application Framework. The Framework now has three components:

- **Development and Integration Tools** - This component incorporates the VisualAge IDE, SanFrancisco Application Components, TeamConnection design repository, and other products.

- **Application Server Software** - The key part of this component is the WebSphere family, incorporating the MQSeries and TXSeries middleware families.

- **Security and Management** - Here is the Security Foundation at last, presented as IBM SecureWay FirstSecure, and followed by a family of security platform components.

IBM's value proposition for the security and management framework component is similar to that for its middleware components. It's a business proposition, about securely connecting islands of computing - both within and outside the organisation. The architecture of the product also carries forward established IBM ideas about what should be open, and where the value-add in the technology lies.

Security Architecture

IBM KeyWorks is at the heart of the security architecture. KeyWorks has two important features: it provides a Common Security Framework API set; this brings the IBM security framework functionality within the range of its middleware platforms. Secondly, it provides a set of management services which, from the developer's point of view, are insulated from underlying services.

Service interfaces are provided to maximise the choice of possible providers, with only the Key Recovery Services Provided exclusively by IBM. However, the company points out that any chosen service must be authenticated to the framework via an authentication procedure performed by IBM.

Delivery: SecureWay

The SecureWay products are comprised of three integrated security solution modules. Together, these provide a comprehensive security framework, built on current technologies, and with interoperable components. The three-way breakdown is a tactical manoeuvre, intended to allow the earliest possible delivery of the core security functionality.

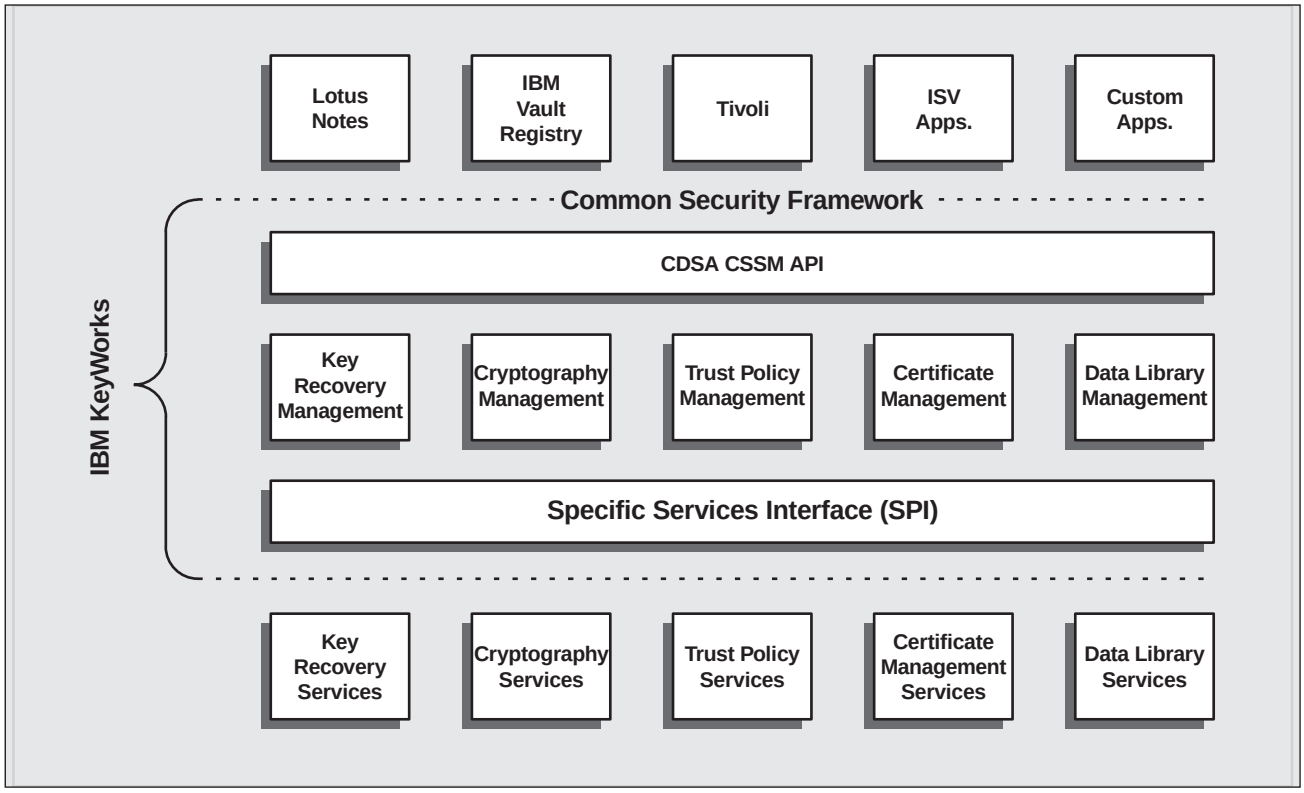

Fig. 3: Open Interfaces for Services & Applications

- The first module - FirstSecure - provides the core components of the security Foundation.
- The second module is the availability offering, integrated with the Tivoli system management products. This extends the foundation by addressing areas where denial of service and continuity of service are critical, such as recovery and continuous operations.
- The third component is the administration offering, again integrated with the Tivoli system management products. It provides mechanisms to manage a security environment, such as controlling access by principals.

FirstSecure

FirstSecure provides virus protection, access control, traffic content control, intrusion detection, encryption, toolkits and access control implementation services. These functions will be delivered by IBM's existing family of security products: IBM firewall, Directory, Vault Registry, VPN, and OEM products.

Release 1 of SecureWay is presented as providing entry-level security for eBusiness, giving non-intrusive security for existing applications.

Release 2 - currently scheduled for Quarter 4 in 1999 provides the first unified, policy-based security environment. Its planned features include:

- **End-to-end security** - for Internet access to legacy applications.
- **Extended Foundation** - integrating network access control with firewall function.
- **PKI** - for extended support of public key infrastructure.
- **Intrusion detection** - Initial enterprise-wide intrusion detection and response capability

Release 2 of SecureWay therefore delivers on more-or-less the complete Security Foundation blueprint, focussed on integration around policy-based services.

Administration and Availability

The administration component of the security platform is addressed by integration of SecureWay and Tivoli products, including Tivoli User Administration and Tivoli Security Management. Tivoli has made significant steps in recent times to new customers, outside of its traditional large business customer space. The value of those steps will now be amplified, once SecureWay introduces new users to its products.

Tivoli availability products will also be employed in the forthcoming SecureWay modules; these in the form of ADSM Servers and ADSM Clients. In addition, Administration and Availability modules will introduce the Security Foundation's Policy Director.

Conclusions

In recent times security for eBusiness has been significantly suppressed in Europe. This has not been because of any one set of laws, regulations or practices. Instead, a host of factors have converged and acted against constructive growth. But there are plenty of statistics which reinforce the view that there is a groundswell of demand for solutions. The following relate to the UK, and are indicative of the European situation.

A 1997 British Telecom survey of 200 UK companies with turnover in excess of £100 million, shows that 85% had Net access; about 43% of those for less than a year. The survey indicated that 92% expected to be online by the end of 1997.

BT sponsored another survey, this time of 300 UK small and medium sized enterprises, again during 1997. Some 39% of those surveyed were already connected to the Net and another 20% intended to go online by August 1998. The report states that most of these enterprises realise the importance of the Net to the future of their businesses. Importantly, the survey noted that:

"The longer [the enterprises] use the Internet, the more important the Internet becomes to their business. Companies that have been using e-mail for over two months are three times as likely to regard e-mail as crucial to their business."

Add to that, estimates of anywhere from 50 million to 91 million Internet users world-wide - of which about 20 million are in Europe and some six million in the UK - and it is easy see not only the scope of the potential growth of businesses coming on to the Net, but also the enormity of the potential risks they face.

United States companies' response to the combined threat-and-opportunity most likely reflects a European position in the near future. According to a 1998 Zona Research study:

1. Spending on firewalls will continue. The report shows that, although 80% of respondents report firewalls installed, a third plan to buy more in 1998.

2. On encryption, the report finds that deployment is on the rise, with 58% of respondents already using encryption in a variety of ways, and 43% planning to buy encryption products that year.

3. Recognising the fact that firewalls alone are not enough, more than 30% or respondents plan to buy intrusion detection systems this year.

4. Most importantly, 35% of respondents are already actively engaged in electronic commerce. Yet 30% of the respondents are unsatisfied with electronic commerce security, fewer than 20% are satisfied and a staggering 50% are undecided on the subject.

Many European customers are therefore in the fortunate position of being able to learn from others' mistakes, effectively leapfrogging over early, over-complex, cumbersome and vulnerable solutions.

Not that all of the European issues can depart at a stroke. Pan-European IT systems are inherently more heterogeneous than their equivalents in North America. More than in any other branch of IT, a security foundation is required to address that heterogeneity and present a consistent view to developers and administrators.

In common with IT functions such as application development and administration, security products add value by embodying knowledge of their domain. With SecureWay, IBM have shown that this is achievable in the security domain, both in core services, and in support of the methodologies required to make these services effective.

Bloor Research is Europe's leading IT research and publishing organisation. Research is available on many subjects such as Data Warehousing, RAD, 4GLs, Development Tools, Client / Server, CASE, Software Testing, Databases, Object Databases, Parallel Databases, Networking, Computer Hardware, IT and IS Strategy, Desktop Strategy, Rightsizing and Object Orientation.

Bloor Research
Challenge House, Sherwood Drive, Bletchley,
Milton Keynes, MK3 6DP,
United Kingdom
Telephone: +44 (0) 1908 373311
Facsimile: +44 (0) 1908 377470
E-mail: mail@bloor-research.com

Web Site: www.bloor-research.com