

End-to-End Encryption: In Search of the Holy Grail

By Dr. Nicko van Someren
nicko@ncipher.com

In this article we will look at how encryption can be used not simply to protect data in transit over the Internet but at all stages of a business process and whether end-to-end security is a reality.

Cryptography, once the domain of spies and the military, has now become part of our everyday lives for securing e-commerce transactions, e-mail communications and protecting sensitive data such as personal financial and healthcare records. With these changes comes the growth in volume and sophistication of internal and external threats that are making information security an increasingly critical issue. Yet most companies still focus their security measures on data in transit—particularly over the Internet—while paying far less attention to what happens to it when it arrives at its destination or is stored in a database. The risks to the data on arrival are often far greater; after all, why crack individual credit card transactions when entire repositories of private information stored in a database may be open for attack? If sensitive data that is protected by encryption—such as passwords and PINs—are ‘unwrapped’ and left unprotected whenever they are used around the business, there might be many other points of weakness just waiting to be exploited.

In the ideal world, data would remain protected in a secure environment at all stages of a process—complete end-to-end encryption. But is this possible or practical?

The high degree of interconnection within business networks challenges today's traditional perimeter approach to security—hard on the outside but soft on the inside. Everyone accepts that it's a dangerous world outside, and protection in the form of SSL and IPSEC is routinely applied to external connections to prevent eavesdropping. However, when considering internal security, many organizations have been quite happy to hide behind the firewall.

Even though most reports show the majority of attacks come from insiders (InterGov <http://www.intergov.org/> put the rate as high as 80%), companies typically rely on perimeter access controls to provide internal security. This ‘all or nothing’ approach does little to prevent legitimate users from doing illegitimate things. It's easy to see why; the internal networks and the processes they support are far more complex than the relatively constrained exchanges that exist over external networks. As documents and messages hop from place to place they are ever more widely shared, modified, archived, and generally left lying around. Of course, these problems are not new; what's new is that your stewardship of these records, whether for reasons of privacy or commercial confidence, is increasingly likely to be audited under threat of penalty.

Often in the current model IT security professionals are continuously locked in a cycle of catch-up—viruses can be zapped, passwords can be strengthened and intruders can be detected, but they are inevitably reacting to limit the spread of new breaches rather than preventing them in the

first place. Unfortunately in an ever more highly connected environment there is increasingly too much to watch and too little time to react. Attention, therefore, must shift from just protecting systems and networks to protecting what really matters—the data itself. It's the same reason that we all instinctively put letters in envelopes. If you don't trust the network or the processes that take place within it, you simply have to seal the message. In the context of the enterprise this means routine encryption—anything you care about, wherever it is, should be encrypted.

This alternative approach to the current ‘armadillo’ model—hard on the outside but soft in the middle—is to recognize the fact that even on the corporate network there may be internal threats. In this case we should protect individual ‘islands,’ defending their shores and controlling all the traffic that crosses in or out. This is a big shift in thinking, documents and messages must default to being unreadable—selectively accessible only to those with the appropriate rights. The challenge for those embracing this brave new world is that encryption, and cryptography in general, is no longer confined to a few specialists or indeed to a few islands. It follows the data, spreading to all the islands and bringing a new dimension to security management.

The Rise of SSL

We are all familiar with SSL (Secure Sockets Layer) protocol—the thing that gives you the padlock on a Web browser. SSL has emerged as the de facto standard for ensuring the privacy and security of electronic transactions passing through Web servers and network appliances, from e-mail to e-commerce. The cryptographic keys used in SSL achieve two things. It authenticates to the user the identity of the organization that is responsible for the site in question and it ensures that any information transmitted between the purchaser's Web browser and the merchant's Web site is protected from potential eavesdroppers or hackers that happen to be listening in from anywhere on the Internet.

So if the padlock is there and SSL is being used, are there still grounds for us to be concerned? Firstly, the SSL connection is only of value if the user checks the certificate to ensure that it is issued to the correct party; a number of “phishing” scams involving getting customers to enter personal information into bogus Web sites supposedly belonging to brand X have included SSL “protection,” but the certificate for the Web site was not issued to brand X but to some other party either with a similar name or with a URL that is confusingly similar. Even when the user does check the certificate, if the private key used by the Web server is not kept secret, then theoretically anyone who obtains a copy of it and intercepts communications can potentially decrypt the communications. Credit card details, personal data and other confidential information could be tampered with or

misappropriated. Best practices must be followed to protect and manage these keys using suitable cryptographic hardware if we are to give customers confidence in these SSL connections.

So, SSL is capable of securing data and transactions as they travel between a browser and a Web server, but what risks lay beyond the Web server? After all, if an SSL session is terminated on a Web server and sensitive information, such as a password and PIN, for example, is unencrypted and left exposed, the point of weakness is shifted but not eliminated. This is in fact a common scenario, as authentication information often needs to be stripped and compared with data stored in a back-end database for validation.

The challenge, therefore, is to extend the security provided by SSL deeper into the Web site infrastructure in order to protect data behind the firewall from both internal and external attacks. As the concept of a secure network boundary becomes outdated, it becomes even more important to protect sensitive information wherever it flows—inside or outside a corporate network. We must be careful not to terminate our SSL connections anywhere that might stand a chance of being compromised, but we must also ensure that we don't do away with what benefits we do get from perimeter security by allowing connections to pass unchecked through the DMZ between our firewalls. To achieve this, we need to address where we store the SSL keys, where we terminate the SSL sessions, and ensure that we process decrypted data in a secure environment in order that traffic can be passed securely on to other back-end applications.

What Else Does SSL Do?

In addition to what goes on behind the Web server and firewall, there is a rapid growth in demand for secure remote access to e-mail and corporate applications for teleworkers, roaming executives, consultants on client sites, 'day-extenders' who work at home in the evenings and for collaborative networks between partners, customers and suppliers.

Virtual Private Networks (VPNs) have been developed to set up secure links across the Internet, but traditional VPNs based on the IPSec protocol require client software to be installed and managed. However, a new generation of VPNs based on SSL are particularly well-suited to supporting remote access, since SSL is already included in the browser and no additional client software is required, giving users the benefit of 'anywhere access.'

For example, business applications may be accessed from an Internet café, airport kiosk, wireless device or from another PC on another corporate network. This means that IT departments do not have the hassle of managing VPN clients on employees' home PCs or laptops, while customers, suppliers and partners are far happier if new remote access software does not have to be deployed and managed on their own desktops by a third party.

Data at Rest

As the network becomes more secure, it is not surprising that hackers who are able to penetrate perimeter defenses usually focus their efforts where the reward is greatest—the database. Credit card numbers, social security numbers, passwords, health records, employment records, Intellectual Property (IP), proprietary source code and other sensitive information often lie virtually unprotected in large data repositories. Security breaches here can have a devastating effect on a company's business and reputation and can severely damage relationships with customers. At one Web electronics retailer, hackers were able to steal from the company's archives nearly 8,000 invoices for online credit card orders and a large inventory database. On an even larger scale, last year three men were

arrested in what is believed to be the largest identity theft case in US history. Over 30,000 Americans' identities were 'stolen' by help desk employees extracting account passwords from a database and downloading credit reports that listed bank account, credit card, mortgage and other financial information.

Increasing concerns about privacy and the security of data at rest have prompted the development of legislation and industry standards that are designed to force companies to follow tighter security practices for the protection of sensitive data. For example, the California SB-1386 demands that anyone doing business in California to disclose any security breaches involving the release or potential release of unencrypted personal information pertaining to any Californian resident and renders the business liable for fines or damages if they fail to disclose this. The Gramm-Leach Bliley Act (GLBA) is designed to protect personal financial information and the European Union's 94/46/EC Directive on Data Privacy (Safe Harbor) sets data privacy standards for companies doing business in the EU. Other regulations focus on specific data, such as protecting personal healthcare information and pharmaceutical records, while the major credit card companies are also taking measures to protect customer data. Visa, for example, has introduced its Visa CISP (Cardholder Information Security Program) and will audit and fine merchants and service providers if they do not take appropriate measures to protect cardholder account and authentication data.

Databases are particularly vulnerable to attack, and while firewalls help to protect private networks from external penetration, once compromised, the database itself is exposed, and firewalls do nothing to prevent against internal attacks. Traditionally companies have attempted to protect databases by using access control solutions provided by the database vendors themselves. This approach has inherent limitations and cannot protect the data if these basic access control measures are circumvented. As demand for Web-based and remote access to applications and data increases, this problem becomes more complex. Database administration and management of policy is also a potential point of weakness. For example, database administrators (DBAs) typically either have full access to view all data in a database or can grant such rights to themselves or others. Sensitive data, such as credit card numbers, should only be viewable by users who need to access that data, as established by the organization's security officer, not the DBA. This policy is known as 'separation of duties' and is critical to the overall database security.


Increasingly companies are looking to add an extra level of database security through the use of encryption. In the past, attempts to integrate cryptographic security mechanisms into large database structures were largely unsuccessful, as it usually involved encrypting the entire database or special schemas to provide basic functionality. As these systems were clumsy and time-consuming to implement, the little improvement in security they offered was often more than outweighed by the major negative impact on cost and performance they incurred.

To overcome these shortcomings, fine-grained data protection through encryption and key management technologies have now been developed so that only those data objects or fields specified by the security policy are encrypted. So instead of building 'walls' around servers or hard drives, a protective layer of encryption is created around individual data-items or objects.

Conclusion

Underpinning database encryption solutions is the use of cryptography and key management. This relies on using long-lived secret keys that need to be carefully protected to ensure the confidentiality of the data.

Encrypted data is only as secure as the keys used to encrypt it, and if these secret keys are compromised, the security of the database is at risk. This means that the keys need to be created, stored, distributed and changed in a manner commensurate with the value of the data being protected.

Many businesses are recognizing the necessity of breaking down their monolithic IT infrastructures and replacing them with islands of secured information, to which only trusted partners, customers and suppliers have access. In an interconnected world, where boundaries are necessarily porous, other users, both good and bad, will gain access to your system. The issue is: What damage can they do? A true sense of security ultimately comes from the knowledge that only the good guys have the access rights that can turn access into action. Since a system is only as secure as its weakest link, end-to-end security only comes when we can rigorously enforce access control at every step; in the network, in the Web servers, on the application servers, and at the database. Cryptography, combined with strong key management, is the only way to secure all your points of risk and deliver true end-to-end security. 



Dr. Nicko van Someren co-founded nCipher in 1996. As Chief Technology Officer, Nicko leads nCipher's research team and directs the technical development of nCipher products.