

## **Hardware v software security**

Dr Paul Galwas, Director of Strategic Planning, nCipher Corporation Ltd

Building a robust, scalable and secure infrastructure for e-commerce requires the integration of many components within a carefully designed architecture. Specialist security hardware and software play an important part in this architecture, providing the basis on which trust between service provider and users develops.

Security architectures must protect against real and perceived threats from unauthorised external access to the system, and also provide checks and balances to prevent unauthorised use by authorised users. By providing clear security measures, system developers can assist the building of trust online. Hardware security is the basis of best practice security, but how well and how far is the hardware integrated into the software architecture?

The challenge now is to extend the radius of protection beyond the security perimeter of black box hardware security solutions, and extend the security which existing systems offer to include protection for the intellectual property within proprietary applications and data. This can be achieved by combining the best of hardware and software features into a single, rigorous, secure environment.

## **Hardware v software**

Financial services and payment processing have led the way in the adoption of advanced security technologies, both within closed networks and on the open network that is the Internet. Financial sector applications remain some of the most demanding in terms of the level of security required, the volume of transactions and the need for interoperability. These users require speed, security and scalability to deliver high-availability services reliably in a competitive environment.

Hardware security is an essential component of e-trust services. The hardware security module (HSM), which secures the keys underlying the security platform (typically a PKI implementation), is an essential part of the system. Features and services provided by good HSMs should include:

- Adherence to industry standards – the US government standard FIPS 140-1 Level 3 is the most widely used, and mandates physical features such as tamper-evident casing in addition to a secure software architecture
- Dedicated security processing hardware to speed the intensive cryptographic calculations required in the creation of keys
- Secret-sharing (K of N) authentication systems, where access keys can be split across multiple tokens with a certain number of shares required to gain access to the HSM
- Key management infrastructure to simplify the task of issuing, administering and revoking multiple keys
- Secure key backup facilities to aid key recovery. In addition to key recovery, storing keys in ultra-secure encrypted formats outside the unit means that unlimited key storage can be offered, with keys being securely loaded into the module before being decrypted for use. Earlier HSMs (with internal key storage) were limited in the number of keys that could be stored and in key recovery facilities.

With all of these features in place, a good HSM is the backbone of a comprehensive security platform for trusted services, providing security for the keys used by applications which initiate SSL transactions, issue and manage digital certificates, or perform custom applications. Major financial services e-trust initiatives, such as IdenTrust, have already adopted and refined this security model, working in close partnership with hardware and software providers to create an overall architecture which serves users and institutions at all levels in the chain of trust.

## Balancing hardware and software

However, in a typical PKI installation, it is the PKI keys which are protected, rather than the data and applications themselves. The traditional PKI architecture shifts the security burden from protecting data to protecting cryptographic keys. Protecting the root (master) keys used to generate subsidiary keys and sign all digital certificates issued by the server becomes the highest priority task.

The most fundamental aspect of good practice in PKI is to secure the keys, and particularly the root key used to generate all other keys. If a root key to a PKI system is lost or compromised, all the certificates it has issued must be invalidated, and any data which it has encrypted is either lost for ever or vulnerable to attack. The HSM provides this; however, the focus of the security is the HSM, when it is the server connected to the Internet which is most at risk of attack.

The obvious next step is to take the strong security offered within the perimeter protected by the HSM, and extend the radius of protection beyond the confines of the black box.

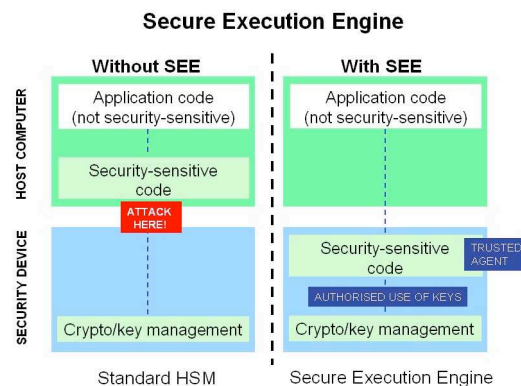
## Extending the radius of protection

Intellectual property, such as applications and data which are run on servers accessible from the Internet, is at risk unless protected. By integrating key-based security into these applications, code and data alike can be protected. Only authorised users performing authorised tasks can execute code or access data. Without the appropriate credentials, users and programs cannot gain access to server resources.

In this model, authorised software is controlled using the HSM's key management apparatus, affording it the same protection as a root key and turning it into a Trusted Agent. This approach is particularly well suited to tasks such as bridging security gaps between systems and protocols, auditing, metering and time-stamping applications where trust is vital, and code which needs to operate beyond the traditional security perimeters.

By integrating the logical security provided by software and the physical security provided by hardware, a greater level of overall security can be provided.

Creating trust online is the essential component in the development of online financial services. Hardware security is a fundamental building block in this process. By harnessing hardware security to flexible software security which can be embedded into users' own applications, developers can create a robust infrastructure and deliver the online trust on which their users and customers depend.



nCipher's Secure Execution Engine extends  
the security perimeter of the HSM to application code