Securing identity in silicon

User authentication is a crucial weapon in the security war. Ry Crozier reports on developments

(reprinted from Electronics News, 2003, Copyright Reed Business Information 2003)

THE PROLIFERATION OF DIGITAL communications has been accompanied by an escalation in "identity" theft. It has become all too easy to intercept a net-borne identity—or one broadcast over a WLAN—and hijack it for illegal use.

Fortunately, security vendors are fighting back. One method of secure identity authentication, using a digital key, is held on an 1C embedded into the access device (for example a personal computer). An alternative is to hold the key on a portable token, such as a USB clip or smart card, claims Brian McKeon, a director of Sentry Project Management (SentryPM).

"The difference [between these examples is that] you can't really take the chip in the PC around with you as you would a token," McKeon explains. "However, that |will change] as PCs evolve into tablets, PDAs and mobile phones."

Embedding the chip

Whether or not the identity information is carried on the PC hardware or a portable token, can he determined by how the devices are distributed, according to Forefront Technologies general manager Howard Small.

"Embedding the chip into the motherboard means the devices need to be distributed in a secure manner because they have the authentication keys in them, and they also need to be tamper resistant so people can't access them," Small explains.

Securing device distribution involves both certification as well as the way the devices are issued since each device contains enough information to authenticate a person, facilitating possible identity theft. Tamper resistance can be added with the provision of a biometric reader, which uses fingerprints to authenticate the user and then provide access to their keys stored internally on the chip.

"The alternative is a smart card, since the security is built-in and the distribution arrangements for credit cards are well and truly entrenched," adds Small.

It is also theoretically possible that a virus could be employed to capture the digital certificate residing on the PC while in decrypted form. The same is not possible with a smart card since it is never connected to the network.

"If you download a digital certificate to your *PC* it's encrypted. But when it needs to be used the *PC* unravels and uses it before reverting to the encrypted form," explains McKeon. "That means someone deliberately chasing your identity could install a virus and capture it in its decrypted form. It's theoretically possible.

"This compares to a smart card where the signing-on operation [using the encryption/decryption keys] happens only on the smart card – so the keys never leave the card," adds McKeon.

Token-based authentication

Both token-based alternatives— smart cards and USB tokens— consist of essentially the same architecture. "It really is the same answer," says McKeon. "The chip where the keys are stored is embedded either into the smart card or the USB token. The only difference is the smart card is the industry-accepted solution for facilitating authentication."

However, the token is only a small part of the authentication picture. "The trickier part is in establishing the certifying authority and the whole public key infrastructure (PKI) around which the system is based," McKeon adds. The certifying authority is responsible for validating the authenticity of the digital certificates it issues by "stamping" them with its own digital signature.

The PKI is a security management infrastructure dedicated to the management of keys and cer- tificates used by public key-based security services. As an example, consider an e-mail context: Telstra's iTrust system establishes a secure link between sender and recipient, both of whom need their own digital certificate to access the service.

The sender encrypts the email using the intended receiver's public key, which can be obtained by either asking them to send a signed e-mail first (in which case their public key will be automatically installed in the browser upon receipt of the e-mail) or by down-loading it from the online iTrust directory using your own digital certificate as proof of identity. The e-mail recipient can then decrypt the e-mail at their end using their private key, which is stored on their smart card.

To do this the smart card holds two credentials: an authentication or identity set for identity purposes that exist only on the smart card and needs to be replaced if the card is lost; and a confidentiality set for encryption purposes. If a user does lose the smart card, the issuer (in this case Telstra) will generally revoke the card's digital credentials and issue the user with a new set.

However, the card issuer may also choose to store the encryption key only off-card and under secure circumstances so that any files the user encrypted before losing the card can be recovered with the key copy. In addition, unauthorised users can't gain access to your keys simply by stumbling across a lost card as all cards are PIN protected.

Random numbering

Authentication issues can also be solved using random number generation (RNG) technolo- gies. "Almost all modern smart cards have a built-in RNG function and undergo a vigorous certification process to prove the number generator is truly random," says Sentry's McKeon. "The reason being that if someone can uncover the pattern used to generate the numbers then the keys are weakened."

Forefront Technologies is adamant that this scenario is not possible with the Todos eCode system it distributes in Australia. ECode uses a keyring reader and the chip on a smart card or GSM SIM to generate a rolling PIN for authenticating user identity in Internet banking and similar applications.

Instead of entering the account number and PIN at the usual Internet banking sign-in, the user still enters the account number but uses eCode to generate a one-off PIN, which they can use to gain access to their account. Once the one-off PIN is entered, the bank's server employs the user's ID and digital keys to generate a sequential number and compares it to the one generated by the user's smart card before authorising entry.

This means that both the software generator on the smart card and the bank's server must be syn- chronised. "One of the risks users face is they may get out of sequence with the server, and we do have mechanisms in place that allow the reader to re-sequence," says Forefront's Small.

"These procedures may require the user to generate two PINs in sequence, which can then be searched in the backend system, although the call centre may be required to use software to re-sequence the card or completely block it out and start over."

Small is vague when it comes to revealing details of the RNG algorithms, preferring instead to reinforce that they are "extremely secure".

"Because the session PIN generated by the server is a sequential number, we can guarantee it should be the next PIN to be generated by the customer," Small explains.

"The session PIN is also generated only at the time required, and is not stored on a database at any time," Small adds.

In terms of reader design, once the smart card is inserted the customer uses a (somewhat fiddly) trackball-type wheel to enter the smart card PIN and generate the session PIN required.

"Todos is now producing a keyboard version at the same size and cost," Small says. "There's also a version for GSM phones where the application sits on the SIM, allowing users to generate the ses- sion PIN on the phone and send it to the bank via SMS to log in."

Small anticipates the system will be picked up by a number of Australian banks and organizations, but admits the system in its current format requires a large user base to be economically viable.

DNA algorithms

Silicon may be providing the solution today, but the future of security could be genetic. Taiwan-based Biowell Technology has developed a unique biotechnology using the ID characteristics of DNA in the fight against counterfeiting.

Under an exclusive licensing and partnership agreement, US-based Applied DNA Sciences has used Biowell's technology to develop a unique anti-counterfeit (AC) chip.

Using proprietary production techniques, the non silicon-based chip contains a 64 kByte EEPROM to hold information determining anything from identity verification to product origin. According to e-inSITE, (www.e-insite.com, a sister website to *Electronics News)* the new biotechnology exploits the fact that every plant and animal possesses a unique DNA "fingerprint", which can be scientifically selected and processed into a unique string of code prior to embedding into various materials such as ink, paint or chips.

The unique ID characteristics of the DNA will allow genuine products to be distinguished from counterfeits, claims the company, by allowing users to access and analyse the characteristics of the attached DNA.

This closely mirrors the verification process for digital certificates, where users can determine the authenticity of e-mail communications by accessing and analysing the sender's keys used encrypt the message. In addition, it is claimed the cost of the DNA chip, card and reader is comparable to that of existing smart card systems.

According to Applied DNA Sciences, the traditional IC widely used today has not only become vulnerable to hacking in the decoding process, but encryption logic has also been bypassed. The structure of DNA is significantly more complicated than electronic signals, and better suited for ver cation applications.

The advantage of using the DNA AC chip is that if it is sabotaged or removed, the chip will cease functioning, thus preventing the data on the chip from being duplicated.

Further information:
SentryPM (02) 9438 4100;
Forefront Technologies (03) 9781 1533