



Join Us Now >>

Principia Local Government
For Local Authorities

Principia Foundation
For smaller organisations

Principia Professional
For medium sized organisations

Principia Premium
For larger organisations

Vendor Engagement Programme



Member's Spotlight
For NCC Focus Member
Keith Isted of Xantus, life is full of challenges... ➔



The walls are falling down

Controlling access to corporate resources has always been a point of risk for businesses. But with the move to de-perimeterised enterprises - where everyone effectively becomes a 'remote' user - the potential for security breaches is increased. **Dr Paul Galwas** looks at how encryption can help to protect your information and why it is equally important to know who has access to that information.

Photograph courtesy of ltd-photography.co.uk



With increasingly extended and dynamic enterprises, the distinction between insiders and outsiders is becoming blurred and what organisations can expect to control is less clear. Before the 80s, IT functions were localised in physically secure and tightly controlled environments. Controlling access to information was pretty straightforward and

secure. The rise of the internet saw the distinction between external and internal networks, with the Firewall and DMZ (De-Militarised Zone) emerging as the perimeter between the two.

But today, with demand for anytime, anywhere access from managers, employees and partners, and more powerful mobile devices, the distinction between 'what's in' and 'what's out' is disappearing. In effect, the walls are coming down and industry attention is turning towards controlling access in a de-perimeterised enterprise.

But any reader of John Le Carré's Tinker, Taylor, Soldier, Spy knows that this is not new. Field agents have operated in the hostile de-perimeterised world for years. They trust no one and protect their true identity and the confidentiality of their information to the highest degree. The difference is that the internet has twice as many users as there are people in the USA, so the focus must change from just detection, prevention and reporting - to securing communications across the open, distributed and potentially very hostile environment, and controlling exactly who has access to that information.

Identify, protect and comply

While perimeter security solutions have been largely effective in corporate IT systems, they are high risk, 'all-or-nothing' solutions which have three significant draw backs:

- Once an intruder successfully breaches the outer defences they typically have potential access to the full range of internal corporate data and applications. In the same way that once a burglar breaks into a house, he has access to all its rooms and the valuables that they contain.
- The perimeter security paradigm does nothing to stop malicious personnel who are already on the inside. For an analogy, think about the disgruntled live-in au pair who can legitimately access the entire house and cause malicious damage.
- Managing 'access control' to allow authorised personnel through the perimeter becomes more complicated when it is necessary to provide access to external parties. Taking the same example: a home help needs access only when the owner is present, a cleaning person may need access to the house when the owner is out, yet a contracted builder may need access to only the garden and the bathroom whether the owner is in or out.

Back in the computer world; with so many external parties and their computer systems being allowed access to business critical systems and information, it is important to keep valuable information secure, only allowing access to those with the right credentials. Customer databases, credit card details, medical records, intellectual property, competitive information should all be protected from prying eyes, both from outside the organisation and within it. Increasingly, cryptographic technologies are being used to obscure data to those without the authority to view or change it, as well as giving permission to those who do have the authority. To achieve accountability, cryptography also



New Professionalism in IT Programme
For end user and supplier communities

NCC Media Centre >>

Find out more about the activities of the National Computing Centre at ncc.co.uk

Weekly Poll

According to Gartner, CRM projects are high on firms' 2006 agendas with businesses starting to implement large company-wide solutions with business-led strategies.

Do you agree that company-wide CRM projects are now moving up the business agenda?

Yes
No

FREE to Members
[Half Day Seminars](#)



NCC bookstore
NCC members receive **25% off** all books.
[Click here to visit](#)

Open Source - are we ready yet?
Free research report reveals that 66% of firms expect to adopt OS



New Professionalism in IS Programme
For end user and supplier communities

enables the generation of unalterable records of when specific information was accessed or altered, and by whom.

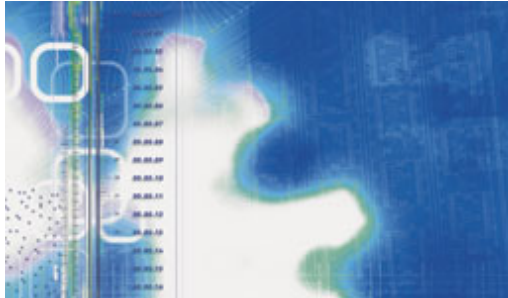
Strong mutual authentication is therefore a pre-requisite for both secure communications and access control. As attackers will always seek to break the weakest link, a simple password is no longer sufficient for identification as it is readily cracked or cloned. Most standard security protocols that support secure communications such as SSL (Secure Socket Layer) do not use passwords but rely on more sophisticated techniques.

However, the strength of mutual authentication depends as much on processes and policy as it does technology. Just as a spymaster devotes time and effort to recruit agents who can exchange messages with the briefest of protocols, strong mutual authentication must be built on secure enrolment to bring a person, program or computer into the circle of trust. This process must also provide economies of scale to prevent costs spiralling as the number of people and devices increases.

Compliance and audit

The increasing pressure to comply with government legislation and industry best practice, means that compliance is never far away when it comes to identity management and access control.

Easier, cheaper and more automated and scaleable ways to audit and to prove compliance are needed to replace largely manual methods. Implementing stronger identities and mutual authentication, in conjunction with content security to control access to sensitive data, are the



essential first steps. However, they must be combined with secure policy automation and audit trails to achieve cost-effective and scaleable compliance.

Cryptography holds the key

Leo Marks, head of codes for the British Special Operations Executive (SOE), set up by Churchill to infiltrate agents into German-occupied countries, understood the de-perimeterised world only too well. Marks realised that cryptography was the only effective way to identify and protect his agents. He produced huge quantities of cryptographic keys written on sheets of silk that could be sewn into an agent's clothes to encrypt their messages and evade detection.

Today's IT security challenge to identify, protect and comply is very similar and is also underpinned by cryptography: digital signatures for strong mutual authentication, message integrity checking and secure audit along with encryption for confidential channel and content security.

Specialist organisations have already demonstrated that controlling access in a de-perimeterised environment is possible, albeit using highly customised system components and relatively limited scope. But, increasingly, off-the-shelf products are becoming available to allow much wider adoption at much lower cost. For example Microsoft Windows now contains highly integrated cryptographic support as standard - at essentially no incremental cost.

In a de-perimeterised world, authorisation and access control decisions can be made uniformly based on the distribution and management of cryptographic keys, rather than by making disparate changes to the various systems and networks in the organisations that house critical information. But as de-perimeterisation moves mainstream across large enterprises, these cryptographic mechanisms must be uniform and scaleable or the costs will be prohibitive.

Providing lifetime management of cryptographic keys across hundreds of applications and thousands of servers, end users and networked devices raise four common requirements:

- Automation of the management and distribution of keys and other credentials both to protect information and identify users;
- Centralised policy enforcement and auditing of the associated processes;
- Extensible support for both legacy systems and new cryptography-enabled applications, such as SSL, VPN, strong authentication, secure messaging, and content, file and database encryption;
- Support for a wide variety of hardware platforms and operating systems.

The part that has been missing in the jigsaw is a set of products that can address these diverse key management needs. As strong identity and authentication schemes, combined with secure messaging and content security, become the cornerstones of security in a de-perimeterised world, so cryptography is essential to underpin the need to identify, protect and control.

*Between Silk and Cyanide: A Codemaker's War 1941-45, Leo Marks

The author

Dr Paul Galwas is director of product management at nCipher (www.ncipher.com) who will be exhibiting at Infosecurity Europe 2006 from 25 to 27 April 2006 at London Olympia www.infosec.co.uk.

(IT Adviser, Issue 41, January/February 2006)

Categories: Special Feature, IT adviser, Securing the Enterprise