# Implementing identity management security - an ethical hacker's view

Peter Wood

Peter Wood, Chief of Operations, First Base Technologies

**Identity management has two principal components – management *of* identity and management *by* identity. Management of identity is the process of issuing and using digital identities and credentials (such as usernames and passwords). Management by identity combines the proven identity of the user with their authorisation, in order to grant access to resources. This article explores the methods of stealing an individual's digital identity and thus gaining the ability to impersonate them and access the resources they have the right to access.**

As we open up our networks to permit access by business partners, customers and suppliers, we are moving from fortress-style security to airport-style security. We have to let everyone in, then rely on their digital identity to determine which resources they should be able to access.

As a result, no matter how much you spend on firewalls, VPNs, anti-virus software and intrusion prevention, anyone who steals the identity of one of your users becomes that user and has access to your most sensitive systems and data. If just one user's identity is compromised, your systems are vulnerable. This is the threat posed by "corporate identity theft".

Identity theft takes many forms – exploiting weak passwords, keystroke capture, phishing, trojan software, social engineering, password sharing and so on. Not every hacker is sitting at home with their computer, trying to hack in to the corporate website. Sometimes all they have to do is call up and ask! As Dorothy Denning, author of *Information Warfare and Security* said, "Any medium that provides one-to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar."

## Tools for exploiting laxity

Social engineering by impersonation is very common. For example, a hacker will call the help desk pretending to be an employee, claim to have forgotten their password and ask the help desk to reset it or give it to them. The help desk will frequently do this without verifying the identity of the caller. Our testing shows that this is a very common scenario – successful at most organizations in all business sectors.

> **"I was able to gain access through the building's back door, read personnel information and customer contracts...and obtain email addresses"**

Another technique involves visiting the premises in person. As a bogus employee, visitor or cleaner, it is simple to look for information lying on desks, overhear conversations, plug in a keylogger or even just use a vacant desk and PC. In one case, I was able to gain access through the building's back door, walk around every floor without challenge, read personnel information and customer contracts in unlocked cabinets, steal the contents of post trays and obtain a staff list containing names, job titles, email addresses and phone numbers.

Removing and studying the contents of bins marked "For Shredding" or "For Recycling" proves very interesting too. Shoulder surfing - looking over someone's shoulder to see door entry codes, their password, information on their screen or what they are writing is also extremely successful. Sometimes the simplest techniques are the most successful and often do not involve any technology at all.

Mail attachments and Web links remain very popular, enticing users to click to gain access to something appealing or illicit whilst silently installing Trojan software on their computer. Once installed, this software can capture every keystroke and mouse click, and even take screen shots, then quietly mail everything to the hacker somewhere else in the organisation or even in another country.

## Dangers on the road

Staff using laptops away from the office are a particular threat, since the opportunities for them to be infected with Trojan software, keyloggers and other malware are much greater than within the corporate environment. Where staff are permitted to use a home wireless network to access the Internet or head office networks, hackers may target an individual at home and use the unsecured wireless connection to sniff traffic or plant malicious software.

When members of staff are travelling, unattended laptops can easily be infected without any obvious evidence of intrusion, or data may be stolen and later used to compromise the office network. This can undermine even the best VPN security by simple impersonation. Even when two-factor authentication is used (for example SecurID tokens), access still depends on good staff education. It is not uncommon for an individual to keep their token and their PIN with their laptop, thus undermining a secure system and providing a back door for hackers.

Since the type of traffic permitted through a VPN connection is seldom restricted, the hacker can use any tool they wish to compromise the corporate network without even visiting the target office. Despite the recent publicity over "phishing" attacks, people are still vulnerable to spoof emails and websites. In one recent project, we crafted an email with a link to a Web page purporting to be a survey on information security hosted by our customer. We used graphics and links from the genuine corporate website on our own server to ensure the pages looked realistic.

Using simple Web forms, we harvested user names and passwords, as well as valuable information about the organization's security procedures and mailed the results to our own email server. No-one noticed that the site was unencrypted, nor that it was hosted on an unrecognised IP address with no DNS name. Until a senior member of staff challenged the email and instructed staff to ignore it, we were receiving mails containing names and passwords from innocent users.

Normal Web browsing can also help steal identities. For example, a specially crafted pop-up on an otherwise innocent website can reap rich rewards. Staff using the corporate network to browse a website will often respond to such a pop-up box saying "Your connection to the network has been lost – please re-enter your username and password". They continue using their network and the Internet none the wiser, whilst their credentials have been harvested by the website.

Another successful technique involves using one of the oldest and slowest method of communication – the postal service (snail mail). It is easy and inexpensive to set up a PO box, providing an ideal way to hide and fake a business. Of course snail mail has no content security so there are no technical controls to bypass! People are more likely to respond to a survey they receive in the post, since it appears much more legitimate when printed on paper. If a stamped, addressed envelope included, then there is little effort or cost on their part. Of course, you offer cash or other prizes for completed and returned surveys.

## Passwords – the common thread

There's a common thread here of course – the password. Passwords are a hassle for users, with multiple passwords always needing changing. They are highly vulnerable and you can never know if passwords have been stolen until it's too late. Gartner (September 2001) said that 65% of all helpdesk calls relate to password problems and that each call costs you at least £25. And of course they're a dream for your enemies - whether internal or external, techie or not - passwords are

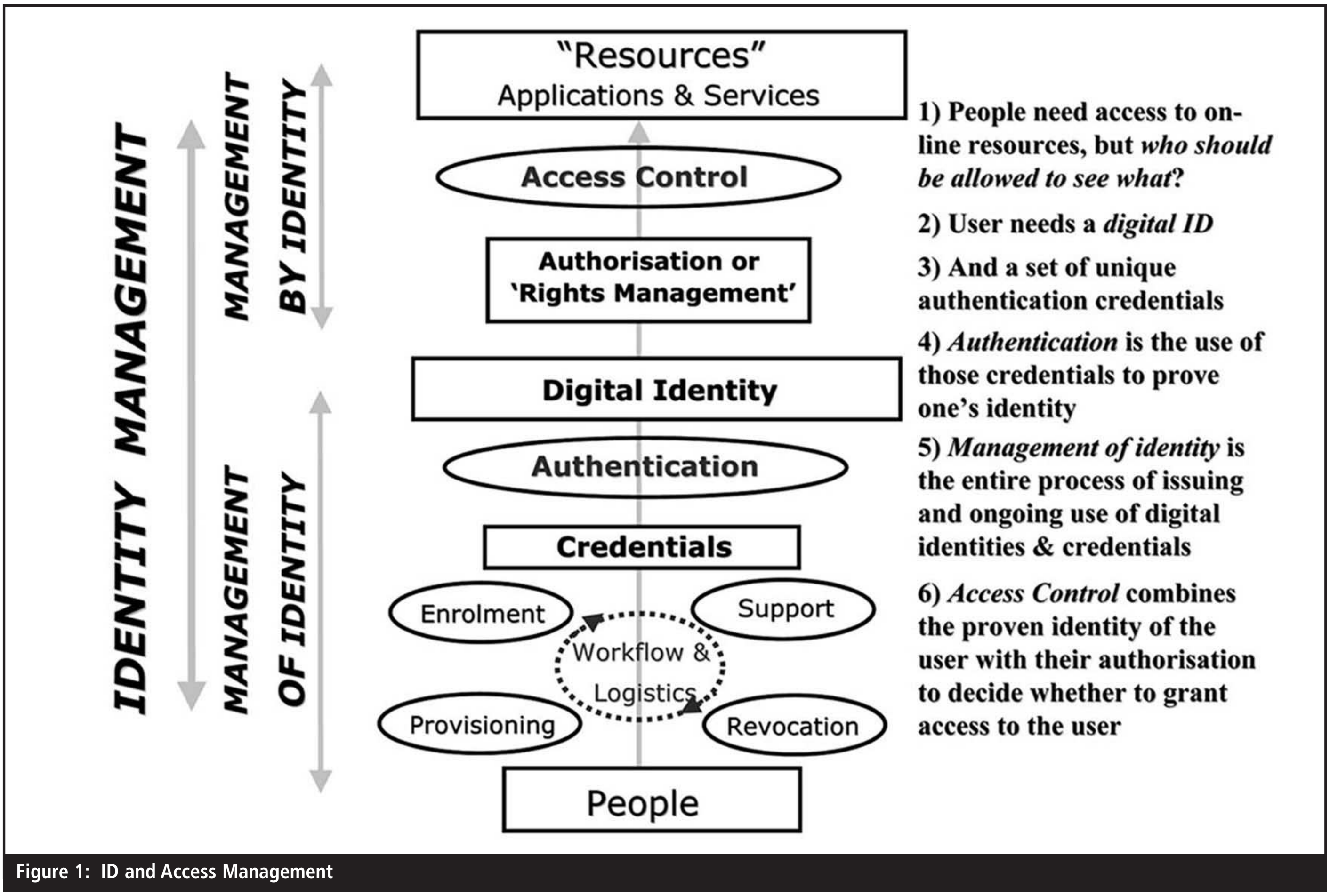
IDENTITY MANAGEMENT
MANAGEMENT BY IDENTITY
MANAGEMENT OF IDENTITY
"Resources"
Applications & Services
Access Control
Authorisation or 'Rights Management'
Digital Identity
Authentication
Credentials
Enrolment
Support
Workflow & Logistics
Provisioning
Revocation
People
1) People need access to on-line resources, but *who should be allowed to see what*?
2) User needs a *digital ID*
3) And a set of unique authentication credentials
4) *Authentication* is the use of those credentials to prove one's identity
5) *Management of identity* is the entire process of issuing and ongoing use of digital identities & credentials
6) *Access Control* combines the proven identity of the user with their authorisation to decide whether to grant access to the user

Figure 1: ID and Access Management

easy to steal by shoulder surfing, social engineering, simple guesswork or by snooping, sniffing, hacking and cracking.

## Tightening the defences

Management must understand that all of the money they spend on software patches, security hardware, and audits will be a waste without adequate prevention of social engineering attacks. So what countermeasures can we implement? Firstly, policies - one of the advantages of policies is that they remove the responsibility of employees to make judgement calls regarding a hacker's requests. If the requested action is prohibited by policy, the employee has no choice but to deny the hacker's request.

> **“Opportunist access to unattended PCs is very common”**

You need to ensure that everyone shreds unwanted phone lists, email lists and other important documents. Some documents will obviously need to be locked away, so you must provide employees with sufficient lockable storage space to enable this. In the end, best practice is to have a clear desk policy which is enforceable and workable.

All staff must use screen savers with password controls and be instructed to lock their PC every time they leave their desk – opportunist access to unattended PCs is very common. Any sensitive information stored on desktops, laptops and PDAs must be encrypted. Smart mobile phones and PDAs should have infrared, and Bluetooth disabled by default and the organization must have a policy restricting their use or the sensitivity of information stored on them.

## Countermeasures – summary checklist

### Desktop Security

- Shred old phone lists, email lists and other important documents you no longer need.
- Some documents will need to be locked away – make sure everyone has a lockable drawer or cabinet.
- Basic best practice is to have a clear desk policy.

### IT security

- Use screen savers with password controls and short timeouts.
- Encrypt sensitive information on desktops, laptops and PDAs.
- Secure your mobiles and PDAs - switch off infrared, wireless and Bluetooth when not in use.
- Secure wireless LANs – use the latest security measures and implement VPNs over wireless.
- Physically destroy unused hard disks, CDs and other media.

### User guidance

- Say what can and cannot be discussed over the telephone
- Say what can and cannot be discussed outside the building
- Say what can and cannot be written in an email
- Don’t use email notification or voicemails when out of the office. It sets up the replacement as a target.
- Ensure everyone knows how to report an incident and to whom

### Helpdesk

- Permit password resets only with call-back and PIN or cherished information authentication.
- Ensure there are clear incident reporting and response procedures.
- And clear escalation procedures.
- Help desk staff should be encouraged to withhold support when a call does not feel right. In other words “just say no …..”

### ‘Training, training, training’

- Train all employees - everyone has a role in protecting the organisation and their own jobs.
- If someone tries to threaten them or confuse them, it should raise a red flag.
- Train new employees as they start.
- Give extra security training to security guards, help desk staff, receptionists, telephone operators.
- Keep the training up to date and relevant.

### Compliance

- Have a security assessment test performed and heed the recommendations.
- Test the company's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack.
- Have the first test performed when the company is expecting it.
- Do a blind test the second time around.

Wireless LANs must be properly configured and tightly secured, whether in the office or at an employee's home. Sensible guidelines must be issued to all staff regarding the risks of using wireless hotspots and Internet cafes. The organization must ensure that all remote access is secured using VPNs and that no sensitive traffic, including email, is transmitted anywhere in the clear.

A process and policy should exist to ensure that all hard disks, CDs and other media are physically destroyed rather than recycled or simply thrown away. A recent survey of 100 hard disks purchased on eBay and at car boot sales showed around 40% had sensitive data easily recoverable and a further 40% had not even been formatted.

Implement strong authentication for all remote users and for all privileged users and accounts. There are many two-factor alternatives to the traditional password, including SecurID, Smart Cards, smart USB keys and even mobile phone SMS texts.

Institute thorough end-user training on secure communications, including what can be discussed over the telephone, what can be discussed outside the building and what can be written in an email. Try not to use e-mail notification or voicemails when away from the office - it sets up the replacement as a target. And most importantly, ensure everyone knows how to report an incident and to whom – most people do not.

> **“Strengthen your helpdesk password reset process”**

Strengthen your helpdesk password reset process. Permit password resets only with call-back and PIN authentication or some other form of cross-verification. Implement incident reporting and response procedures for all help desk staff, together with clear escalation procedures for everyone in the incident chain. Help desk staff should be encouraged to withhold support when a call does not feel right. In other words “just say no …..”

To adapt Tony Blair's mantra ‘Education, education, education,’ organizations must place priority on ‘Training, training, training’. Train all employees - everyone has a role in protecting the organization and their own jobs. If someone tries to threaten them or confuse them, it should raise a red flag. Train new employees as they start. Give extra security training to security guards, help desk staff, receptionists and telephone operators, all of whom have a vital role to play in blocking identity theft. Make sure you keep the training up to date and relevant.

Finally, have a security assessment test performed and heed the recommendations. Test the company's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack. Have the first test performed when the company is expecting it, then do a blind test the second time around.

### About the author

*Peter Wood is Chief of Operations at First Base Technologies, an ethical hacking firm based in the UK. He founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas spanning network security reviews, firewall penetration testing and policy and procedures.*

# The case for federated identity

**Roger K. Sullivan, VP, Oracle; Chair, Liberty Alliance Conformance Expert Group**

Roger K. Sullivan

**More than 80 years ago, a reporter asked the infamous thief Willy Sutton why he robbed banks. Sutton's reply was, “Because that's where the money is, stupid.” Today, the money is in information and there's a lot of information out there - vulnerable in databases, exposed in transactions and circulating on the Web - helping to make identity theft the fastest growing crime in the world. Organizations across the globe are quickly learning that one of the best ways to prevent identity theft is through ‘federation’.**

A federated framework or model makes it extremely difficult to steal private information and directly mitigates against a wide range of attacks. To understand how federation works, it's important to first step back and look at how information is organized and stored. Today most organizations have disparate proprietary applications, data repositories and identities in use within applications (stovepipes). Every large enterprise knows that these stovepipes are difficult to integrate within a specific organization, let alone among outside trading partners.

## Liberty Alliance's approach to free exchange

Enter the Liberty Alliance, an organization representing 150 leading banks, technology companies, wireless providers and government agencies from around the world. Liberty Alliance has designed standards, specifications and a framework that enable organizations to securely interoperate with their partners and customers by leveraging federated identity to establish “Circles of Trust” among different Web sites, intranets and other points of electronic platform contact. A Circle of Trust represents a business relationship formed by organizations to allow them to share identity information seamlessly and based