

Identity – Key to IT and Business Security

In an increasingly connected world, user identity is becoming the most critical and yet the least satisfactory aspect of IT security. However strong the defences around castles of information, the contents are vulnerable - unless we can keep the bad guys out. Furthermore, it's increasingly difficult to know who the bad guys are – statistics show that internal attacks are the by far the most common. People inside the castle wearing the uniform are not necessarily all good guys and we rarely know who is guarding the gatekeepers.

So, to assure the level of security needed to protect critical assets and/ or comply with legislation, it is high time to deal with the subject of “who’s that user?”

So far, this is a very inexact science where a chaos of ineffectual measures including unmanaged passwords etc. contribute to a situation where, all too often, people can easily access information and services that they should not.

Furthermore, because of the plethora these half-solutions, it's often hard for people to access those services to which they **are** entitled. How many of us have multiple usernames and passwords / PINs that we can't remember yet should not write down?

With the current technologies of Public Key Encryption, Digital Signatures, and Biometrics etc., we have the potential to solve this problem but not the standards, processes, disciplines and infrastructure.

Point solutions do not cut the mustard. It's virtually impossible to manage identity anywhere outside a corporate firewall because, as every system developer rolls their own solution, the overall picture is unmanageable.

As supply chains are increasingly bridging multiple enterprise policy domains, this has created a very serious situation. As networked business increases at an alarming rate so security decreases proportionately.

The result: a disturbing trend in ID-based theft – reportedly it has grown 5 fold in as many years. MI5 and others highlight that this is not just stealing from individuals; it's actually fuelling terrorism. And, with this move to an e-economy, the reasons to attack and the points of access are ever increasing.

Where next?

Supply chains are both inter-enterprise and international, so global solutions are clearly needed. Ideally, a single global solution would be best. If this is not possible a global standard framework providing interoperability is the next best alternative.

If we look at existing systems of identity that work today there are a few notable examples. The inter-bank clearing systems such as Cirrus, Visa, Mastercard etc. work well-enough in the roles for which they were intended. Cross-recognition of passports between countries is not without merit. Some more direct attempts have been made to address identity online, one of which was M\$ “Passport”. However,

none has caught on to any significant extent. Interesting initiatives such as Sender-ID (for email) and Liberty Alliance and commercial organisations such as Sxip and PrefPass are also working in this area.

The right solution would address trust and reputation issues and be simple and viral in its potential uptake. It would need to cover off the weaknesses in existing systems.

Currently all solutions fail if the user is falsely identified. For example, even the most secure “Biometric” passports can get issued against a false identity.

The right solution will probably be User-centric because there is unlikely to be any organisation that all users will choose to trust. A number of “trust hubs” would be needed and these would need to be linked into a standardised framework.

This is a tough challenge and we’re certainly not there yet. However, if the problem is recognised and the pain of not solving it is increasing and the technology exists, a solution cannot be too far off.

It is also worth noting that a single best practice solution will be unlikely to cover all circumstances (certainly not in the first iterations) – and that the decisions on inclusion and exclusion may provide for great difficulty in the public domain.

What’s to do meanwhile?

Awareness, education, tools and good application design can help to contain the problem; so we should be looking to promote these types of initiative. These will have lasting value as the true solution, when and if it comes, will take a considerable period of time to penetrate the world’s innumerable IT systems.

Awareness

- **Advocacy:** The issues around identity need more airing to help people understand the risks they face and how to both protect themselves and recover more easily in the event of attack.
- **Advertising:** Current adverts put out by insurance companies offering cover against identity-based risks are no bad thing. It would be useful if there was rather less emphasis on shredding paperwork and more in other equally important areas such as password discipline.
- **Lobbying:** Government and business decision-makers need to be aware that over-emphasis on project-specific return on investment can deflect attention from good practice. ITT’s for big projects should take account of the need for convergence.

Education

- **Access to relevant continuing professional development:** Companies, especially SMEs need encouragement to invest in this area, just as they have been encouraged to adopt broadband and other enabling technologies.

- Professional certification: Vendors such as Microsoft have adopted this approach in relation to their own products. In view of the nature of the threats, a vendor-independent approach is needed to address aspects of identity.

Tools

- Monitoring: Some tools to detect intrusions are already available – more are needed, in particular to automatically highlight changes in behavior. Tools to detect private information “in the wild” would also be useful in identifying identities at risk.
- Audit: A structured approach to review and correction is valuable. [Examples to be included here.] – especially who is guarding the gatekeepers
- Insurance: It is not clear how useful this is, other than at an individual level to cover the cost of recovery. – for those who can afford this.

Design

- Adoption of good practice has a major part to play. This is partly about incorporating the right technologies and supporting policies and decoupling interim solutions so that they are replaceable. It is also about avoiding development from scratch and instead using proven solutions.
- International standards, or at least proven architectures, should be used wherever possible.
- It is important to avoid the use of unnecessarily weak mechanisms, such as unsecured email, for managing identity.

Transition

- Cleaning - a common failure in all attempts to improve standards is the unwillingness of organisations when moving to more secure systems to clean and verify its legacy information. A brilliant new system can be worth precisely **zero** if old user information is just dumped in there.

Paul Tanner 15th Jan 2007 ©Virtual-Techno.com