INFORMATION INTEGRITY SOLUTIONS

Trust and the Critical Role of User Centric ID Management

In the online context, trust is critical to e-commerce and e-government. Central to this is identity management. Most online organisations have been confronted in some way by the question of how to handle the risk of trusting end users and have addressed it by attempting to build a secure identity management system that allows an organisation to know it is talking to the right person.

The problem, with providing services over the internet is that the internet was designed without a system of digital identity.[1] The internet is mainly a protocol for connecting networks to each other to allow information exchange. It does not have a way of showing users who they are dealing with. This makes online service delivery an inherently risky business.

1. The dominant paradigm – one way trust

As a way of reducing identity fraud and providing better services governments and private sector organisations have been keen to ensure that they are talking to the right person. In order to do this they have been collecting more and more information about individuals with the UK "Privacy and Data Sharing"[2] and "Responsive Government: A New Service Agenda"[3] in Australia just a couple of examples of this strategy. While the organisation usually sees itself as inherently trustworthy in such circumstances it considers that it needs reasons to trust the individual.

However, access to and use of information collected for identity management, both for identification and authentication can be a point of contention. Organisations usually assess risk and manage such information from their own perspective. Such organisations often require individuals who want to use a service to submit their personal information before they can use it.

A simple example is the everyday "User Name and Password" sign on for accessing networks, bank accounts and many other services and entitlements. An organisation providing a service being accessed through a computer, asks the individual to make an assertion which is then authenticated, in this instance a name and a secret. But rarely does the organisation offer the same in return.

This one way trust approach suffers from at least three weaknesses.

The first is simply lack of common courtesy. The entity asking for the User Name and Password is basically indicating that it does not trust the other party, but is not recognising that the other party may have no more reason to trust the entity. The move towards stronger authentication, i.e. beyond simply asking for user name and password, will accentuate this.

The second is that it has created a security weakness that is now being very rapidly exploited. Lack of authentication by the entity to the individual, for example, is a significant component of 'phishing' whereby an individual is tricked into giving away such information as User Name and Password to an impostor or a fake website. The information is then used for such purposes as stealing money from the individual's bank account.

The third and possibly most fundamental weakness is the asymmetric sharing of control over personal information. Often this happens by requiring the individual to submit information over which it then loses control instead of the individual retaining the information and control over its release. This commonly leads to a corresponding asymmetry of risk allocation. This comes to light particularly when there is a failure of some sort, such as inadvertent or inappropriate accessing, disclosure or theft of personal information. In

---

1 "Microsoft's Vision for an Identity Meta-System: A Microsoft White Paper" available online at: www.identityblog.com/stories/2005/10/06/IdentityMetasystem.pdf

2 "Privacy and data-sharing: The way forward for public services", UK Cabinet Office, April 2002, online at: www.strategy.gov.uk/downloads/su/privacy/index.htm

3 "Responsive Government: A New Service Agenda" Australian Government Information Management Office, March 2006, online at: www.agimo.gov.au/government/e-government_strategy

such circumstances the individual is usually the party least able either to bear the risk or mitigate the risk, yet is also the party that bears a disproportionate share of the consequences. Consequences range from direct financial loss all the way through to extreme difficulty over a lifetime in re-establishing reputation and identity.

Severe consequences for e-commerce are coming to light as a result of these weaknesses. Especially in the USA, evidence is emerging that individuals are turning away from using the internet because lack of control over personal information is creating high levels of perceived risk.

Individuals may therefore be particularly sensitive to and lack trust in, strong identity management arrangements that do not work to create mutual trust and share control over information with the user.

There are many examples of the failure of these types of 'one way trust' identity management projects. The French government recently abandoned plans to introduce a more robust electronic ID card[4], as has the government of Taiwan.[5] The ID card proposals by the UK government have also been dogged by controversy for similar reasons.[6] Microsoft has acknowledged that passport.net failed for similar reasons.

2. The emerging paradigm – mutual trust or user centric identity management

A market response to the problems of one way trust is emerging. Businesses are finding that mutual trust is greatly facilitated by mutual authentication and shared control. This development is often referred to as user centric identity management. Organisations that have begun to develop user centric identity management in both the public and private sector include:

- Privacy and Identity Management for Europe (PRIME) - www.prime-project.eu
- The Higgins Project - www.eclipse.org/higgins
- Microsoft - www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf
- IBM Idemix - www.zurich.ibm.com/security/idemix
- Trustguide - www.trustguide.org.uk
- IIS - www.iispartners.com/trustcluster.pdf
- Lockstep - www.lockstep.com.au.

Commercial applications of this thinking are already emerging. For example, in a recent study for an Australian bank,[7] the move by a number of banks towards various forms of mutual authentication was obvious. Bank of America, for example, has begun trialling the Pass Mark program which includes the bank authenticating itself to the consumer by sharing back a shared secret in the form of a mutually agreed image that only both parties know. PKI based credentials also allow for mutual authentication.

The move towards user centric ID management is about to accelerate massively. Vista, the next release of Microsoft Windows, will incorporate a program called 'CardSpace'.[8] This is based on plans recently released by Microsoft for a digital identity meta-system based on the so-called "7 laws of identity". Microsoft is working with others to develop this thinking as an industry wide standard. This program enables individuals to easily manage, in the one place, the various personal authentication mechanisms that they may hold as users. IBM is developing Idemix which enables trusted transactions over the internet even though the parties remain pseudonymous.[9]

3. The way ahead

User centric identity management has moved from the realm of academics and privacy advocates to mainstream commerce. This is likely to have considerable impact on expectations that citizens have of governments and their approach to identity management.

---

4 "Launch of French e-ID card could be postponed", government News, 20 July 2005, online at: www.europa.eu.int/idabc/en/document/4476/194

5 "Taiwan Constitutional Court places fingerprinting plan on hold", Privacy International, 22 June 2005, online at: www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-249615

6 "ID Cards – UK's high tech scheme is high risk", London School of Economics News Release, 27 June 2005, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

7 "Report on Strong Authentication Initiatives By Banks In North America and Europe", completed by Glenbrook Partners LLC and Information Integrity Solutions Pty Ltd for Westpac Banking Corporation, October 2005; copy available for sale through IIS

8 For information about CardSpace see http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx

9 "Idemix: Pseudonymity for e-transactions", online at www.zurich.ibm.com/security/idemix