The Identity Metasystem: A User-Centric, Inclusive Web Authentication Solution

Position paper for the
W3C Workshop on Transparency and Usability of Web Authentication
New York City, March 2006

Michael B. Jones

Microsoft Corporation
One Microsoft Way, Building 42/4812
Redmond, WA 98052
USA

mbj@microsoft.com
http://research.microsoft.com/~mbj/

1. The Web's Problems are often Identity Problems

Many of the problems facing the Web today stem from the lack of a widely deployed, easily understood, secure identity solution. Microsoft's "InfoCard" project and the Identity Metasystem vision underlying it are aimed at filling this gap using technology that all can adopt and with solutions that all can endorse, putting users in control of their identity interactions on the Web.

A comparison between the brick-and-mortar world and the online world is illustrative: In the brick-and-mortar world you can tell when you are at a branch of your bank. It would be very difficult to set up a fake bank branch and convince people to do transactions there. But in today's online world it's trivial to set up a fake banking site (or PayPal, …) and convince a significant portion of the population that it's the real thing. *This is an identity problem.* Web sites currently don't have reliable ways of *identifying* themselves to people, enabling imposters to flourish. One goal of InfoCard is reliable site-to-user authentication, which aims to make it as difficult to produce counterfeit services on the online world as it is to produce them in the physical world.

Conversely, problems identifying users to sites also abound. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today's Web. Password reuse, insecure passwords, and poor password management practices open a world of attacks by themselves. Combine that with the password theft attacks enabled by counterfeit web sites and man-in-the-middle attacks and today's Web is an attacker's paradise.

The consequences of these problems are severe and growing. Last year the number of "phishing" sites was growing at over 1000% per year [Anti-Phishing 05]. Online banking activity is declining [Gartner 05]. The recent FFIEC guidance on authentication in online banking reports that "Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation" [FFIEC 05]. Consumer trust of the Web is low and dropping. The status quo is no longer a viable option.

2. "InfoCard" and the Identity Metasystem

The code-named "InfoCard" project at Microsoft is a joint effort with a diverse coalition of contributors across the computer industry to produce an authentication solution for the Web that can:

- be widely accepted,
- work in a broad range of identity contexts,
- utilize existing authentication technologies, including multiple factors,
- incorporate new authentication technologies as they are invented,

and possibly most importantly,

- enable users to simply and consistently make informed and positive authentication decisions on their own behalf.

The result of this effort is known as the Identity Metasystem [Microsoft 05a], an overview of which is contained in this section.

The Identity Metasystem is based upon a set of principles called the "Laws of Identity" [Cameron

05b]. The Laws are intended to codify a set of fundamental principles to which a universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet [Cameron 05a]. Taken together, the Laws define the architecture of the Identity Metasystem.

What do we mean by an "Identity Metasystem"? This concept is probably most easily introduced through an analogy.

Before 1982, the networking world was fragmented. If you wanted to write a network-enabled application you had to choose what network to write it for: Ethernet, Token Ring, ArcNet, X.25, etc. The invention of a Network Metasystem, the Internet Protocol (IP), changed all that. It made it possible to write networking applications that worked across networks without knowing the particulars of each network. It even enabled those applications to work with new networks that hadn't been invented yet, such as 802.11 wireless networks.

Digital identity is similarly fragmented today. If you want to write an identity-enabled application you have to choose which identity system to write it for, such as Kerberos, SAML, X.509, Liberty, custom username/password systems, etc. The Identity Metasystem is intended change all that, just like IP did for networking. It will make it possible to write identity-enabled applications that can work across multiple identity systems and can even use new identity systems as they are invented and connected to the Identity Metasystem.

This analogy holds true in another way. IP didn't compete with or replace the individual networks such as Ethernet — it *uses them*. Similarly, the Identity Metasystem doesn't compete with or replace individual identity technologies such as Kerberos, Liberty, X.509, SAML, etc. — it uses them. That's why it's called an identity ***metasystem*** — because it's a system of systems, tying individual identity systems into a larger interoperable metasystem. (See Law 5.)

3. Claims-Based Identities and InfoCards

In the Metasystem, digital identities consist of sets of claims made about the subject of the identity, where "claims" are pieces of information about the subject that the issuer asserts are valid. This parallels identities used in the real world. For example, the claims on a driver's license might include the issuing state, the driver's license number, name, address, sex, birth date, organ donor status, signature, and photograph, the types of vehicles the subject is eligible to drive, and restrictions on driving rights. The issuing state asserts that these claims are valid. The claims on a credit card might include the issuer's identity, the subject's name, the account number, the expiration date, the validation code, and a signature. The card issuer asserts that these claims are valid. The claims on a self-issued identity, where the identity provider and subject are one and the same entity, might include the subject's name, address, telephone number, and e-mail address, or perhaps just the knowledge of a secret. For self-issued identities, the subject asserts that these claims are valid.

Each of the user's digital identities used within the metasystem is represented by a visual "Information Card" in the client user interface. The user selects identities represented by "InfoCards" to authenticate to participating services. The cards themselves represent references to identity providers that are contacted to produce the needed claim data for an identity when requested, rather than claims data stored on the local machine. Only the claim values actually requested by the relying party are released, rather than all claims that the identity possesses. (See Law 2.)

4. Putting the User in Control

One of the fundamental tenets of the InfoCard work is that users must be in control of their identity interactions. (See Laws 1 & 2.) Among other things, this means that users must be given the choice of which identities to use at which services, they must know what information (which claims) will be disclosed to those services if they use them, and they must be informed how those services will use the information disclosed.

In the offline world, people carry multiple forms of identification in their wallets, such as driver's licenses or other government-issued identity cards, credit cards, and affinity cards such as frequent flyer cards. People control which card to use and how much information to reveal in any given situation.

Similarly, the Identity Metasystem makes it easier for users to stay safe and in control when accessing resources on the Internet. It lets users select from among a portfolio of their digital identities and use

them at Internet services of their choice where they are accepted. The metasystem enables identities provided by one identity system technology to be used within systems based on different technologies, provided an intermediary exists that understands both technologies and is willing and trusted to do the needed translations.

Part of being in control that's all too often overlooked is that to be in control, you must be able to understand the choices you're presented with. (See Laws 6 & 7.) Unless we can bring users into the identity solution as informed, functioning components of the solution, able to consistently make good choices on their own behalf, we won't have solved the problem.

Many identity attacks succeed because the user was fooled by something presented on the screen, not because of insecure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers — a channel that might extend thousands of miles — but in the two or three feet between the browser and the human who uses it. The Identity Metasystem, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the use of a consistent, comprehensible, and self-explanatory user interface for making those choices.

One key to securing the whole system is presenting an easy-to-learn, predictable user interface that looks and works the same no matter which underlying identity technologies are employed. Another key is making important information obvious — for instance, displaying the identity of the site you're authenticating to in a way that makes spoofing attempts apparent. Likewise, the user must be clearly informed which items of personal information relying parties are requesting, and for what purposes. This allows users to make informed choices about whether or not to disclose this information.

5. Authenticating Sites to Users

To prevent being fooled by counterfeit sites, there must be a reliable mechanism enabling users to distinguish between genuine sites and imposters. Our solution utilizes a new class of higher-value X.509 site certificates being developed jointly with VeriSign and other leading certificate authorities. These higher-value certificates differ from existing SSL certificates in several respects.

First, these certificates contain a digitally-signed bitmap of the company logo. This bitmap is displayed when the user is asked whether they want to enter into a relationship with the site or not, the first time that the site requests an InfoCard from the user.

Second, these certificates represent higher legal and fiduciary guarantees than standard certificates. In many cases, all that having a standard site certificate guarantees is that someone was once able to respond to e-mail sent to that site. In contrast, a higher-value certificate is the certificate authority saying, in effect, "we stake our reputation on the fact that this is a reputable merchant and they are who they claim to be".

Users can visit sites with these certificates with confidence and will be clearly warned when a site does not present a certificate of this caliber. Only after a site successfully authenticates itself to a user is the user asked to authenticate himself or herself to the site.

6. Authenticating Users to Sites

InfoCards have several key advantages over username/password credentials:

- Because no password is typed or sent, it can, by definition, not be stolen or forgotten.
- Because authentication is based on unique keys generated for every InfoCard/site pair (unless using a card explicitly designed to enable cross-site collaboration), the keys known by one site are useless for authentication at another, even for the same InfoCard.
- Because InfoCards can release claims to relying parties (for example, name, address, e-mail address, and/or whatever claims are appropriate for that kind of identity), that means that relying parties need not store this data between sessions. Retaining less data means that sites have fewer vulnerabilities. (See Law 2.)

7. Protocols Behind the Identity Metasystem

The Identity Metasystem is built on a small number of interoperable Web Services (WS-*) protocols. Specifically, the encapsulating protocol used for claims transformation within the Metasystem is WS-Trust. Format and claims negotiations between participants are conducted using WS-MetadataExchange and WS-SecurityPolicy (which is based on WS-

Policy). Finally, messages are secured using WS-Security.

These protocols enable building a platform-independent Identity Metasystem and form its "backplane". Like other Web services protocols, they also allow new kinds of identities and technologies to be incorporated and utilized as they are developed and adopted by the industry.

To foster the interoperability necessary for broad adoption, the specifications for these (and other) WS-* protocols are published and are freely available, have been or will be submitted to open standards bodies, and allow implementations to be developed royalty-free.

Deployments of existing identity technologies can be leveraged in the metasystem by implementing support for the small number of WS-* protocols above. Examples of technologies that could be utilized via the metasystem include LDAP claims schemas; X.509, which is used in Smartcards; Kerberos, which is used in Active Directory and some UNIX environments; and SAML, a standard used in inter-corporate federation scenarios.

8. Status and Plans

Microsoft has been actively working with innovators and industry players since 2004 developing the principles behind the Identity Metasystem and developing interoperable implementations. For instance, in May 2005, we demonstrated interoperation with an open source Java identity provider written by Ping Identity [PingID 05]. Implementation guides [Microsoft 05b] have been published enabling (and encouraging) people on non-Windows platforms to build interoperable Identity Metasystem implementations. Several beta versions of Microsoft's implementations have been released [Microsoft 05b], with more to come.

Microsoft recognizes that, for the Identity Metasystem to succeed, that it must be widely adopted, including on non-Windows platforms and by non-Microsoft browsers and web servers. We are heartened by the widespread recognition that, while Microsoft may be competing with other platforms and others' software offerings, we all share a common interest in seeing a viable, ubiquitous Web authentication solution deployed.

Microsoft will be shipping its "InfoCard" client implementation as part of WinFX [Microsoft 06] — a set of managed APIs that will be available on all of Windows Vista, Windows XP, and Windows Server 2003. WinFX will ship at the same time as Windows Vista.

While we are not at liberty to disclose others' implementation plans, we are excited at the possibilities of implementations on non-Microsoft platforms as well. Stay tuned for future developments!

9. Conclusions

Many of the problems on the Internet today, from phishing attacks to inconsistent user experiences, stem from the patchwork nature of digital identity solutions that software makers have built in the absence of a unifying and architected system of digital identity. The Identity Metasystem, as defined by the Laws of Identity, would supply a unifying fabric of digital identity, utilizing existing and future identity systems, providing interoperability between them, and enabling the creation of a consistent and straightforward user interface to them all. Basing our efforts on the Laws of Identity, Microsoft is working with others in the industry to build the Identity Metasystem using published WS-* protocols that render Microsoft's implementations fully interoperable with those produced by others.

We believe that many of the dangers, complications, annoyances, and uncertainties of today's online experiences can be a thing of the past. Widespread deployment of the Identity Metasystem has the potential to solve many of these problems, benefiting everyone and accelerating the long-term growth of the Internet by making the online world safer, more trustworthy, and easier to use. Microsoft is working with others in the industry to define and deploy the Identity Metasystem. We hope that you will join us!

References

[Anti-Phishing 05] Anti-Phishing Working Group. *Phishing Activity Trends Report*, February 2005. http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf.

[Cameron 05a] Kim Cameron. *Kim Cameron's Identity Weblog*, May 2005. http://www.identityblog.com/.

[Cameron 05b] Kim Cameron. *The Laws of Identity*. Microsoft Whitepaper, May 2005. http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/lawsofidentity.asp.

[FFIEC 05] Federal Financial Institutions Examination Council. *Authentication in an Internet Banking Environment*, October 2005. http://www.ffiec.gov/press/pr101205.htm and http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[Gartner 05] Gartner. *Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce*, June 2005. http://www.gartner.com/press_releases/asset_129754_11.html.

[Microsoft 05a] Microsoft. *Microsoft's Vision for an Identity Metasystem*. Microsoft Whitepaper, May 2005. http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/identitymetasystem.asp.

[Microsoft 05b] Microsoft. *Windows Vista Developer Center: InfoCard.* http://msdn.microsoft.com/windowsvista/building/infocard/.

[Microsoft 06] Microsoft. *WinFX Developer Center*, January 2006. http://msdn.microsoft.com/winfx/.

[PingID 05] Ping Identity. *SourceID InfoCard STS Toolkit for Java*, August 2005. http://www.sourceid.org/projects/infocards/.