Distributed Identification and Consumer Data Protection

Khaja Ahmed – Microsoft Corporation
Threats to Online Safety

- Consumer privacy has steadily declined as internet use grew over the years
- Greater use and greater value attract professional international criminal fringe
  - Exploit weaknesses in patchwork
  - Phishing and pharming at 1000% CAGR
- Identity theft is approaching crisis proportion
- …
There are no simple solutions!

A Holistic approach requiring commitment from all the key players is necessary
Each Must Play a Part

- Thought leaders and Consumer Advocates
- Industry
- Standards Bodies
- Governments
- Relevant NGOs and Quasi-Governmental bodies
- The consumers have already spoken – they want privacy
A PLOT to Protect Consumer Data

- Policies need to be respectful of consumer privacy needs
- Legal framework needs to be conducive to privacy
- Operational practices must evolve to defend and enhance privacy
- Technological solutions must be developed and adopted
Microsoft’s Efforts
The Roles of Microsoft

- Industry leader
- Developer of, Contributor to and Driver of Standards
- Software Product Provider – OS and applications
- Online service provider – MSN & Live ID
The Roles

- Industry leader
  - Thought Leadership
  - Identity Metasystem and the 7 Laws of Identity
- Develop, Contribute to and Drive Standards
  - Drive the right standards
  - The WS* suite
- Software Product Provider – OS and applications
  - The right technology and development practices
  - Windows Vista security features
- Online service provider – MSN & Live ID
  - The right operational practices and technology
  - Information Security Program
What is a Digital Identity?

- Set of *claims* one subject makes about another
- Many identities for many uses
- Required for transactions in real world and online
- Model on which all modern access technology is based
The Laws of Identity
Established through Industry Dialog

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com
Identity Metasystem

- We need a unifying “Identity metasystem”
  - Protect applications from identity complexities
  - Allow digital identity to be loosely coupled: multiple operators, technologies, and implementations
- Not first time we’ve seen this in computing
  - Emergence of TCP/IP unified Ethernet, Token Ring, Frame Relay, X.25, even the not-yet-invented wireless protocols
Identity Roles

Identity Providers
Issue identities

Relying Parties
Require identities

Subjects
Individuals and other entities about whom claims are made
CardSpace ("InfoCard")

- Self-Issued
  - Contains self-asserted claims about me
  - Stored locally
  - Effective replacement for username/password
  - Eliminates shared secrets
  - Easier than passwords

- Managed
  - Provided by banks, stores, government, clubs, etc.
  - Cards contain metadata only!
  - Claims stored at Identity Provider and sent only when card submitted
CardSpace Experience

Choose a card to send to: www.identityblog.com

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Cards you've sent to this site:

- Minimal InfoCard

Your other cards:

- Anonymous Card
- Full Information Card
- Kerberos AD Card
- Managed InfoCard

To send this card now, click Send. To review the data before you send it, click Preview.
Empowers the User…

Applications
Existing & New

Technologies
X509, Kerberos, SAML

Governments

Devices
PCs, Mobile, Phone

Organizations

You

Individuals
Work & Consumer

Private Businesses
CardSpace Overview

- Simple user abstraction for digital identity
  - For managing collections of claims
  - For managing keys for sign-in and other uses
- Grounded in real-world metaphor of physical cards
  - Government ID card, driver’s license, credit card, membership card, etc…
  - Self-issued cards signed by user
  - Managed cards signed by external authority
- Shipped as part of .NET 3.0
  - Runs on Windows Vista, XP, and Server 2003
- Implemented as protected subsystem
Protocol Drill Down

1. Client wants to access a resource
2. RP provides identity requirements
3. Which IPs can satisfy requirements?
4. User selects an IP
5. Request security token
6. Return security token based on RP’s requirements
7. User approves release of token
8. Token released to RP

Identity Provider (IP)

Relying Party (RP)
Implementation Properties

- Cards represent references to identity providers
  - Cards have:
    - Address of identity provider
    - Names of claims
    - Required credential
  - Not claim values

- Information Card data not visible to applications
  - Stored in files encrypted under system key
  - User interface runs on separate desktop

- Simple self-issue identity provider
  - Stores name, address, email, telephone, age, gender
  - No high value information
  - User must opt-in
An Identity Metasystem Architecture

- Microsoft worked with industry to develop protocols that enable an identity metasystem: WS-* Web Services
  - Encapsulating protocol and claims transformation: WS-Trust
  - Negotiation: WS-MetadataExchange and WS-SecurityPolicy
- Only technology we know of specifically designed to satisfy requirements of an identity metasystem
Uses Existing Technologies

- Managed Card Authentication Methods
  - X.509 Certificate
  - Kerberos Ticket
  - Self-Issued Information Card
  - Username/Password

- Managed Card Token Type
  - Can be anything (including SAML, X.509, …)

- Self-Issued Card Token Type
  - SAML

- Self-Issued Card Schema
  - Uses LDAP element names
Components Microsoft is Building

- CardSpace identity selector
  - Component of .NET 3.0, usable by any application
  - Hardened against tampering, spoofing
- CardSpace simple self-issued identity provider
  - Self-issued identity for individuals running on PCs
  - Uses strong public key-based authentication – user does not disclose passwords to relying parties
- ADFS V2 managed identity provider
  - Plug Active Directory and other identities into the metasystem
  - Full set of policy controls to manage use of simple identities and Active Directory identities
- Windows Communication Foundation for building distributed applications and implementing relying party services
Not just a Microsoft thing…

- Based entirely on open protocols
- Identity *requires cooperation* – and it’s happening…

- Interoperable software being built by
  - Sun, IBM, Novell, Ping Identity, BMC, …
  - For UNIX/Linux, MacOS, mobile devices, …

- With browser support under way for
  - Firefox, Safari, …

- Unprecedented things happening
  - Microsoft part of JavaOne opening keynote
  - Joint Information Card demos with IBM, Novell
By Doc Searls
- Linux Journal Editor
- Author of the “cluetrain manifesto”

Introducing “The Identity Metasystem”
Can Microsoft Save the Net?

By Lawrence Lessig

A new system would replace today's hodgepodge of security measures.

We celebrate the brilliance of the Internet — and in particular, its end-to-end open design — but we ignore the vulnerabilities that increasingly infect it. The Net was built on trust, and it lacks an adequate mechanism to prevent fraud. Then, it's no surprise that phishing and identity theft are so rife. The result is a muckrake hodgepodge of security measures that are too easy to evade.

Today, the Internet is facing an unprecedented surge in online fraud and identity theft. 

Yet the solution is not only right, it could be the most important contribution to Internet security since cryptography.
Microsoft Open Specification Promise (OSP)

- Perpetual legal promise that Microsoft will never bring legal action against anyone for using the protocols listed
  - Includes all the protocols underlying CardSpace
- Issued September 2006

http://www.microsoft.com/interop/osp/
WS* Standards

- Developed cooperatively by industry partners
- Submitted to standards bodies (OASIS) and adopted
- Interoperable implementations from multiple parties exist
SDL

- A major step towards more secure software
  - Now recognized as an industry leading best practice
- SDL tools being made available to third parties
- Tools, Training, Development Methodology and Corporate Commitment
Information Security Program

- MSN has an ISP that provides for:
  - Data Classification into MBI, HBI, LBI
  - Different and appropriate handling and security measures are applied
  - Separation of duties and restricted access policies mitigate risk of administrator abuse
(Backup Slides)