CardSpace and the Identity Metasystem

Threats to Online Safety

- The Internet was built without a way to know who and what you are connecting to
  - Internet services have one-off “workarounds”
  - Inadvertently taught people to be phished
- Greater use and greater value attract professional international criminal fringe
  - Exploit weaknesses in patchwork
  - Phishing and pharming at 1000% CAGR
- Internet missing an “Identity layer”
  - No simplistic solution is realistic

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

Lessons from Passport

- Passport designed to solve two problems
  - Identity provider for MSN
    - 300M+ users, 1 billion logons per day
  - Identity provider for the Internet
    - Unsuccessful
- Learning: solution must be different than Passport

Microsoft Passport

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

CardSpace ("InfoCard")

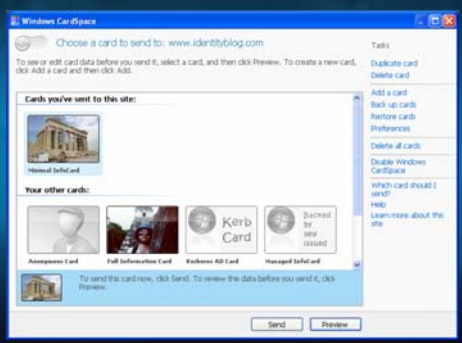
SELF - ISSUED

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

MANAGED

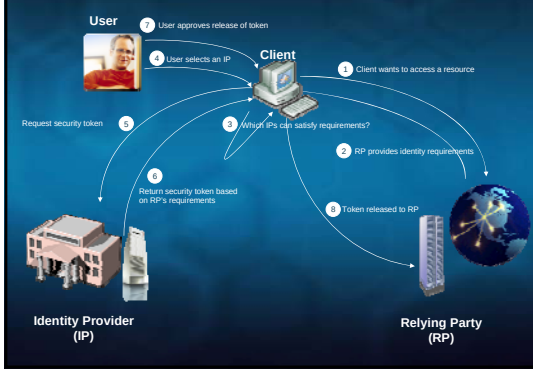
- Provided by banks, stores, government, clubs, etc.
- Cards contain metadata only!
- Claims stored at Identity Provider and sent only when card submitted

CardSpace Experience



Empowers the User…

Protocol Drill Down



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

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

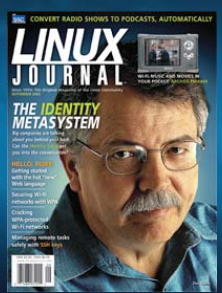
Components Microsoft is Building

- 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
- Active Directory managed identity provider
  - Plug Active Directory users 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

LINUX Journal Sep '05 Cover



- By Doc Searls
- Linux Journal Editor
- Author of the "cluetrain manifesto"
- Introducing "The Identity Metasystem"

WIRED Magazine - Mar '06

- By Lawrence Lessig
- Influential Internet & Public Policy Lawyer
- Special Master in antitrust case against Microsoft
- Quotation:

> 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/

For More Information

- Visit http://cardspace.netfx3.com/

- Whitepapers
- Documentation
- Code and samples

- Mike Jones – mbj@microsoft.com
- Steven Woodward – stwood@microsoft.com