Jeffrey Friedberg
Chief Trust Architect
Microsoft Corporation

Microsoft Research
Faculty Summit 2010
Delivering End to End Trust
Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable

Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready

Commitment to customer-centric Interoperability
- Technology Accessibility
- Recognized industry leader, world-class partner
- Open, transparent
Path to End to End Trust

- 2002: Security Development Lifecycle
- 2005: Privacy Standard and Process
- 2006: Internet Battlefield, Identity Theft Analysis
- 2007: Trust User Experience (TUX) Team
- 2008: E2E Trust White Paper
- 2008: E2E Trust Team
- 2009: E2E Trust Roadmaps
• Many believe need better security, privacy
• Greater connectivity and valuable targets lead to new threats and greater cybercrime
• Criminals anonymous and untraceable

• Need greater accountability
• Need to know who is who
• Need to have a trust framework
End to End Trust White Paper

- Conceptual vs. operational
- Who does what when?
- Apply standard PM techniques
- Create a roadmap
Roadmap Goals

- Help stakeholders see the “big picture”
  - Demystify, make it easy to see their piece
  - Analyze dependencies, critical paths
  - Highlight long poles like new standards, laws
  - Spot common building blocks across initiatives
  - Collaborate on implementation strategy

- Make insightful “calls to action”
  - Inspire and enable

- Track progress
  - Map activity, show trajectory
Start with a big play that has big impact for ecosystem

Identify high level wish list by stakeholder

Craft scenarios that embody the vision

Layout key building blocks by owner over time with dependencies

Online Health Care ...

Patient, provider, payer, regulator, researcher ...

Mary is traveling, feels sick ...

In person proofing, safe harbor, audit data standards ...
“SPICIER” Scenarios

- Tell a **STORY**
- **PERSONAL** details
- **IMPLEMENTATION FREE**
- **CUSTOMER** voice
- Deep **INSIGHT**
- User **EMOTIONS** and **ENVIRONMENT**
- Real **RESEARCH**
Example: Remote Care

- Annie from Ontario is visiting her aunt in Saskatoon for the first time
- She develops throat pain and difficulty swallowing
- She is relieved to find a local walk-in clinic but they have no records for her
- Annie gives the doctor permission to see her online records just for this visit
- The doctor is able to access her records from his own computer
- Based on her history and allergies, the doctor confidently prescribes an appropriate medication
- Annie stops by the pharmacy, takes the medication, and starts feeling better
Key Initiatives

- Enable online health care
  - Manage privacy risks
- Enable eCommerce
  - Reduce online fraud
- Protect critical infrastructure
  - Preserve personal freedoms
- Enable secure online collaboration
  - Manage distrust between parties
Trans-global Secure Collaboration Program (TSCP)

Unique Requirements
- Policy based, cross org, cross platform
- Fine grain access control
• Jim is able to securely collaborate and share sensitive project data
• With partners in multiple organizations
• Based on a common project taxonomy
• Regardless of the application being used
Building Blocks for Scenario

Identity Claims

Universal Policy Based Access

Machine Health Claims
Identity Claims: Projects

Step 1: In Progress
- Establish company for issuing and consuming minimum disclosure claims
  - Develop specifications for minimum disclosure claims
  - Custom code running on Windows provides minimum disclosure claims services (e.g., for access to sensitive project documents)
  - Windows OS natively enables minimum disclosure claims access decisions for enabling sensitive data access and records-related audit events

Step 2: Existing sites (SharePoint, Office, Exchange, AutoCAD)
- Minimal disclosure claims enabled
  - Apply claims-based access to sensitive data

Step 3: Accelerator
- Applications become unified and consistent policy enforcement points for access policies

Scenario
- Deploy policy decisions that enforce policies and claims
  - Policy enforcement begins (e.g., access
  - Enforce minimum disclosure claims

Class of client and/or server side code (partners) to enable legacy access to be claims aware

Existing and new regulations requiring usage of varying levels of identity and access

July 12, 2010
Microsoft Corporation
Identity Claims: Standards Example

Creation & adoption of interop and open standards for issuing and consuming minimum disclosure claims

**Step 1:**
- Submit U-Prove to standard bodies (e.g., NIST)
- Engage with ecosystem partners to enable solutions for minimum disclosure claims tokens

**Step 2:**
- Submit POC solutions with partners for industry standards adoption
Universal Policy: Standards Challenge

Step 1: Stalled
- Identify pros and cons for policy definition languages (XACML, industry standard, SAML and XRML)
- Identify and submit needed changes to industry standard XACML to incorporate TSCP requirements
- Launch efforts to standardize Microsoft groups around one policy definition language (SAML vs XRML)

Step 2:
- Alternatives to XACML with a Microsoft and/or industry solution that has the right architecture to satisfy high level requirements for secure collaboration across v-orgs
- Work with the ecosystem partners to create/enhance standards for common policy definition language
Roadmap: Financial
High Value Internet Transactions

Building Blocks

Scenarios

Dream States

July 12, 2010
Microsoft Corporation
"Building Block" Families

- System and Device Health
- Digital Identity, Claims-based AuthN and AuthZ
- Rule Based Data Access
- Reputation Services
- Verification (post-transactional, aka Audit)
- Trusted User Experience (TUX)
- Assurance and Integrity
Trust User Experience (TUX)

• TUX is when you are put in the hot seat and need to make trust decision
  • Is this really your bank site
  • Is it OK to click on a link in your email
  • Is it safe to install new software?
  • Should I share my data?
  • How do I set the right permissions?
• Creating great TUX is hard and essential
• Must consider UI, underlying architecture, and user’s mental model
Name is different, is that OK?

Has a “lock” but need to inspect – *bad guy can get one too!*
Have to click here to learn what checking was done – no standard!

Can click here to see additional information - *but it won’t indicate which fields were verified by CA*

Name of site, not organization

Should I trust this CA?

Not branded
Which field lists organization and location?
And Dig Some More ...

Need to click on “Subject” to learn details like organization or location.
Better Mutual Authentication
What About Visual Secrets?

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey also shows you that it's safe to enter your Passcode and click the Sign In button.

An asterisk (*) indicates a required field.

Your SiteKey:

Coffee

If you don't recognize your personalized SiteKey, don't enter your Passcode.

Passcode: [masked]

[Sign In]
Ignored by Almost All – 92%!

Bank of America Higher Standards

Confirm that your SiteKey is correct

If you recognize your Sitekey, you'll know for sure that you are at the valid Bank of America site. Confirming your Sitekey is also a way you’ll know that it’s safe to enter your Passcode and click the Sign In button.

An asterisk (*) indicates a required field.

SiteKey Maintenance Notice:

Bank of America is currently upgrading our award winning Sitekey feature. Please contact customer service if your Sitekey does not reappear within the next 24 hours.

* Passcode:

(4 - 20 Characters, case sensitive)

Sign In

Forgot your Sitekey?

Incorrect Sitekey showing?
TUX Vision

• Consumers
  • Safer, more confident
  • Not distracted from enjoying digital lifestyle

• Businesses
  • Better able to connect with customers, partners, and other businesses
  • Can honor trust promises, reduce breaches, and protect and build their brand
TUX Research Areas

• Authentication
  • Secret questions (IEEE Symposium on S&P 08)
  • Social Auth (CHI09)
  • Backup Auth Configuration (SOUPS09)

• End-user warning/consent
  • Application Authorization (submitted to CHI10)

• Access-control management
  • Laissez-faire file sharing (NSPW09)
  • Expandable Grid
  • Advanced Permissioning Experience
Access Control – Status Quo

- Use ACL Editor
- Really hard if groups and deny rules in play
- 19 screens!
1. Click “Advanced”

2. Click “Effective Permissions”

3. Select User

4. View Effective Permissions
Bring up Computer Management interface

Click on “Users”

Double-click Jana

Click “Member Of”

Read group membership

TAs 2006

TAs 2007
Click on TAs 2006

Inspect Group Permissions

Click on TAs 2006

Read permissions for TAs 2006

Click on TAs 2007

Read permissions for TAs 2007
Click on TAs 2006

Change permissions for TAs 2006
16. Click "Advanced"

17. Click "Effective Permissions"

18. Select Jana

19. View Effective Permissions
Challenges with ACL

• Key information is distributed
• Easy to make silly mistakes
• Need a way to directly check and manage permissions
Expandable Grid

Legend
Read
- Allow
- Deny
Some access allowed

Subgrid shows:
- Read
- Write
- Execute
- Delete

Music 101
Admin
- calendar.scv
- gradebook.xls
- syllabus.doc
Handouts
Lecture Notes

Showing result 1 of 1
Prev Next
<table>
<thead>
<tr>
<th>Task type</th>
<th>Small-size</th>
<th></th>
<th>Large-size</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accuracy</td>
<td>Time</td>
<td>Accuracy</td>
<td>Time</td>
</tr>
<tr>
<td>View simple</td>
<td>89%</td>
<td>29s</td>
<td>61%</td>
<td>61%</td>
</tr>
<tr>
<td>View complex</td>
<td>94%</td>
<td>35s</td>
<td>72%</td>
<td>39s</td>
</tr>
<tr>
<td>Change simple</td>
<td>61%</td>
<td>50s</td>
<td>Insufficient data</td>
<td>67%</td>
</tr>
<tr>
<td>Change complex</td>
<td>89%</td>
<td>39s</td>
<td>72%</td>
<td>103s</td>
</tr>
<tr>
<td>Compare groups</td>
<td>67%</td>
<td>55s</td>
<td>72%</td>
<td>104s</td>
</tr>
<tr>
<td>Conflict simple</td>
<td>89%</td>
<td>29s</td>
<td>Insufficient data</td>
<td>100%</td>
</tr>
<tr>
<td>Conflict complex</td>
<td>100%</td>
<td>20s</td>
<td>74%</td>
<td>105s</td>
</tr>
<tr>
<td>Memogate simulation</td>
<td>89%</td>
<td>42s</td>
<td>78%</td>
<td>71s</td>
</tr>
<tr>
<td>Precedence rule test</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Secret questions
(IEEE Symposium on Security and Privacy 2009)

<table>
<thead>
<tr>
<th>Fact-based questions</th>
<th>Statistically</th>
<th>Guessed by untrusted partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grandfather’s occupation</td>
<td>18%</td>
<td>32%</td>
</tr>
<tr>
<td>Favorite historical person</td>
<td>17%</td>
<td>35%</td>
</tr>
<tr>
<td>Mother’s birthplace</td>
<td>17%</td>
<td>14%</td>
</tr>
<tr>
<td>What is your father’s middle name?</td>
<td>12%</td>
<td>5%</td>
</tr>
<tr>
<td>What was your first phone number?</td>
<td>5%</td>
<td>17%</td>
</tr>
<tr>
<td>What was the name of your first school?</td>
<td>8%</td>
<td>9%</td>
</tr>
<tr>
<td>Where was your first job?</td>
<td>13%</td>
<td>21%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preference-based questions</th>
<th>Statistically</th>
<th>Guessed by untrusted partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best childhood friend</td>
<td>11%</td>
<td>18%</td>
</tr>
<tr>
<td>Favorite teacher</td>
<td>4%</td>
<td>21%</td>
</tr>
<tr>
<td>What is your favorite restaurant?</td>
<td>7%</td>
<td>25%</td>
</tr>
<tr>
<td>Who is your favorite singer?</td>
<td>8%</td>
<td>15%</td>
</tr>
</tbody>
</table>
Warnings – Latest Thinking

- No TUX is good TUX
- If you have to warn, be safe by default and don’t interrupt
- If you have to interrupt, give users realistic steps they can follow
Open Questions

• Does an interruptive warning, when well-written and actionable, actually help users avoid attacks?
• What can we realistically ask users to decide?
• When should we warn versus just take action?

• What is the sweet spot for “informed consent” and how do we get there?
• How do we facilitate minimal disclosure?
Want to Learn More?

• End to End Trust
  • [http://www.microsoft.com/endtoendtrust](http://www.microsoft.com/endtoendtrust)

• Symposium on Usable Privacy and Security (SOUPS)
  • At the Microsoft commons 7/14-7/16

• Jeff’s Email Address
  • [Jeffreyf@microsoft.com](mailto:Jeffreyf@microsoft.com)