Toward a Scalable Approach to Privacy and Security
Toward a Scalable Approach to Privacy and Security

Contents

• Internet Identity Today
• NSTIC
  • Governance
  • Pilots
• Scalable Privacy
  • MFA and the Cohortium
  • Privacy Management
  • Anonymous Credentials
• Where We’re Headed
  • The Attribute Ecosystem
• How to Get Involved and Stay Informed
Internet Identity Today

- Social identity, at least in the US, is reaching saturation, close to 100%
  - Emphasis is shifting to mining data for cross purposes, third party auth
  - Protocol may be evolving from OpenId to OpenId Connect
  - OAuth to handle all the non-web and mobile apps
  - Continued efforts to climb LOA stack with MFA
- Federated identity continues to grow and dominate inter-organizational interactions
  - Other verticals building multi-lateral federations now
  - Interfederation is moving forward, slowly but steadily...
- Hybrids grow
  - Social2SAML and SAML2Social Gateways
  - New aggregators, e.g. PingOne
Government Efforts

- **FICAM**
  - Classic identity services for government
  - Steadily growing, successful
  - Includes PIV cards and PKI, federated identity, etc.
  - Provides the LOA certifications that motivates the InCommon assurance program, including Silver

- **NSTIC**
  - Aimed at Next Gen – services, privacy, etc.
  - Has distinct governance and pilots efforts
  - Applicable more broadly than just US Gov services
NSTIC

- National Strategy for Trusted Identities in Cyberspace – major White House Initiative on citizen-gov security/privacy
- Scoping is a finesse: affecting government identity interactions (along with FICAM), influencing a commercial marketplace, influencing a global identity ecosystem
- Has both governance and development components
- OMB Directive issued Fall of 2011 to move to external identities where appropriate
- [www.nist.gov/nstic](http://www.nist.gov/nstic)
- Faces challenges with limited resources, ambiguities in scope, the Facebook ToS, existing business models, etc.
- The vision works for R&E needs…
  - A placemat from an Ethiopian restaurant in 2001
NSTIC Governance

• Intended to define the rules for electronic identity transactions, at least with the federal government, but more broadly as anchor tenant for the general marketplace
  – Privacy, security, robustness, usability, standards, etc.
• Most of the big players, across identity providers, relying parties, state and local governments, businesses from start-ups to Mastercard and Microsoft to ACLU, EFF, CDT, etc.
• Had to navigate public-private partnership, NPO status, IPR, elections, etc.
• Wrapped around axles of role, authority, processes for a long time; now moving a bit into substance.
• www.idecosystem.org
NSTIC Pilots

• Grants to develop aspects of the Identity Ecosystem – from privacy to monetization, from government to business, from hardware approaches to citizen use…
• Five grants awarded in September 2012
  – http://gcn.com/Articles/2012/12/19/5-elements-identity-ecosystem.aspx?Page=1
• Very different world views represented
• Scalable Privacy award to Internet2/InCommon
NSTIC Pilots – Round 1

• A variety of efforts, some highly experimental business models, some foundational infrastructure. Most are private partnerships, with limited visibility into their efforts

• Third-party ID verification that uses drivers' licenses and state motor vehicle departments for authentication.

• *Commercial, open-source ID verification network that allows multiple relying parties to verify a user’s identity by referring to the authoritative sources.

• Multi-factor mobile authentication that uses varying levels of trust from PINs to geolocation.

• Data encryption with broker verification that enables access to personally identifiable information.

• **Scalable privacy - https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy+Home
“Monetization of attributes” pilot

- Commercial, open-source ID verification network
- Criterion/ID Dataweb are the leads
- Move from bulk verification (e.g. credit reports from Experien, Equifax, etc) to per-attribute verification
- Operate an auction marketplace for verifiers to post their prices and terms
- Access, by businesses, is open source; operating the auction is proprietary
- Raises interesting issues, from privacy and consent to strength and methods of verification to ...
- We are a year 2 of this pilot, verifying “studentness” and perhaps others
CSDII/AAMVA Pilot

- Partnership of AAMVA (American Association of Motor Vehicle Departments), Microsoft, and a few others
- Remarkable parallels, in a different context, to our world
  - Use of anonymous credentials for unobservability
  - Multi-lateral federation
  - Citizen-centric use cases
- MS as a major IdP, as an RP, as a technology provider
Scalable Privacy

• Two year grant (second year pending) to Internet2/InCommon
• Development partners are CMU, Brown, with expertise from Wisconsin, Ohio State and others
• Several focal points
  – Promotion of multi-factor authentication
  – Introduction of anonymous credentials
  – Development and deployment of privacy managers
  – Citizen-centric attributes and schema
• https://spaces.internet2.edu/displaySCALEPRIV/Scalable+Privacy+Home
Key deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Citizen-centric attribute activities
  - For transactions, for accessibility, for social government
- Trusted metadata
  - About the relying party and the IdP
  - Vetted by the federation and by third-parties
- Anonymous credentials
  - Integrated at key junctions into the ecosystem, leveraging existing infrastructure
  - In software, use of metadata, and user experience
- Pushing policy issues
- Pilots and cohortium
How it all fits together

• A user, in their context as a university student, uses a privacy manager to release their institutional affiliation to student discount services
• A user, in their context as a citizen, uses a privacy manager to release sufficient residence information that allows them to then anonymously post to the neighborhood-only wiki.
• A user, in their context as a consumer, uses a privacy manager to manage the release of preferences (e.g. zip code, preferred language, geolocation, etc) to customize commercial services while preserving privacy
• With your paper diploma and your identity-rich e-transcript, you get issued an anonymous token asserting affirmation of graduation and degree, year, honors, major
• A user, in their context as a worker, uses a privacy manager to release anonymous credentials (such as security clearances and personal medical information) to third party contractors.
• A parent uses a privacy manager to manage their children’s on-line privileges to COPPA-compliant applications
Promotion of multi-factor authentication (MFA)

- Good privacy begins with good security
- MFA addresses a significant number of security threats
- A variety of second factor alternatives are now viable – USB devices, NFC devices, cell phones, certificates, etc., and technology can bridge across them
- Advantages of MFA and Federated identity
  - Combining MFA with WebSSO and federated identity allows MFA to be leveraged by many services/SPs
  - If biometric factors are used, “privacy spillage” limited to IdP
  - Potential to help achieve higher levels of assurance
MFA: Two major thrusts

- MFA Pilot Institutions: support wide-scale deployments of MFA technologies at three institutions:
  - Massachusetts Institute of Technology (MIT)
  - University of Texas System
  - University of Utah

- MFA Cohortium: Create and facilitate a cohort of additional institutions, establishing a collaborative environment for sharing questions, requirements, planning, expertise, experience, artifacts, etc. related to deploying and supporting MFA, leveraging the pilot institution activities.
The MFA Pilot Institutions

- Massachusetts Institute of Technology, University of Texas System, University of Utah
- Project funds Duo licenses for wide-scale deployment
- Diverse environments, services, planning approaches, deployment approaches, etc.
- Pilot deployment plans include a focus on integration of MFA into federated identity and SSO environments (Shibboleth IdP, CAS).
- The outcome of this work will be documents and possible presentations of deployment experiences for the solutions utilized.
Expected MFA Pilot Outcomes

- Support for flexible MFA integration with the Shibboleth IdP and CAS
- Sample/example application risk assessment process; i.e. which services should require MFA?
- Planning documents
- End-user experience
- Observed risks
- Performance impacts and scalability
- Lessons learned
- Issues specific to the use of MFA within an identity federation
- Recommendations for future deployments by other institutions
The MFA Cohortium

• A focused and facilitated initiative to help scores of institutions move along with multifactor authentication
• Experiences and artifacts from pilot institutions will provide one key source of input into the Cohortium
• Comprehensive approach
  – Technology and Policy
  – Deployment and Maintenance
• Large scale but finite length initiative (15 month)
• MFA technology agnostic
• Can leverage Net+ security service offerings as appropriate
The MFA Cohortium (continued)

• Collect and create extensive set of resources and artifacts on “all things MFA planning and deployment” for Higher Ed
  – Plans, ROI, Rollout Strategies, etc.
  – Critical code contributions (e.g. Shib and CAS login handlers, InCert)
• Build public web site to serve as lasting (and hopefully living) resource site
Citizen-centric attribute deliverables

- Schema Catalog and Attribute Registry
- Attribute annotated Use-Cases
- Cookbook “To Serve Citizens” 😊
- GPII Proof of concept
- Bindings and refactoring
- Engagement with the privacy manager
Categories of use cases

• Accessibility
  – Physical, cognitive, age-related, etc.
  – Global Publicly Inclusive Internet (gpii.net)
• Operational Government
  – Transaction based
  – May be out of scope
• “Social Government”
  – Community wikis, on-line discussions, news feeds, etc
  – Generally local in nature, often requiring anonymous but attribute-controlled access (e.g. resident, registered voter, over legal age, etc.)
• Envision It Scenarios
  – Contained in Full NSTIC Strategy (April 2011)
• UMA developed
• IdeSG provided – see
The purpose of the Global Public Inclusive Infrastructure (GPII) is to ensure that everyone who faces accessibility barriers due to disability, literacy, digital literacy, or aging, regardless of economic resources, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety.

- Automatic personalization of user interfaces and user context adaptation based on user preferences, across platforms.
- Schema standard is (ISO/IEC JTC1 24751).
- gpii.net.
- Proof of concept will establish user preferences stored in an authorization server being used with open credentials to adaptively present content.
Privacy managers  (Carnegie-Mellon Univ)

• Consoles to help users manage the release of attributes
• Can leverage trust, informed consent, default settings and preferences, etc.
• Must be carefully engineered
  – Across the variety of contexts
  – Across a variety of credential types
  – In ways that are user-effective
• Similar, less leveraged approaches are successfully deployed in a few settings.
Key design considerations

- Usability
- CMU Tech Report, Warning Design Guidelines, Bauer et al
- Informed consent
- GPII
- MFA
- Awareness of out-of-band considerations
- Minimal disclosure for constrained purpose
Anonymity, unlinkability, and unobservability

• **Anonymity** assures that public data cannot be related to the owner.

• **Unlinkability** assures that two or more related events in an information processing system cannot be related to each other.
  – Untraceability assures that two or more events at autonomous systems by the same user cannot be correlated

• **Unobservability** assures that an observer is unable to identify or infer the identities of the parties involved in a transaction.
Anonymous Credentials

- Special credentials issued by attribute authorities
- Allows for minimum disclosure of attributes of bearer
  - Over legal age; graduate of university in year X; resident; first-responder certifications; access to age-restricted services; etc
- Built on several similar technologies, including ABC4Trust (open source from IBM) and uProve (open licensed from MS)
- Tamper-proof
- Unobservable
- Long-time cool technology in search of use cases and modern enhancements (mobility, informed consent, etc.)
- Several pilots looking at integrating them in various ways
- Our work is being led by Brown University
Abc4trust flows
To use this site, you must have at least one valid Identity Mixer® credential. Most likely you got such a credential from your school. If you did not, you may ask your parents to...
Deployment Models

• Classic ABC4Trust, Idemix, etc.
  – Credentials held in a cert store on the user’s desktop or smart card
  – RPs accessed via Web Browser
  – Processing done in User’s desktop by previously downloaded plugins

• Enterprise-based
  – Credentials held in enterprise directory
  – Processing still done in desktop
  – Addresses mobility
  – May serve important enterprise needs

• Cloud-based
  – Processing and storage moved to the cloud
  – Addresses mobility issues
Metadata and trust implications

• At scale, there needs to be ways to establish and convey trusted information about applications and services to users
  – Implies “vetting” or auditing processes for services
  – Implies metadata that can convey this information in real time to users
  – Implies trust in the metadata
• Dynamic metadata services
  – Work is already underway on this in other places
• Federation operations need to evolve
• Auditing applications
  – For “privacy-preserving” approaches (minimal attribute requests, informed consent, proper handling and disposal, etc.), for COPPA compliance, for …
  – Prototype approaches are successful; market needs to grow
The Attribute Ecosystem

- Those parts of the identity ecosystem that focus on attributes in the ecosystem
- Centers on the creation, exchange and use of attributes associated with those in the identity ecosystem
- Critical to privacy, scalable access control, etc.
- Depends heavily on other aspects of the identity ecosystem, including authentication, trust, etc.
- The relatively unexplored part of the landscape.
A part of the attribute ecosystem
Elements of the Attribute Ecosystem (an evolving understanding)

- IdP’s
- SP’s
- Attribute authorities and providers
- Attribute verifiers
- Trust frameworks and trust framework providers
- Third parties, portals, etc.
- Federation operators
- Application auditors
- The user, and, if applicable, the subject
Decomposing Google

• Google plays many roles within the attribute ecosystem:
  – As a very very large IdP
  – As an applications provider for many applications
  – As an applications auditor for third party apps in their stores
  – As an attribute authority for “harvested” attributes
  – As an attribute authority for self-asserted attributes (e.g. groups)
  – As a trust framework provider for its business partners
  – And more...

• The multiple roles, while essential to the business model, introduces complexity and tradeoffs that can raise public or market issues
• Other current organizations in the biz can also be reviewed.
What Flows Within the Ecosystem

• Attributes
  – May be externally asserted (e.g. student, citizenship), self-asserted (e.g. preferred language), third party asserted (e.g. resident of a town), etc.

• Management of attributes
  – Trust, certification marks and vetted application information, user consent flows, etc.
  – Can flow as metadata or in-stream

• Others?
  – Liability,
Types of attributes (by authority)

- Enterprise/employer-asserted
- Self-asserted
- Reputation systems asserted
- Government asserted
- Third-party asserted
  - Business
  - Certification authority
  - Device asserted?
Standard enterprise attribute flow
Anonymous attribute flow
Associated metadata and trust flow

Federation

Privacy Manager

Associated metadata and trust flow
How to stay informed and participate

• The web site:
  https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy

• Join the ongoing processes:
  – Track the Cohortium and start some local work

• Try the products:
  – InCert, CAS and Shib login handlers