Capstones:
Internet Identity Begins to Bridge the Gaps

Ken Klingenstein, Internet2

Topics

- What is Internet identity
- What are the successes
- Addressing the gaps
  - Stabilizing the software and standards – TIER
  - Expanding federation and starting interfederation
  - Bridging social and organizational identity
  - Developing a set of incident handling approaches
  - Solving the attribute release and consent challenges
- What a mature Internet identity world might look like

INTERNET 2

Internet identity

- Has evolved as a layer of the Internet over the last 20 years, providing users with the ability to authenticate and get access to resources around the world
- A mix of social, organizational and governmental identity providers, using PKI, SAML and OIDC protocols to carry payloads
  - Identity providers (IdP) and relying parties (RP)
  - Sovereign identity advocates persist
- A mix of assurance levels, from unknown to very high
- The payload of the assertions – attributes and claims (Boolean values) – are the most important component, for privacy, accessibility, access control, etc.

INTERNET 2

Kim Cameron's Laws of Identity

Kim Cameron's

Laws of Identity

1 User Control and Consent
Technical identity systems must only reveal information identifying a user with the user's consent.

2 Minimal Disclosure for a Constrained Use
The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 Justifiable Parties
Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 Directed Identity
A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies
A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 Human Integration
The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 Consistent Experience Across Contexts
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Download the poster. Read the explanation of the Laws of Identity.

Successes

- Federated identity as a paradigm
  - Dramatic growth within R&E and other sectors
  - Now the operational model in governments around the world
  - Has become with variants, the Internet Identity layer
- Multifactor authentication
- Internationalization
  - Working with privacy and security differences
  - Working with cultural and societal differences
- Initial integration with social identities

Capstones – Addressing the Gaps

- Stabilizing the software and standards
- Growing federation and starting interfederation
- Bridging social and organizational identity
- Developing a set of incident handling approaches
- Solving the attribute release and consent challenges

INTERNET 2

Stabilizing the software and standards

- Key open source components of the software ensemble, such as Shibboleth and Jagger (the most common federation metadata manager) are inadequately supported
- TIER is an Internet2 effort in trust and identity to leverage previous work into a sustainable set of basic but sufficient components to run campus IAM
  - Includes Shibboleth, Grouper, Comanage, attribute release and consent, provisioning, etc.
  - Trust and Identity includes management of community standards such as eduPerson, Baseline Practices, etc.
- Organizations such as Kantara and IETF are being used to distill interoperability specs about federated metadata, the move to dynamic metadata, etc.

INTERNET 2

Growing federation and starting interfederation

- K-12 Steward Program
  - Allows members to register and manage local organizations in InCommon, serving K-12, local non-profits, etc
  - A scaling extension of the trust model that must be managed very carefully
- Baseline Practices being adopted
  - So that you can count on your federated partners
  - Some ops thoughts (key rollover, software patches, etc)
  - Some IdM thoughts (identifiers)
- eduGAIN - International interfederation
  - 40+ countries, 2500 IdP's and thousands of Relying Parties
  - Addressing current stresses
    - Metadata size
      - Driving the need for dynamic metadata and metadata query
    - Semantic and syntactic differences
      - Names, affiliations, etc.
    - GDPR and international privacy laws

Bridging Social and Organizational Identity

- Social2SAML and SAML2Social Gateways
  - Allows students, their parents, the public, citizen scientists, etc access to organizational resources
- Raises lots of devils in the details
  - Identity proofing, authentication strength, etc.
  - Identifier discrepancies – in format and policy
- Building federations that include OpenId Connect
  - OpenId intended for bi-lateral relationships
  - Multi-lateral R&E SAML federations designing infrastructure to add richer trust, identifier mappings, etc.

INTERNET 2

Incident handling

- In a federated world, a critical need to exchange identity security information in a trustworthy fashion among partners.
  - Account take-over in the social world; password recovery impacts
  - Federated logout
  - Malfunctioning software, e.g. the ORCID incident
  - Account compromise at IdP
- Several efforts developing elements to improve incident handling
  - SIRTFI
    - CERN-initiated trustmark for security contacts, timely responses, etc
  - The sec-event work within IETF
    - JSON token and a variety of transports to communicate identity events (password reset, account takeover, etc)

INTERNET 2

The ORCID incident

- Two IdP's (out of 2000) discovered to be misconfigured and potentially compromising trust by leaving a door open that could allow a user to claim another's scholarly record.
- There was no known compromise, but the event exposed a set of gaps in process.
  - IdP federated integrity testing
  - Event notification from IdP
  - Responsibilities of federated operator, interfederation operator and campus IdP not understood.
  - Measured response mechanisms by relying parties
- An interesting, and overdue, opportunity to mature

INTERNET 2

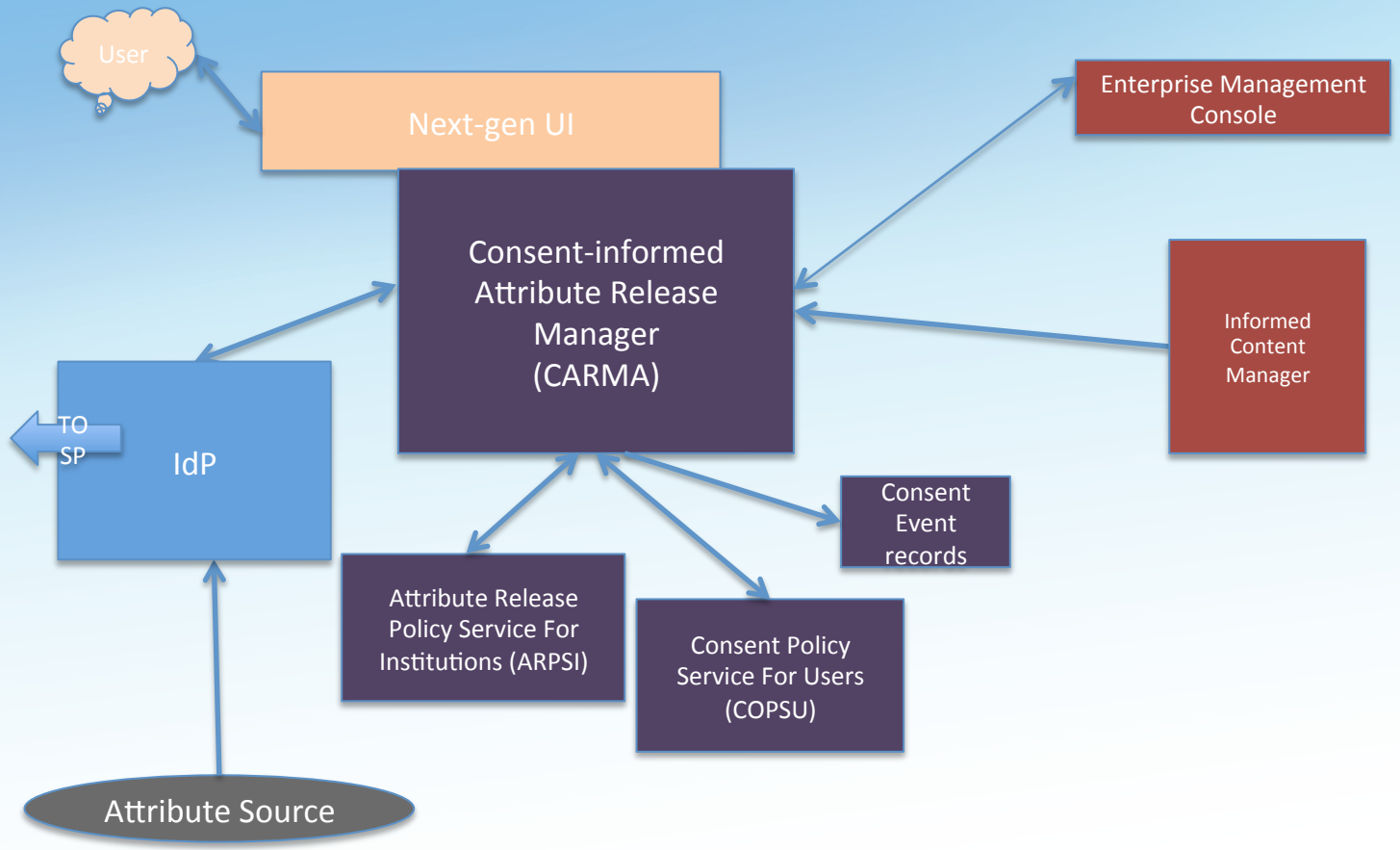
Solving attribute release and consent challenges

- Attribute release has proven to be an unexpected challenge
  - (Over-) Protective data stewards
  - Lack of consent infrastructure
  - Primitive policy management tools
- Policies and practices vary widely
  - European policies inconsistent; GDPR changes everything
  - Trust marks such as R&S have limited success
  - Social apps incent bad privacy
- Hub-and-spoke federations and homogeneous countries do better

Scalable Consent

- Components to create a scalable consent experience and infrastructure
  - An infrastructure that delivers the capabilities and the information to allow users and administrators manage their attribute release from their identity provider at scale
  - A user interface that enables a user to make effective and informed decisions about attribute release
  - Tools for an enterprise to manage that user experience
- Catalyzed by an NSTIC grant from NIST, becoming part of the TIER suite
- Web site
  - https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home

CARMA



INTERNET 2

Informed Content

- The fuel that drives effective and informed user consent decisions
- Limited, though extensible sets of marks, assessments, policies, etc. that are part of the UX
  - Icons for IdP and SP
  - SP IsRequired and Optional Attribute Needs
  - Display-names and display-values for attributes
  - Trustmark information
  - Explanatory application-specific dialogue boxes (e.g. why attribute is needed)
  - Privacy and third-party use policy pointer
  - Additional information feeds
    - Vetted, self-asserted, reputation systems, etc
    - Far-reaching insights - https://arxiv.org/abs/1608.05661

INTERNET 2

Getting the right user experience

- ”You are what you release”
- Blind click through is not the goal; An informed and effective decision.
  - Good first time dwell experience; good further suppression or revocation options
- Original next-gen interface designed by CMU Researchers in Usable Privacy
- Adapted and enhanced by Duke UI/UX group with iterative user testing
  - http://people.duke.edu/~mkm16/projects/consent/
- Some surprising results
  - Users understand what’s happening
  - In both US and European testing, users show some interest in controlling consent

INTERNET 2

CARMA opening up new capabilities

- Consistent, informed user experience across a variety of platforms and protocols
- Integration of institutional and individual attributes
  - Location
  - Emergency contact and medical information
  - Personal schedules
- Teaching students how to manage their privacy
  - Well-designed approaches appear to be well-received
  - By shaping their expectations, we help them shape a marketplace
- Providing new options for accessibility
  - Accessibility with Privacy

INTERNET 2

Where we're headed

- Users have informed and effective tools for managing their identities and attribute release preferences
- Applications become attribute-aware and implement privacy strategies such as data minimization and targeted opaque identifiers
- Identity providers operate schema and business processes to support rich user attribute information, including citizen and accessibility needs, and adopt identity portability approaches for creating a marketplace
- Trust marks provide users with valuable information in making content and trust mark issuers use standard audit approaches for validating mark holders

INTERNET 2