Internet Identity and Access Control

Dr Ken Klingenstein,
Director, Middleware and Security, Internet2

INTERNET®

Topics

- What's happening/ impacts
  - See lunch talk
- The Research Angle
  - Researchers as users
  - Security Researchers
  - New areas for Research

kjk@internet2.edu

Researchers as Users

- Use your local login to access
  - NIH, NSF grant submission and management
  - CIlogon for CyberInfrastructure
  - GENI
- Scholarly Identity
- No local federation? Push for it…

Security Research

- Leveraging the trust fabric
- SES as a model
  - Analytics beyond the border
  - http://www.ren-isac.net/ses/
- Federated security tools

New Areas of Research

- Anonymous Credentials
- Scalable privacy management
  - UI, Correlation attacks, Contexts
- Attribute Ecosystem
  - LOA, Revocation, Terms of use, Metadata

kjk@internet2.edu

Anonymous Credentials

- Special credentials issued by attribute authorities
  - When queried by RP, will do minimal disclosure of encoded attributes
    - E.g. Over 18, True/False on specific sets of attributes, such as citizen, medical, etc.
  - Can be done so that IdP does not know either the values being released or the RP's requesting information
  - Deep crypto techniques underlie – e.g. Idemix.
- Ten year old research -> proprietary technology development ->open source capability
- No use of SAML but heavy need for SAML metadata

Anonymous Credentials Use Cases

- Medical records
  - HMO can put attributes about patient medications into an IdP and have authorized RP query
  - Student health can store information restricted to RP with a need to know, protected from general IdP.
- Citizen record
  - Answer general official queries such as over legal age queries, citizenship, etc.
  - Enable specific services such as parking by zones, privacy-preserving neighborhood discussions
- Private access controls
  - By good and evil

Key Directions in Anonymous Credentials

- Radical new capabilities, but lacking any infrastructure at all to support deployment at scale
  - Delivering credentials to user and storing
  - Scalable query controls
  - Audit and policy issues
  - Metadata for informed consent
  - Others
- Enter federated identity
  - Provides secure credential transport and storage
  - Provides framework for discussion on policy
  - Fills other deployment gaps

kjk@internet2.edu

Scalable privacy management

- UI
- Attack vectors
  - E.g. Correlation
- Contexts

kjk@internet2.edu

Attributes

- LOA
- Revocation
- Digital rights management
- Use of metadata

kjk@internet2.edu