CSci530: Computer Security Systems
Authentication (continued)
15 October 2003

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute

Administrative

- This weeks office hours for Dr. Neuman are today from 12:30 to 1:00 PM (or as late as necessary if students are waiting to see me). (No Friday office hours since Friday's 555 lecture is by Dr. Ryutov)
- Jonathan Kelly's office hours until Mid-term are Friday from 1PM to 2PM, and Tuesday 1PM-2PM in SAL 1-10a.
- First assignment returned today.
- Mid-term in class next week.

Passport v Liberty Alliance

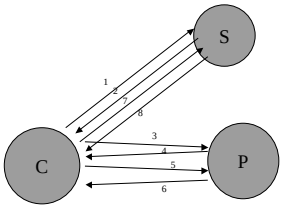
- Two versions of Passport
  - Current deployed version has lots of weaknesses and is centralized
  - Version under development is "federated" and based on Kerberos

Liberty Alliance

- Loosely federated with framework to describe authentication provided by others.

Passport v1

- Goal is single sign on
- Implemented via redirections



Assigned reading: http://avirubin.com/passport.html

Federated Passport

- Announced September 2001
- Multiple registrars
  - E.g. ISPs register own users
- Kerberos credentials
  - Embedded authorization data to pass other info to merchants.
- Federated Passport is predominantly vaporware today, but .net authentication may be where their federated model went.

Liberty Alliance

- Answer to MS federated Passport
- Design criteria was most of the issues addressed by Federated Passport, i.e. no central authority.
- Got off to slow start, but to date has produced more than passport has.
- Use SAML (Security Association Markup Language) to describe trust across authorities, and what assertions means from particular authorities.
- These are hard problems, and comes to the core of what has kept PKI from being as dominant as orginally envisioned.
- Phased approach: Single sign on, Web service, Federated Services Infrastrcture.

Review for Mid-term

- Cryptography
  - Basic building blocks
  - Conventional
    - DES, AES, others
  - Public key
    - RSA
  - Hash Functions
  - Modes of operation
    - Stream vs. Block

Review for Mid-term

- Key Management
  - Pairwise key management
  - Key storage
  - Key generation
  - Group key management
  - Public key management
  - Certification

Review for Mid-term

- Authentication: Know, Have, About you
  - Unix passwords
  - Kerberos and NS
  - Public Key
  - Single Sign On
  - Applications and how they do it
  - Weaknesses