Public-key Support for Collaborative Groups

Stephen Dohrmann
Staff Software Engineer
Corporate Technology Group
Intel Corporation

April 25, 2002
Introduction

- Our work sprang from a field trial project for wireless collaboration software.
- We wanted to build a system suitable for both business and personal use.
- A good user model for building secure workgroups was a primary focus.
Outline

• Phased model for group building
  – Discovery – becoming connectable
  – Introduction – establishing identity
  – Invitation – granting authorization
  – Use – exchanging secure traffic

• User interface

• Developer interface

• Conclusions & future work
Discovery Phase

- Exchange of IP address data via multicast IP or out-of-band channel
- This phase has no security role – the only result is the ability to make a TCP connection between users.
- We could include the default key in discovery package, but we did not.
Introduction Phase

• Establishing identity
  – Public key exchange
  – Binding a received key to a person
  – Local naming of a received key

• We allow multiple identities; useful but a complexity for the user.
Establishing Identity

Frances

John

Leanna

Digital

Physical

Mental

AAAAB3NzaC1kc3MAAACCBAPJQkdHPKOgrjxD55GQUJmo
m3Je8/Up9XPeczYHG6089V16ToSyTr2BUVulcP92i05
DFMxUlu1RraKVwiV38sg67UPcCUPYsRMmP6ASrTQyNg
eZxcyPkv9+30V97BH86UA8cn8k+Dhc0zZuo+kkTvGc
8pPYhpIPDguKrQwblNhAAAAFQDHmD6d/aXFLm+cp+
6wyhX3KXhQAAAAIEA7v+J71XMN7XDQ6JEuinGMapaQXg

03 5b 97 83
6e 04 2c 04
2a c9 b5 22
14 3b c6 42

AAAAB3NzaC1kc3MAAACCBAPJQkdHPKOgrjxD55GQUJmo
m3Je8/Up9XPeczYHG6089V16ToSyTr2BUVulcP92i05
DFMxUlu1RraKVwiV38sg67UPcCUPYsRMmP6ASrTQyNg
eZxcyPkv9+30V97BH86UA8cn8k+Dhc0zZuo+kkTvGc
8pPYhpIPDguKrQwblNhAAAAFQDHmD6d/aXFLm+cp+
6wyhX3KXhQAAAAIEA7v+J71XMN7XDQ6JEuinGMapaQXg

03 5b 97 83
6e 04 2c 04
2a c9 b5 22
14 3b c6 42

Leanna
Leanna’s Identity via TTP

- **Digital**
  - <certificate for Frances Chamish>
  - AAAAB3NzaC1kc3MAAACBAPJQkdHPKOfgrxD55GQUJmom3Je8/Up9XPeczYHg6089V16ToSyTr2BUVvUlCPB205DFMxUlu1FtralVvw38s967UPcCUPYsRmF6ASr...
  - {credentials for Frances Chamish}

- **Physical**
  - Frances
    - Leanna
  - TTP
    - Decide to generate certificate

- **Mental**
  - Frances
  - TTP
  - John

**Slide 7**

Intel Labs
John’s Identity via TTP

John

TTP

Frances

John Wilson

{credentials for John Wilson}

Digital

<certificate for John Wilson 39>

<certificate for John Wilson 39>

<certificate for John Wilson 37>

Physical

Mental

Decide to generate certificate

AAAAB3NzaC1kc3MAAACBAPJQk dHPKOgrjxD55GQUJmom3Je8/Up9 XPeczYHG6089V16ToSyTr2BUVul oP92i5DFMxUu1RraKWy1V38sg6 7UPcCUPYsRMnP6ASr . . .
Invitation Phase

- Granting authorization to participate in a collaboration group
- Inviting others into a group is an authorized operation, otherwise policy is flat.
- In some cases, multiple flat-policy groups substitute for fewer rich policy groups.
- We used SDSI certificates with nested namespaces.
- We did not address revocation.
Use Phase

• The use of cryptography is transparent to the user: all traffic is signed, encrypted, and checked for authorization.

• The need to offer security choices to user usually stems from performance issues.
User Interface

- Should be easy to use correctly
- Mistaken identity (people / groups) is the largest source of errors.
- Sign-on names are weak identifiers.
- Distasteful user interface elements will be avoided by the user if possible.
- Key verification UI needs the most attention. Graphics / sound help...
  - Faster
  - Less intimidating
As with the user interface, we wanted to create developer tools that were easier to use correctly.

Integrated APIs for crypto, key exchange and authorization

- **Crypto**: key generation and storage, signatures, digesting, ciphering
- **Key Exchange**: simple interface to signed D-H
- **Authorization**: unified API for credentials, ACLs, and AuthCompute certificate reduction
- **Provide “Model T” choices of algorithms and parameters**: (1024-bit DSA, 3DES)
Future Work

• Variety of user interfaces for key verification step
• Revocation of authorizations
• Fine grained authorizations
Conclusions

- Identity is the cornerstone of authorization.
- The toughest problems involve expectations we place on the user when establishing identity; the user must bind a key into her local namespace.
- Simple models and interfaces for user and developer are helpful; eliminating choice is not a bad thing here.
- Global PKI unacceptable for our purposes; CA lacks knowledge of relationships and authority to make statements about them.
Backup

• Securing a message rather than a pipe scales better to different network topologies.