Dartmouth PKI Lab Update

August 2001
Snowmass, Colorado

Sean W. Smith, Ph.D.

Department of Computer Science/
Institute for Security and Technology Studies

Dartmouth College, New Hampshire

www.cs.dartmouth.edu/~pkilab/

Copyright 2001, S.W. Smith
Dartmouth PKI Lab

Chartered 4Q2000, by Internet 2

Department of Computer Science (Research)
- Sean Smith, David Nicol
- Yasir Ali, Alex Iliev, Shan Jiang, Evan Knop,
  John Marchesini, Sean Richardson, Eileen Ye

Dartmouth Computing Services (Academic)
- Robert Brentrup, Larry Levine

Institute for Security and Technology Studies (Society)
- Ed Feustel (and Dave and Sean)
Objective

**Trusted Information Services**
- ...in the emerging information environment
- ...that is *heterogeneous* on every level...
  - machines
  - organizations
  - relationships
  - mobility
  - dynamic

- *Trust requires PKI.*
- *PKI requires Trust.*

Academic community as a prototype lab

(and... PKI ≠ X509, SDSI/SPKI, PGP, XML...)
Initial Plan

**Server:** How do we establish *foundation for trust*, when computation is vulnerable to *insider attack*?

**Client:** How can *user tools* enable effective *trust judgments*?

**Infrastructure:** How do we *deploy* and *manage* the *certificates*, keys, etc., that enable this trust communication?

**Applications:** How can *applications* engage in PKI-based *trust judgments*?
Status, Aug 2001

**Server:**
- Trusted Third Parties, immune to insider attack
  - *Completed:* PIR, Amored Vault, WebALPS
  - *In Progress:* Box Office, S/MIME

**Client:**
- *Completed:* Web/SSL/Certificate Spoofing
- *In Progress:* Secure Web Client

**Infrastructure:**
- *In Progress:* Set up COTS, open-source testbeds, LDAP
- *In Planning:* Campus PKI
  (using server, client tools)

**Applications:**
- *In Progress:* Early Adopters, Pilots
- *In Planning:* Quite a bit...
  (using server, client, infrastructure tools)
Servers

*Problem:* How can users *trust* remote computation?

*Our Approach:* Build *trusted third parties*:
- protect computation inside armored coprocessor...
- that destroys secrets upon tamper (FIPS 140-1 Level 4)
- and can proves it’s *the real thing, doing the right thing*

*Enabling Technology:* IBM 4758 (Sean’s IBM project)
(open development environment... so *real deployment path exists*)
Completed: Private Information Retrieval

Protecting query privacy from insider attack

Consider domains with sensitive data:

- health information
- unfashionable politics
- oil exploration information
- MP3 files

Problem:

- How do we build a server that efficiently provides material to authorized users...
- ...so that the server op learns nothing, not even statistics?

Solution:

- Use coprocessors.... and careful data structures
Completed: Armored Vault

Protecting archived private material from insider attack

I’ll get that data!

No you won’t!

You’ll only get what we all agreed. Neither cash nor guns can change that!
Armored Vault

“DRM for Big Brother”: How can stakeholders trust that policy is followed?

- Prototype domain: network data
- Archive is encrypted and bound to policy
- **Security**: Armored vault follows policy *exactly*, despite rogue insiders
- **Flexibility**: The policy can consist of any computation.
- Prototype built from Snort and the IBM 4758-2 [1][1],[2][2]

**Future:**
- look at other areas of selective weakening of privacy: *key escrow*, administrative access to *encrypted data*
- PKI *authorization*
- DRM, policy with Wisconsin
Completed: WebALPS

Protecting SSL Web servers from insider attack

SSL doesn’t help, *if you can’t trust the server at the other end*

- **WebALPS**: move the server end into an armored co-server [Sm00]
- **Security**: rogue insiders cannot access sensitive client data and computation

- Prototype built from Apache, OpenSSL, and the IBM 4758-2 [Ji01, JSM01]
WebALPS: Extending the Tunnel

Client

- ClientHello
  - Server Random
  - Server’s Public Key
  - ClientKeyExchange
  - ChangeCipherSpec
  - Finished

Server

- Client Hello
  - Server Random
  - Server’s Public Key
  - Certificate
  - Server Hello
  - ChangeCipherSpec
  - Encrypted Premaster Secret
  - Finished

WebALPS Co-Server

- Certificate for WebALPS Co-Server
- Encrypted Premaster Secret
- Client Random, Server Random
- Finished

Client is ready to use the agreed cipher to send messages.
Client is ready to use the agreed cipher to read and send messages.
Co-Server is ready to use the agreed cipher to send and read messages.
In Progress: Hardened Box Office

Protecting campus e-commerce server from insider attack

*Ties in:* campus PKI is channel for trust

**Problem:**
- Many campus agents want to sell tickets, etc., online
- Computing Services is happy to set up a server, but does not want to risk exposing private customer data

**Solution:**
- Use a WebALPS-hardened server
- Internal application catches customer data, then signs and encrypts it for entity, and emails it

**Status:**
- target: online by 10/2001
In Progress: Hardened S/MIME Web Mail

Protecting user private keys from insider attack

Ties in: prototype for one approach to “where do we keep the private keys?”

Problem:
- Web-based mail offers **client mobility** ...
- ...but adding PKI requires **trusting the server with the private keys**

(thanks to a grumble by Wisconsin’s Eric Norman)

Solution:  
[Knopp01]
- Use a WebALPS-hardened server
- Generates, certifies, stores user keys..
- ...and applies them only when authorized by user
- **Neither bribery nor subpoena** reveals user keys!
How can users make good trust judgments?
The Current Infrastructure

Problem 1:
- Web/SSL tries for server **identity**, not **attributes**

Problem 2:
- Does it work?
  - URL?
  - Location bar information?
  - SSL Icon?
  - SSL warning window?
  - Certificate information?
  - Status bar
“Build a Better Browser”

**Completed:**
- www.cs.dartmouth.edu/~pkilab/demos/spoofing/

**In Progress:**
- Extending clients to have unspoofable windows [Ye02]

**Future:**
- Use attribute certificates to communicate security properties of machines...within these windows
Infrastructure

Use COTS and open-source tools to setup and administer institution scale PKI environment

- deploying Unicert, CDSA, CryptLibs, IBM 4758

Transition to Institutional LDAP Directory

Tools to Support Research Projects

Interconnect with our legacy Entrust PKI

Research goal: real prototypes, solving real problems!
Applications

Existing:
- Early Adopters-Middleware
- Payroll Authorization Development Project

Planning:
- Rights Management (with Wisconsin PKI Lab)
- Privacy
- Integrity
- Federal apps
Conclusion

*Initial Plan:* Trusted services in the emerging information environment...
- *Research*
- *Infrastructure*
- *Applications*

*Follow-on Plan:* CRITICAL MASS
For More Information

www.cs.dartmouth.edu/~pkilab/

- Robert Brentrup  Robert.J.Brentrup@dartmouth.edu
- Ed Feustel  efeustel@ists.dartmouth.edu
- Sean Smith  sws@cs.dartmouth.edu