

PKI Obstacles and Action Plan (My top three list)

Sean W. Smith

**Department of Computer Science
Dartmouth College**

`www.cs.dartmouth.edu/~sws/`

April 14, 2004



Missing Obstacle #3

Does it say what you want it to say?

Suppose we closed our wireless network with EAP-TLS.

- Why can't end users authorize visitors?
- (Why did we have to play tricks with SPKI/SDSI in cookies?)
- Why can't the Dartmouth net recognize a Princeton visitor?

Why are proxy certificates necessary?

Why will the doctor's office have a post-it note with the PIN?

Action: Find better ways to have signed assertions follow real-world trust flow

Missing Obstacle #2

Do the humans understand it?

Can Johnny encrypt yet?

Is it easy to do the right thing?

Do mental models match what the machines are doing?

Action: HCISEC.

Missing Obstacle #1

Does it work?

PKI is a lot of work. But there's a point to it.

Besides asking...

- “Do the users get it?”
- “Does the code work?”

Action:...we should also ask:

- “What are the security goals of using PKI in this application, and do we achieve them?”

Server-side SSL?

Question: If Alice's browser gives her all the right signals that she has an SSL connection to Bob's server, does she?

What we learned: with Netscape/Linux and IE/Windows then current, no. With a lot of work, you can add a trusted path to Mozilla.

Ye Smith 2002

<http://www.cs.dartmouth.edu/~sws/abstracts/ys02.shtml>

Digital Signatures?

Question: Does Bob's valid digital signature on document D mean that Bob approved the contents of D ?

What we learned: With standard office tools and many "best of breed" PKI tools, it was easy to construct documents:

- whose contents changed in usefully malicious ways
- without invalidating the signature

Kain Smith Asokan 2002

<http://www.cs.dartmouth.edu/~sws/abstracts/ksa.shtml>

Client-side SSL?

Question: If Alice submits her request to Bob's server with client-side SSL under her cert, did Alice approve that request?

What we learned:

- If the adversary has access to a server, be careful
- With IE, if the adversary gets a user-level program on your machine, game's over...
- ...even with hardware tokens

Marchesini Smith Zhao 2003, 2004

<http://www.cs.dartmouth.edu/~sws/abstracts/msz04.shtml>