Expressing Human Trust in Distributed Systems: the Mismatch Between Tools and Reality

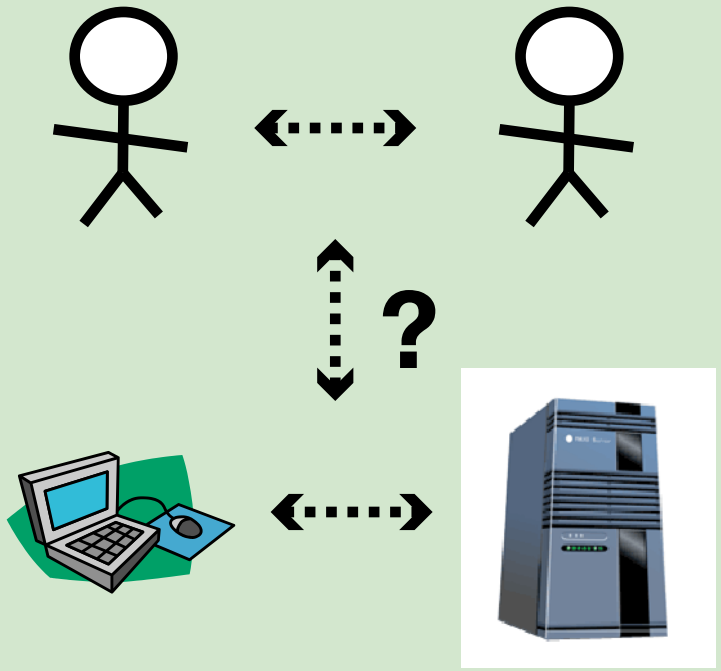
Sean W. Smith
Department of Computer Science
Dartmouth College
Hanover, NH USA

http://www.cs.dartmouth.edu/~sws/

April 15, 2005

joint work with various students

Overview



- Background on ***PKI***
- Problems with ***mental models***
- Problems with ***expressiveness***
- (research)

Public Key Cryptography

Public Key ~~Cryptography~~ Infrastructure

Public Key ~~Cryptography~~ Infrastructure

Basic Uses:

- Signed communication
- Encrypted communication
- Authentication

Public Key ~~Cryptography~~ Infrastructure

Basic Uses:

- Signed communication
- Encrypted communication
- Authentication

Basic Problem:

- Alice needs to learn Bob's public key

Basic Approach:

- A ***CA***
- signs an ***X.509 identity cert***
- binding Bob's name to his public key

Basic Worries:

- How does Alice obtain Bob's cert?
- How does she decide to believe his CA?
- How does she check if this CA has changed its mind?

Problem: Mental Models

Does what people think the machines do match what the machines really do?

- digital signatures on office documents
- server-side SSL
- client-side SSL
- passwords

Digital Signatures

If Alice's tools tell her that *X* has a valid signature from Bob, should she conclude that Bob signed that virtual piece of paper?

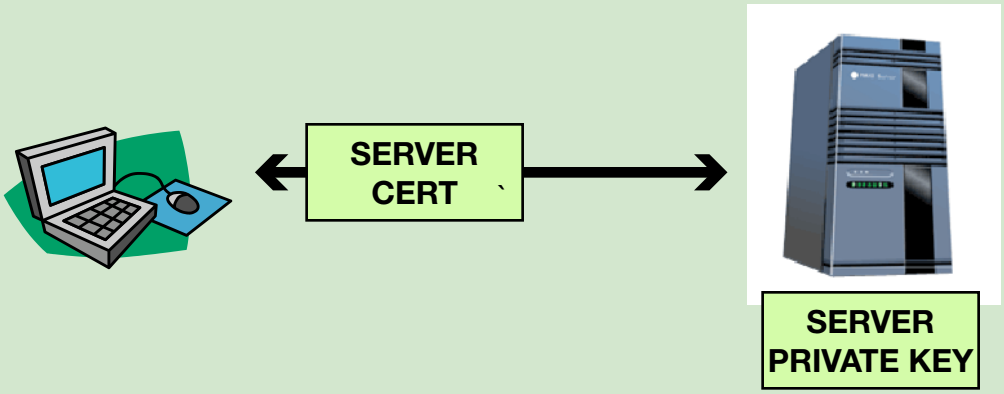
With a quick exploration, we could subvert:

- Word (without macros)
- Excel (without macros*)
- PDF
- HTML email

using:

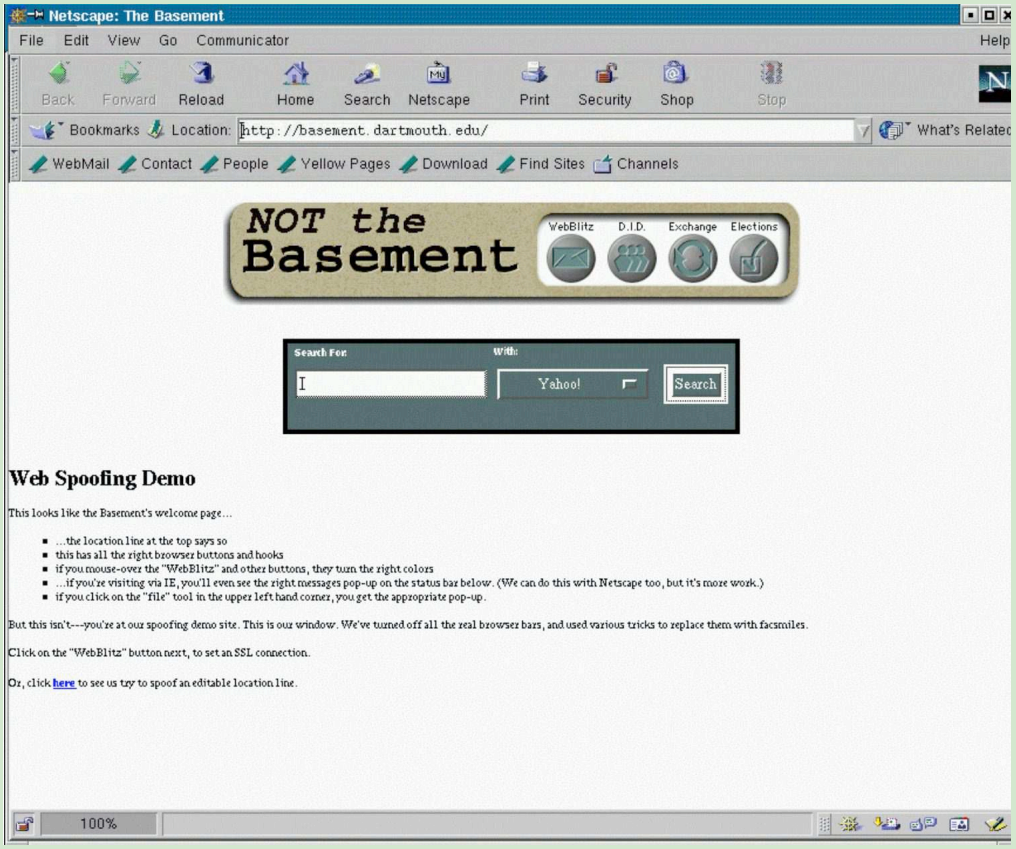
- PGP and S/MIME signatures
- DST's CertainSEnd
- Assured Office/ProSigner/E-Lock
- Acrobat Visible Signatures

Server-Side SSL

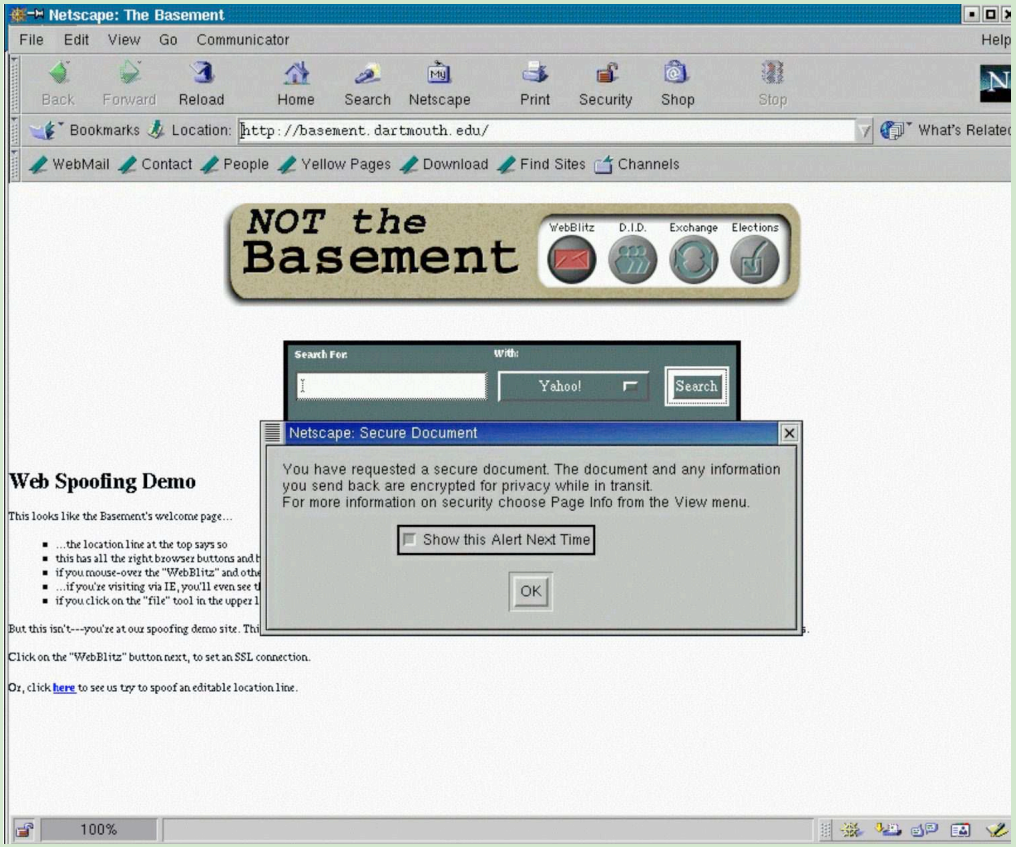


If Alice's browser tells her that she has an https connection to bob.com, should she believe it?

Standard Browser Signals

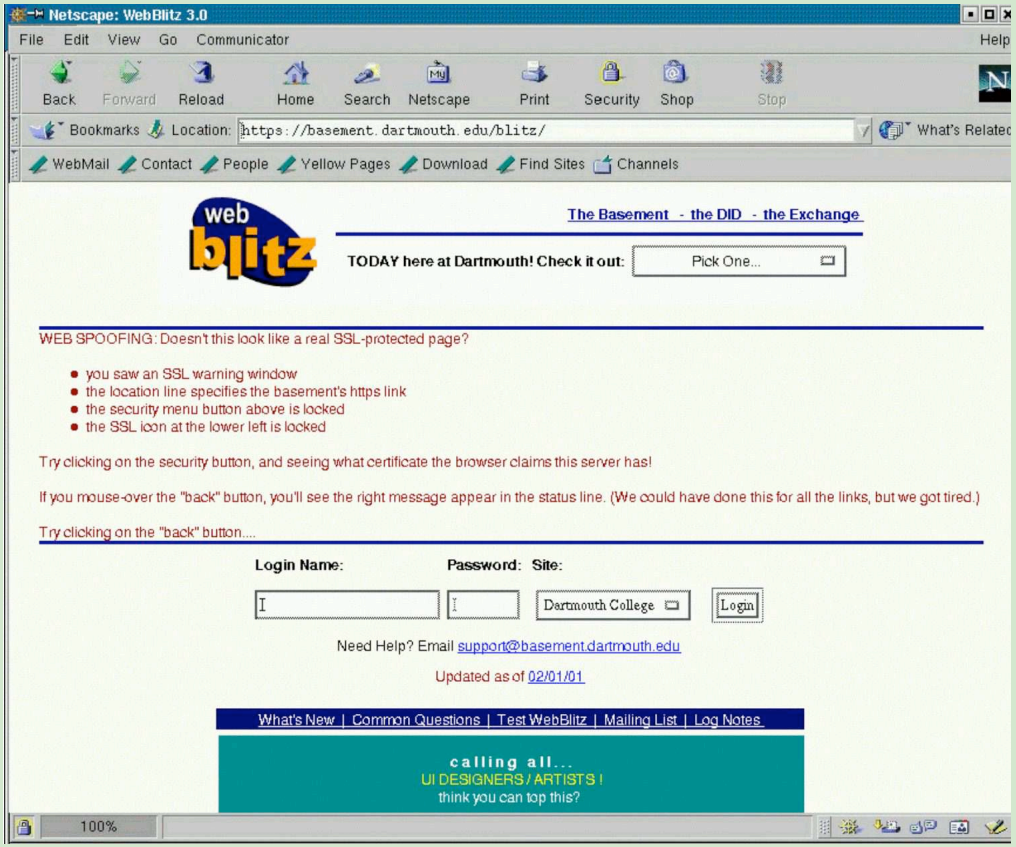


Standard Browser Signals



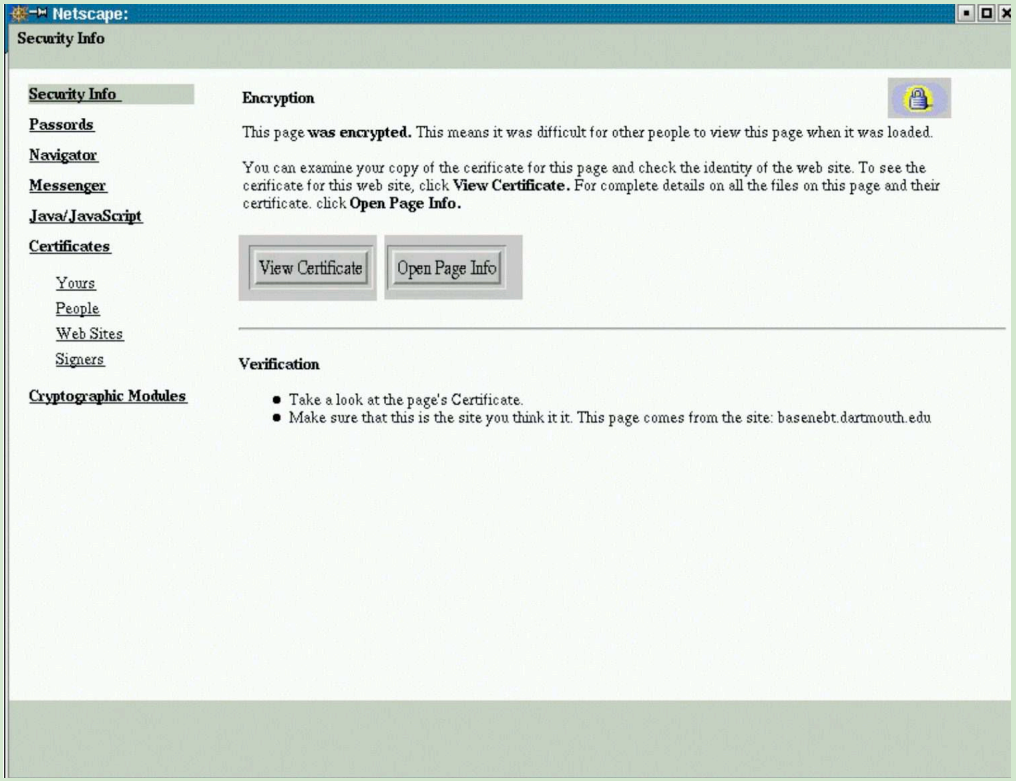
SSL warning window

Standard Browser Signals



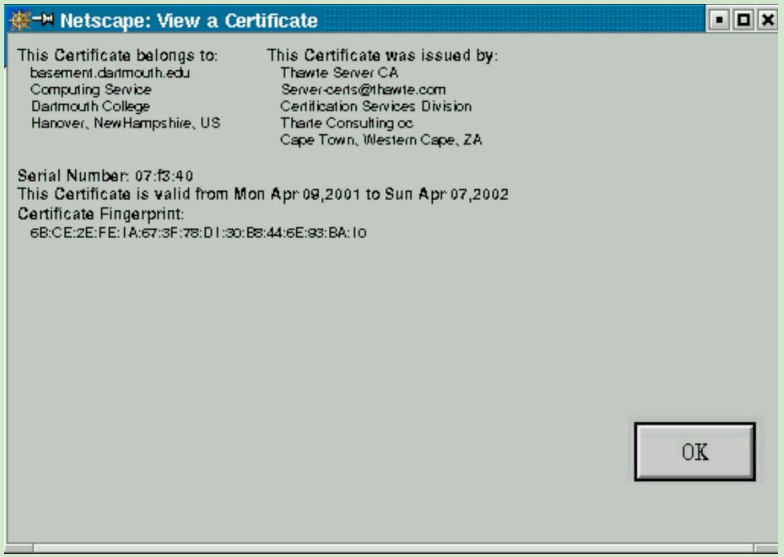
"https", security icons

Standard Browser Signals



security page

Standard Browser Signals



server certificate

Web Spoofing Revisited

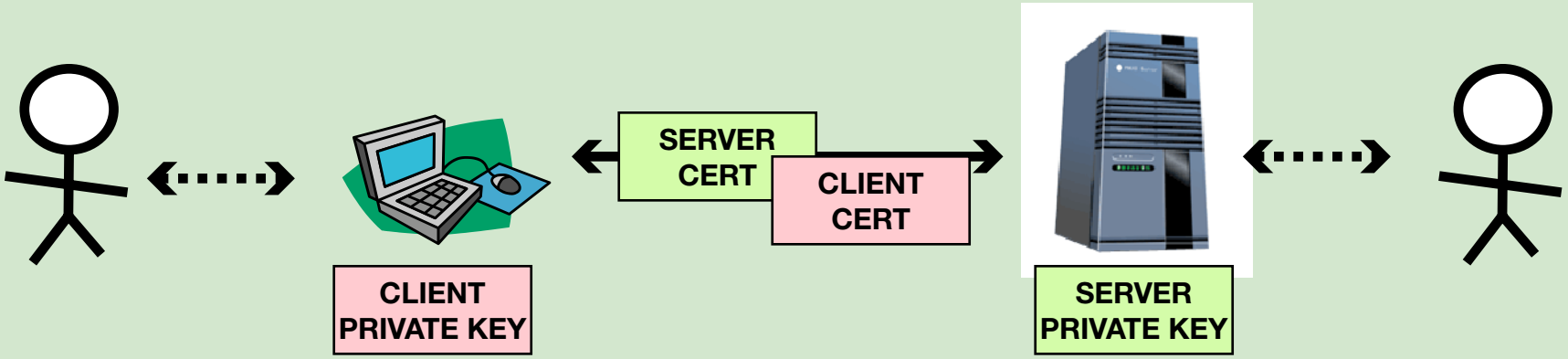
Attacks: For IE/Windows and Netscape/Linux (circa 2001 -2002), we built a malicious server that spoofed:

- Location bar
- SSL icon
- SSL warning windows
- SSL certificate info
- (and password prompts)

Defenses: Prototyped and validated "secure GUI" countermeasures in Mozilla (Usenix 02)

- Didn't get adoped
- Users have strange beliefs about online trust
- The problem has only grown worse

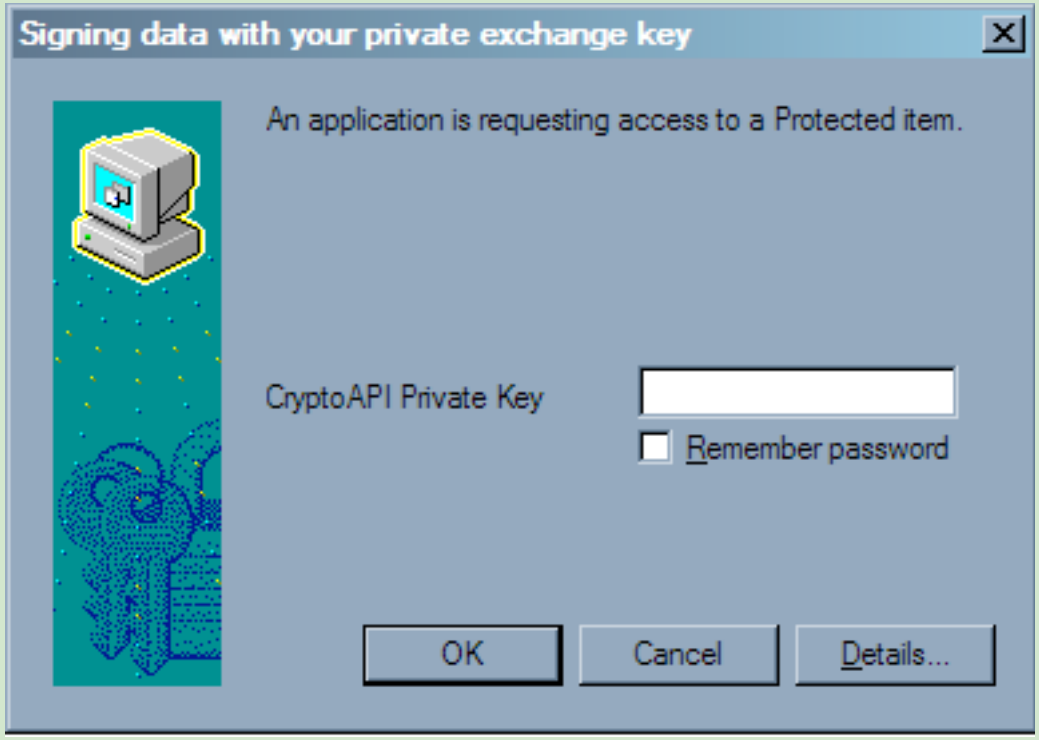
Client-Side SSL



Does "client-side authenticated request" ⇒

"user authorized the request" ?

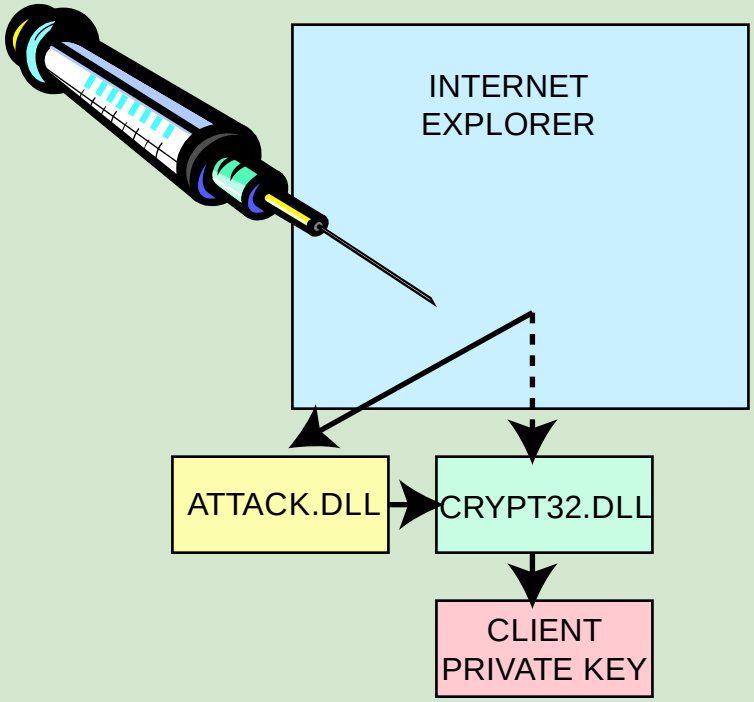
The "Browser" Keystore



Microsoft CSP, "high" or "medium" security keypair

Keyjacking #1

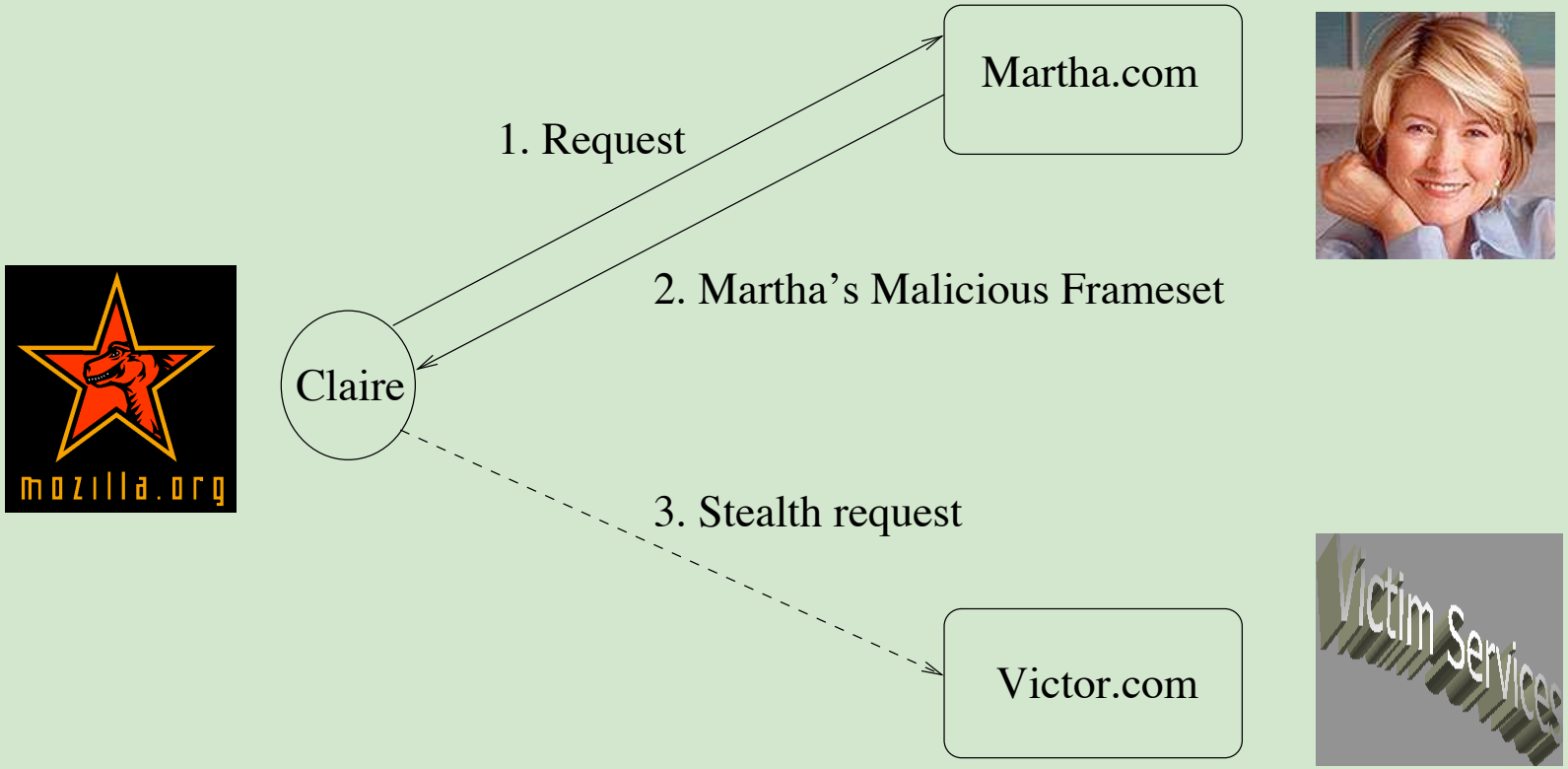
Suppose the adversary adds one user-level executable...



Result: adversary gets key, even with medium/high security
Countermeasure: make key non-exportable

Keyjacking #2

Suppose the adversary writes devious server content...



Result: often, adversary fools victim server
Countermeasure: careful server content, browser configs

Mystery

If Claire approves using her key for victor.com once, IE appears happy to keep using it for SSL handshakes to that server.

Let's follow all the rules:

- WinXP Pro, current SP, current updates
- "High security" key
- Followed DoD DMS key hygiene guidelines

Result: IE will still use Claire's key without telling her

Keyjacking #3

Add one user-level executable, with two parts...

Countermeasures?

- Magic button? ("kill SSL state" or kill browser)
- Make key non-exportable?
- Aladdin eToken USB?
- Spyrus Rosetta USB
- Careful server content?

Keyjacking #3

Add one user-level executable, with two parts...

Countermeasures?

- Magic button? ("kill SSL state" or kill browser)
- Make key non-exportable?
- Aladdin eToken USB?
- Spyrus Rosetta USB
- Careful server content?

All your keypairs are belong to us

Keyjacking #3

Add one user-level executable, with two parts...

Countermeasures?

- Magic button? ("kill SSL state" or kill browser)
- Make key non-exportable?
- Aladdin eToken USB?
- Spyrus Rosetta USB
- Careful server content?

All your keypairs are belong to us

SHEMP: Proxy certs, TPMs, XACML

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.
- ***Email link to spoofed site, using IE URL flaw***

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.
- ***Email link to spoofed site, using IE URL flaw***
  83% success rate.
  36% had vulnerability.
  3% of the rest noticed.

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.
- ***Email link to spoofed site, using IE URL flaw***
  83% success rate.
  36% had vulnerability.
  3% of the rest noticed.
- ***Self-signed SSL site***

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.
- ***Email link to spoofed site, using IE URL flaw***
  83% success rate.
  36% had vulnerability.
  3% of the rest noticed.
- ***Self-signed SSL site***
  93% success

Passwords

Assumption: knowledge of password ⇒ identity of user

Reality: CS38 hw

- ***Plastic Dinosaurs and Squirt Guns***
  80% success rate.
  "Alice" got 100%.
- ***Email link to spoofed site, using IE URL flaw***
  83% success rate.
  36% had vulnerability.
  3% of the rest noticed.
- ***Self-signed SSL site***
  93% success
  including two faculty
  (from social science)

Problem: Expressiveness

Does standard PKI express what's important in human scenarios?

- name ≠ person
- name ≠ property
- property ≠ property
- formal delegation
- ad hoc delegation

Name ≠ Person

Did that mail really come from the "John Wilson" I'm thinking of?

One name, many persons

One person, many names

One person, many accounts

- John.Wilson@dartmouth.edu
- jwilson@ists.dartmouth.edu

One account, many capitalizations

- John.Wilson@foo.com
- john.wilson@foo.com

Name ≠ Property

Did that mail really come from the person with property *P* ?

What about the name-P binding?

- TCPA/TCG attestation about a remote machine
- Is "Martin Wyburne" the Dean?
- Who should sign the mail firing the CEO?

Multiple people speak for P

- "Effie Cummings" sent the mail from "Dean Wyburne"

Property ≠ Property

What does property *P* over there really mean?

Name of predicate

- Who is the "Office of the Registrar" at UVM?

Natural implications of predicate

- Dave Nicol and the soccer coach at UIUC

Similarly named predicates may mean opposite things

- "Dean's List" at MSU
- "Dean's List" at Princeton

Delegation

How do we express formal and ad hoc delegation relationships?

Subcontracting

- "Modus Media" vs. https://www.palmstore.com
- john@linklings.com is the "Dartmouth Ph.D. Admissions committee

Less formal authorization

- Sharing passwords at NYU
- Dean of First-Years... and her admin assistant
- Stopping forgery of mail from the college president

Ad hoc relationships

- Giving a visitor "inside" access in EAP-TLS WLAN

Research Angles

Expressiveness:

- name equivalence
- non-identity attributes
- delegation
- ontology mapping

PKI Tools:

- X.509 SubjectAltName
- X.509 attribute certs/PERMIS
- X.509 proxy certs
- SDSI/SPKI, XACML, hybrids
- HEBCA

Other areas:

- Trust Management
- HCISEC

And in Conclusion

"It hurts to straddle the fence."

Web spoofing: http://www.cs.dartmouth.edu/~sws/abstracts/ys02.shtml

Signature hacking: http://www.cs.dartmouth.edu/~sws/abstracts/ksa.shtml

Keyjacking: http://www.cs.dartmouth.edu/~sws/abstracts/msz04.shtml
http://www.cs.dartmouth.edu/~sws/abstracts/shemp.shtml

Plastic dinosaurs: http://www.cs.dartmouth.edu/~sws/papers/eq.pdf

Mismatch: http://www.cs.dartmouth.edu/~sws/abstracts/sm04.shtml

Thanks: NSF Career, DoJ/DHS, Mellon, Internet2/AT&T, Cisco, Sun, Intel