Reputation in Privacy Enhancing Technologies

Paul Syverson

Naval Research Laboratory

E-mail: syverson@itd.nrl.navy.mil

URL: www.syverson.org

joint work with

Roger Dingledine,

Nick Mathewson

The Free Haven Project

URL: www.freehaven.net

PETs does more than you think for privacy

Privacy Enhancing Technologies Workshop (www.pet2002.org)

Basic research on defining anonymity (information theory)

- Allows us to measure the privacy provided by a system

Surprising system designs

- Private Information Retrieval (PIR):
  - Server cannot tell what was downloaded
- Location protected communication: Cell phones, Smart Tag

Available systems

- Bugnosis: tells users when they get a web bug
- LPWA/Proxymate: stateless, cryptographically robust, single signon
- Safe Cookies: Sanitizing proxies
- Cookie cooker: exchange cookies of participants

PETs does more than you think for security

Law Enforcement

- Anonymous communication makes people more comfortable when contacting authorities
- PETs protects activities of law enforcement

Business

- Liability reduced if business
    1. properly manages private data
    2. understands and is consistent with its privacy policy
- Liability is really reduced if business can show it could not have (or access) private data

Everyone

- Pseudonymous certificates and authorization reduce identity theft and fraud

Reputation in Privacy Enhancing Technologies

Reputation can *enable* privacy by reducing demand for information

Remailer Networks

How do you know if your message got through?

Pinging only works for small, static networks

Censorship-resistant Publishing

Distributed (peer) servers store shares of documents for each other.

Reputation keeps servers honest about storage.

If a server reliably stores shares, it gains reputation

Server (client) can "spend" reputation to store its own shares.

Conclusions: New Directions

Reputation is not pixie dust.

Reputation is already being used: eBay, Amazon, Slashdot, Google

Reputation is itself a source of vulnerabilities

Can we treat reputation as currency?

To handle our pseudonymous future, we need good reputation systems

PETs can solve a surprising variety of privacy problems

Security and Privacy are not at odds, they are mutually dependent.