Privacy Enhancing Technologies for the Internet, Parts I and II

Ian Goldberg, David Wagner, Eric Brewer

presented by Nikita Borisov

ECE598NB - Spring 2006

Motivation

- Threats to privacy
  - – Online actions monitored
  - – Information recorded and preserved for years
    - Hard drives cost ~40 cents/GB
  - – Mining and extraction of information
    - Phone number, address, SSN
  - – “dossier effect”
  - – Government

Anonymity

- Tool to achieve privacy
  - Data not tied to you nearly as good as private data
  - “physical security through anonymity”
- Anonymity commonplace outside internet
  - Federalist papers
  - HIV tests
  - Police tips
  - Journalists
  - Postal service
  - Phone calls
  - Cash

- Double edged sword
  - Good and bad uses for anonymity
  - Q: The political climate has changed since 1997; is anonymity doomed?

Past (pre 1997)

- Type 0 remailers
  - Strip off headers
  - Create reply address

From: nikita@uiuc.edu -> From: anon123@anon.penet.fi

  - Store reply mapping:

To: anon123@anon.penet.fi -> To: nikita@uiuc.edu

- Type 0: Problems
  - Single point of trust
  - Identity table - permanent storage of private information
  - Eavesdroppers
- Anon.penet.fi shut down after subpoena

Cypherpunk Remailers

- Type I
  - Basically Chaumian mixes (next week)
  - Chain of remailers
    - Distributes trust
  - Reorder messages
  - Layered Encryption
    - Prevents eavesdropping

Present (as of 1997)

- Type II remailers
  - Constant size messages
  - Replay attack prevention
  - Smarter Reordering
  - Cover traffic (in theory)

Other Anon. Mail Technologies

- Nym servers
  - Reply blocks
- alt.anonymous.messages
- premail
  - User interfaces matter
- Anonymous email “nearly solved”
  - What do you think?

Privacy for not mail

- Anonymous web browsing: anonymizer.com
  - Like type 0 remailers
  - Still (!) exists
- DigiCash
  - Note: needs anonymity to be useful
  - Limited anonymity: payer only
  - Lack of adoption

Future (predictions in 1997)

- DigiCash improvements
  - Bi-directional anonymity
  - More flexible use model
  - Netscape plugin
- Low-latency anonymity
  - Pipenet Design
  - Onion Routing
    - Trades off security and privacy in favor of peformance and robustness
- Is it better to have weak privacy and deployability, or strong privacy and no user base?

Abuse

- Abuse
  - Already becoming a problem in 1997
  - Spam
  - Harassment
- Dealing with abuse
  - Simplistic spam alarms
  - Receiver filtering (!)
  - Responding to political pressure
- What kind of abuse is there today?

Other challenges

- Anonymous publication
- Electronic voting
- Application-specific privacy
- Deployment

Motto

- “Privacy through technology, not legislation”
  - What do you think?

Part II: Present (2002)

- Crowds: anonymous web surfing
  - Forward requests among a crowd before going to the web server
  - No cryptography
  - Plausible deniability
- JAP
  - Remailer concept for network traffic

Anonymous Publication

- Free Haven
- FreeNet
- Publius
  - Distribute data among many nodes
  - Encrypt contents, protecting servers

Onion Routing

- NRL Onion Routing project
- Zero-Knowledge System's Freedom Network
  - Commercial venture
  - Paid other organizations to operate servers
  - User base too small, costs too high
  - Is there hope for commercial anonymity?

Electronic Cash

- The death of electronic payments
  - DigiCash failed
  - So did other payment schemes
  - Critical mass problem
  - Financial regulations
- Private credentials
  - Generalize electronic cash

Failure of Privacy Technology

- Anonymizer.com is the only success
  - Weak protection
  - Little infrastructure
  - Other models of revenue
- Privacy barriers
  - Infrastructure costs
  - Network effects

Privacy Technology Spectrum

- Single party
  - – ad blocker, cookie scrubbers, …
- Centralized intermediary
  - – Anonymizer.com, anon.penet.fi
- Distributed Intermediary
  - – Freedom Network, remailers, Crowds
- Server support
  - – Digital cash

Peer-to-peer

- A natural fit for privacy technologies
  - Address the issue of expensive infrastructure
  - Distribute trust
  - P2P users tend to *want* privacy
- Reputation becoming important
  - Ebay, Slashdot, Advogato
  - (all of these centralized)
  - Are there any P2P reputation systems today?

Identity vs PII

- Identity versus Personally Identifiable Information
  - Credit card #
  - Zip code
  - Favorites
- Personal information tools
  - Cookies
  - P3P
  - Enterprise privacy

Tech vs. Law

- A lot of privacy legislation has been introduced
- Were technologists wrong?
- They were right for security, but not for privacy
- Privacy involves how *other* people handle your data
  - You want your doctor to know your history, but not share it with marketers

Tech vs. Law

- What about anonymity, digital cash?
- If laws are the answer, what are we as technologists to do?

Other Comments on the Paper

Part III?

- 4 more years have passed
- What do you think has changed?