Privacy-enhancing technologies for the Internet

Ian Goldberg David Wagner Eric Brewer
University of California, Berkeley
{iang,daw,brewer}@cs.berkeley.edu

Organization

- Motivation: why worry about privacy on the Internet?

- Some history lessons

  - A representative example:
    Email privacy, from past to present

- Future challenges and directions

Motivation

Threats to online privacy:

- Unwanted monitoring
- Long-term storage of personal information
- The “dossier” effect
  - Cross-linking
  - Information mining and search

Motivation

Personal information available electronically:

- Usenet posts
- Web browsing habits
- Online phonebooks, e-mail and street address databases
- Public-access government archives; SSNs, credit reports sold

We are entering an information-centered age.

Controlling spread of personal information is fundamentally *hard*, yet increasingly important.

Motivation

Anonymity is useful:

- Privacy of identity information is central.
- Databases are usually cross-linked by identity.
- "Physical security through anonymity."
- Anonymity is the technique, privacy is the goal.

Motivation

The legitimacy of anonymity:

- Anonymity is widely accepted by society in non-Internet life.

- Some potential abusers:
  - “warez”
  - Spammers
  - Crackers, intruders

- But also many legitimate uses:
  - Privacy for everyday online activities
  - Support groups
  - Internet tip lines
  - Whistle-blowing, political dissent

History

- Early efforts on net privacy focused on e-mail.
- Lots of experience with anonymous e-mail.
- Lessons learned from e-mail apply to many other online apps.
- Some current developments mirror the history of e-mail privacy.

Therefore, we'll concentrate on the history of e-mail privacy technologies.

History

- Problem: headers identify sender of e-mail.

- Primitive solution: send message to a trusted friend, who manually strips headers and resends to the ultimate destination.

- Disadvantages: poor scaling, extremely weak security.

History

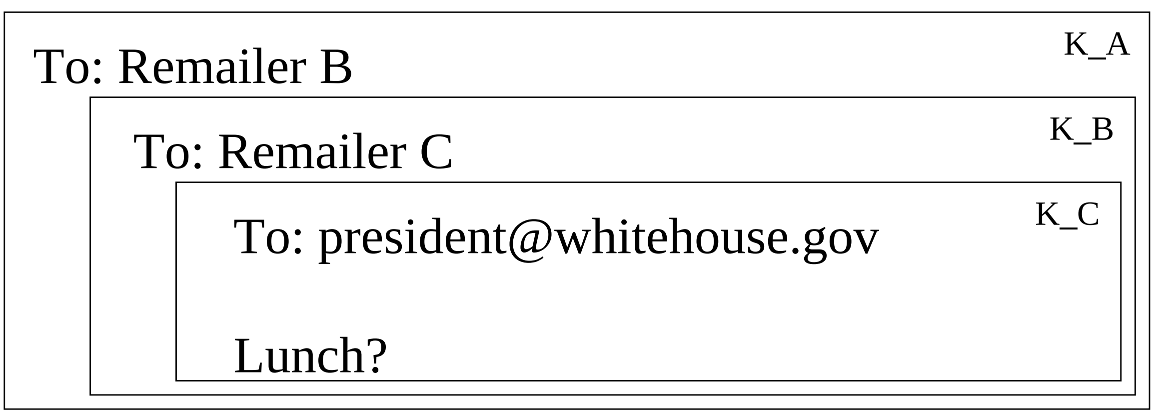
Next leap in technology:

- Type 0 anonymous remailer:
  - Automate the header-stripping and resending process.
  - Impact is a greatly expanded userbase.
  - Single trusted third-party.
  - `anon.penet.fi` the canonical example.
- Also, support for:
  - Pseudonyms: persistent anonymous identities.
  - Recipient anonymity: incoming e-mail to a pseudonym is remailed to owner.

History

Type I remailers:

- No logs; encryption; re-ordering
- Chaining support—a key idea!
  - Distributed infrastructure; no single point of failure
  - Example: Sender $\rightarrow$ A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ president



- Stronger threat model: compromised or colluding remailers, eavesdroppers, "after-the-fact" log recovery

History

Type II remailers:

- Full encryption and chaining, improved message re-ordering
- Cover traffic
- Constant-length messages
- Defenses against replay attacks
- Even stronger threat model: active attacks, eavesdroppers everywhere, statistical analysis

History

More advances:

- Anonymous Usenet posting
- “newnym” pseudonyms, via chained reply blocks
- Message pools
- Push some work to specialized clients
- Perfect forward secrecy
- Improved abuse management

Anonymous e-mail is largely solved.

History

Trends:

- Manual $\rightarrow$ automated $\rightarrow$ distributed
- Special-purpose solutions $\rightarrow$ general infrastructure
- More stringent threat models
- Greater use of cryptography
- Push more work to clients

Future

Directions:

- Anonymous web browsing, publishing
  - Current technology at about "type 0" level (at most)

- Anonymous digital cash

- Pipenet: general infrastructure for anonymity for low-latency Internet traffic

- Other specialized apps: voting, Eternity service, etc.

Future

Cross-cutting challenges:

- Abuse management and prevention
- Political and social acceptance
- Widespread deployment and user-friendliness

Conclusions

- Reviewed history of e-mail privacy-enhancing technologies, as representive case study.

- Directions for future research suggested.

- "Privacy through mathematics, not through legislation."