

# Privacy Considerations for Internet Protocols

Matt Blaze (AT&T Labs)

John Morris (CDT)

# What's the point here?

- We're working on a draft, called "Privacy Considerations for Internet Protocols".
  - what are privacy considerations?
  - advice to protocol designers on identifying and avoiding privacy problems
  - identify norms and expectations
- Many WGs are grappling with privacy
- Not our purpose to suggest that every RFC have a "privacy considerations" section
  - but if someone does, this draft will be helpful

# What is privacy?

- We're usually good at security
  - or, at least we usually know we're bad at it
  - a big focus is on protecting data from outsiders
- Privacy concerns data in transit *and* at rest
- Privacy violations can happen even when there has been no security violation
  - misuse of data (even by those with access)
  - legal processes
  - inadvertent disclosure
- Privacy protection (or violation) may be technical, procedural, or legal

# Why consider privacy?

- It's surprisingly easy to inadvertently make a protocol that violates privacy
  - architecture matters a lot
- The way we naturally do things sometimes has privacy implications
  - e.g., persistent identifiers (IPv6 addrs)
- People (the public) care about privacy
  - can make the difference between real-world acceptance of a protocol and not
  - laws sometimes affect this

# But why bother? Technology can't enforce this stuff

- Often, privacy rules will NOT be self-enforcing - our protocols will often not *technically* prevent privacy violations
- Privacy will often require enforcement based on legal and social norms
- But there is still value in expressing privacy expectations - privacy expectations in a protocol can facilitate later legal or social enforcement

# Personally identifiable and persistent information

- There are sometimes natural engineering and security reasons to exploit or require persistent identifiers
  - public key certificates
  - machine identifiers (ethernet address used to create IPv6 address, etc).
- Easy to design protocols that inadvertently include personally identifiable data in every packet or log entry, or hand this data to many different people

# Legal protections for “private” information

- Treatment under (US) law depends a lot on architecture:
  - your data stored with 3<sup>rd</sup> party may have less protection than if stored by you
  - different protection for data in transit vs. storage
  - data that doesn't exist has greatest protection
- Different standards for
  - law enforcement access
  - civil discovery
  - commercial use (data mining)

# Law Enforcement & Government Access

- Standards for government access vary widely, and may be surprisingly low
  - government may require handing over private data on request
- In most places, there is a legal mechanism to compel disclosure to government of data held by a third party (ISP, etc)
- In some places, there are requirements to *retain* data to facilitate future gov't access

# Civil Disclosure

- In US and elsewhere, parties to civil cases can “discover” data relevant to a case, even when it contains private info about others
  - telephone/ISP/customer records, etc.
  - server logs
  - email (in transit, in storage)
- People identified in such data may never know that their private information has been disclosed, or may learn only after the fact

# Commercial Use and Data Mining

- There may be few limitations on how someone who has handled data is allowed to use or disclose it in the future
- Scale has a big practical effect here:
  - data mining of multiple data sources makes it possible to draw inferences that reveal very private data
  - even small, innocuous disclosures can have privacy implications in the future, as technology and linked databases improve

# Europe

- Europe (EU) has specific privacy laws
  - limitations on commercial use and disclosure
- Protocols that reveal (or allow inferring) personally identifiable information may have implications in Europe
  - they may be illegal
  - they may impose surprising or cumbersome obligations on the users of the protocols
  - they may make it difficult to interoperate with other countries

# Example norms: Fair Information Practices

- Dates from 1970's, OECD, others
- Establishes norms for handling personal data:
  - no secret personal-data record keeping systems
  - must be a way to find out data held about you
  - must be a way to prevent personal data collected for one purpose from being used for another
  - must be a way to correct data held about you
  - must assure reliability and prevent misuse
- Some of these have significance to IETF

# What does this mean for us?

- By considering privacy early in the design process (maybe at the requirements stage), we can avoid inadvertently creating or worsening privacy issues
- At a minimum, we should identify privacy issues in our protocols
- We might want to ensure that every protocol has a “must implement” set of options that provides adequate privacy protection
- There’s no privacy directorate in the IETF...

# Contacts

- Wait for the draft (soon, we promise)
- Or send comments to:
  - `privacy-draft@crypto.com`
  - not a mailing list, just an alias for John and Matt
  - include name and social security number with all comments