Changes to Internet Architecture Can Collide With Privacy

draft-brim-mobility-and-privacy-00

Scott Brim
Bryan McLaughlin
Marc Linsner
Klaas Wierenga

Presentation Summary

- Privacy is important
- Location privacy for mobile users is a big issue
- Internet protocols that affect mobility architecture may unintentionally compromise location privacy
- Principles to keep in mind when designing
- What's next

Some of Us Stumbled On This

- Some of us were working on routing, addressing and mobility and stumbled on privacy issues
  - The others were a little more aware
- Now we realize that privacy issues pervade everything we do

Why Has It Become Such a Problem?

- Trends toward one user / one device, and to all-in-one devices
- Services that offer mappings between IP prefixes and locations
- Easier to find correlates and map to person
- If a correlation between device and human can be found in one context, then information can be gathered about that human in other contexts with less knowledge

Location Privacy Issues

- "… the interpretation of location data (e.g. which locations are visited, suggesting which shops are frequented, and which products and services are bought), may in the future permit the identification of the health, social, sexual or religious characteristics of the data subject."
    - RAND review of the European Data Protection Directive, May 2009

Privacy by Design

"Here we need a change of approach: Businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle**.** ***Privacy by Design is a principle that is in the interest of both citizens and businesses*****.** Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn have a positive impact on the economy. I have seen some encouraging examples, but much more needs to be done."

-- Viviane Reding, EU Information Commissioner, Jan 2010

Why Are We in INTAREA?

- The Internet must support constraint of personally identifying information to those scopes where it is required to fulfill service obligations
- Location leaking isn't just a higher layer problem
- Underlying protocols might make assumptions that compromise location privacy
- At worst they ***require*** loss of location privacy

Avoiding Making Users Trackable (details follow)

- Avoid correlatable data
- Do not require loss of location privacy
- Do not require persistent identifiers in ordinary packets
- Endpoint decides when to reveal confidential information

Avoid Correlatable Data

- Do not use personally identifiable information outside of its intended scope of confidentiality
- For example, access authorization tokens should not be used as global identifiers
- The more information that is casually leaked, the more possible, unexpected, correlations are possible

Do Not Require Loss of Privacy

- Do not require endpoint to reveal location to unintended parties in order to use the Internet
- A routing and addressing design must not assume that locations should always be known
- Particularly a problem if location can be discovered without knowledge or consent

Do Not Require Persistent Identifiers in Ordinary Packets

- Persistent identifiers in packets make it easier to make correlations
- Use temporary identifiers whenever possible

Endpoint Gets to Decide When to Reveal Confidential Information

- The decision on when to reveal information is up to endpoint
- Support route optimization, but not require it
- Default to location privacy
- This means hiding location in data plane too

Does This Affect You?

- Do you understand privacy?
- Do you understand the potential privacy implications of your designs?
- What are your deployment considerations for privacy?

What Next?

- Merge this draft with other privacy work
- Make privacy a consideration in every draft's security section
- Discuss on <https://www.ietf.org/mailman/listinfo/privacy>