New Opportunities and Challenges for Internet Privacy using ICN

Satyajayant Misra (New Mexico State University),
Hiroshi Nakagawa (University of Tokyo),
Dave Oran,
Thomas Schmidt (Hamburg University of Applied Sciences),
Jeff Burke (UCLA) - Chair

ACM ICN 2016, Kyoto, Japan

Objectives

1. Discuss the **unique opportunities and challenges that ICN presents for supporting end-user privacy**, in comparison with the existing Internet architecture as actually deployed and operating in the real world today.

2. Suggest **important research topics** for the community to consider at the **intersection of ICN technical innovation and societal objectives** with respect to end-user privacy.

Setup: **Privacy as *Contextual Integrity***

- In a widely cited article, Helen Nissenbaum (2004) argues for conceptualizing privacy as about **contextual integrity**: There is a context for the flow of information, and violations to this context are what cause privacy concerns.

- The three typical principles of concern:
  1. limiting surveillance of citizens and use of information about them by agents of government,
  2. restricting access to sensitive, personal, or private information, and
  3. curtailing intrusions into places deemed private or personal.

- Seems like ICN should be better at providing context for data… ?

Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev. 79* (2004): 119.

New Opportunities and Challenges for Internet Privacy using ICN.

Satyajayant “Jay” Misra
Associate Professor
Computer Science
New Mexico State University

ACM ICN
2016 KYOTO

Internet Privacy using ICN Panel

How to define end-user privacy as an *end-user* and as the *society*?

- One (of the many) way(s) to look at end-user privacy?
  - Minimum level of privacy that the end-user expects and needs in different dimensions: communication, activities, decisions, thoughts, and information.
    - end-to-end, location and identity anonymity, unlinkability.
  - Control over profiling by the state, cloud companies, multimodal datamining and machine learning (Google, Reddit, Power utilities, etc.) – Access to my data!
  - Sliding-scale based on users and applications (tunable), but with a "we got your back" approach.

- What should we as a society expect for end-user privacy?
  - Allow the user fine-grained control of how her data is stored, used, and shared.
  - Conditional-privacy with rigorous protection of fundamental rights
    - Prevention of information-based harm, information inequality, autonomy, freedom of speech, …

Privacy *challenges* and *opportunities* with ICN (specifically looking at NDN/CCN)

Challenges

- The bane of "identifiable" names: *Censorship*
- The downsides of caching: *Timing & probing attacks*
- Signature undermines privacy: *No identity anonymity*
- *Protocols can induce attacks and also increase overheads*

Opportunities

- Built-in security leads to better privacy
- Simultaneous use of multiple interfaces and paths improves privacy
- Use of caching can increase the anonymity set at the edge
- Use of trusted anonymizers improves identity anonymity
- Schematized trust to help with data storage and maintain privacy

Efficient privacy that expands into IoT and 5G looking into the future.

Slide 3: What privacy papers I would like to see in 2017?

- Challenges and responses for privacy at the ICN edge, IoT, and the new 5G paradigm?
  - IP framework will be poor at scalability and privacy, especially for IoT. Can ICN be better?
  - Can we leverage the lack of identity to improve privacy without affecting application efficiency?
  - Can application name transcend to the network level without undermining privacy?
  - Can we use ICN to give users more control on their privacy (data, actions, location, etc.) and how their diverse data can be fused and used?
  -

Location Privacy For ICN

Hiroshi Nakagawa

The University of Tokyo

End User's Location Should Be Kept Protected

- IT companies such as AOL, Facebook, etc. in the US might transfer or even sell user profiles to the government authorities.
- Location based internet services are everywhere.
- Users' location is an important element of user profile
  - Should it be protected from internet service (companies) , but how?
  - User name based routing makes hard to protect her/his location privacy.

- Then, users of internet services should employ technologies that protect her/his location and identity.

- Hopefully ICN routers are trusted to keep secret user's location and identity from internet service companies, but currently it is not .
- If we introduce Trusted Third Party in ICN, the problem is solved, but it seems to be unrealistic.

- User's own protection is needed.
  - Application of Private Information Retrieval Tech. is promising.
  - Several users nearby make a group, and send the set including all users locations in the group is sent to the service provider.
    - Each user only adds her/his location to the list and relay to the next user, and so on.
    - If the final user sends the list to router of ICN, the problem solved.
    - Question: does the final user's location become known?
    - Is a group easily made of users nearby on the fly?
  - Solution at ICN: If such a ICN router can anonymize name of a group when this type of packet arrived, it can be a solution.
  - It is one of add-on technologies of ICN for protecting user privacy.
- In Japan
  - Personal Information Protection Act has been passed the congress last year.
  - The act is not strict enough to protect privacy as EU GDPR does.
  - Independent Org. is not powerful enough as FTC of USA.
  - Privacy protection technologies are needed to ensure user privacy on ICN.

What privacy papers I would like to see in 2017?

- The proposal of add on tech. to ICN
  - Example1: shown in the previous slide
  - Example 2: k-anonymity added on.
    - A group consists of k-anonymized users whose locations are very nearby, get the same location based services from service provider without re-identification.
- Combination of privacy protection tech. and ICN, meaning ICN (router) understands the contents of ICN packet
  - It violates the secrecy of communication, is it?

ICN Privacy Panel

Dave Oran

~~Cisco Systems~~
Unaffiliated

Privacy in ICN is hard

May be harder than in IP – Why?

- Imputed properties of ICN have set expectations at odds with privacy:
  - Name-based routing to application-meaningful object names are visible to all forwarders
  - Global/ubiquitous caching provides significant benefits (if you believe all the papers…)
  - Objects are encryption at creation time with non-ephemeral keys rather than time of transmission
- The bar is higher than ever, so starting with something demonstrably less than IP won't fly:
  - State actors with lots of $$$ and surveillance capability
  - Confidentiality of data insufficient – need to protect the metadata, especially the names
  - Traffic analysis more powerful than ever (e.g. ML)

What do we do?

When going gets tough, the tough … go shopping?

- **Routing:**
  - Give up on granular routing to application names unless obfuscation/anonymization turns out to work well enough – jury is out – maybe more research will provide something compelling
  - Maybe don't try to do global ICN routing – just tunnel among mutually/transitively trusted domains. What do we lose? Is there really enough global multi-homing that routing in the core wins?
  - Give consumers trust-mediated control over routing (e.g. like SCION in XIA). Wide open possibilities for interesting research here?
- **Caching:**
  - Only cache in trusted forwarders near producer or consumer
    may be ok as edge caching arguably gives most of the benefits
  - Shared cache only for group-keyed objects– how effective is group keying? Is key lifetime short enough to be secure and long enough to be effective?
- **Encryption:**
  - Default to ephemeral keys
  - Give up on PFS?
  - Make group keying and broadcast encryption easy for applications
  - Can Proxy-re-encryption by cooperating producers help? Cost is high since all PK operations. Feasible at scale?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

ICN Privacy

Thomas C. Schmidt

t.schmidt@haw-hamburg.de

Internet Technologies Group

Two Dimensions in Privacy Violation

1. Personal data leaks to the public
   - Someone can learn (and may exploit) that I adore Michelle Obama
   - Always true for peers in conversational settings
2. Institutional data collection in silos
   - Some (single) entity can learn that I adore Michelle Obama + Red Bull + Suzuki Cars +++
   - May exploit (collection of) personal data and information asymmetry (i.e., information is only at the one party)

- In today's Internet, OTT service providers build their business on 2.
  - E2E encryption strengthens information asymmetry

Changes with ICN?

- ICN shifts information access towards the public
  - Names (content meta data) broadly visible
  - Reduces information asymmetry
- For an open ICN standard:
  - Publishing and consumption assisted by various ISPs
  - No E2E conversation, no obvious service monopoly (provided ICN works without central services)
  - Increases decentralized access (break-up CDNs ++)
- Research Question: "*What changes can we expect for the Internet infrastructure (stakeholders, topology, peerings, access …) when ICN governs deployment*"

Paper Ideas for 2017?

- Who pays for Youtube on an information-centric Internet? – a new economic model
- PURGE – An information-centric versioning network with history extinction