Dagstuhl Seminar on Information-centric Networking and Security

Summary

Börje Ohlman
Edith Ngai
Ersin Uzun
Gene Tsudik

June 2016
Attendees
Goals / Outcome for ICN 2016
(Topics that we listed in the seminar proposal)

1) Security and Privacy Attacks in ICN
2) Using object-level encryption for access control
3) Trust and Credential Management
4) Alternatives to end-to-end encryption in today’s Internet
Major Discussion Threads

• “Non-private” security
• Trust and identities
• Name privacy
Breakout Groups

• General security [Craig Partridge]
• Transport privacy [Christian Tschudin]
• Name privacy [Christopher Wood]
• Trust and identity [Jan Seedorf]
• ICN and IoT [Edith Ngai]
• Locators and Identities [Marc Mosko]
General Security

• What ICN entities need identities?
  – Producers: yes.
  – Consumers: mostly yes.
  – Routers: yes (for management)
• What entities can operate with a public/private key pair but no formal name?
  – ?
• Does splitting routing out as an application help?
• Do interests need to be authenticated at each router?
Trust and Identity

• End-hosts are superset of the “network layer”
• Can any application advertise any name it wants?
  — No.
  — … but how to manage this without a global authority?
• What’s the minimal trust information that we can factor out of a model?
• Applications should be able to specify model and middleware should enforce it
  — e.g., via schemas
Name and Transport Privacy

- Ideal name privacy: reveal no more than an IP address and port
- (Unsurprisingly) not possible without upper-layer service
- Encryption for name privacy:
  - How to route on them (efficiently)?
    - Use locators and hide the application name
  - How to obtain locators?
    - TBD
- Transport privacy:
  - Use flat names that are always different for the same content
    - No more caching
Forward Secrecy

• Not an essential feature of the architecture
• If it’s needed, build a protocol to do it on top
  – e.g., CCNxKE
• Key management in ICN is as hard as it is today
  – So, very hard...
Misc. Comments

• Make the architecture agile enough to move from boring crypto to post-quantum crypto for ICN eventually
• Routers should not do unbounded lookups or crypto in the dataplane
Looming Questions

• Do we really have to redo everything we do today in ICN? What is then the point?
• It seems that privacy/security are not significantly stronger or more attractive with ICN – so that’s not going to be the key differentiator that will drive ICN deployments (so what is?)
• How to achieve data persistency and some level of confidentiality, also after publishers have disappeared?
• Are we done with ICN yet?
Possible collaboration topics

• How to get ABE to work for IoT in an ICN context
• Possible draft on Simple security model for ICN
• Application of the end-to-end argument in systems design to ICN security functions (which security functions need to be placed into the network?)
Possible future Dagstuhl topics

• ICN Namespace Authority structure
  – Publication policies (e.g. to avoid FIB fragmentation)
• ICN and regulation, IPR, etc.
• How to build high performance ICN devices (in particular routers)
• How to build applications taking advantage of named data
After we finish...

- Things to think about and discuss during the seminar:
  - How to get out of the current situation:
    - ICN people trying to do security
    - Security people trying to do ICN
    - Did we find ways to make them to collaborate?
  - Yet another ICN Dagstuhl?
    - What would the next topic be?
    - Think about the format of this seminar, come with feedback
    - What is the MVP (minimal viable product) for ICN? What is going to drive actual deployment?
- How to best document seminar? CCR article?
  - Edith Ngai and Christopher Wood will drive the work
  - If you want to contribute, please talk to them
Practicalities: Agenda, Notes & Connectivity

• Agenda
  – On the Wiki
    • http://boemund.dagstuhl.de/wiki/index.php/16251
    • User name: 16251; Password: 5362
  – We’ll use Google Docs for notes, link at the Wiki

• Please upload your slides to the document server
  – Preferably upload them in pdf-format.