Private Communication in ICN

ICNRG 95 – Buenos Aires – 4/3/16

Mark Stapp, Cisco
Christopher Wood, PARC

Internet Privacy Threats (RFC 6973)

- Identification
  - reveal the identity of a user
- Correlation
  - connect actions performed by a single or multiple users
- Secondary use
  - replay user information without consent
- Disclosure
  - reveal (sensitive) information about a consumer
- Exclusion
  - hide outside usage of personal information

Today's Mitigation Strategy

- The IP model is converging
  - The environment has changed since 2006, 2009 (RFC7258)
  - RFC6973 as a guiding baseline
- Encryption by default (c.f. IAB statement 11/2014, DPRIVE,TCPINC)- It's a pretty bright line
  - minimizes data disclosed to the network
  - hides the details of all traffic (modulo packet headers)
  - ephemeral traffic and identifiers (intermediate caching doesn't help beyond retransmissions)
  - no correlation of user activity (modulo side channels)

What Does Private Mean?

	Encrypt Content	Forward Secure	Shared Cache	No Correlation Among Users
In the clear	X	X	✓	X
Per-user public key	✓	X	X	✓
Group key[1]	✓	✓2	✓	X
Private context	✓	✓	X	✓

1) Conveying the group key probably requires the 'private context'
2) Assuming the group key is used for a single object or a limited set of objects

What Does Private Mean?

	Encrypt Content	Forward Secure	Shared Cache	No Correlation Among Users
In the clear	X	X	✓	X
Per-user public key	✓	X	X	✓
Group key[1]	✓	✓2	✓	X
Private context	✓	✓	X	✓

The Internet and IETF are here.

Our claim: ICN communication should use a private context for Internet applications unless it impairs some necessary network feature.

What Does Private Mean?

- If ICN is to **complement or replace IP** as a general networking architecture, it needs parity with the emerging IP consensus
- Support major application models for the Internet
  - CDN-supported content delivery requiring authentication and access control
  - a la facebook, google search, youtube, netflix, bluejeans, twitch.tv
- Forward secrecy or not?
  - Resist passive data collection
  - Requires use of ephemeral keys, and key-negotiation protocol
- Separable authentication if we can't use identifiable/ bound/traceable public keys
- Resist/reject injected messages
  - Esp. if Interests can "actuate"

Implications

- DTLS-like exchange that establishes ephemeral, symmetric keys
- Private session packets don't name "objects”
- Need a top-layer protocol to setup a "private (outer) context” to carry messages (inner context)
  - CCNx-KE [1] is one way to do this
- Name prefixes become ’service context' names rather than 'object' names
  - Which actually aligns with our use of the Internet to reach services

[1] https://github.com/PARC/ccnx-keyexchange-rfc

Outer and Inner Context

- Private ICN messages have an outer and inner context
- Outer context identifies a service (by a locator) and an inner context carries ICN messages
- Inner context messages have all the existing properties of ICN messages
- Outer context messages still have plenty of ICN goodness:
  - Active, intelligent forwarding features
  - Receiver-driven flow control
  - In-network local repair, local retransmission (for individual clients)
  - Mobility still may benefit
  - Provenance/'publisher' concepts still available
  - Opportunity for in-network congestion control
  - Opportunity for *native* CDN support
  - New "layering" model
  - Opportunity for API clarity and richness
- Shift focus away from "content sharing" and towards other network functions: flow and congestion control, mobility, SP needs, CDNs, TE, QoS, VPN, P2P

Outer and Inner Context Implications

- Outer context does not eliminate provenance information
- No opportunistic caching for outer context
  - And some "natural multicast" properties may go away
  - But no more cache poisoning
- Opens questions about binding 'publisher' to 'content'
- No single reliance on well-known public keys for protecting all traffic
- Some of the MTU/fragmentation issues change
- New DoS vectors?
  - Maybe we can finally use client puzzles

Questions to Answer

- What are the privacy requirements for ICN applications that are not inherited from the TCP/IP world?
  - The TCP/IP model shouldn't define or constrain the ICN model
- What use cases or features are **impaired** by forward-secret communication?
  - The Internet worked to build on top of forward-secrecy, not around it
- What about the application interface?
  - For IP, privacy happens 'above' the 'base' network (OpenSSL, other frameworks)
  - How do ICN applications express their preferences or requirements?
  - How do ICN applications learn what is happening?

Backup

Discussion

- Where does the community stand?
  - comfortable saying "Parity with IP doesn't matter", or "It's fine to propose stepping backward"?
  - comfortable saying "Name exposure is acceptable, but encrypt content"?
  - uncomfortable with an ICN architecture that offers *less* than IP?