Private Communication in ICN

Mark Stapp, Cisco

IETF Prague, July 19 2015

What Does Private Mean?

- Doesn't ICN need parity with emerging IP consensus?
  - The environment has changed since 2006, 2009 (RFC7258)
  - Encryption by default (c.f. IAB statement 11/2014, DPRIVE,TCPINC)- It's a pretty bright line
- Support applications that need confidentiality, variety of authentication schemes, resistance to MITM and eavesdropping
  - Personal finance, Healthcare, On-line Commerce, IM, politically sensitive search, blogging, B2B
- Forward secrecy
  - Resist passive data collection
  - Indicates use of ephemeral keys with short lifetimes - distinct from typical ICN 'content verification' key lifetime
  - Probably also indicates use of symm ciphers with frequent key changes
- Separable authentication if we can't use identifiable/bound/traceable public keys
- Resist/reject injected messages
  - Esp. if Interests can "actuate"
- Useable for network infra?
  - Routing updates, fragments, control/hop-by-hop messages (whatever those turn out to be)
- Application Interface
  - For IP, privacy happens 'above' the 'base' network (openssl, frameworks)
  - How do ICN applications express their prefs/requirements?
  - How do ICN applications learn what is happening?

Object Privacy?

- Different goal from media protection schemes, where long-lived content is encrypted with keys that can be retrieved by authorized consumers
- Negotiate ephemeral master key (ECDHE, e.g.), derive symm key(s)
- Authenticate (at least S -> C for retrieval, mutual for interaction)
- Encrypt content at S with ephemeral key
  - And 'produce' it with some sort of unique-ified name?
  - How does client know what name to use?
    - Can't be a self-certifying name, since C doesn't know the content in advance
    - Could use a short-lived manifest?
  - Does ephemeral 'content' need a 'signature' also, to 'bind' the name to some anchor?
- How long should "private objects" be valid if they're encrypted with ephemeral keys that can't be recovered?
  - Is there any value in caching them, beyond local-repair?
- C + S have to engage somehow to negotiate keys
  - Or they have to do some very expensive per-Interest D-H operation
- Client might need to store objects, and then ... what?
  - No value in storing the un-recoverable version
- If the name exposes the communication ... what was the point?

Session Privacy?

- Plenty of existing well-understood schemes with varying properties
- ICN *names* themselves expose information
  - Can we provide just enough *name* to route, but leak as little as possible?
  - Mandate link encryption?
- Challenging to ensure that entire series of Interest messages reach a consistent destination
- Are there other potential advantages to interactive "sessions" that leverage the expense of asymm crypto and generation of key material?
- What would the implications for ICN be?

Implications

- Private session packets don't name "objects"
  - [Routable prefix] + [session/client nonce] + [sequence] ?
  - Need distinct messages for setup of "private sessions"?
  - Are the messages inside still Interest and Data?
- No opportunistic caching?
  - And some "natural multicast" properties may go away
  - But no more cache poisoning, so ...
- Opens questions about binding 'publisher' to 'content'
- May need to understand/control paths "private" message streams take
- "Just use well-known public keys" ... goes away
- Some of the MTU/fragmentation issues change
- New DoS vectors?
  - Maybe we can finally use client puzzles

Implications (2)

- Still 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 more explicit signalling
  - 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

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?

Backup