parc®
A Xerox Company

IDENTITY IN ICN "INTERESTS"

Marc Mosko

Palo Alto Research Center

ATIS eCON Presentation (June 30, 2016)

IDENTITY

- For our purposes:
  - A cryptographic MAC or Signature that can be used to uniquely identify the producer of the Interest.
  - This presentation is on the mechanisms to include Identity in a CCNx or NDN Interest message.
  - We will not get in to details about the cryptographic protocol usage of the identities (e.g. replay attacks, current possession of the private key, trust).
  - We will not discuss identity privacy.
- A cautionary note:
  - In general, it is not a good idea to verify signatures on Interests if it is not part of some explicit protocol. Otherwise, it is an easy computational DoS attack.

NDN TWO PACKET ENVELOPES

```
Data ::= DATA-TLV TLV-LENGTH
           Name
           MetaInfo
           Content
           Signature
Signature ::= SignatureInfo
              SignatureValue


Interest ::= INTEREST-TYPE TLV-LENGTH
               Name
               Selectors?
               Nonce
               InterestLifetime?
```

No Signature

NDN Packet Format (0.2-alpha-3), http://named-data.net/doc/ndn-tlv/

NDN SIGNED INTEREST

```
+-------------+----------+----------------------------------------------------------------------------------+
|  Interest   | Interest | +------+--------+-------------------------------------------------+ +----------+ |
| Type (0x01) |  length  | | Name |  Name  | +----------+--   --+---------+---------+---------+| | Other    | |
|             |          | | Type | Length | |Component|  ...  |Component|Component|Component|| | TLVs ... | |
|             |          | |      |        | |  TLV 1  |       | TLV n-2 | TLV n-1 |  TLV n  || | in       | |
|             |          | |      |        | +----------+--   --+---------+---------+---------+| | Interest | |
|             |          | +------+--------+-------------------------------------------------+ +----------+ |
+-------------+----------+----------------------------------------------------------------------------------+

                                              \                                    /\         /
                                               ----------------  ------------------  ---  ---
                                                              \/                        \/
                                                     Signed portion of Interest       Signature


/signed/interest/name/<timestamp>/<random-value>/<SignatureInfo>/<SignatureValue>

                     \                                                         /
                      -----------------------------  --------------------------
                                                   \/
                                  Additional components of Signed Interest
```

Identifies the signature (KeyLocator or KeyId)

Ndn-cxx documentation, http://named-data.net/doc/ndn-cxx/0.4.0/tutorials/signed-interest.html

NDN IN CONSTRAINED ENVIRONMENTS

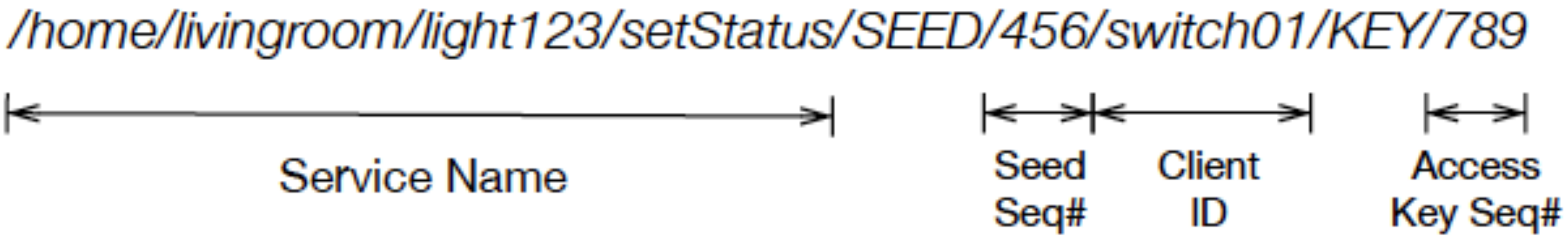
/home/livingroom/light123/setStatus/SEED/456/switch01/KEY/789
Service Name
Seed Seq#
Client ID
Access Key Seq#

Fig. 4: Naming convention for the access key

An access control server verifies the client identity and issues it a derived key based on "/456/switch01/789"
Uses an HMAC Signed Interest.

NDN Technical Report NDN-0036, 2015. http://named-data.net/techreports.html

CCNX SINGLE ENVELOPE

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|    Version    |  PacketType   |         PacketLength          |
+---------------+---------------+---------------+---------------+
|           PacketType specific fields          | HeaderLength  |
+---------------+---------------+---------------+---------------+
/ Optional Hop-by-hop header TLVs                               /
+---------------+---------------+---------------+---------------+
/ CCNx Message TLV                                              /
+---------------+---------------+---------------+---------------+
/ Optional CCNx ValidationAlgorithm TLV                         /
+---------------+---------------+---------------+---------------+
/ Optional CCNx ValidationPayload TLV (ValidationAlg required)  /
+---------------+---------------+---------------+---------------+
```

Validated region

Identifies the signature (KeyLocator or KeyId)

CCNX INTEREST NAME

- Because the validation is outside the name
  - A forwarder cannot distinguish between two different validations and the same name.
  - Therefore, one must still include a nonce in the name (like the NDN <random-value> component).
  - The ValidationAlgorithm has a Signature Time field to facilitate detection of time-based replay attacks, so that does not need to go in the name.

COMPARISON

- CCNx has a single packet envelope.
- NDN puts the SignatureInfo and SignatureValue in the Name, which makes the Name very long. It must be stored at each hop. The responding Data object must carry the same name prefix, so it must echo back all the bytes of the SignatureInfo and SignatureValue.
- The CCNx approach is to put a de-multiplexer in the name and all the large fields elsewhere. The responding ContentObject only needs to have a name that matches that shorter name.
- The CCNx method allows for CRCs and MACs over the validation region, not just the name.
- CCNx allows for payload in an Interest, so identity could be conveyed in application-specific messages.

COMMON SHORTCOMINGS

- As described, these mechanisms can be used in “one-shot” Interests
  - Can allow replay attacks
  - If there are multiple authoritative produces, replay attacks are much simpler unless the producers share state
  - There is no proof of current possession of the private key, apart from the freshness of the timestamp, but that is not witnessed so it could have been generated in the past.
  - These identity mechanisms are best used as part of a larger protocol, not as “one-shot” Interests.