Asymmetric Manifest-Based Integrity (AMBI)

Jake Holland <jholland@akamai.com>
Kyle Rose <krose@krose.org>
Akamai Technologies, Inc.
Problem statement

Inter-domain multicast has security issues

● Why multicast?
  ○ Same data to many clients
  ○ Loss is okay
  ○ Data with a deadline
Integrity scheme requirements

- Line-rate verification
- Asymmetric crypto
- Efficient (power, CPU time)
- Loss-tolerant
Single manifest

anchor

signature

manifest

integrity info

... 

hash

packet id

data packets

packet id

data

packet id

data

packet id

data

...
Manifest tree

- Anchor
- Root manifest
- Signature
  - Integrity info
- Child manifests
  - Packet id
    - Integrity info
  
- Data packets
  - Packet id
    - Data
Rolling root manifest
Example threat model
Anchor discovery

Fetch anchor using DNS:
5.2.0.192.in-addr.arpa. RRTYPE AMBI
→ https://example.com/anchor1.json

untrusted traffic

AMBI IS

RPF signaling

join(S,G) = 192.0.2.5 → 232.2.2.5
Next steps?

- Analyze loss resiliency and determine optimal overlap/redundancy
- Use a Merkle tree-like structure to combine data and authentication in the same packet?

Reopen msec?
Looking for feedback

- Improvements to protocol
- Improvements to data model for anchor message
- Feedback on the DNS thing