ICN Content Security Using Encrypted Manifest and Encrypted Content Chunks

Dante Pacella
Verizon Labs
dante@verizon.com

Mani Tadayon
Verizon Labs
mani.tadayon@verizon.com

Ashish Sardesai
Verizon Labs
ashish.sardesai@verizon.com

Venkat Josyula
Verizon Labs
venkat.josyula@verizon.com

March 2017
Abstract and Background

Ubiquitous/opportunistic caching in ICN:
• Benefit: enables receiving content from nearest node with content in cache
• Drawback: content owner loses distribution control and analytics info

Proposal solves aforementioned issue by:
• Generating encrypted content
• Encrypting manifest per consumer
• Modifying the Namespace in initial Interest message for authentication, authorization, and analytics
Design – Chunking and Encryption

Chunk (divide into pieces) Content File
Encrypt Chunks using a separate Key(or Key Pair) for every set of Chunks (1 ... \( n \)) to Node Group (1 ... \( n \)) pairing
Design: Manifest Generation

Create the Manifest (include Nameless Object Reference (Hash of Encrypted Chunks) and encryption credentials)
Design: Namespace Modification

Namespace modification for Interest messages takes the form of a consumer_ID plus nonce encrypted with the public key of the producer/provider.

Example: namespace modification from different consumers for the same content
/foo/bar/content1/ID=dfdec888b72151965a34b4b59031290 --encrypt(<random> + consumer1234)
/foo/bar/content1/ID=21596697d99734b8ac04c4baa3988a --encrypt(<random> + consumer5678)

Example: namespace modification from same consumer for any content
/foo/bar/content1/ID=22f65b72888151965a90329034b1b5 --encrypt(<random> + consumer1234)
/foo/bar/content2/ID=855c3697d9979e7804c4ba2c6653 --encrypt(<random> + consumer1234)
Design: Delivery

[Diagram showing the flow of content delivery from Producer to Consumer through a Forwarding Node, with details on the exchange of INTEREST and CONTENT OBJECT messages with encrypted Manifests and Chunks.]
Summary

ICN Content Security:

• Provides a scalable and distributed method for content access control and usage analytics

• All chunks can be cached ubiquitously achieving bandwidth savings

• Consumer Identifier in namespace guarantees uniqueness for Manifest Interest allowing discrete distribution control

• Longest prefix match results in efficient and manageable FIB sizes across the network
Thank you.