Data Authentication in NDN
Trust Schema

Alex Afanasyev (FIU)
Automating the use of crypto keys via named data

◊ Use name semantics to enable applications to reason about security, and

◊ Utilize NDN naming/naming conventions to automate key management in
  o Secure sign-in
  o Certificate issuance
  o Signing and verification
  o Content encryption
Data-Centric Security in NDN

Data-Centric Authenticity (Trust Schema)

Data-Centric Secrecy (Name-Based Access Control, etc.)

Signed by

Availability

Confidentiality

Authenticity
Data Authenticity

KeyLocator: /home/.../KEY

Signed by

KeyLocator: /AlexHome.com/.../KEY

Signed by
Not Just Signature, but Whose Key Signed It?

A frame from a camera I have installed in my living room

A forged frame pretending to be an image of my living room
Defining Trust Model for My Smart Home

◊ Room’s video feed can only come from a camera in the room

◊ Cameras in the room can be configured by someone I have authorized

◊ Only I can authorize users to play with my cameras
Defining Limits via Namespace Design

/home/Users/Alex/KEY/_id=42

Local trust anchor

/home/.../KEY/_id=12

LivingRoom
Kitchen
1st Floor

VideoFeed
Temperature
Humidity

Household

Police
Emergency

2017-02-28
2017-03-01
2017-03-02
Restricting Power of Keys

The new key is now restricted to authorize data and operations within the **living room** only.
Restricting Power of Keys

The delegate key is now even more restricted: to publish "camera" data in the living room with a static frontal view.
Restricting Power of Keys

Camera’s key has a very narrow privilege
A formal language to formally describe trust model

- Schematize data and key name relationships

<CONST> <>

(token*) (token?)

[func]

(:group:token)
Schematizing Rules: Specific Restriction

<home><Users>[user]<LivingRoom><KEY>[key-id]

Can only be signed by

LocalAnchor

User rule
Schematizing Rules: Broader Restriction

<home><Users>[user](:Location:<>?)<KEY>[key-id]

Can only be signed by LocalAnchor

User rule (parametrized by Location)
Schematizing Rules: Generalized Restriction

(User rule (parametrized by Prefix and Location)

(:Prefix:<>*)<Users>[user](:Location:<>?)<KEY>[key-id]

LocalAnchor(Prefix)

Can only be signed by

/KEY/_id=1

/other-home

/home

/other-home

/Users

/Alex

/Users

/LivingRoom/<KEY>/KEY/_id=42

/other-home

/other-home

/Users

/Users

/LivingRoom/<KEY>/KEY/_id=1

/other-home

/Users

/LivingRoom/<KEY>/KEY/_id=......
Schematizing Rules: Generalized Restriction

(:Prefix:<>*<Users>[user](:Location:<>?)<KEY>[key-id]

Can only be signed by

LocalAnchor(Prefix)

User rule (parametrized by Prefix and Location)
Privilege Separation Through Naming

Local Trust Anchor

Limit to LivingRoom

Limit to a specific video feed view

/home
/Users
/Alex
/LivingRoom
/Camera
/CSP750
/View/FrontView
/_id=1
/_id=42
/VideoFeed
/BackView
/Kitche
n
/Frame=1
/Frame=2
/Frame=3
Camera rule (can be parametrized with Prefix, Location, and View)
Schematizing Data-Key Naming Rule: VideoFeed

Camera(Prefix, Location, View)

Must be signed by VideoFeed rule (can be parametrized with Prefix, Location, and View)
Complete Example of Smart Home Trust Schema

(:,Prefix:<>*)(:Location:<>?)<VideoFeed>[View]<mp4><frame><chunk>
Camera(Prefix, Location, View)

(:,Prefix:<>*)<Cameras>[cam-id](:Location:<>?)<View>[View]<KEY>[key-id]
User(Prefix, Location)

(:,Prefix:<>*)<Users>[user](:Location:<>?)<KEY>[key-id]
LocalAnchor(Prefix)

/home/Users/Alex/KEY/_id=1

General Trust Model

Trust Model Specialization
for my smart home
Trust Schema as an Automation Tool

Usable Data Authenticity
Trust Schema Summary

◊ Hierarchical data/key name relations embed real power
  ○ Differentiated levels of security and separate privileges

◊ Trust schema influence the application namespace design and is influenced by the namespace design

◊ Enables automation for data validation and signing

◊ Enables automation of NDN certificate management
Demo

Example of simple trust schema in ValidatorConfig (“old”) format