Building a CCN Trust Model

Karthikeyan Natarajan
Vahab Pournaghshband

UCLA

June 3, 2010

Overview

- Problem Formulation
- Current Approaches
- Our Approach
- Security Analysis

Problem Formulation

Interest Packet

Content Name
Selector (order preference, publisher filter, scope, …)
Nonce

Data Packet

Content Name
Signature (digest algorithm, witness, …)
Signed Info (publisher ID, key locator, stale time, …)
Data

- **Digital Signatures**
  - **Private key signs, public key verifies**
- **But, are we using the "right" public key?**
  - **Key verification problem**

Current Approaches

- Leap-of-Faith
- Pretty Good Privacy (PGP)
- Certificate Authority (CA)
- DNSSEC

Our Approach

Alice

Bob's Key?

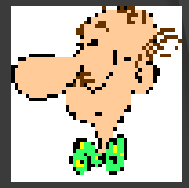
Bob's Key?

Hello,Bob

K_A F

K_A F

K_A



Bob

K_A

K_A K_A K_A Bob's Key?

Offered Key

Observations

K_A F

Client Policy		
	Consistent	Accept Key, Continue
	Inconsistent	Reject Key, Abort Connection

Key Interest Message

- **Name Convention**
  - `/myfriend/key_service/pubkeyID--keyLocator--issuer's nonce`
- **Requires Signature by Issuer**
- **Maintaining a Table**
  - **Pairs of <issuer's nonce, pubkeyID>**

Interest Packet

Content Name
Selector (order preference, publisher filter, scope, …)
Nonce

Key Response Message

- Two Possible Response Messages
  - *Signed(publisher's name* || *publisher's key)*
  - *Signed(publisher's name* || *I don't have it)*
- Why publisher's name?
- Why signed?
- Why "I don't have it" response?

Trust Bootstrapping

Trust Community

- Friends
  - Who are my friends?
  - Out-of-band mechanism

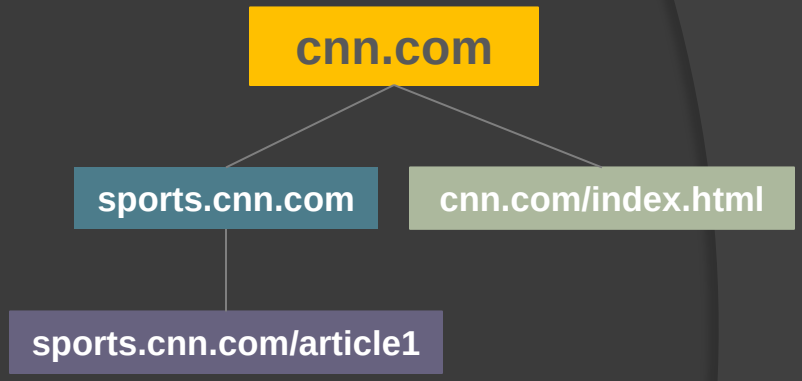
    (e.g. Facebook, visit cards)

- Notaries
  - What are notaries?
  - How to obtain keys?

    (e.g. Security through Publicity)

Notion of Master Key

- **What is a master key?**
  - Public Key
  - Longer Lifespan
  - Used Only to Sign Keys in Sub-domain
- **Role of Master Key?**
  - Plays as the Certifying Authority
  - Signs (certifies) Sub-domain Keys
- **Why is it useful?**
  - Less Network Overhead:
    - Less Key Verification by Flooding Trust Zone
    - Less Frequent (master) Key Changes
  - Flexibility
- **Why better than current CA?**
  - Does not Involve Third Party



Key Revocation

- A Key consists of:
  - `Public Key`
  - `Key Identifier`
  - `Expiration Date`
- How to Revoke?
  - Key Expiration Date
  - Immediate Rollover by *Notifying Notaries*
- How to Learn?
  - When Verification Fails

Trust Policy

Quorum: minimum agreement needed to consider a key valid

Notary #1	Friend #1	Notary #2	Friend #2	Friend #3
K_A	K_A	K_A	K_B	K_A

If offered key is K_A:

if Q ≥ 80% then Accept
else then Reject

Security Analysis

- Man-in-the-Middle Attack
  - Accepting Fake Key
  - Key Change Deception
- Denial-of-Service Attack
  - Dropping Key Response Messages
- Replay Attack

Security Analysis

- Compromised/Malicious Notary
  - Incorrect Responses
- Compromised/Malicious Friend
  - Incorrect Responses
  - Issuing frequent bogus key interest messages

Reputation System

Factors to Consider:

- Correctness
- Cooperativeness
- Personal Trust
- Responsiveness?

Summary

- Basics Implemented
- Avoids One-fits-all Model
- Higher degree of client control over trust decision
  - Chooses who to trust
  - Trust community
  - Defines security
- No need to trust/pay third party
- Robust against attacks
- Privacy issues