An Overview of Security Support in Named Data Networking

Zhiyi Zhang, Yingdi Yu, Haitao Zhang, Eric Newberry, Spyridon Mastorakis, Yanbiao Li, Alexander Afanasyev, and Lixia Zhang

Presenter
Md Bulbul Sharif

Outline

- Introduction
- Background
- An Example Application
- Goals, Challenges and Solutions of the NDN Security Design
- NDN Security Bootstrapping Process
- Comparison of NDN and TCP/IP Security
- Personal Opinions

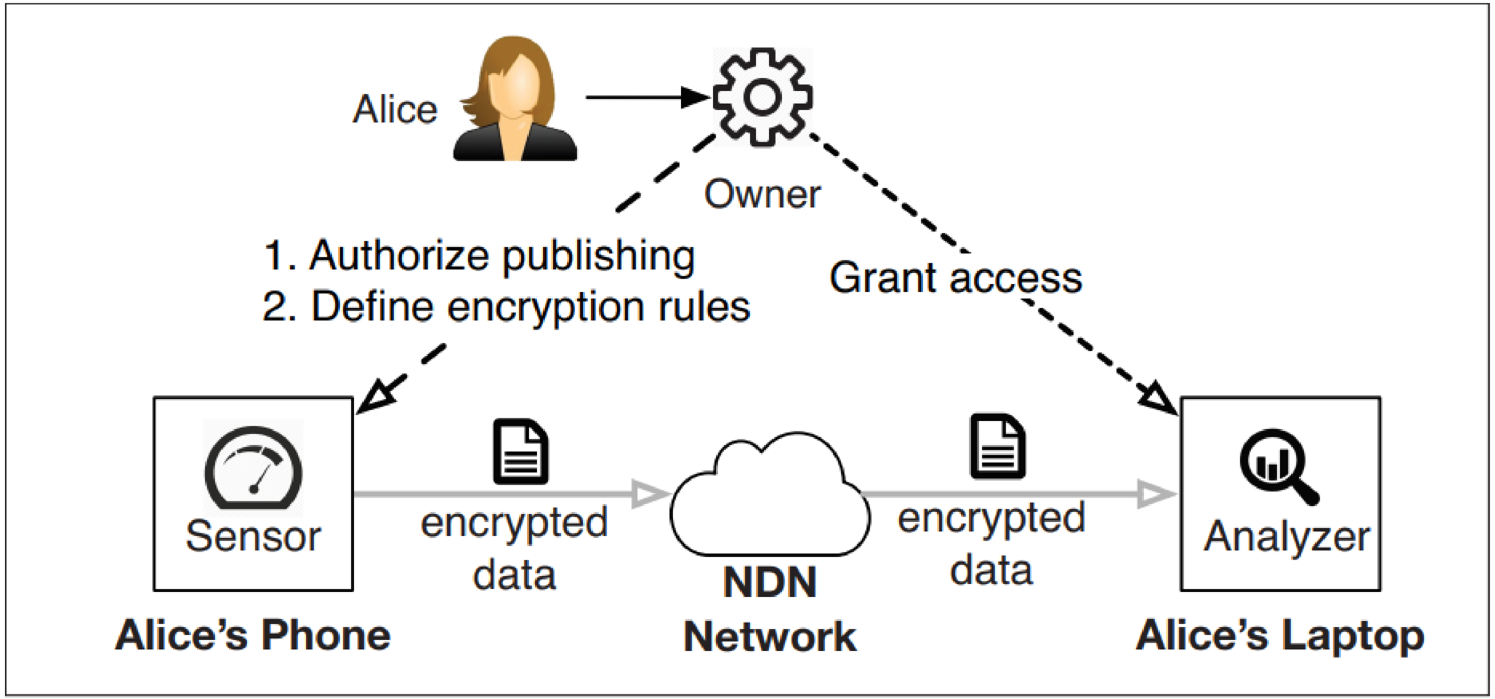
Introduction

- Named data networking (NDN)
  - Internet architecture which changes the network communication model.
  - Application-layer names instead of delivering packets to receivers identified by IP addresses.
  - Secure data at the network layer.
- An overview of NDN's security framework
- Illustrate the developed mechanisms
- Illustrate how applications can utilize name semantics

Background

- Shifting HTTP's request and response to the network layer.
- Request carried in an NDN Interest packet containing the name of the requested data.
- Producers: Produce data, Consumers: Request data.
- NDN and HTTP data differs in two ways
  - All NDN Data packets are immutable
  - NDN Data packet carries a signature

An Example: NDNFit



NDN Security Design Goals

- Secures data directly
- Provide highly usable security
- Cryptographic key management and operations should be automated
- Minimizing the reliance on manual configuration

NDN Security Design Challenges

- Establishing Trust Anchor(s)
  - Cryptographic verifications must terminate at a trust anchor.
  - Authority of each networked system establishes its own trust anchor(s).
  - Entities under authority can discover trust anchors through local system settings.
- Providing Effective Solutions for Trust Management
  - Must enable applications to express their own trust policies.
  - Entities are able to obtain certificates and learn policies from trustworthy parties.
  - Inform entity which keys should be used for signature generation and verification.
- Providing Usable Key Management Solutions
  - Requiring mechanisms to assign and deliver the correct keys to the parties automatically.
  - Enables developers to define naming conventions to construct the names of the cryptographic keys.

Basic Components of NDN Security

- Digital Keys
  - NDN treats cryptographic keys as any other named data and allow them to be retrieved using Interest-Data exchanges at the network layer.
- Certificates
  - A certificate is a Data packet carrying a public key and can be fetched like any other Data packet.
  - /ndnfit/alice/KEY/001/N-testbed/002
- Trust Policies
  - Applications define trust policies
  - A trust policy can require that the key used to authenticate data must not be used to sign encryption keys.

Security Bootstrapping in NDN

- Obtaining Trust Anchors
  - An entity needs trust anchors to verify other entities' authenticity.
  - NDN security design assumes that different systems establish their own trust anchors.
- Obtaining Certificates
  - To generate Data packets with valid names and verifiable signatures, a producer must first obtain a name and a certificate.
  - Developed the NDN certificate management system to process certificate requests automatically.
- Learning Trust Policies
  - To determine cryptographic key's legitimacy an application needs to obtain trust policies.
  - Default policy may define that Data packets carrying trust policies must be directly signed by a trust anchor with a given name.

Data Authenticity

- Validation by Trust Policies
  - Data name, the signing key name, the relationship between the key name and Data name, and the trust anchor name must follow application-defined rules.
- Signature Verification
  - To verify the signature in a received Data packet, a consumer retrieves the certificate of its producer.
  - The received data packet is considered valid only if all the certificates in the above chain have valid signatures and satisfy the trust policies.

Data Confidentiality

- Developed named-based access control (NAC) and its enhancement with attribute-based encryption (NAC-ABE)
- Name-Based Access Control
  - Key Generation
  - Data Production
  - Data Consumption
- Access Control Granularity

Data And Certificate Availability

- Improving Data Availability Via In-network Storage
  - NDN secures data directly, so Data packets can be retrieved from anywhere
- Certificate Availability
  - NDN certificates are carried in Data packets
  - Authors have developed the NDN certificate bundle to allow each producer to collect all the certificates

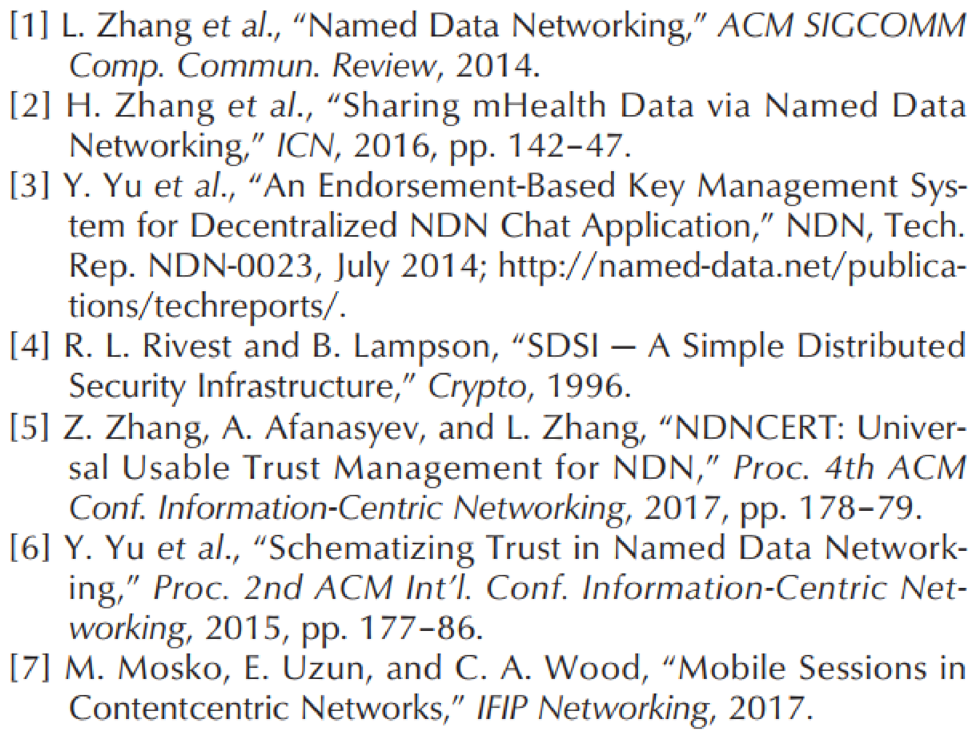
Comparison of NDN and Tcp/Ip Security

- Securing Data vs Securing Channels
    - TCP/IP - a channel between two processes.
    - Data could have been altered before entering the channel and loses cryptographic protection as soon as it leaves the channel
    - NDN secures data directly, removing any reliance on the security of intermediate communication channels
- Establishing Trust Using Name Semantics
    - Existing certificate authentication solutions lack the means to effectively reason about trust.
    - In NDN, entities may utilize local authorities instead of commercial certificate authorities as trust anchors.

Personal Opinions

- The authors assume that readers have some basic knowledge of cryptography.
- Authors have claimed that they omit details because of space.
- Developed other tools.
- How to solve scalability and manageability issues?
- What if local authorities compromise?

Reference



[1] L. Zhang *et al*., "Named Data Networking," *ACM SIGCOMM Comp. Commun. Review*, 2014.

[2] H. Zhang *et al*., "Sharing mHealth Data via Named Data Networking," *ICN*, 2016, pp. 142–47.

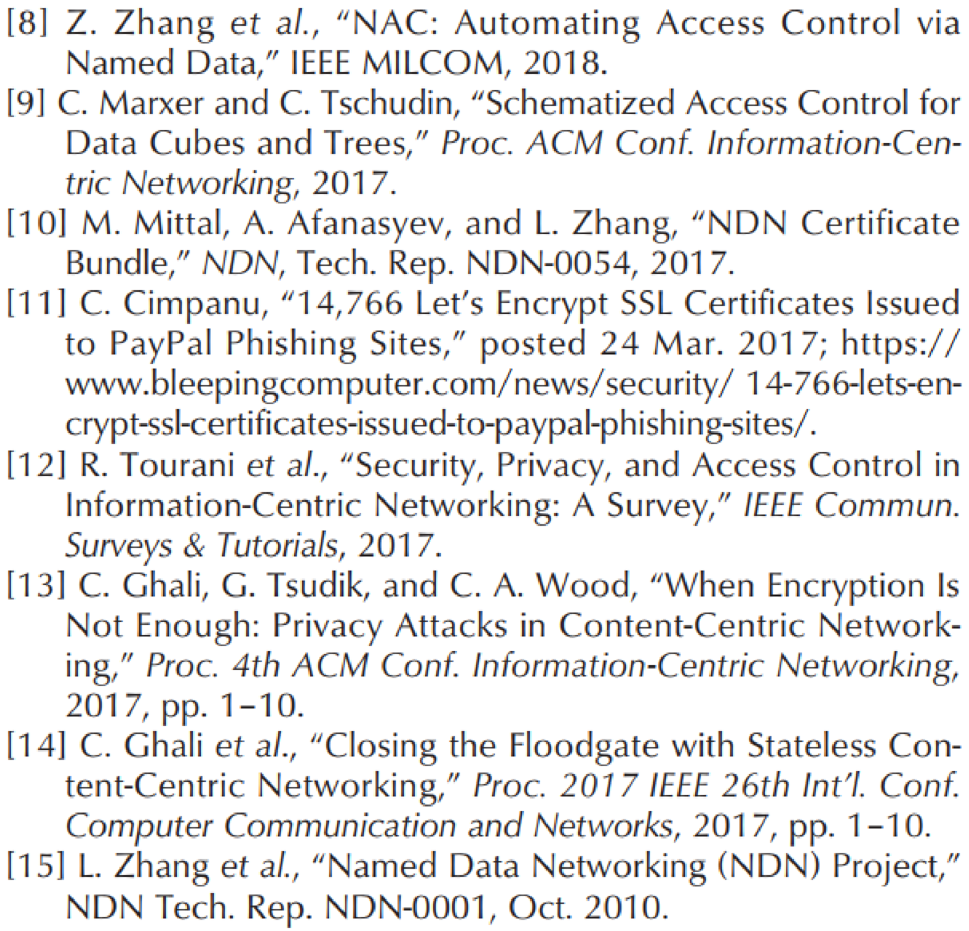
[3] Y. Yu *et al*., "An Endorsement-Based Key Management System for Decentralized NDN Chat Application," NDN, Tech. Rep. NDN-0023, July 2014; http://named-data.net/publications/techreports/.

[4] R. L. Rivest and B. Lampson, "SDSI — A Simple Distributed Security Infrastructure," *Crypto*, 1996.

[5] Z. Zhang, A. Afanasyev, and L. Zhang, "NDNCERT: Universal Usable Trust Management for NDN," *Proc. 4th ACM Conf. Information-Centric Networking*, 2017, pp. 178–79.

[6] Y. Yu *et al*., "Schematizing Trust in Named Data Networking," *Proc. 2nd ACM Int'l. Conf. Information-Centric Networking*, 2015, pp. 177–86.

[7] M. Mosko, E. Uzun, and C. A. Wood, "Mobile Sessions in Contentcentric Networks," *IFIP Networking*, 2017.



[8] Z. Zhang *et al*., "NAC: Automating Access Control via Named Data," IEEE MILCOM, 2018.

[9] C. Marxer and C. Tschudin, "Schematized Access Control for Data Cubes and Trees," *Proc. ACM Conf. Information-Centric Networking*, 2017.

[10] M. Mittal, A. Afanasyev, and L. Zhang, "NDN Certificate Bundle," *NDN*, Tech. Rep. NDN-0054, 2017.

[11] C. Cimpanu, "14,766 Let's Encrypt SSL Certificates Issued to PayPal Phishing Sites," posted 24 Mar. 2017; https://www.bleepingcomputer.com/news/security/ 14-766-lets-encrypt-ssl-certificates-issued-to-paypal-phishing-sites/.

[12] R. Tourani *et al*., "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Commun. Surveys & Tutorials*, 2017.

[13] C. Ghali, G. Tsudik, and C. A. Wood, "When Encryption Is Not Enough: Privacy Attacks in Content-Centric Networking," *Proc. 4th ACM Conf. Information-Centric Networking*, 2017, pp. 1–10.

[14] C. Ghali *et al*., "Closing the Floodgate with Stateless Content-Centric Networking," *Proc. 2017 IEEE 26th Int'l. Conf. Computer Communication and Networks*, 2017, pp. 1–10.

[15] L. Zhang *et al*., "Named Data Networking (NDN) Project," NDN Tech. Rep. NDN-0001, Oct. 2010.

Thank You