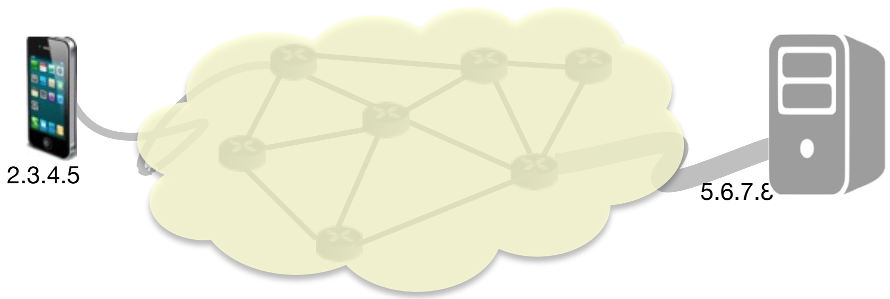
NDN Security Concepts and Tools

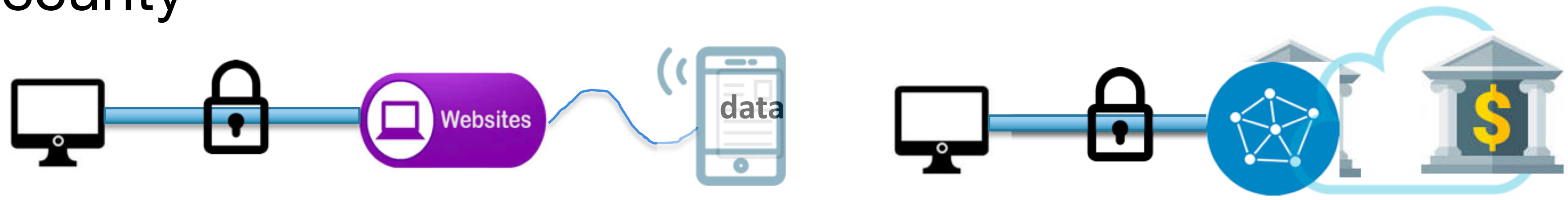
LIXIA ZHANG (UCLA)

- ◊ Secure networking: a great challenge
- ◊ Big efforts, largely incremental progress

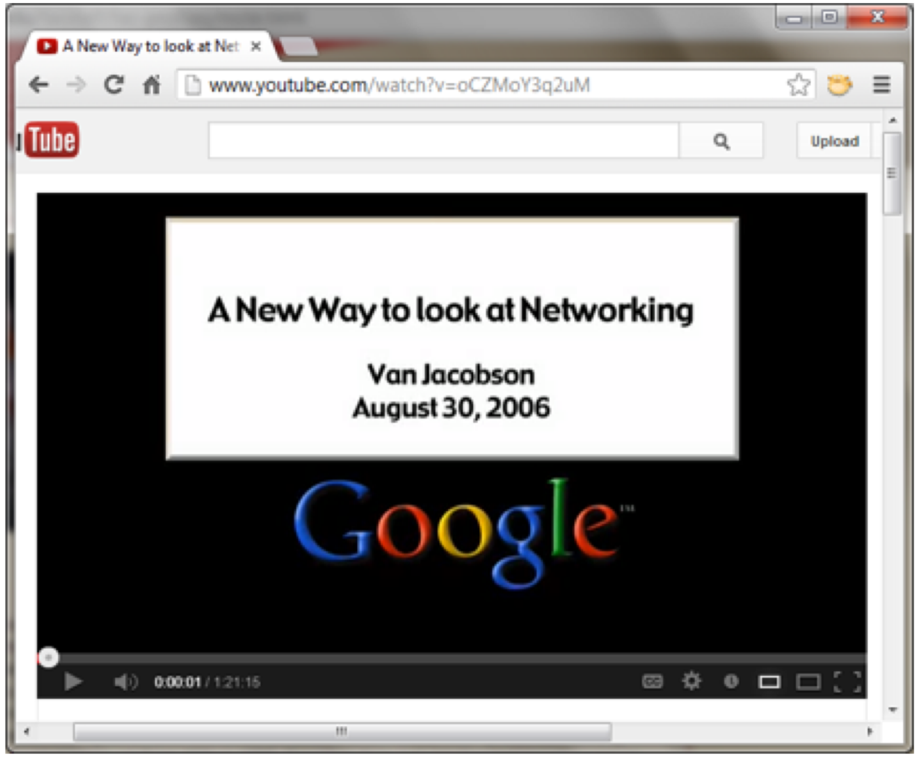
- Today's networking



- Today's security



- How to achieve end-to-end data security?



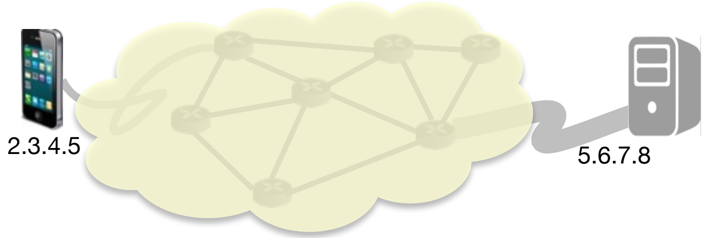
A New Way to look at Networking

Van Jacobson
August 30, 2006

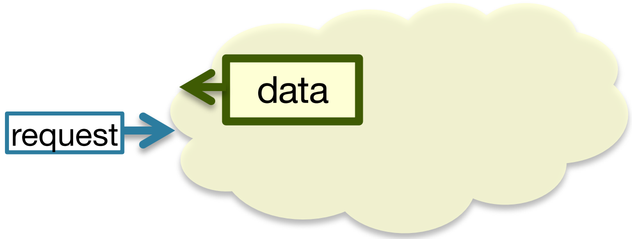
https://www.youtube.com/watch?v=oCZMoY3q2uM

What’s the new way:

- IP delivers packets to hosts based on numeric IP addresses

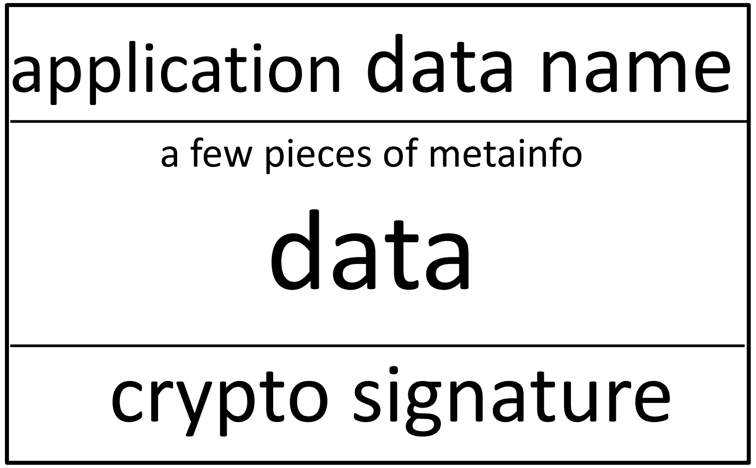


- Named Data Networking fetches data by using application data object names



- Example data names
  - www.nist.gov/document/ndnagendav5docx
  - www.youtube.com/watch?v=oCZMoY3q2uM
    - Large objects fragmented to multiple packets, each fragment uniquely named

Naming data enables securing data directly



application data name

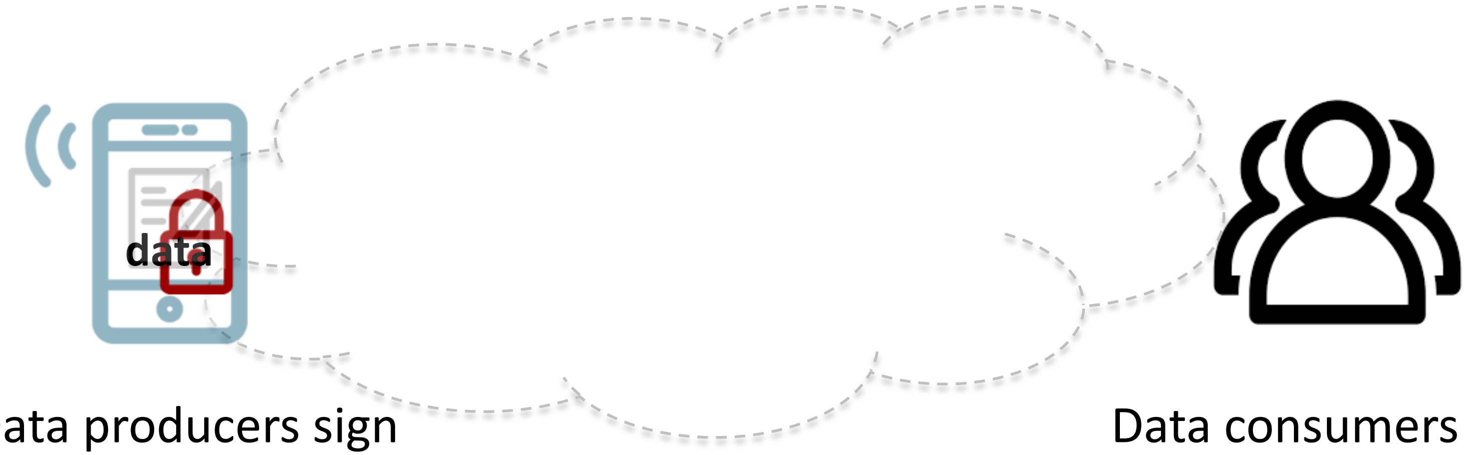
a few pieces of metainfo

data

crypto signature

The signature binds the name and content at data production time

End-to-end data security



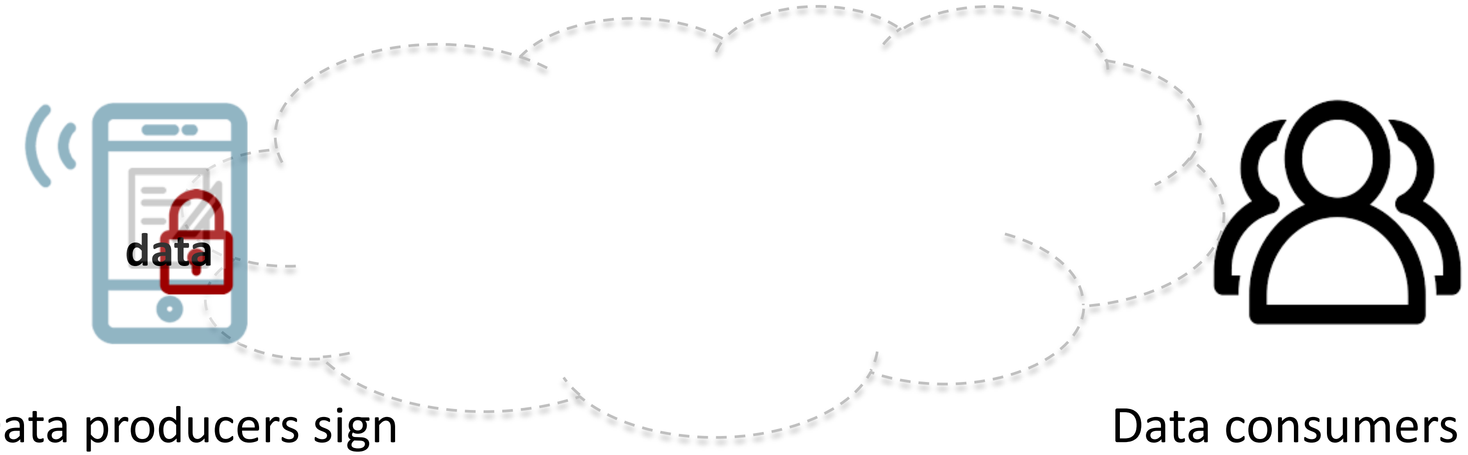
Data producers sign

Data consumers verify

End-to-end data authenticity

independent from intermediate communication channels, middle boxes, intermittent connectivity

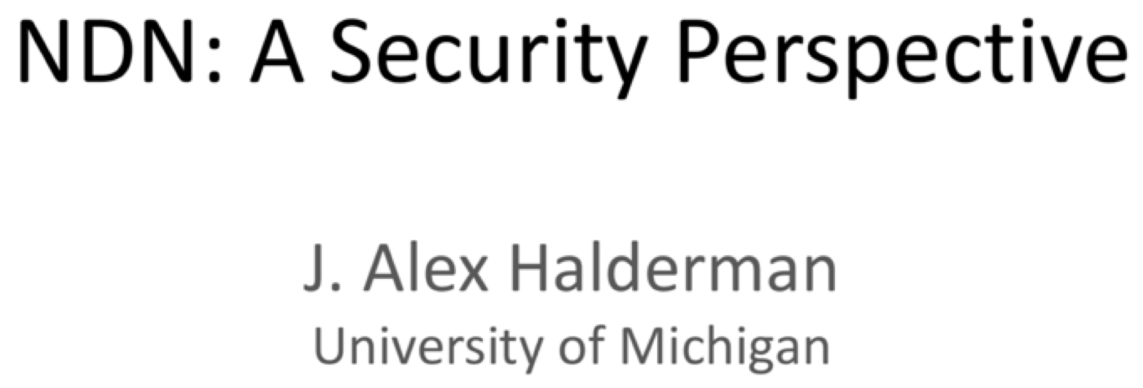
End-to-end data security



Data producers sign

Data consumers verify

Requiring every data producing entity possess cryptographic key(s)
Requiring security bootstrapping
Requiring efficient signing and verification for resource constrained devices



NDN: A Security Perspective

J. Alex Halderman
University of Michigan

Security Lessons

Data-centric security philosophy allows us to convert hard security problems (e.g., host security) into ones that are relatively easier (crypto, key management).

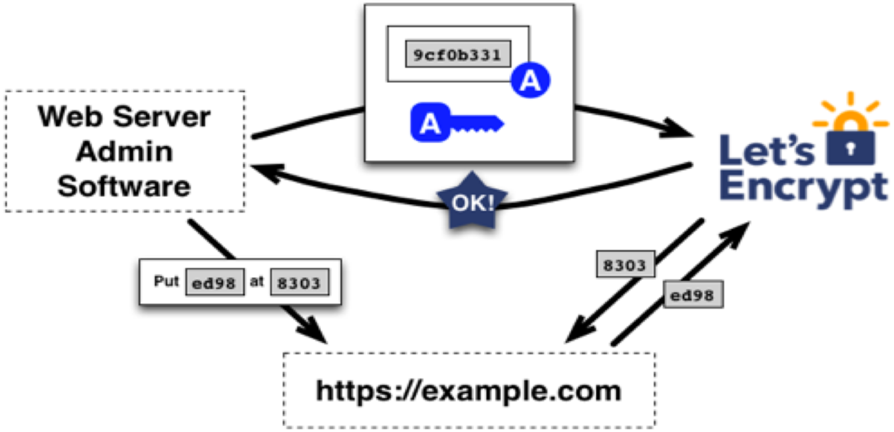
Security priorities will continue to evolve, and no network architecture will solve them all for all time— but architecture can give us a more solid foundation.

Data-centric security potentially a better fit for network security needs of IoT than traditional IP, can provide exciting building blocks for secure applications.

Crypto usage starts from trust anchors

- ◊ Today's common practice: commercial certificate providers

- ◊ More recent solution: automated certificate issuance



Trust anchor establishment in NDN:

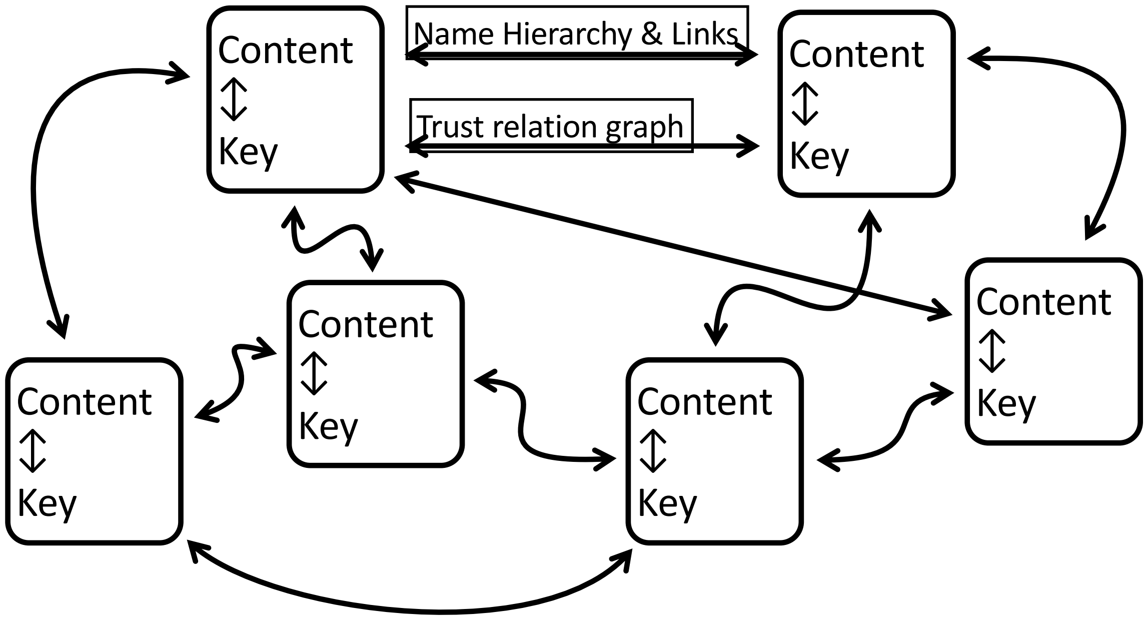
- ◊ Each individual entity may establish its own (local) trust anchor
- ◊ Trust anchors may establish relations between each other

Local trust anchors

Evidentiary trust

(from NSF FIA kickoff 2010)

A rich web of trustworthy information arises from named, signed data:



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
  - Secure sign-in
  - Certificate issuance
  - Signing and verification
  - Content encryption