Washington University in St. Louis

Security, Privacy & Future Networks

Patrick Crowley

HPSR 2014

Vancouver, BC
7/3/2014

My View on Privacy & Security

Genuine end-to-end encryption will soon become the norm

Why is end-to-end crypto inevitable?

- People want privacy (i.e., react badly to spies)
- Companies that deal in information (Google, Apple, Amazon, …) will either **protect** or **lose** their users
- Technologically, I believe that privacy trumps surveillance

Consequences of end-to-end crypto?

- No more man-in-the-middle
  - Governments, criminals & enterprise security teams cannot easily tap
- Creates a big opportunity for my startup company!

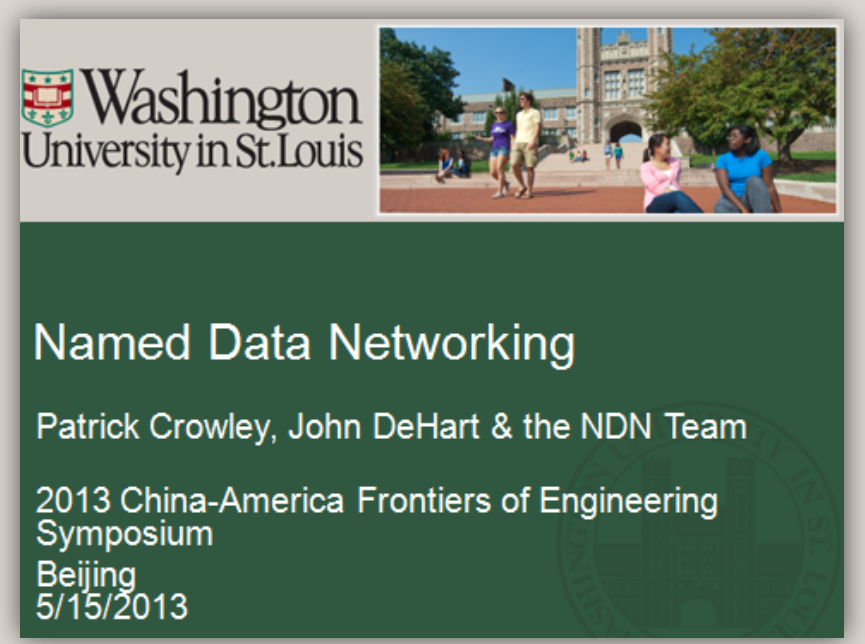
- Google, Apple & Amazon will grow larger, and will be harder to displace due to barriers to entry

Where does SDN/NFV fit in?

- Largely irrelevant! A mechanism that generalizes controls that have always been present.
- Biggest impact of SDN/NFV
  - Further commoditization of networking gear
  - Shift value from hardware to controller software
- Strong SDN/NFV directions
  - Cross-stack integration (e.g., VMWare, OpenStack)
  - Controlling data center topologies

Are there real problems in networking that require research?

Share This Presentation?



What is the best way for me to share these slides with you right now?

What about video? What would happen if it became popular?

Trust This Message?

From: C. D. (Dan) Mote, Jr. <dmote@email.edu>
Date: Mon, May 13, 2013 at 7:39 PM
Subject: Congratulations!
To: Patrick Crowley pcrowley@wustl.edu

Dear Prof. Crowley,

I write to inform you that you have been elected a Fellow to the National Academy of Engineering. As you may understand, this designation follows a process of nomination and subsequent vote by existing Fellows. Congratulations.

Sincerely,
C.D. Mote, Jr.
President-Elect, National Academy of Engineering

Easy to forge Internet communications!

Use Connected Environment/IoT?

3 Challenges Caused By 1 Problem

Telephony/Internet Process

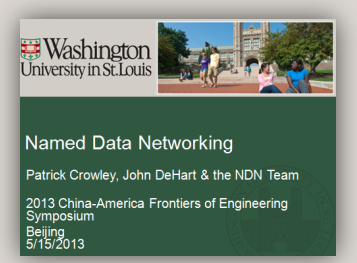
1. Find the **number/address** for the one you want to talk to.
2. Use that number to establish a **point-to-point connection**.
3. Communicate!

Sharing	*Must know address*
Trust	*Place trust in address*
IoT	*Know & trust all addresses*

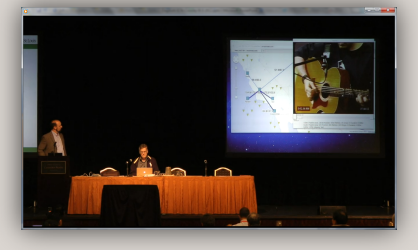
A Simpler Way

Suppose your device could ask for what it wanted?

/wustl.edu/pcrowley/talks/CAFOE_2013.pdf



/wustl.edu/pcrowley/video/thinkpad



/room/thermostat/1/status

The Web Has Named World's Data!

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

/www.youtube.com/watch?feature=player_detailpage&v=oCZMoY3q2uM#t=1736s

Named Data Networking: Core Idea

Modern **communication** consists of
requests for named data

Today's **networks** are based on
host-to-host connections

NDN is a general-purpose network protocol built on requests for named data

NDN & Other ICN approaches

Dramatically reduce the importance of “where data comes from” by securing the content itself rather than the channel

Consequently, you do not need a vast infrastructure to securely deliver content

The NDN team has conducted global demonstrations that illustrate this concept with real software and modest resources

Summary

End-to-end encryption will “turn out the lights” on man-in-the-middle techniques

In the near-term, large organizations will build and maintain vast infrastructures to keep our information secure and (for them) profitable

Longer-term, Named Data Networking (and other ICN ideas) will level the playing field and swing the pendulum back towards distributed networks