NDN: A Security Perspective

J. Alex Halderman
University of Michigan
**Named-Data Networking (NDN)**

- **Interest Packet**
  - **Content Name**
  - Selectors
    (order preference, publisher filter, exclude filter, …)
  - Nonce
  - Guiders
    (scope, Interest lifetime)

- **Data Packet**
  - Name
  - MetalInfo
    (content type, freshness period, …)
  - Content
  - Signature

Participant: /youtube/video/343

Flow:
- Interest
- Data

Found in cache
Publisher
Architectural Security

**Start with Properties**
- Data integrity
- Access control
- Privacy protections
- User authentication
- Server authentication
- Denial-of-service prevention

**Start with Mechanisms**

NDN begins with seemingly simple architectural concepts that provide significant security leverage.

Research explores implications and applications of those core ideas.

We can define actual future mechanisms.
We don’t get to define actual future threats!
Names, not addresses.

Data flows only in response to an interest request.

+ Reduced attack surfaces
+ Resistance to some kinds of denial-of-service
+ Benefits for privacy
Securing the Data vs. Securing the Channel

Securing the data is:
- Lighter weight
- More friendly to intermittent connectivity
- Readily able to transverse heterogeneous network environments without security loss
Data-Centric Security

Interest Packet

Content Name

Interest

Data

Found in cache

Publisher

All content must be signed.
Routers may, clients shall, verify.
Validation policy defined by applications.
+ Flexible foundation for many security properties:
  - Integrity, authentication, access control, provenance

Data Packet

Name

MetalInfo
(content type, freshness period, …)

Content

Signature
**Signatures in NDN**

**Big idea:** Certificates are just named, signed data.
Get them “for free” in the data-centric security approach.

RSA, ECDSA, exploring *lighter-weight* symmetric mechanisms too.
Signature Format Details

Ensure flexibility, trust agility, robustness for long-lived signatures.

**Big idea:** With appropriate mechanisms, signatures can outlive the keys that signed them, even if compromised.
Automatically Provisioning Trust

How does a publisher get their keys signed?

**Big idea:** Abstract identity verification and automate issuance.
Namespaces and Security

Who is allowed to sign what?

Big idea: Namespace design can convey capabilities, structure trust.
**Big idea:** Abstract validation based on structure of namespace, allow applications to define rules for trust or adopt pre-defined templates designed by experts.

Achieves vastly greater flexibility and security than existing TLS PKI.
Optimizing Performance: Key Bundling

Have producers/publishers provide evidence up front, rather than making consumers collect it.

Data-centric model enables such optimizations without security loss.
Confidentiality and Privacy

Confidentiality is **not** part of NDN’s core architecture, left up to applications.

However... design provides certain inherent privacy advantages over IP.
Name-based Access Control

An old idea: Encryption-based access control
New opportunities: Use namespace hierarchy to express fine-grained access rules
Confidentiality/Privacy Tensions

Tension between allowing caching and privacy...
Enterprise Building Automation and Management Systems (EBAMS)

Enterprise-controlled, but authorization hierarchy may not match deployment structure. Resource constrained platforms.

Light-weight crypto for command- and data access control. Explore use of key publishing and naming instead of interactive security services.
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.
NDN: A Security Perspective

J. Alex Halderman
University of Michigan