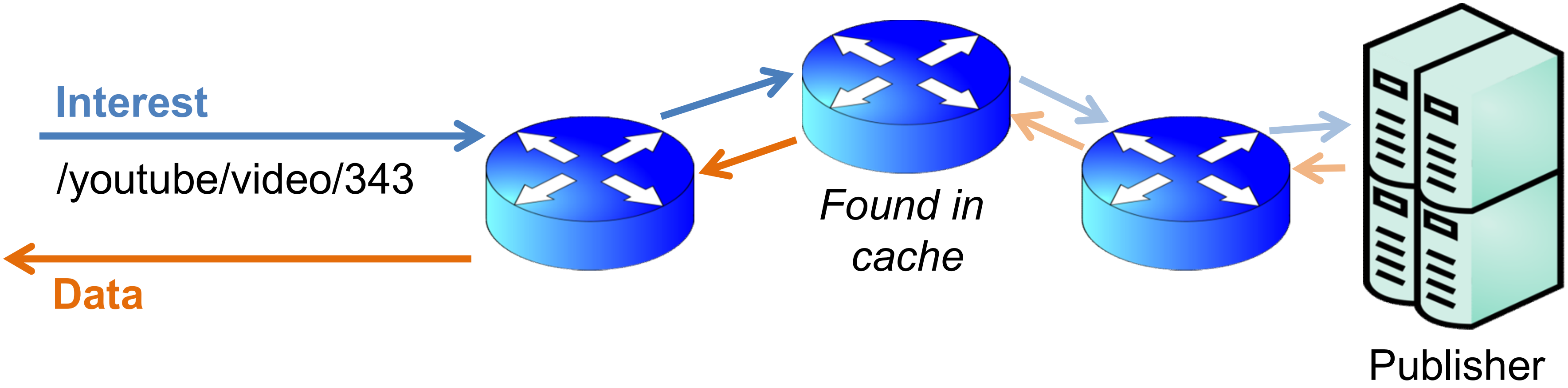
NDN: A Security Perspective

J. Alex Halderman
University of Michigan

Named-Data Networking (NDN)



Interest

/youtube/video/343

Data

Found in cache

Publisher

Interest Packet

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

Data Packet

Name
MetaInfo (content type, freshness period, …)
Content
Signature

Architectural Security

Start with Properties

Data integrity

Access control

Privacy protections

User authentication

Server authentication

Denial-of-service prevention

⋮

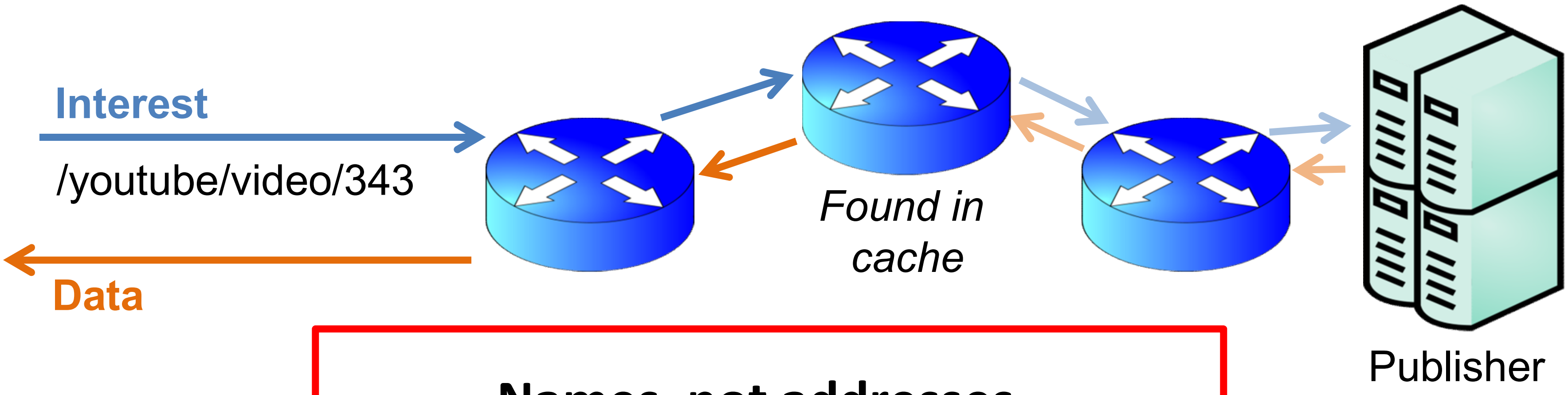
Start with Mechanisms

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!

Data-Centric Security



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

Inte

ket

Co

(order pr

e

, ...)

(scope, Interest lifetime)

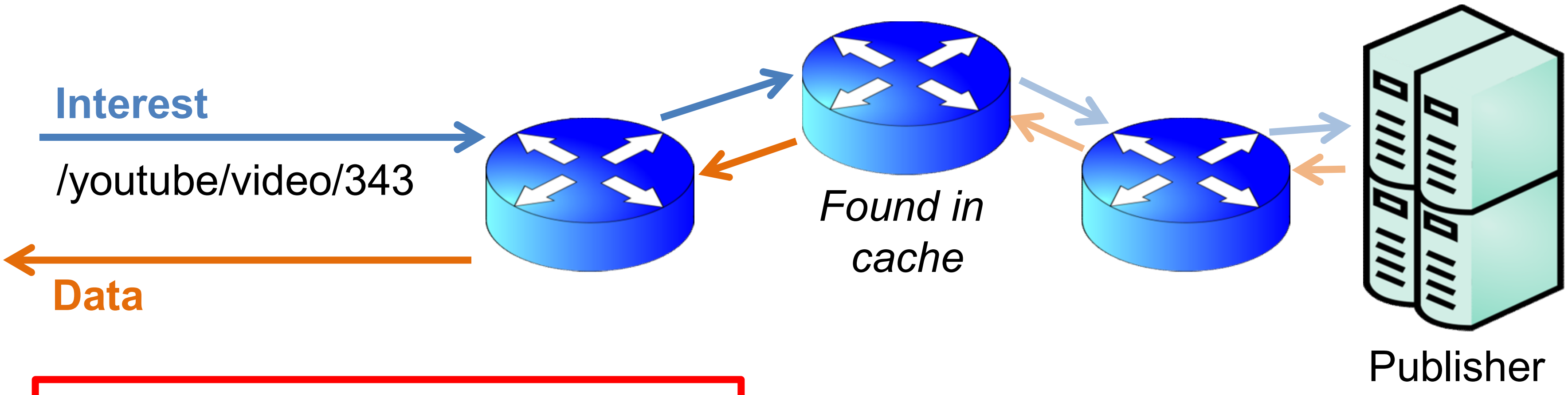
Signature

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



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

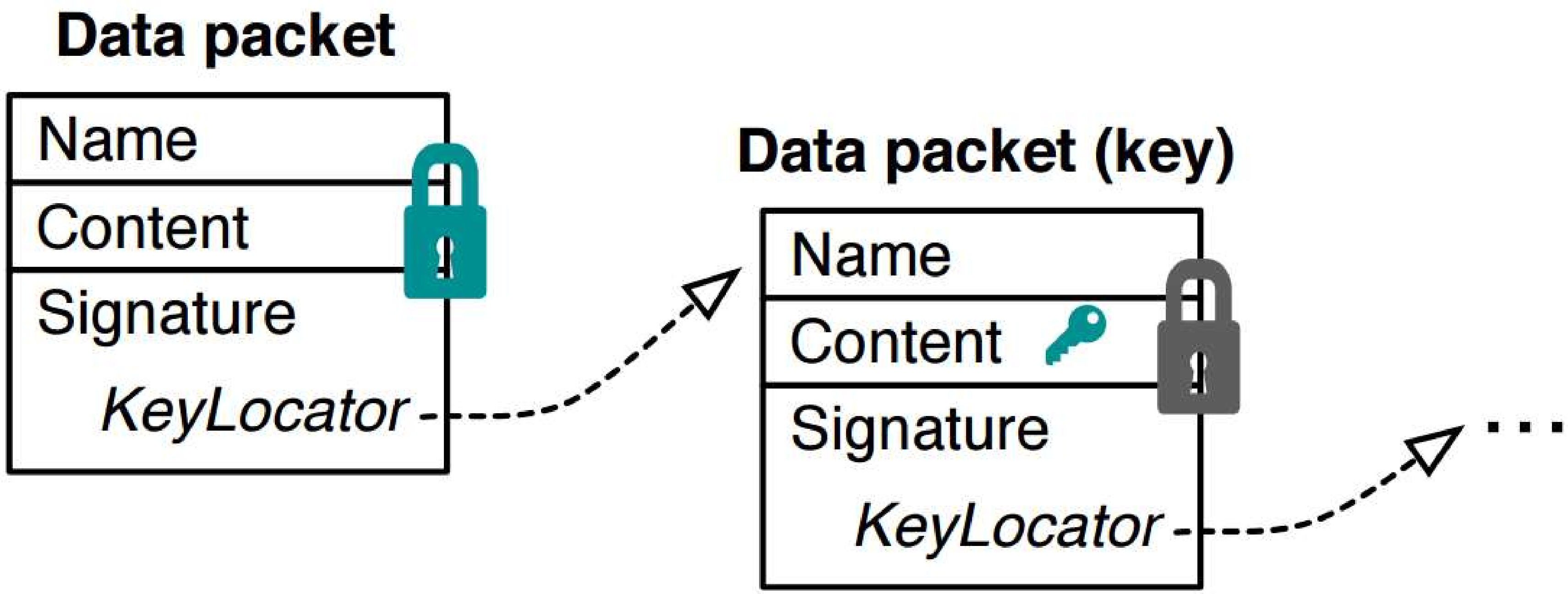
Name

MetaInfo
(content type, freshness period, …)

Content

Signature

Signatures in NDN

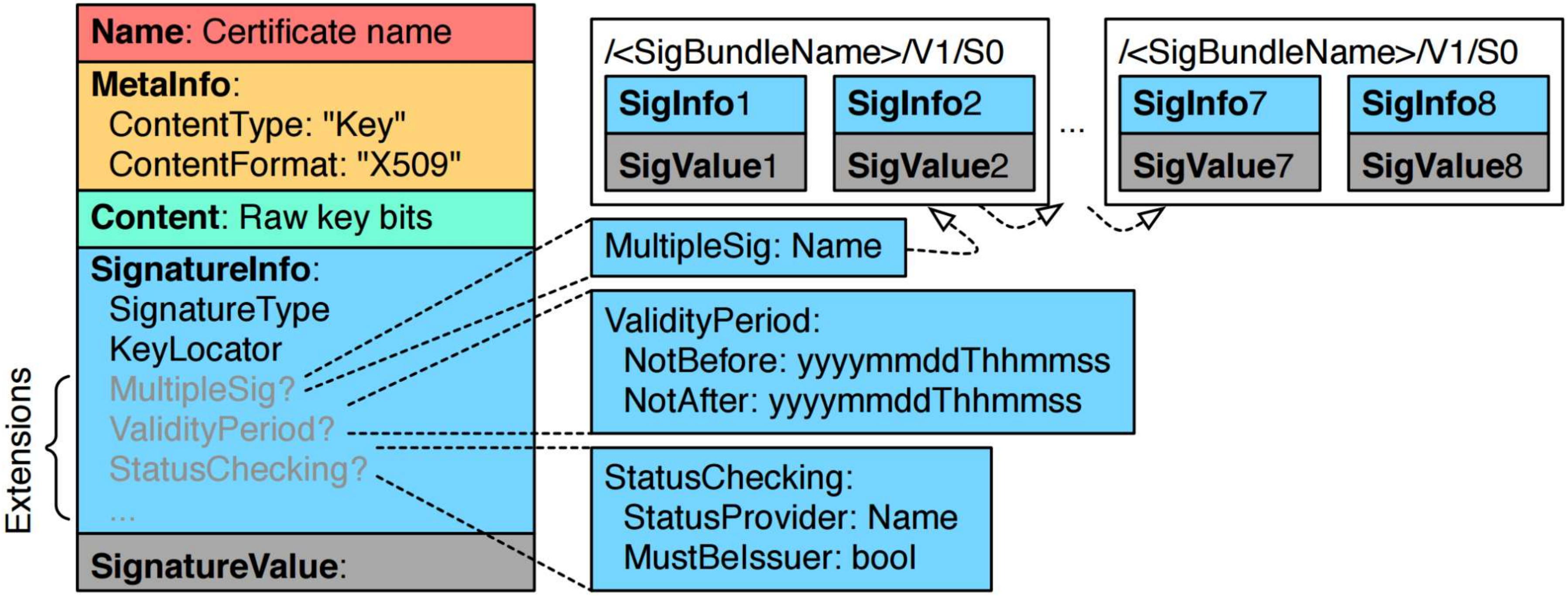


Big idea: Certificates are just named, signed data.
Get them “for free” in the data-centric security approach.

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

Signature Format Details

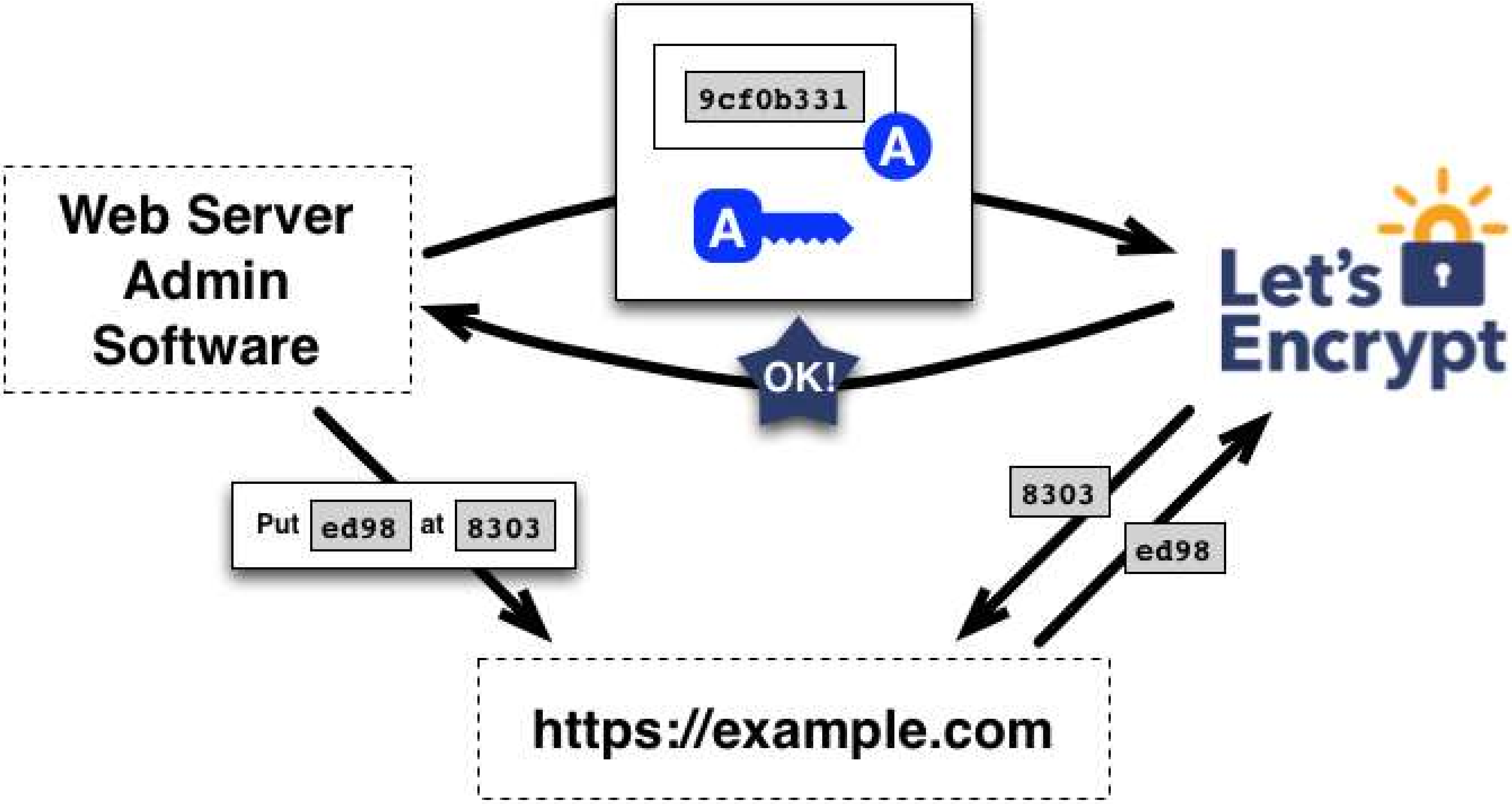
Ensure flexibility, trust agility,
robustness for long-lived signatures.



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

Automatically Provisioning Trust

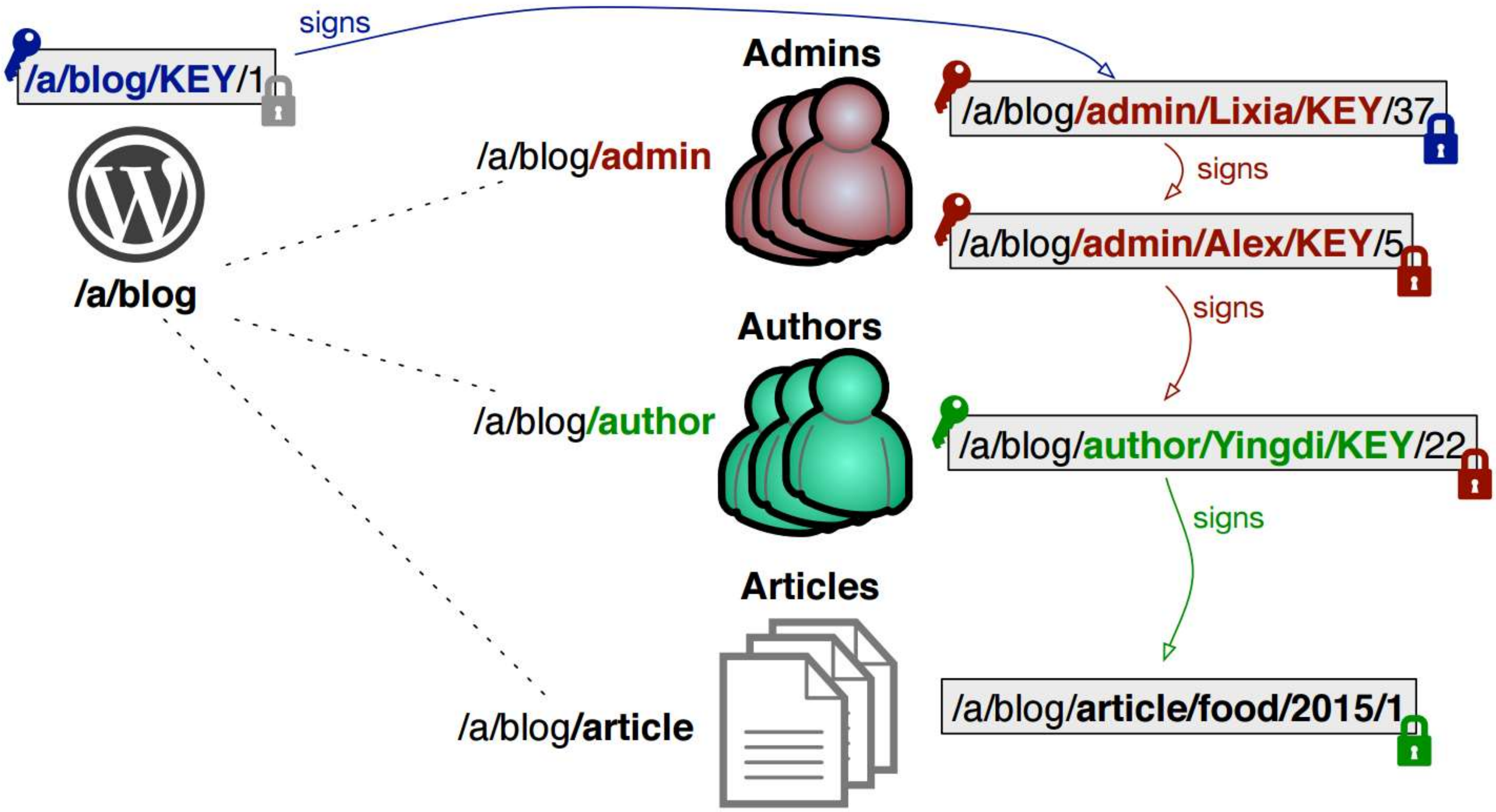
How does a publisher get their keys signed?



Big idea: Abstract identity verification and automate issuance.

Namespaces and Security

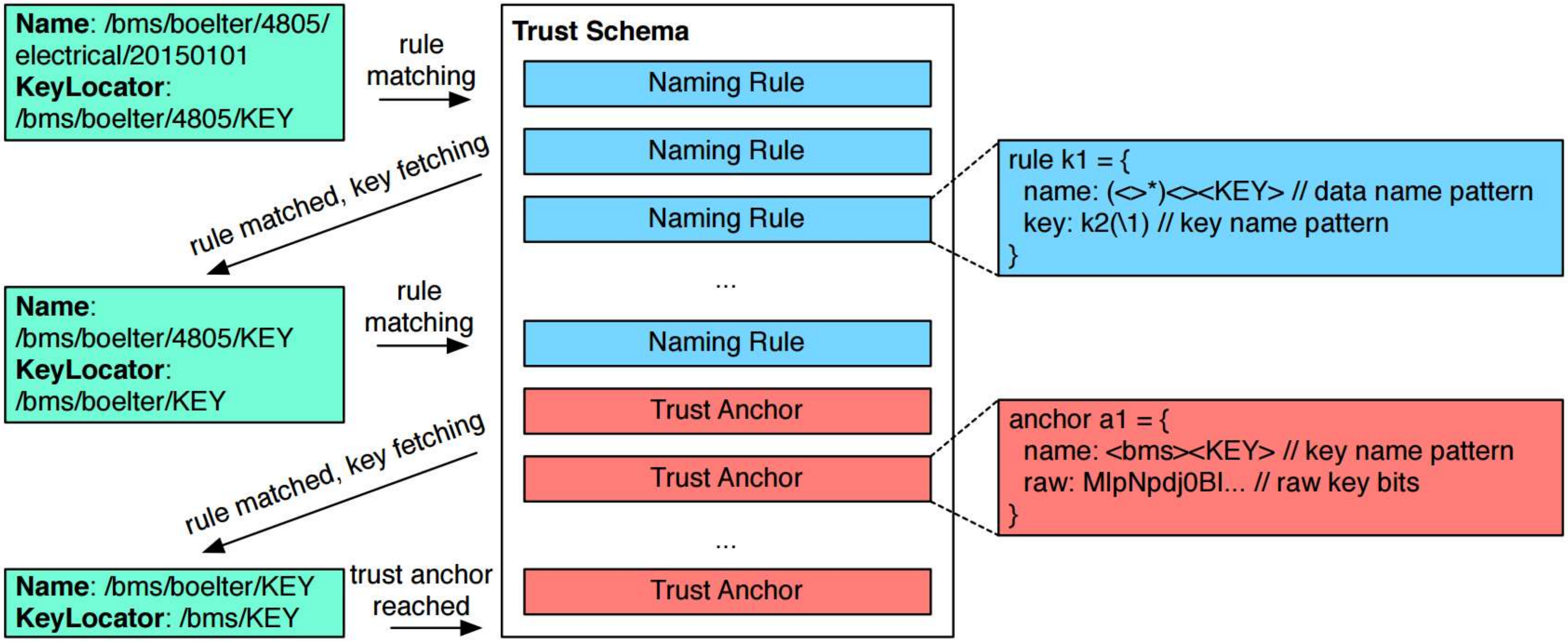
Who is allowed to sign what?



Big idea: Namespace design can convey capabilities, structure trust.

Schematizing 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.



Name: /bms/boelter/4805/electrical/20150101
KeyLocator: /bms/boelter/4805/KEY

rule matching

rule matched, key fetching

Name: /bms/boelter/4805/KEY
KeyLocator: /bms/boelter/KEY

rule matching

rule matched, key fetching

Name: /bms/boelter/KEY
KeyLocator: /bms/KEY

trust anchor reached

Trust Schema

Naming Rule

Naming Rule

Naming Rule

...

Naming Rule

Trust Anchor

Trust Anchor

...

Trust Anchor

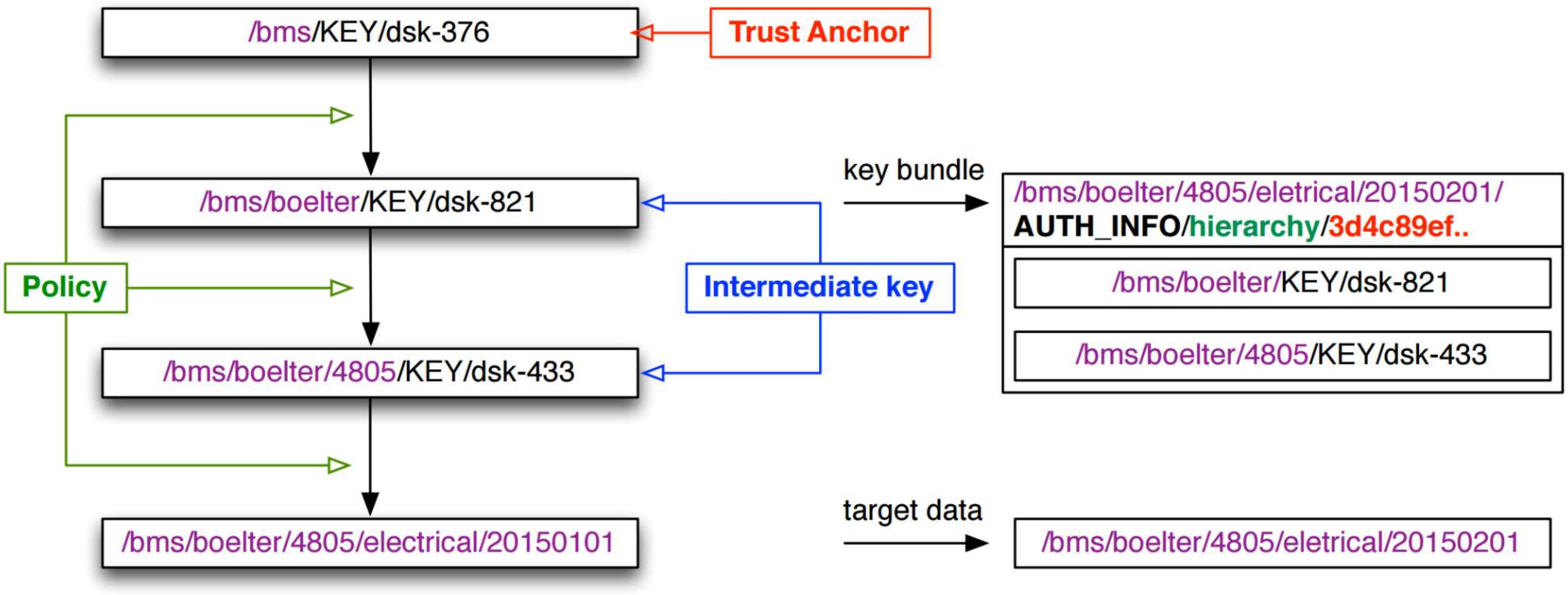
```
rule k1 = {
  name: (<>*)<><KEY> // data name pattern
  key: k2(\1) // key name pattern
}
```

```
anchor a1 = {
  name: <bms><KEY> // key name pattern
  raw: MlpNpdj0BI... // raw key bits
}
```

Achieves vastly greater flexibility and security than existing TLS PKI.

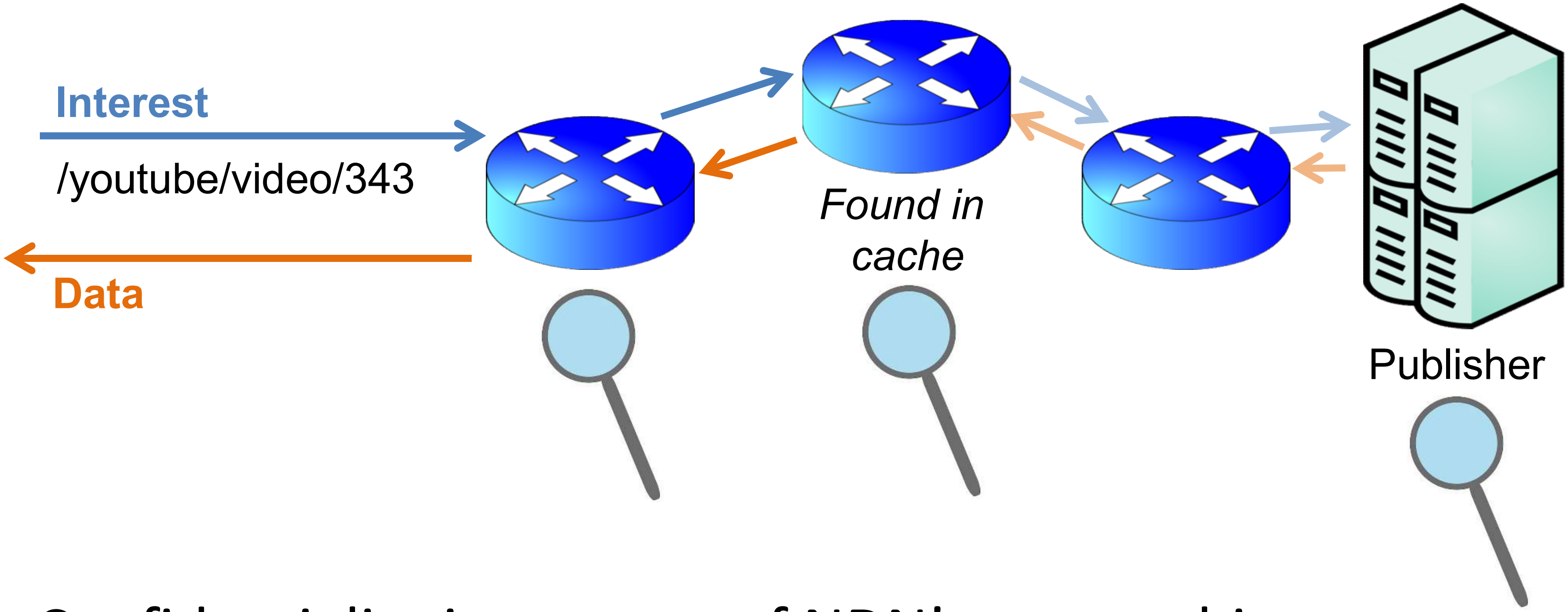
Optimizing Performance: Key Bundling

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


/bms/KEY/dsk-376
Trust Anchor
/bms/boelter/KEY/dsk-821
Policy
Intermediate key
/bms/boelter/4805/KEY/dsk-433
/bms/boelter/4805/electrical/20150101
key bundle
/bms/boelter/4805/eletrical/20150201/
AUTH_INFO/hierarchy/3d4c89ef..
/bms/boelter/KEY/dsk-821
/bms/boelter/4805/KEY/dsk-433
target data
/bms/boelter/4805/eletrical/20150201

Data-centric model enables such optimizations without security loss.

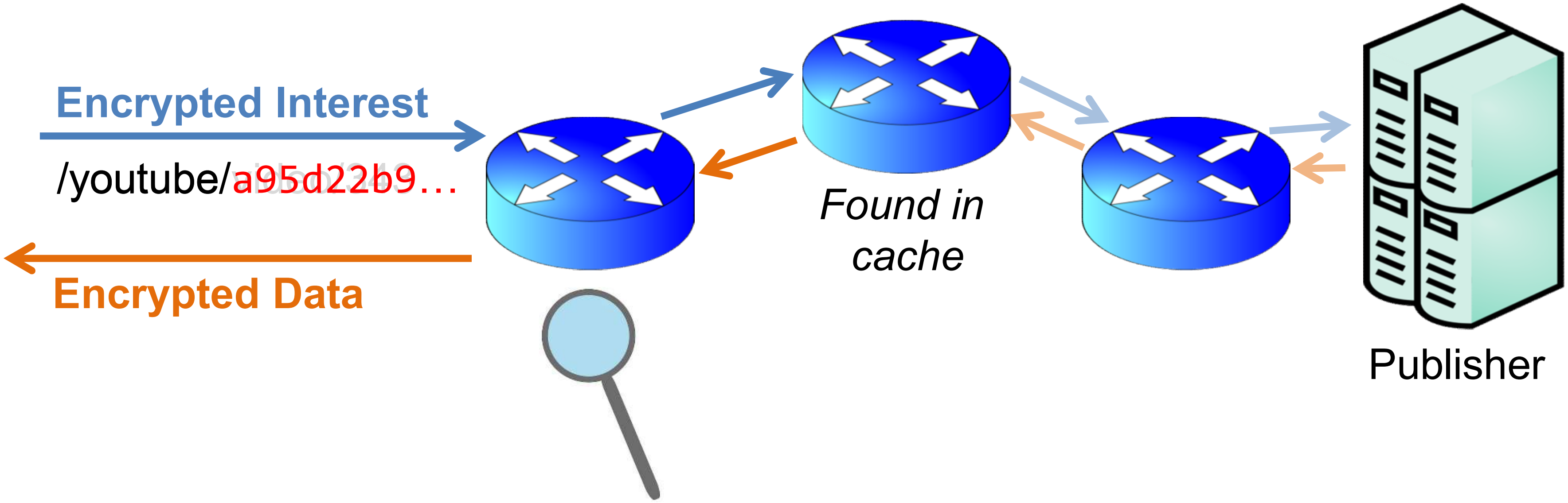
Confidentiality and Privacy



Confidentiality is <u>not</u> part of NDN's core architecture, left up to applications.

However… design provides certain inherent privacy advantages over IP.

Name-based Access Control



Encrypted Interest

/youtube/a95d22b9…

Encrypted Data

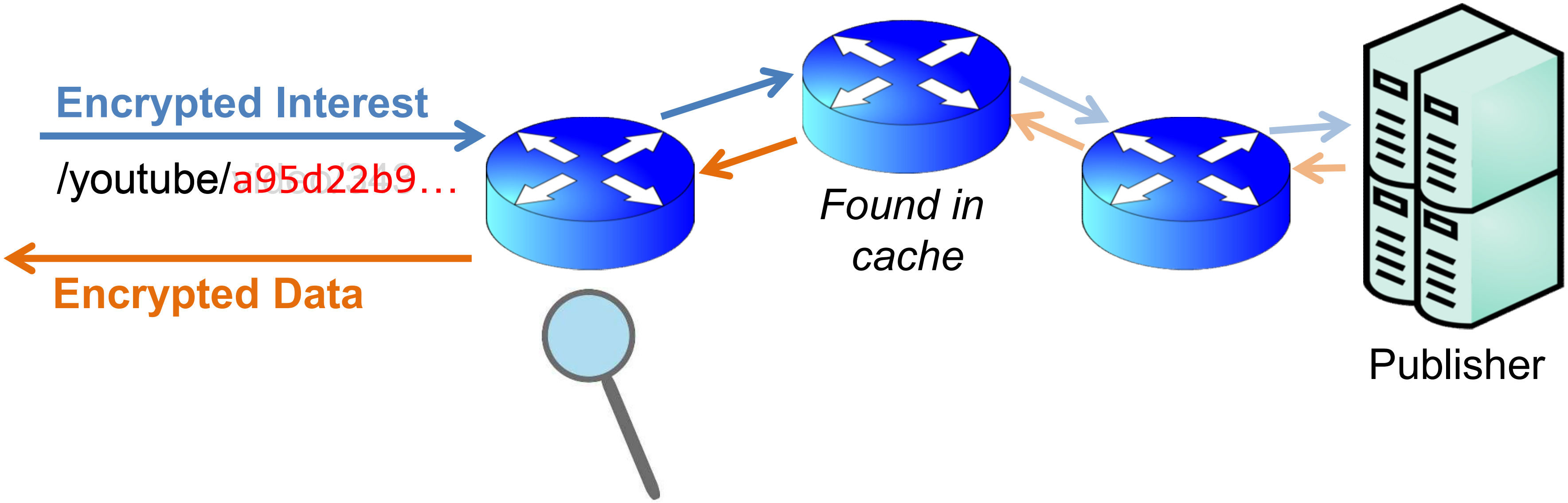
Found in cache

Publisher

An old idea: Encryption-based access control

New opportunities: Use namespace hierarchy to express fine-grained access rules

Confidentiality/Privacy Tensions



Encrypted Interest

/youtube/a95d22b9…

Encrypted Data

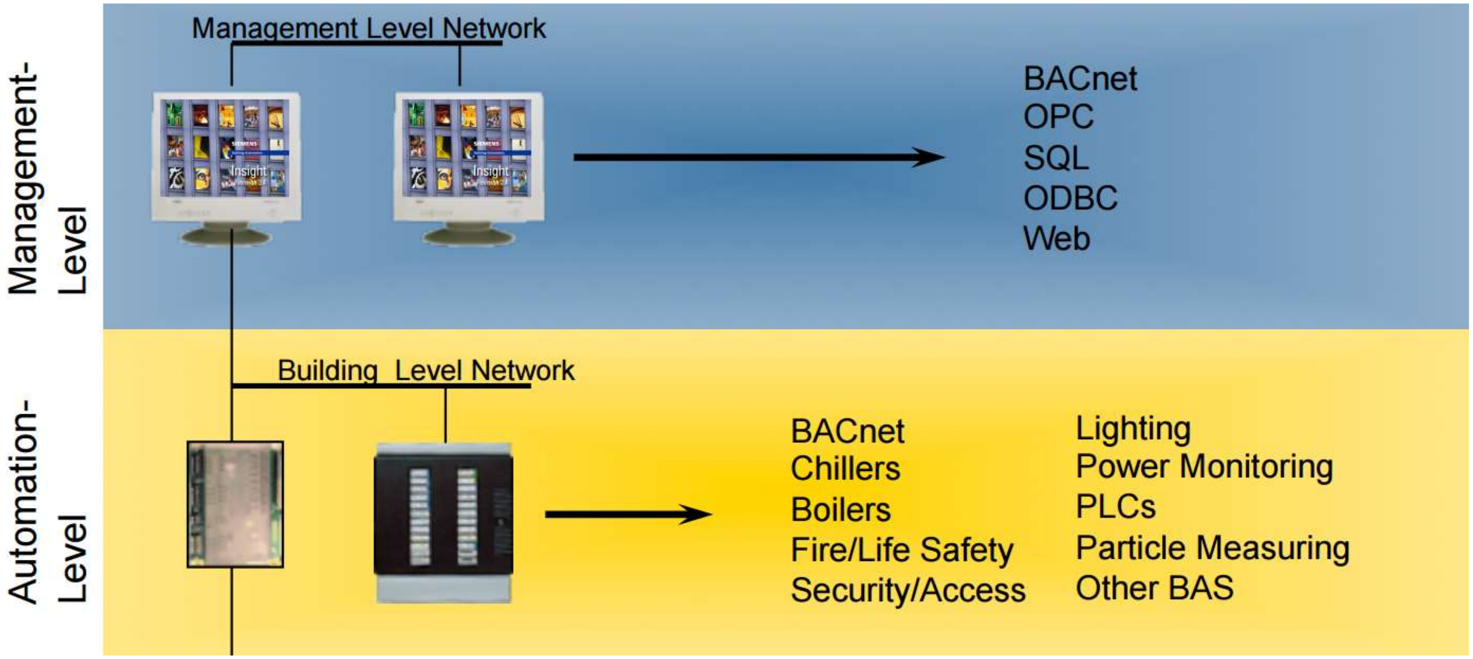
Found in cache

Publisher

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