Security and Privacy Analysis of NSF Future Internet Architectures

Moreno Ambrosin[1], Alberto Compagno[2], Mauro Conti[1], Cesar Ghali[3], Gene Tsudik[3]

[1]University of Padua, Italy
[2]University "La Sapienza" of Rome, Italy
[3]University of California Irvine, CA, USA

Internet Security & Privacy

- S&P in the current Internet are certainly NOT a success story
- Retrofitted, incremental, band-aid-style solutions, e.g.:
  - SSH,
  - SSL/TLS,
  - IPSec + IKE,
  - DNSSec,
  - sBGP, etc.

NSF Future Internet Architectures (FIA) program

- Targeted NSF-funded program, 2-tiered competition
- Major goals:
  - Design comprehensive next-generation Internet architectures
  - Accommodate current and emerging communication paradigms
  - Security and privacy from the outset (by design)
- Projects:
  - NDN: Named-Data Networking (Phases I and II)
  - MobilityFirst (Phases I and II)
  - XIA: eXpressive Internet Architecture (Phases I and II)
  - ChoiceNet (started in 2012, not strictly speaking FIA)
  - Nebula (Phase I)

NSF Future Internet Architectures (FIA) program

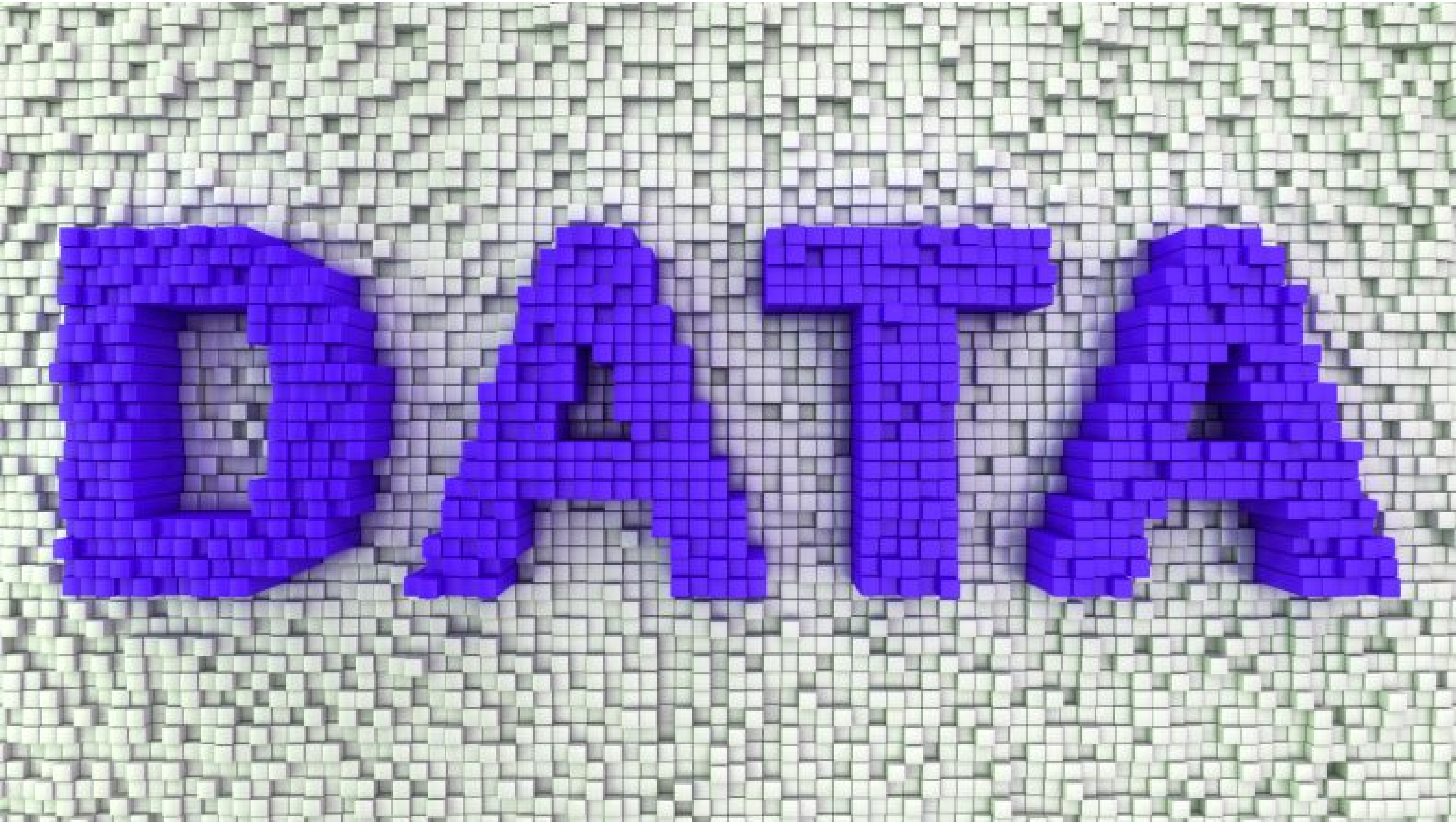
- Targeted NSF-funded program, 2-tiered competition
- Major goals:
  - Design comprehensive next-generation Internet architectures
  - Accommodate current and emerging communication paradigms
  - Security and privacy from the outset (by design)
- Projects:
  - NDN: Named-Data Networking (Phases I and II)
  - MobilityFirst (Phases I and II)
  - XIA: eXpressive Internet Architecture (Phases I and II)
  - ChoiceNet (started in 2012, not strictly speaking FIA)
  - Nebula (Phase I)

Our Comparison

- S&P of the network layer (data plane) of 4 FIA architectures with IP (IPSec)
    - Trust, Data origin authentication, Peer entity authentication, Data integrity, Authorization and access control, Accountability, Data confidentiality, Traffic flow confidentiality, Anonymous communication

- Here, we discuss only some of them for **NDN, MF, and XIA**
    - The more interesting ones

NDN & CCNx



- "Named data networking project (NDN)", http://named-data.org
- "Content centric networking (CCNx) project", http://www.ccnx.org
- "Networking named content", ACM CoNEXT, 2009.

Security

- Integrity and trust as properties of content
  - Every content packet carries a signature
  - Producer generates the signature (producers have identities)

- Confidentiality through encryption

NDN/CCN vs IP: S&P Comparison (1/3)

- Trust:
  - IP: In IPSec end-hosts are trusted
  - NDN: Trust is on content, not host. Different granularity (namespace, content object)

- Data Origin Authentication and Integrity:
  - IP: Available only within an IPSec pipe (e.g., gateway-to-gateway).
  - NDN: Content signature bound to producer identity no matter where they come from

NDN/CCN vs IP: S&P Comparison (2/3)

- Peer entity authentication:
  - IP: During SA establishment peers of an IPSec connection are authenticated
  - NDN: Not available. However, signed interest helps to authenticate consumers

- Authorization & Access Control:
  - IP: No suitable access control for content at this layer
  - NDN: Access control on content mainly through encryption

NDN/CCN vs IP: S&P Comparison (3/3)

- Availability (resilience to DoS):
  - IP: Bandwidth depletion (flooding) easy to achieve (IP spoofing, amplification, reflection)
  - NDN: Bandwidth depletion harder due to pull-based communication and aggregation

Attacks on NDN & CCN

- Router resource exhaustion:
  - Interest flooding attack exhaust PIT

- Cache Related attacks
  - Content poisoning
  - Cache pollution

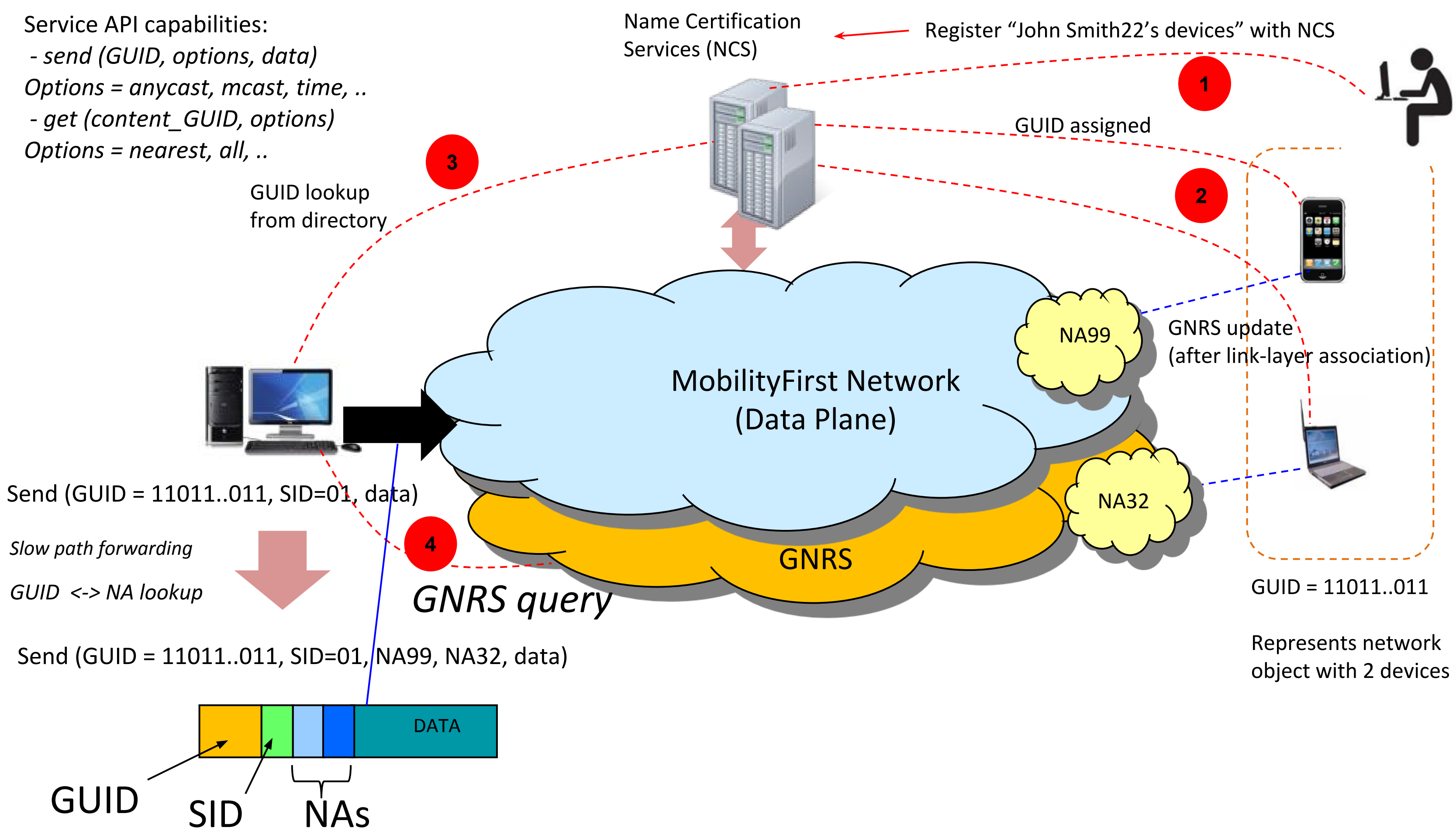
MobilityFirst

Overview:
MobilityFirst: A Mobility-Centric and Trustworthy Internet Architecture, ACM CCR 2014.

Project webpage:
http://mobilityfirst.winlab.rutgers.edu/

MobilityFirst – Example

Service API capabilities:
- *send (GUID, options, data)*
Options = anycast, mcast, time, ..
- *get (content_GUID, options)*
Options = nearest, all, ..



Packet sent out by host

Source WINLAB

MF vs IP: S&P Comparison

- Trust:
  - IP: In IPSec end hosts are trusted
  - MF: trust on hosts, content and services. Self-certifying GUID increase trust.

- Peer Entity Authentication:
  - IP: ISAKMP relies on PKI or pre-shared keys
  - MF: SCN for GUID makes easy to achieve without PKI

MF vs IP: S&P Comparison

- Data Integrity:
  - IP: Apply to packets coming from the other end of the IPSec pipe
  - MF: Only for content principals. GUID is the hash of the content

- Data origin authentication, Data confidentiality, Traffic flow confidentiality, Anonymous communication, Accountability, Availability:
  - No difference between MF and IP

Attacks on MobilityFirst

- Information manipulation:
  - AS can withdraw IP address storing GNRS mapping
  - All (orphan) mappings move to next AS
  - Original AS is responsible for moving them
  - GNRS is not secure → adversary can inject (orphan) mappings
- Late binding: slow path can be abused to launch DoS attacks on routers
- Nasty GUID-NA mapping: adversary sends PDU with fake GUID-NA mapping. Destination border router forced to query GNRS to discover correct NA

eXpressive Internet Architecture

XIA

- Current internet focuses on one principal, e.g., IP
- Communication with others add complexity
- Future internet should be x-centric
- XIA is a principal-centric approach
- Principals: host, domain, service, content …
- XIA Goal:
  - Intrinsic security: principals should be secure without external validation information

XIA – Design Requirements

- Users and applications must be able to express their intent:
  - Any intent types should (will) be supported
- Principal types must be able to evolve:
  - Adding principals should be possible and easy
  - Network adaptation could be incremental
- Principal identifiers should be intrinsically secure
- Host-to-host communication, hosts should be authenticated
- Content retrieval, data integrity and validity

XIA – Design Requirements

- Must define:
  - Semantics of communicating with the principal
  - Unique XID (principle ID), e.g. HIDs, SIDs, CIDs, and ADs
  - Way to generate these ID and map them to intrinsic security properties
  - In-network processing and routing of packets (should be consistent and distributed)

XIA Data Plane

- XIP: allows communication, and defines address, header format, per-principal processing

- Principal type-specific support: e.g.
  - Host principle might use traditional routing
  - Content principal might check local cache before forwarding requests

XIA – Principals

- Host:
    - HID: hash of public key
    - Constant regardless of the host's network
- Network:
    - NID: hash of public key
    - Networks contains multiple hosts
- Service:
    - SID: hash of public key
    - Similar to destination port
    - Destination address: NID:HID:SID

XIA – Principals

- Content:
    - CID: hash of content
    - Address Usually has fallback
    - Can be retrieved from host or cache
    - Packet contains content-specific header
- All routers must be able to process NID and HID principles
- For other principles, routers must perform at least basic processing, e.g. forwarding

XIA vs. IP: S&P Comparison

- Trust:
  - SCION is used for trusted path selection
  - SCION provides control and isolation for secure, available end-to-end communication

- Data origin authentication, Peer entity authentication:
  - IPSec provides these features
  - Not provided by design
  - Self-certifying names can be used to provide these features

XIA vs. IP: S&P Comparison

- Integrity:
  - Provided by IPSec in IP
  - Only available for content principals since identifiers generated based on content hash
  - Deferred to application for other principal types

- Authorization & access control:
  - Combination of IP and NDN
  - Content principals: at content granularity
  - Other principal types: ACLs can be used

XIA vs. IP: S&P Comparison

- Availability:
  - Bandwidth depletion easy to achieve, similar to IP
  - Self-certifying names obviate content poisoning attacks

- Anonymous Communication:
  - Can be provided by IP using, e.g., TOR
  - Suffer from same problem as IP: src and dst included in packets
  - XIA also contains the entire path … even worse
  - IP-like methods can be used, e.g., TOR.

Summary

Security & Privacy Features	Network layers			
	Nebula	**NDN**	**MF**	**XIA**
Trust	✓	✓	✓	✓
Data Origin Authentication	◎	✓	✗	✗
Peer entity Authentication	◎	◎	◎	◎
Data Integrity	◎	✓	✗	✗
Authorization and Access Control	✓	◎	◎	◎
Accountability	✓	◎	◎	◎
Data Confidentiality	✗	✓	✗	✗
Traffic Flow Confidentiality	✗	✗	✗	✗
Anonymous Communication	✗	✗	✗	✗
Availability	◎	◎	◎	◎

Thank You…
Questions?

Who is NDN?

THE UNIVERSITY OF MEMPHIS

Colorado State University

parc A Xerox Company

Northeastern University

ARIZONA

Washington University in St. Louis

UCSD

UCIRVINE

University of Colorado Boulder

UCLA

ILLINOIS UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

UNIVERSITY OF MARYLAND 1856

NDN Basic Concepts

- Name:
  - Human-readable, path/url - like
- Roles:
  - Consumer
  - Producer
  - Router
- Objects:
  - Content

NDN: quick recap (1/2)

- PRODUCER
  - Announces name prefixes
  - Names and signs content packets
  - Injects content by answering interests

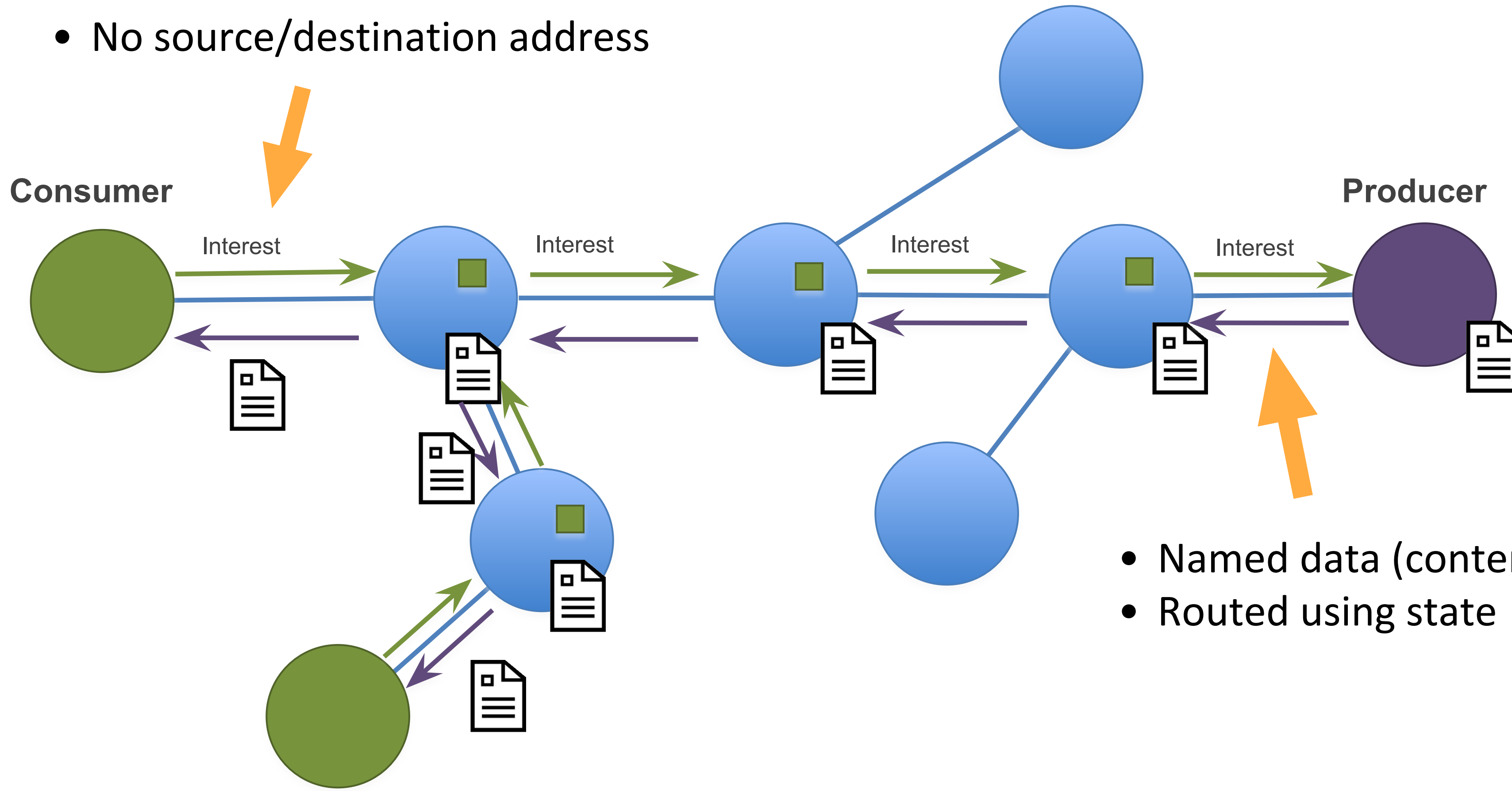
- CONSUMER
  - Generates interest packets referring to content by name
  - Receives content, verifies signature, decrypts if necessary

NDN: quick recap (2/2)

- ROUTER
  - Routes interests based on (hierarchical) name prefixes
    - Inherently multicast
  - Remembers where Interests came from (PIT)
    - Returns content along same path
  - Optionally caches content (in CS)
  - May verify content signatures

How NDN works (abbrv. version)

- Carries content name
- No source/destination address



- Named data (content)
- Routed using state

The Players:

- Rutgers University
- University of Massachusetts – Amherst
- Duke University
- MIT
- University of Wisconsin, Madison
- University of Nebraska

MobilityFirst Design Concepts

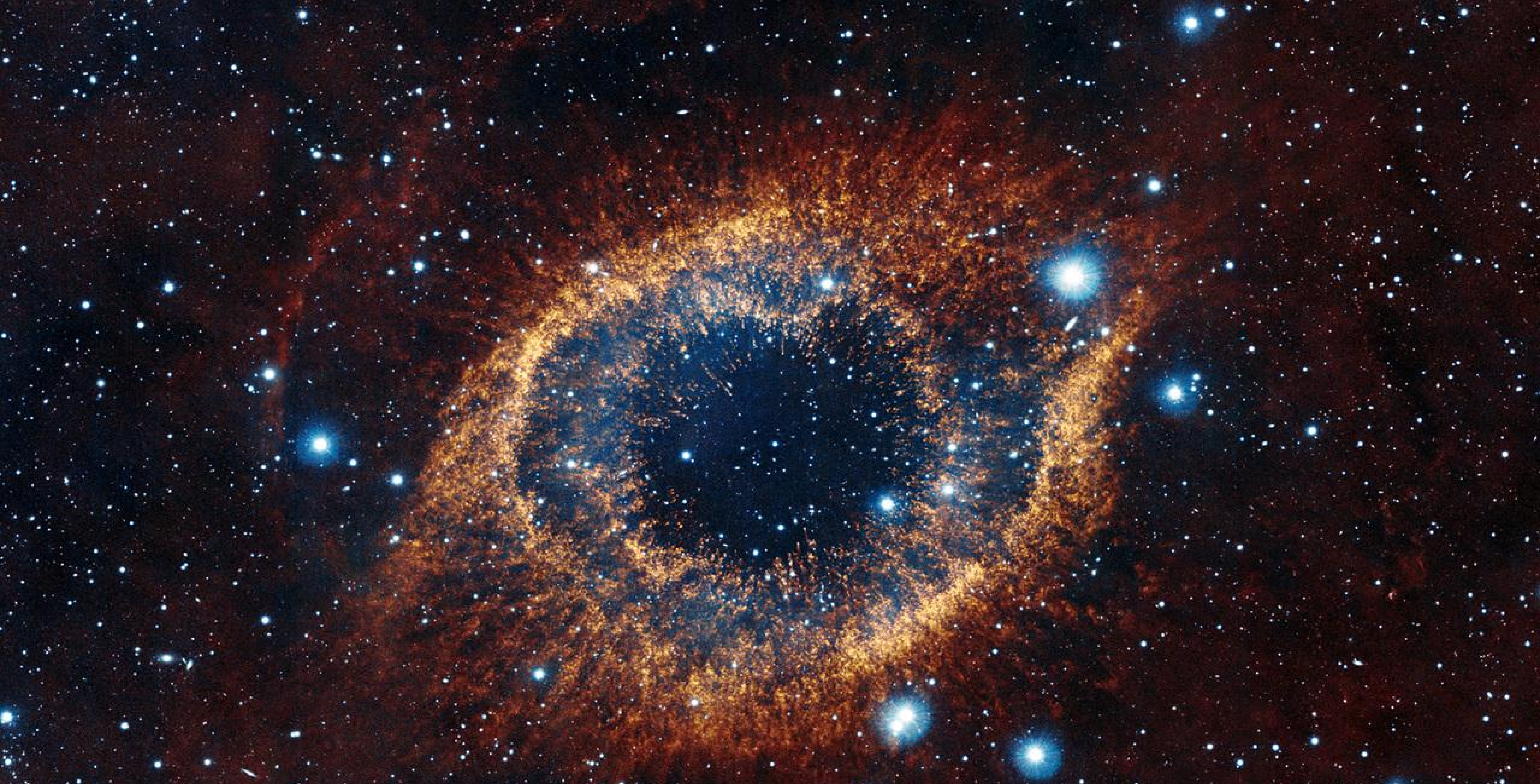
- Design principles:
  - wireless connections are ubiquitous and pervasive
  - seamless mobility in endpoints
  - network resilience to endpoints and router compromission
- Key idea:
  - separate identity from location
- Three types of identifiers:
  - Human Readable Names (HRN)

Self Certifying

MobilityFirst

- GUID uniquely identifies a principal: host or content
- HRN-s are not used for routing; translated to GUID-s
- GUID-s and NA-s are used for routing/forwarding
- Two translation services:
    - Name Certification Service (NCS):
        - Translates HRN ⟵⟶ GUID
    - General Name Resolution Service (GNRS):
        - Translates GUID ⟵⟶ NA

Nebula



Summary: “A Brief Overview of the NEBULA Future Internet Architecture,”, ACM Computer Communication Review, July 2014.

http://nebula-fia.org/

Nebula Partners

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Massachusetts Institute of Technology

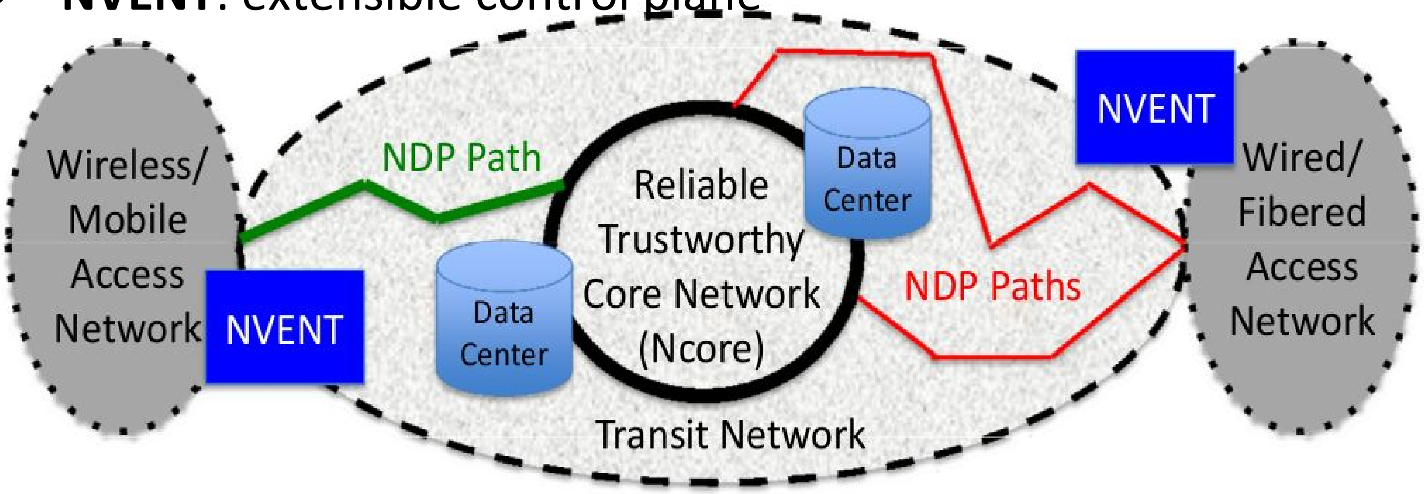
STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

PURDUE
UNIVERSITY

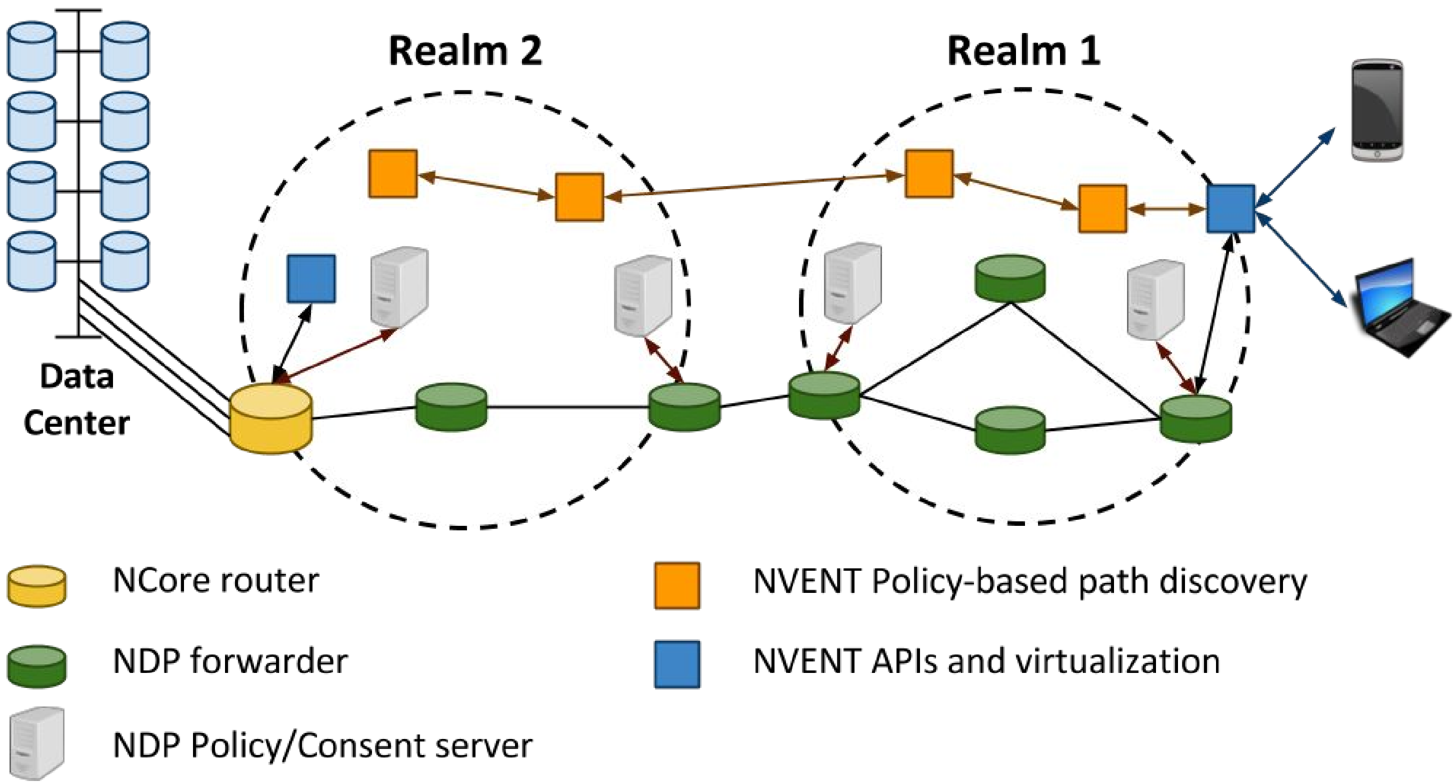
Cornell University

Architecture

- Goal: provide a secure cloud-oriented networking architecture
- Three components
  - **NCore**: ultra-reliable, redundantly-connected core routers
  - **NDP**: multi-path, policy-enforcing control plane
  - **NVENT**: extensible control plane



Security Overview



- **NVENT:** establishes trustworthy routes based on policy routing
- **NDP:** constrains data packets to NVENT-selected routes by enforcing consent and provenance
- **NCore:** ensures availability via ultra-reliable routers and interconnection architectures for data centers

Nebula Data Plane (NDP)

- Offers secure communication
    - When all relevant parties agree to participate
- Uses ICING: http://www.cs.utexas.edu/icing/
- ICING provides:
    - Path verification mechanism (PVM)
    - Path selection
    - Topology discovery
    - Forwarding

NDP - Naming

- NDP realms use self-certifying names (SCNs)
- Realm name is a self-generated PK (Public Key)
  - Can create spurious realms but not impersonate
- No need for central naming authority
- Node names also SCN-based
- NDP nodes use non-interactive Diffie-Hellman (NIDH) to establish pairwise PoP keys
  - But, how are DH PKs distributed? SCNs…

NDP - ICING

- Path Verification Mechanism (PVM):
  - Path Consent via *Proof-of-Consent (PoC)*:
    - Each intervening node agrees to be part of path based on its (realm) policy
  - Path Compliance via *Proof-of-Provenance (PoP)*:
    - Forwarding node checks whether:
      - Path has been approved
      - Previous nodes followed forwarding policy
  - PoC-s and PoP-s are implemented as cryptographic tokens (MAC)

NDP - ICING

- Prior to communication, sender requests *PoC_i* from each path node *N_i*
    - Actually, from each distinct provider on the path
- *PoC_i* generated by consent server at *N_i*'s provider (Here, provider = realm)
    - Not session-specific
- Each provider has at least one consent server
- *PoC_i* means:
    - *N_i*'s provider agrees to carry packets on the path

NDP vs IP: S&P Comparison (1/3)

- Trust
  - **IP**: IPSec secures communication between two or more network entities (hosts or networks) ⟵ “end-to-end” trust
  - **Nebula**: ICING guarantee path consent and provenance ⟵ trust among sender and intermediate nodes of a path
- Peer entity authentication
  - **IP**: During SA establishment peers of an IPSec connection are authenticated
  - **Nebula**: path consent authenticate sender and intermediate nodes

NDP vs IP: S&P Comparison (2/3)

- Integrity
  - **IP**: given by AH or ESP header
  - **Nebula**: comes with consent and provenance. Mainly gateway will verify integrity
- Authorization & Access Control:
  - **IP**: Routers applies access control list on IP addresses (or prefixes)
  - **Nebula**: Consent server grant access to a network through PoC
- Accountability

NDP vs IP: S&P Comparison (3/3)

- Availability:
  - **IP**: Bandwidth depletion easy to achieve (IP spoofing, amplification, reflection)
  - **Nebula**: Bandwidth depletion hard to mount due to path consent
- Anonymous Communication:
  - **IP**: not provided. Tor “guarantee” anonymity
  - **Nebula**: hard to achieve due to path consent and provenance

Attacks on Nebula (1/2)

- NDP (ICING) Router “slow path” attacks:
    - PoP computation by router may required NIDH to compute pairwise keys – time-consuming
    - Packets with fake node IDs can force routers to perform expensive crypto operations
    - ICING uses explicit “hardeners” in the header to prevent such attacks:

$$V_i.\text{hardener} = \text{PRF-32}(\text{PoC}_i.\text{proof}, 0 \mid\mid \text{HASH}(P \mid\mid M))$$

Attacks on Nebula (2/2)

- NDP (ICING) packet-level attacks:
  - Replay attacks:
    - Adv replays copies of valid packets
    - Sequence number (16 bits)
  - Injection attacks:
    - Adv injects fake packets
    - Easy to detect (most crypto ops are lightweight)