XIA and the DARPA Scenario

Peter Steenkiste – prs@cs.cmu.edu

Dave Andersen, David Eckhardt, Sara Kiesler, Jon Peha, Adrian Perrig, Vyas Sekar, Srini Seshan, Marvin Sirbu, Hui Zhang
Carnegie Mellon University

Aditya Akella, University of Wisconsin

John Byers, Boston University

Bruce Maggs, Duke

FIA-NP PI Meeting, Arlington, Nov 19-20, 2015

Carnegie Mellon BOSTON UNIVERSITY Duke UNIVERSITY THE UNIVERSITY of WISCONSIN MADISON

Public Internet versus Scenario (Broadly Interpreted)

- ≈ Rapidly evolving technologies: communications, storage, computing, …
  - ≠ More heterogeneity in scenario, including legacy
  - – Suggests some need for evolvability
- ≈ Relatively stable core with mobile edge
  - ≠ More radical mobility, dynamic topology in scenario
  - – Need for proactive topology management
- ≠ Trust management and security requirements
- ≠ All-to-all versus restricted communication
- ≠ Richer in-network functionality, e.g., DTN, multicast

2

Outline

- XIA overview
  - Typed identifiers
  - Flexible addressing: fallbacks and scoping
  - Intrinsic security
- Applying XIA to the scenario

3

1. Multiple Principal Types

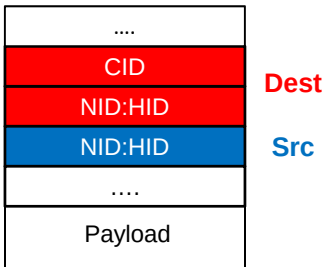
- Associated with different *forwarding semantics*
  - Support heterogeneity in usage & deployment models
- Identifiers for hosts, content, networks, services, …
  - Supports push, pull, …
  - Content/service centric support
- XIDs need control plane consistent with semantics
- Set of principal types can evolve over time
  - Dynamic content, pub-sub, …, DTN, multicast, …

4

Supporting Evolvability

- Introduction of a new principal type will be incremental – no "flag day"!
  - Not all routers and ISPs will provide support from day one
- Solution is to provide an *intent* and *fallback* address
  - Intent allows the network to optimize based on user intent
  - Fallback must be guaranteed to be reachable and is used if the intent "fails"

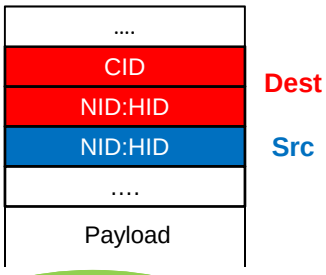
– Also enables heterogeneity and customization

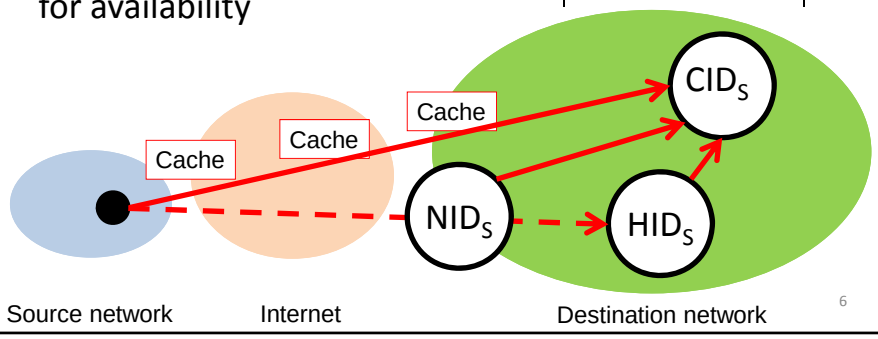


5

2. Flexible Addressing: DAGs

- Combining fallbacks and scoping offers flexibility for network in completing request
- Supports network heterogeneity and in-network error recovery for availability





6

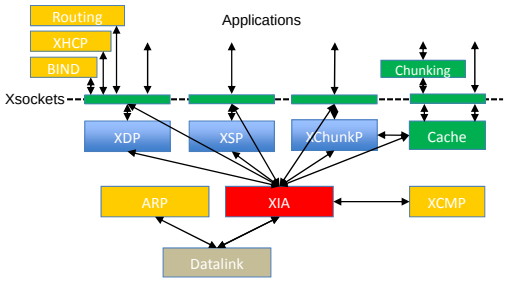
3. Intrinsic Security in XIA

- XIA uses self-certifying identifiers that guarantee security properties for communication operation
  - Host ID is a hash of its public key – accountability (AIP)
  - Content ID is a hash of the content – correctness
  - Does not rely on external configurations
- Intrinsic security is specific to the principal type
  - For example, to DoD trust management systems
- Useful for bootstrapping e-e security solutions
  - Address spoofing, DoS defense, …
  - Also useful for bootstrapping networks and operation in disconnected and partitioned networks

7

Open Source XIA Release

https://github.com/xia-project/



- XIA prototype released in 2012
- Used for evaluation, applications, services
- New functionality is being added regularly

- Full XIA protocol stack - support for NIDs, HIDs, SIDs, and CIDs
- Basic inter and intra domain routing protocols for the XIDs
- Support services and utilities, including name service; caching; equivalents for XHCP, ARP, ICMP; wireshark; socket remapping
- Vehicular and video distribution use cases push development

8

Outline

- XIA overview
- Applying XIA to the scenario
  - Requirements
  - Discussion focuses on
    - Novel security concepts
    - Availability
    - Topology control

9

Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

Assumption for now: XIA only network using diverse technologies

Hybrid network layers will be discussed later

10

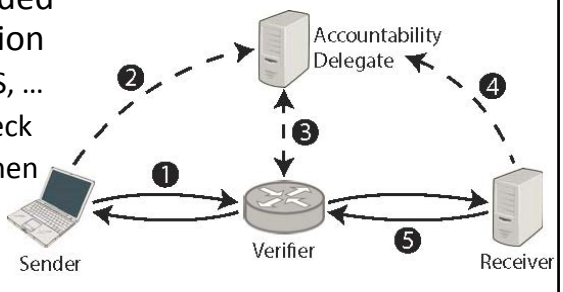
Authentication and Accountability

- XIDs are securely bound to an identity based on XID type
  - Service, host, content, etc.
  - Can be used to verify authenticity of the end-point
  - Properties target public Internet
- Roles, organizations, area of operation, etc. can either be:
  1. Incorporated into new XID types
  2. or looked up externally with other secure XIDs

11

A Closer Look at Accountability

- Intrinsic security can be used to prevent spoofing
  - Routers can ask sender to sign a challenge with the private key matching public key of the HID in the source address
  - Can be viewed as authorization for basic network service
- Idea could be expanded for richer authorization
  - Network access, QoS, …
  - Local or external check
  - Non-repudiation, when disconnected and breaking the rules is necessary



12

Disconnected Operation

Most Basic Address

Smart In-Path Service

- XIDs are not effected by changes in the network configuration
  - No reconfiguration of end-points required
  - Easier to manage address spaces
- As networks split and merge, or nodes get disconnected, their identity remains the same
  - Can use HID to verify that one is communicating with the same entity w/o third party
  - Change NID to locate it in a network
  - Smart in-network services can help manage

13

Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

14

Topology Control

- Multiple organizations are represented by multiple "domains" represented by NIDs
  - Managed independently
  - Can be very heterogeneous
- Topics related to communication topologies
  - Controlling access to links and networks (requirement 1)
  - Asynchronous communication
  - Controlling paths

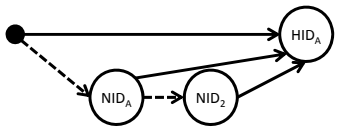
15

Intermittent Connectivity, DTN and Data Mules

- Caches can be used as a building block for asynchronous end-end communication
- Caches manage content (chunks) using CIDs
  - Chunks can be pushed to a cache (authorization)
  - Chunks can be discovered/fetched using different XID thypes, e.g., CIDs, "request" IDs (names), …
- Mule: push chunks to a rendez-vous cache where they are fetched by a UAV
- DTN: chunks "hop" from cache to cache as "links" become available

16

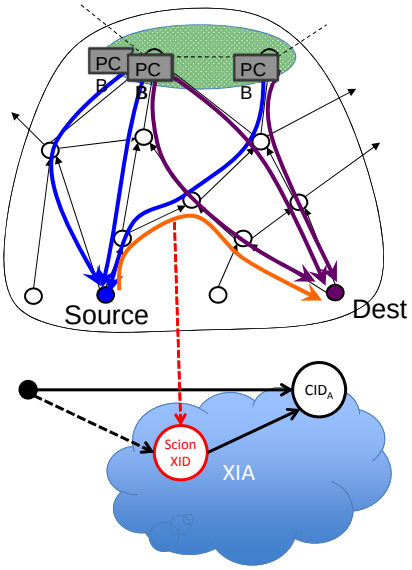
Source Routing



- Flexible DAG address format allows source routing to a destination
  - Specify full or partial path
  - Use in Internet raises policy and economic issues
- Can be used to reach destination
  - Before routing has stabilized
  - In the presence of failures
- Anything else?

17

Path-based Forwarding



- XIA supports forwarding based on a cryptographically enforced Scion path
  - Path defined as a sequence of cryptographic MACs
  - Represented by a "Scion ID"
- Receiver can verify path was followed
- Variety of mechanisms for picking paths
  - Alternate paths can have different properties

18

Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

19

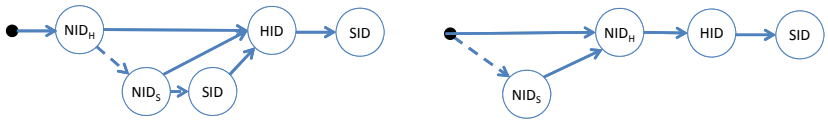
Redundancy

- Different XID types can provide alternate means of completing the communication
  - E.g., reach content using CID, SID, or HID
  - Can use completely independent forwarding and control plane mechanisms
- Some XID types inherently support replications
  - Caching of data inside network
  - Replicated services

20

Flexible Addressing

- Fallbacks support in-network error recovery in the presence of failures
  - Alternatives tend to take time:
  - Waiting for new routes to stability
  - Relying on retransmission from sender
- Fallbacks can use alternate paths or services
  - Paths can include loose source routing



21

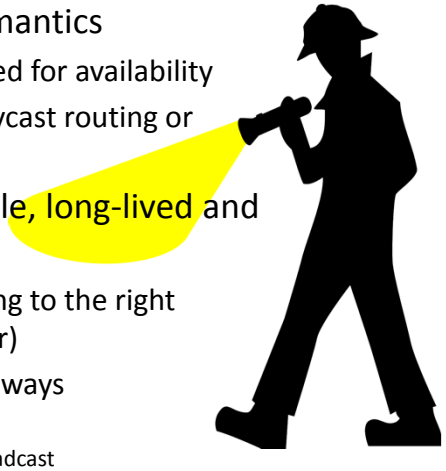
Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

22

Discovery of Dynamic Storage and Computing

- CIDs (storage) and SIDs (computing) provide discovery with anycast semantics
  - Destination can be replicated for availability
  - Reach destination using anycast routing or broadcast
- HIDs/CIDs/SIDs are portable, long-lived and secure
  - You can verify you are talking to the right endpoints (discussed earlier)
  - Can be distributed in many ways
    - Out of band or pre-deployment
    - Through registry service, or broadcast



23

Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

24

Bootstrapping Networks

- Bootstrapping networks requires establishing trust; discovering nodes, services, storage; and authorization for access to those services/storage
- Initially, trusted can be established based on pregenerated XIDs (hosts, SIDs, CIDs, ..) and authorization can be based on preloaded policies
- Discover mechanisms discussed earlier
- Once more infrastructure is in place, trusted name services, resource directories (time stamp, …) can be deployed for more scalable, efficient and secure operations.

25

Connecting Networks

- Connecting networks involves
  - Trust management (credentials; NIDs, names, …), exchange service capabilities, agreement on sharing/using services, configuration, …
- Example is “network joining” protocol being developed for vehicular networking use case
  - Offers flexibility for how each step is performed, depending on the configuration of the parties
  - Tries to optimize latency of connect time
- Requirements are likely to be radically different here

26

Key Requirements Scenario

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links and QoS

27

Heterogeneous Links

- Network management control typically uses a abstractions of actual links
  - Basic properties in public Internet: bandwidth, …
  - Can be more sophisticated, e.g., for wireless: range, bit rate, dynamics, …
- Link abstraction that is shared by end-points/ users and the network
  - Users can specify their requirements
  - Network can advertise capabilities, or configure link based on user requirements

28

Providing QoS

- Real-time, low latency, priorities, …
- Mechanisms for QoS are well understood
- Policies are specific to the context
  - Agreement on end-end policies in multi-organization network is a hard problem
- Authorization is a key requirement
  - Senders cannot mark all packet as “real-time”
  - Can leverage mechanisms under requirement 1

29

Mixing XIA and IP

- We have experience with 3 “types” of mixes:
  - Running protocol over the networks in parallel
  - One protocol runs as overlay over other (static)
  - XIA network clusters separated by the public Internet (uses an 4ID identifier)
  - IP applications communicating over XIA (~NAT)
- More general combinations would probably use a combination of these concepts
  - Quantify loss of benefits

30

Conclusion

XIA Concepts

1. Multiple identifiers type
   - Evolvability
   - Accommodates heterogeneity
2. Fallbacks, flexible address
   - Evolvability, heterogeneity
   - Availability
3. Cryptographic identifiers
   - Built-in authentication
   - Simplify configuration
   - Mobility, disconnected, …

Scenario Requirements

1. Existing and novel security constructs
2. Topology control; DTN and data mules
3. Availability
4. Dynamic storage and computation
5. Bootstrapping networks
6. Heterogeneous links, QoS

31