XIA: eXpressive Internet Architecture - A Proposal for a Future Internet Architecture

15-441/641: Computer Networking

Lecture 28: What is Next?

Peter Steenkiste

Fall 2016

www.cs.cmu.edu/~prs/15-441-F16

Outline

- Background
- The eXpressive Internet Architecture – a proposal
- Research examples: AIP and APIP
- User privacy survey

NOTE: this lecture describes a research project.

The goal is to have you think outside of the box.

2

Key Internet Features

What we learned about the current Internet:

- Simple core with smart endpoints
- The IP narrow waist supports evolution
- Packet based communication
- All IP hosts can exchange packets
- Non-essential functions are services
- End-to-end transport protocols
- Security is not part of the architecture

But maybe there are better ways?

3

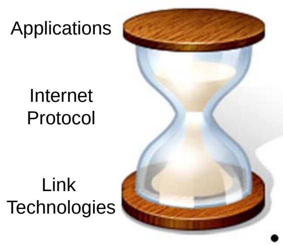
Outline

- Background
- The eXpressive Internet Architecture – a proposal
  - Not on final
- Research examples: AIP and APIP

4

"Narrow Waist" of the Internet Key to its Success

- Has allowed Internet to evolve dramatically
- But now an obstacle to addressing challenges:
  - No built-in security
  - New usage models a challenge – content and services, not hosts
  - Hard to leverage advances in technology in network
  - Limited interactions between network edge and core



- But where do we get started?

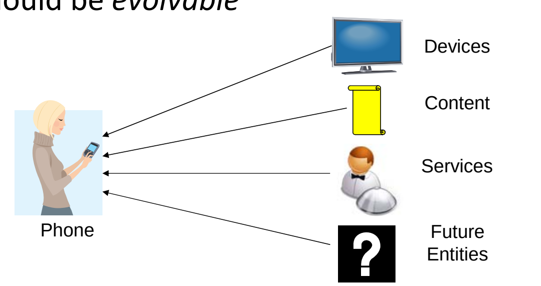
Three Simple Ideas

- Support multiple types of destinations
  - Not only hosts, but also content, services, etc.
  - Not having to force communication at a lower level (e.g., hosts) reduces complexity and overhead
- Intrinsic security guarantees security properties as a direct result of the design of the system
  - Do not rely on external configurations, data bases, ..
- Flexible addressing gives network more options for successfully completing communication operations
  - Include both "intent" and "fallback" address
  - Supports evolvability, network diversity, fault recovery, mobility, ..

6

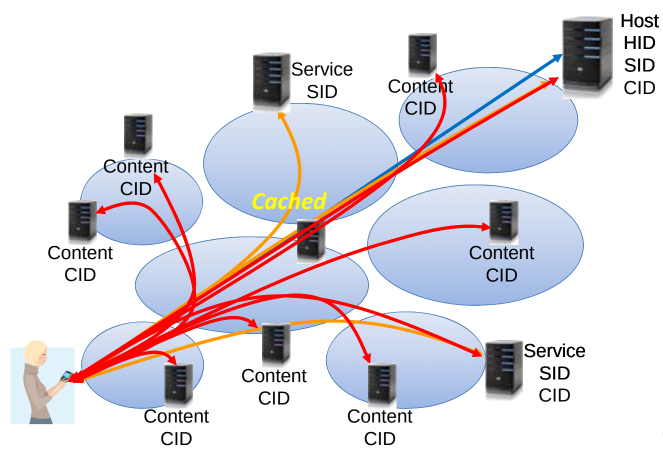
Multiple Principal Types

- Identifying the intended communicating entities reduces complexity and overhead
  - Have different forwarding semantics
- Set should be *evolvable*



7

Multiple Principal Types - Example



8

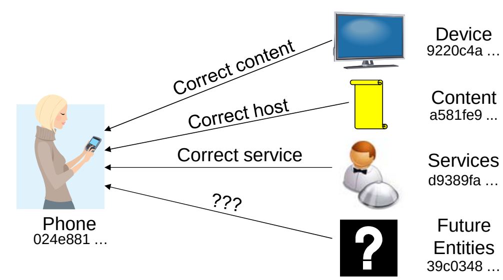
Using Principal Types

- Content and service addresses directly supports cross-application service selection and caching
  - Complex today: DNS indirection infrastructure, deep packet inspection, transparent proxies, etc.
- Routing protocols for hosts, content and services
  - Metrics driving by context, different concerns
  - Public internet: policies, business, …
  - Intra-networks: usage models, super fast recovery, …
- Add new (custom) functionality to the network
  - E.g., caching + service -> diverse multicast variants
  - Dealing with disruptions

9

Security as Intrinsic as Possible

- Communication security properties are a direct result of the design of the system
  - Do not rely on correctness of external configurations, actions, data bases



10

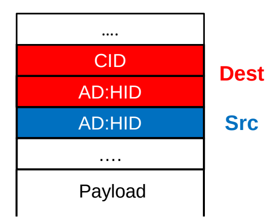
Use of Intrinsic Security

- Name-> address look automatically provides public key associated with the address
  - May not need for separate key management infrastructure
  - Can help, e.g., with network partitioning
- Changing of addresses in session in network layer
  - Sign change with private key associated with old address
- New types of intrinsic security that might
  - Variants for services, contents and hosts; new types
  - Support for existing key management processes
- Simplify comprehensive security mechanisms

11

Supporting Evolvability: Flexible Addressing

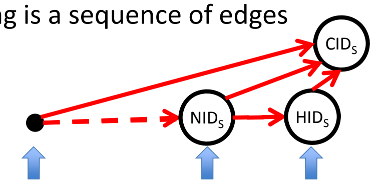
- Introduction of a new principal type will be incremental – no "flag day"!
  - Not all routers and ISPs will provide support from day one
- Creates chicken and egg problem - what comes first: network support or use in applications
- Solution: provide an *intent* and *fallback* address
  - Intent address allows in-network optimizations based on user intent
  - Fallback address is guaranteed to be reachable



12

Flexible Addressing

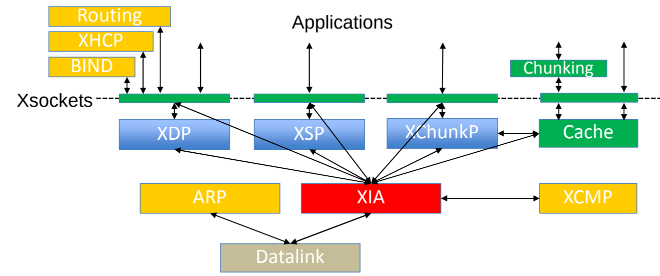
- Addresses are represented as Directed Acyclic Graphs of typed identifiers
  - Fallbacks are different, ordered edges
  - Scoping is a sequence of edges



- Used to deal with mobility, incremental deployment, …

Open Source XIA Release

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

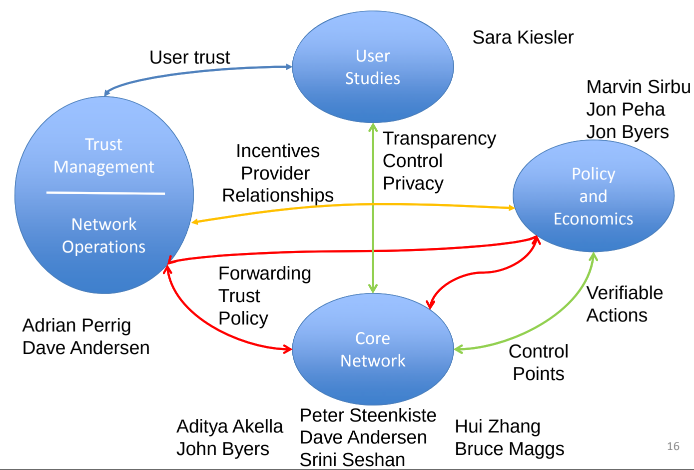


- XIA Prototype released in May 2012
  - Includes full XIA protocol stack and utilities
- Being used to support evaluation, applications, services
- New functionality is being added regularly

Ongoing Networking Research

- Transport protocols: congestion control, error recovery
- Intrinsic security and mobility, …
- Incremental deployment of network architectures (features)
- Verification of third party services using TPMs
- Very fast lookup of flat IDs in huge tables
- Optimize use of network features under user control
- Native Unix XIA implementation – extreme evolvability
- Design of a network control plane
- Supporting DTNs, pub-sub systems, group communication, …
- Routing and forwarding for services, content
- Network diagnostics, centralized versus distributed control
- Video streaming as a use case for XIA
- Economic incentives and implications of cryptographic identifiers
- Balancing user accountability and privacy

Broader XIA Research Agenda



Outline

- Background
- The eXpressive Internet Architecture – a proposal
- Research examples: AIP and APIP
  - Accountability AND privacy

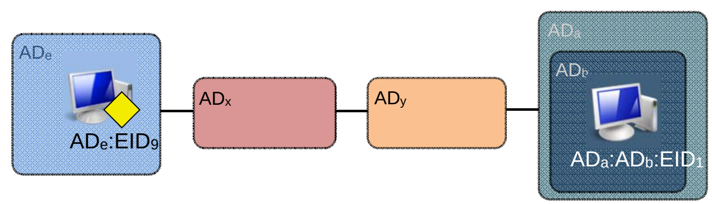
Examples of XIA-related Research

- The Accountable Internet Protocol
  - Accountable Internet Protocol (AIP). David Andersen, et al, ACM *SIGCOMM* 2008
  - Example of a protocol that provides accountability for host-based communication
- The Accountable and Private Internet Protocol
  - Balancing Accountability and Privacy (APIP). David Naylor, et al, ACM *SIGCOMM* 2014
  - Expands on AIP to support user privacy

AIP Motivation

- Many security challenges are a result of not being able to unambiguously determine who is responsible for a specific action
  - Source spoofing, DOS attacks, untraceable spam, ..
- Add accountability to the Internet architecture
- Key idea is to use "self-certifying" addresses for both hosts and domains
- Avoid dependence on external configurations
  - E.g. global trust authority

Addressing and Routing



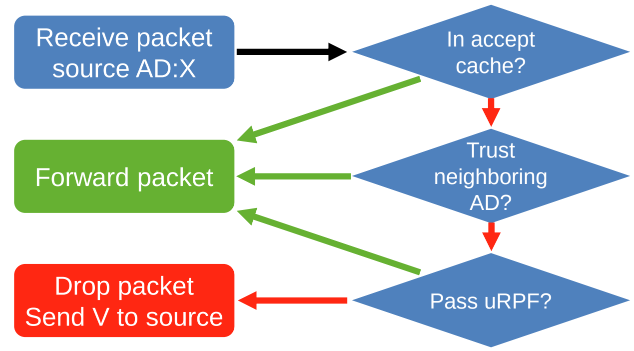
- Addresses are hierarchical, similar to today's Internet
  - But each level has a flat address, i.e. no CIDR
- Until packet reaches destination AD, intermediate routers use only destination AD to forward packet
  - Effectively uses a pointer in a stack of domain identifiers
- Upon reaching destination AD, forward based on EID

Self-Certifying Identifiers

- Identifier of object is public key of object
  - Convenient to use hash of object (e.g. fixed size)
  - Need way of securely mapping user readable name into the identifier
- AD is hash of public key of domain
- EID is hash of public key of host
- Provides a means of verifying the correctness of the "source" identifiers in a packet
  - Effectively by sending a challenge to the source that it must sign with its private key

21

Example: AD verification



22

Verification Packet

- Router sends a challenge V to Source containing:
  - Source and destination identifier
  - Hash of the packet P
  - Interface of the router
  - A secret signed by R
- Source signs V with its private key and sends it back to R
  - But only if it recognizes the hash
- R verifies that it was signed correctly using the public key from the source field
- If they match, R add S to its cache

23

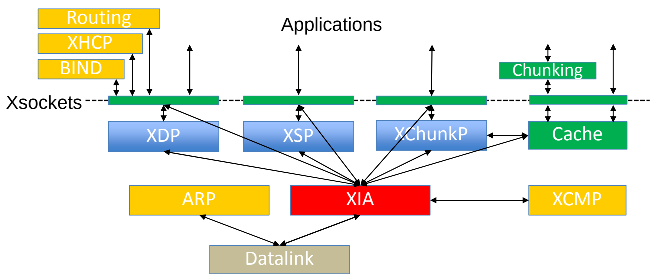
AIP Discussion

- AIP adds complexity to routers …
  - Crypto support, caches, larger forwarding tables, ..
- … but accountability helps address number of security challenges
  - Reduces complexity and cost in rest of networks
- Research question
  - Fast look up in large tables of flat identifiers
  - Managing keys (revocation, minting, …)
  - Evolving of the crypto

24

Open Source XIA Release

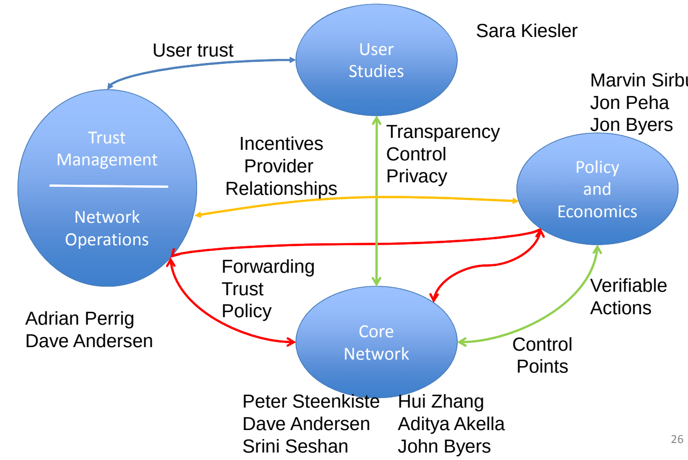
https://github.com/xia-project/



- XIA Prototype released in May 2012
  - Includes full XIA protocol stack and utilities
- Being used to support evaluation, applications, services
- New functionality is being added regularly

25

Broader XIA Research Agenda



26

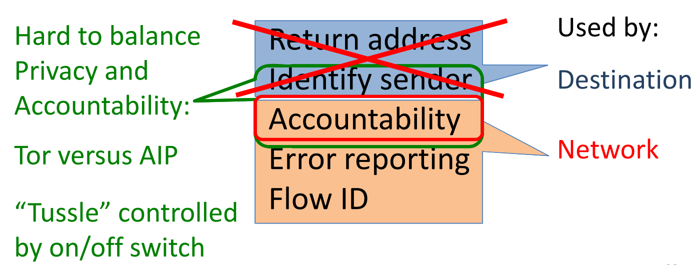
Growing User Concern about Privacy

- Fueled by personal experience and reports, e.g., social networks, vendors, Snowden, …
  - More privacy is always better?
- Privacy can be expensive
  - Obvious example: strong anonymity using TOR
  - More subtle costs associated with HTTPS
    - "The Cost of "S" in HTTPS", Naylor et. al., ACM CoNext, Dec 2014
  - Lack of accountability
- AIP provides accountability – price is loss of privacy
  - TOR is the other way around!

27

Source Addresses, or Balancing Privacy and Accountability

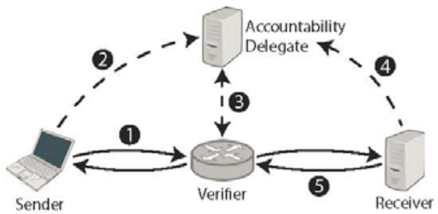
- Source address are assumed to be essential but you can build a network without them
- What are source addresses used for?



28

Accountability and Privacy

- View source addresses as accountability addresses
  - Uses AIP style accountability, but …
  - Accountability can be delegated to a “service” that takes responsibility for packet
  - Return address can be (hidden) inside packet
- Many “details”: nature of delegate, fate sharing, …



29

Final Announcements

- P3 due on last day of classes
- HW4 due today
- Final on Dec 18, 5:30-8:30
  - Closed book
  - Full semester, with emphasis on second half
  - Special office hours next week (see web)
- Liked the course and the projects?
  - Maybe you want to TA next fall
  - Or maybe you want to get involved in research
  - Or take Wireless Networking: 18-452/755 in S17

30

XIA Project

- More information:
  - http://www.cs.cmu.edu/~xia
- XIA faculty
  - Peter Steenkiste, CS/ECE, Carnegie Mellon
  - Dave Andersen, David Eckhardt, Srini Seshan, Hui Zhang, CS, Carnegie Mellon
  - Sara Kiesler, HCII, Carnegie Mellon
  - Jon Peha, Marvin Sirbu, EPP, Carnegie Mellon
  - Adrian Perrig, ETH/Carnegie Mellon
  - Aditya Akella, CS, University of Wisconsin
  - John Byers, CS, Boston University
  - Bruce Maggs, CS, Duke

Carnegie Mellon BOSTON UNIVERSITY THE UNIVERSITY of WISCONSIN MADISON

Outline

- Background
- The eXpressive Internet Architecture – a proposal
  - Example and concepts
  - Research thrusts
- Research examples: AIP and APIP
  - Accountability AND privacy
- User privacy survey

32

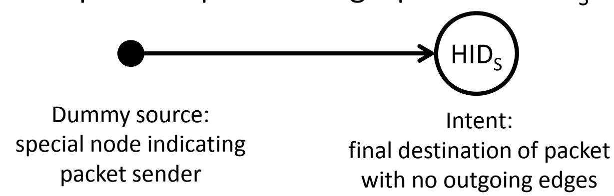
Addressing Requirements

- Fallback: intent that may not be globally understood must include a backwards compatible address
  - Incremental introduction of new XID types
- Scoping: support reachability for non-globally routable XID types or XIDs
  - Needed for scalability
  - Generalize scoping based on network identifiers
  - But we do not want to give up leveraging intent
- Iterative refinement: give each XID in the hierarchy option of using intent

33

Our Solution: DAG-Based Addressing

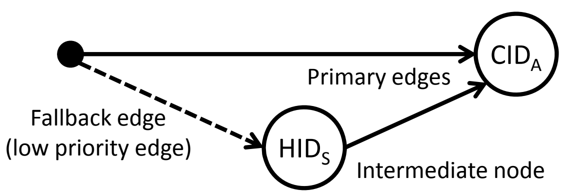
- Uses direct acyclic graph (DAG)
  - Nodes: typed IDs (XID; expressive identifier)
  - Outgoing edges: possible routing choices
- Simple example: Sending a packet to HID_S



34

Support for Fallbacks with DAG

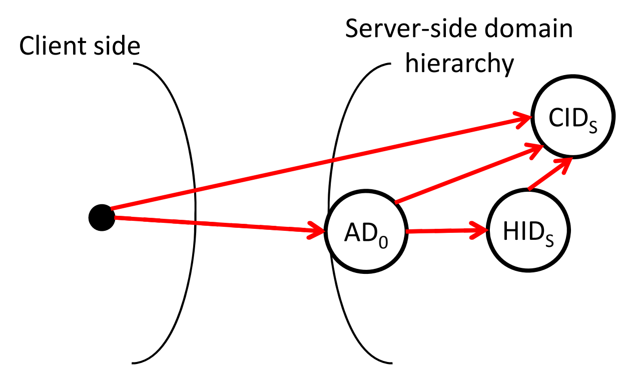
- A node can have multiple outgoing edges



- Outgoing edges have priority among them
  - Forwarding to HID_S is attempted if forwarding to CID_A is not possible – Realization of fallbacks

35

DAGs Support Scoping and Iterative Refinement



"XIA: Efficient Support for Evolvable Internetworking", NSDI 2012

36