The eXpressive Internet Architecture: from Architecture to Network

Peter Steenkiste
Dave Andersen, David Eckhardt, Sara Kiesler, Jon Peha, Adrian Perrig, Srini Seshan, Marvin Sirbu, Hui Zhang
Carnegie Mellon University
Aditya Akella, University of Wisconsin
John Byers, Boston University

NSF Workshop,
Istanbul, June 4, 2012

NSF Future Internet Architecture

- The Internet has been unbelievably successful
  - Has sustained tremendous growth
  - Supports very diverse set of applications and services
  - Integral part of our society and economy
- Lots of exciting research on how to improve Internet
  - Security, routing, wireless/mobile, management, …
  - But Internet architecture constrains what can be modified
- Future Internet Architecture frees researchers to go beyond today's IP architecture and infrastructure
  - Five teams funded by NSF, including XIA

Outline

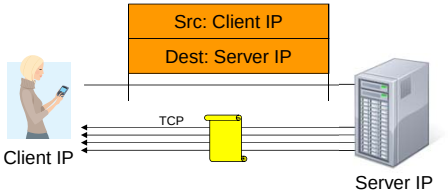
- XIA architecture concepts
  - Motivating example
- Building an XIA network
- Research directions

Predicting the Future is Hard!

- A lot of really smart people don't agree:
  - Named Data Networking: content centric networking - data is a first class entity
  - Mobility First: mobility as the norm rather than the exception – generalizes delay tolerant networking
  - Nebula: Internet centered around cloud computing data centers that are well connected

We love all of them!

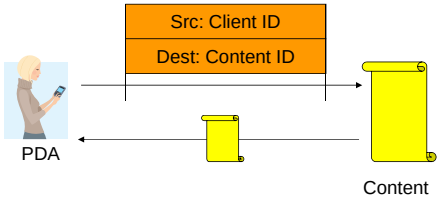
Today's Internet



- Client retrieves document from a specific web server
  - But client mostly cares about correctness of content, timeliness
  - Specific server, file name, etc. are not of interest
- Transfer is between wrong principals
  - What if the server fails?
  - Optimizing transfer using local caches is hard
    - Need to use application-specific overlay or transparent proxy – bad!

5

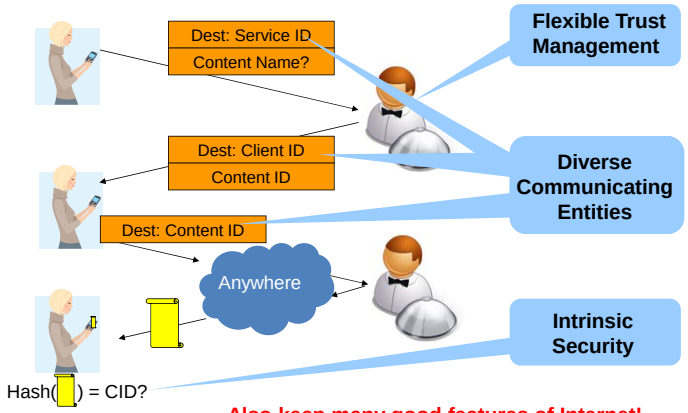
eXpressive Internet Architecture



- Client expresses communication intent for content explicitly
  - Network uses content identifier to retrieve content from appropriate location
- How does client know the content is correct?
  - Intrinsic security! Verify content using self-certifying id:
    hash(content) = content id
- How does source know it is talking to the right client?
  - Intrinsic security! Self-certifying host identifiers

6

A Bit More Detail …



Also keep many good features of Internet!

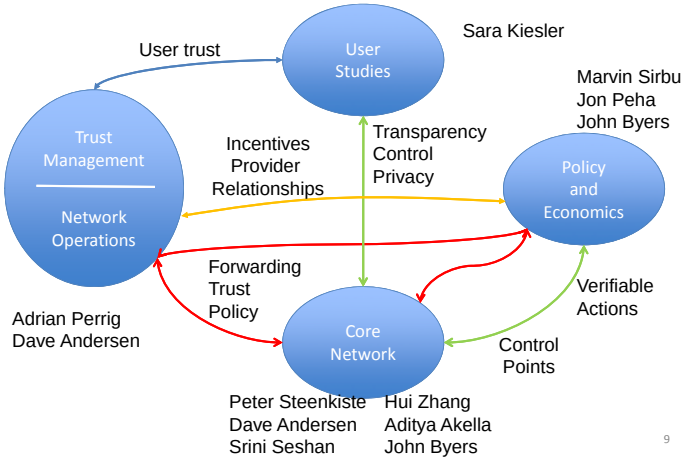
7

XIA: eXpressive Internet Architecture

- Each communication operation expresses the intent of the operation
  - Also: explicit trust management, APIs among actors
- XIA is a single inter-network in which all principals are connected
  - Not a collection of architectures implemented through, e.g., virtualization or overlays
  - Not based on a "preferred" principal (host or content), that has to support all communication

8

Interactions between Actors



Outline

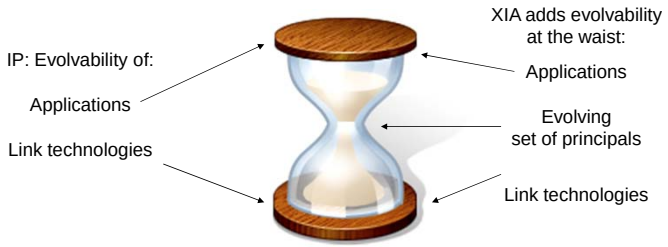
- XIA architecture concepts
- Building an XIA network
  - Making it work
- Research directions

Multiple Principal Types

- Hosts XIDs support host-based communication similar to IP – *who?*
- Service XIDs allow the network to route to possibly replicated services – *what does it do?*
  - LAN services access, WAN replication, …
- Content XIDs allow network to retrieve content from "anywhere" – *what is it?*
  - Opportunistic caches, CDNs, …
- Autonomous domains allow scoping, hierarchy
- Associated with different forwarding semantics
- Set of principal types can evolve over time

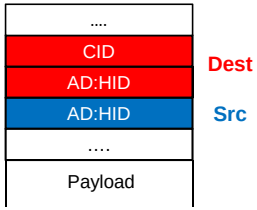
What Do We Mean by Evolvability?

- Narrow waist of the Internet has allowed the network to evolve significantly
- But need to evolve the waist as well!
  - Can make the waist smarter



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
- Creates chicken and egg problem - what comes first: network support or use in applications
- Solution is to provide an *intent* and *fallback* address
  - Intent address informs network of user intent
  - Fallback address is guaranteed to be reachable



13

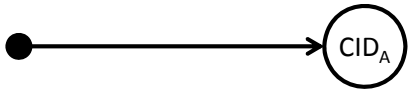
Addressing Requirements

- 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
- Support for mobility, in-path services, …
- Want to combine the above requirements

14

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 CID_S



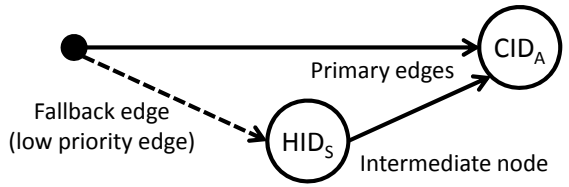
Dummy source: special node indicating packet sender

Intent: final destination of packet with no outgoing edges

15

Support for Fallbacks with DAG

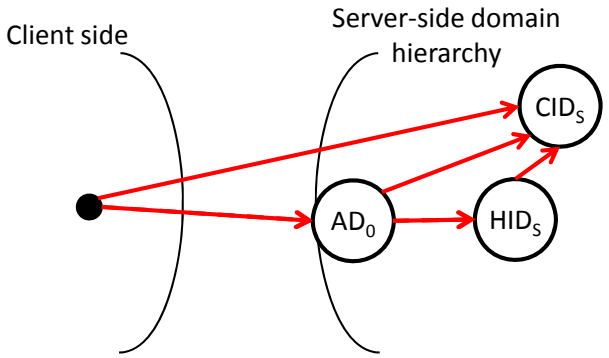
- A node can have multiple outgoing edges



- Outgoing edges have priority among them
  - Forwarding to HID_S is attempted if forwarding to CID_A is not possible – Realization of fallbacks
  - Helps routers deal with routing failures

16

DAGs Support Scoping and Iterative Refinement



Raises many interesting questions!

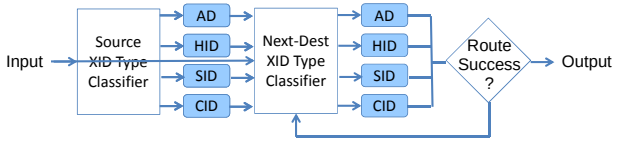
17

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
- Example: retrieve content using …
  - Content XID: content is correct
  - Service XID: the right service provided content
  - Host XID: content was delivered from right host

18

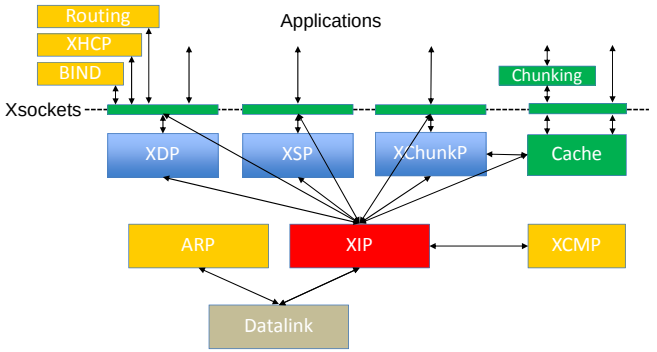
Packet Processing Pipeline



- Principle-independent processing defines how to interpret the DAG - core XIA architecture
- Principle-dependent processing realizes forwarding semantics for each XID type
- Implemented in Click – see NSDI 2012
- Optimizations possible: fast path processing, packet level and intra-packet parallelism

19

Full XIA Prototype

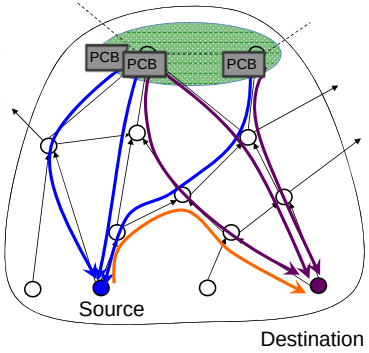


- Open source release: http://www.cs.cmu.edu/~xia
- Support for GENI and VM-based experiments

20

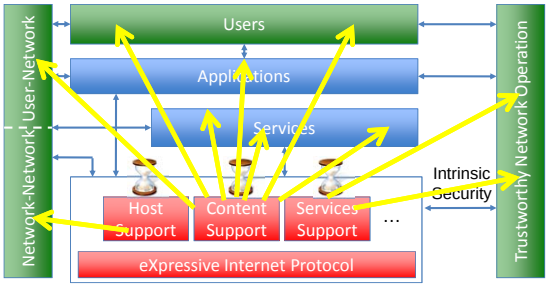
Path Selection in SCION Architecture Overview

- Source/destination can choose among up/down hill paths
  - Path control shared between ISPs, receivers, senders
- Desirable security properties:
  - High availability, even in presence of malicious parties
  - Explicit trust for operations
  - Minimal TCB: limit number of entities that must be trusted
  - No single root of trust
  - Simplicity, efficiency, flexibility, and scalability
- Porting to XIA DP this summer



21

XIA Components and Interactions



22

Outline

- XIA architecture concepts
- Building an XIA network
- Research directions
  - What is different?

23

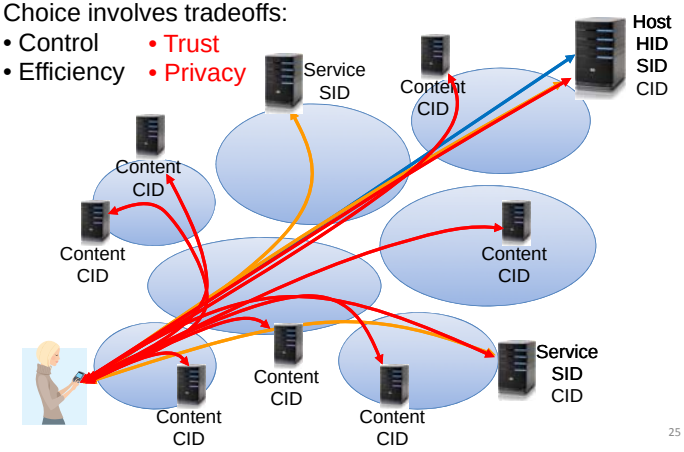
Balance of Control between Network Core and Edge

- Internet places most control in the network
- XIA provides more control to the edge
  - Choice of principal, DAGs, Scion path selection
  - Also offers flexibility to service providers: control path properties, new services, …
- Many research opportunities
  - Other mechanisms + other functions/layers
  - Customizing roles depending on context
  - How to manage the tradeoff at runtime

24

Multiple Principal Types

Choice involves tradeoffs:
- Control
- Efficiency
- Trust
- Privacy



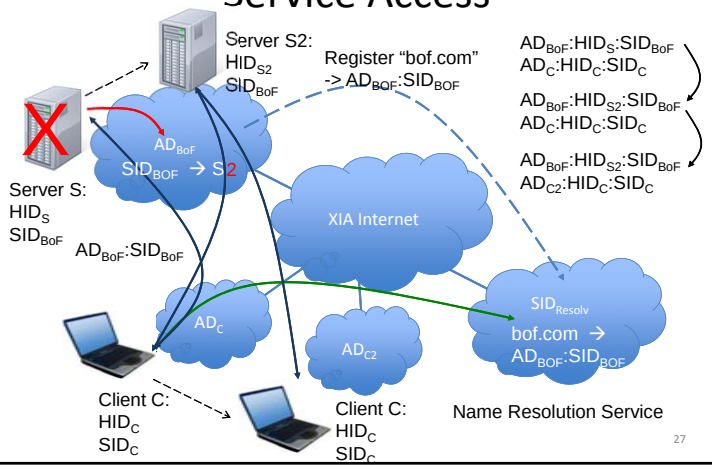
25

Using DAGs

- DAG is "locator" that helps network reach "destination"
  - Provided by destination through a name service
  - Has the right incentive!
- DAG is created jointly by all parties involved
  - Source can modify destination DAG, pick from options, ..
  - DAG can be modified during session
  - Networks can limit what DAGs they accept
- Many other options exist
  - Path based options, locator services, different headers, ..

26

Example: Secure Mobile Service Access



27

Functionality in Network versus Edge

- Internet had notion that higher level functions were implemented at the edge
  - Currently lots of functionality in the network
- XIA addressing flexibility simplifies adding functions to the network
  - Services, new principal types
  - Does not require universal agreement (DAGs)
  - Example: supporting diversity at edge (Tapa)
- Many alternative solutions
  - Service-oriented architectures, active nets, …

28

How Much and What Security in the Network

- XIA uses "intrinsic security" to guarantee some properties of communication operation
  - XIA: cryptographic identifiers, Scion paths
  - Several other projects are using cryptographic ids.
- Many alternatives to explore
  - Different types of cryptographic identifiers
  - Alternative approaches, evolving the mechanisms
  - Verifiability of network functions

29

What About the Users?

- Who are the users?
  - Human end-users, applications, or edge networks
- Trust management, naming
  - Hosts – DNS – nice and hierarchical
  - Services and content – different
    - Important: want to skip hosts
- User trust in network
  - Visibility + control
  - "Privacy button"

30

Conclusion

- XIA supports evolution, expressiveness, and trustworthy operation.
  - Multiple principal types, flexible addressing, and intrinsic security
  - More information (including on release)

    http://www.cs.cmu.edu/~xia
- Broad research agenda on key tradeoffs in network
  - Edge versus core, security in network, evolvability, …
  - Affects all aspects of the network: transport protocols, trust management, applications, services, …

31