eXpressive Internet Architecture: Overview and Next Phase

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
Bruce Maggs, Duke University

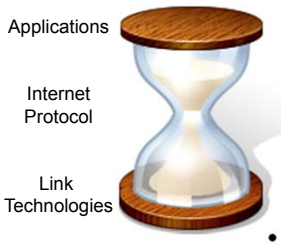
May 2014, NSF PI Meeting

Outline

- XIA overview
  - Architecture review
  - Prototype
  - Research activities
- Research nuggets
- Next phase direction

"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.
  - Network can adapt over time - reduces complexity and overhead at higher layers
- Flexible addressing gives the network multiple options for completing a communication operation
  - Includes both an "intent" and "fallback" address
  - Supports evolvability, in-network error recovery, network diversity, mobility, …
- Intrinsic security guarantees security properties as a direct result of the design of the system
  - Do not rely on external configurations, data bases, ..
  - Network level management of addresses

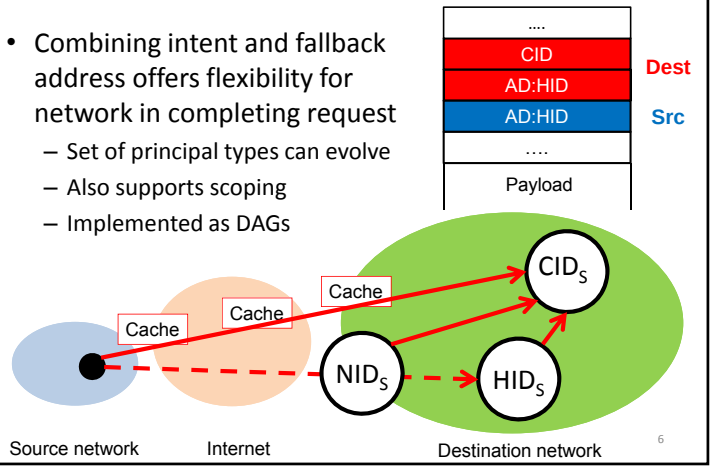
Multiple Principal Types

- 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
- Set of principal types can evolve over time

5

Flexible Addressing

- Combining intent and fallback address offers flexibility for network in completing request
  - Set of principal types can evolve
  - Also supports scoping
  - Implemented as DAGs



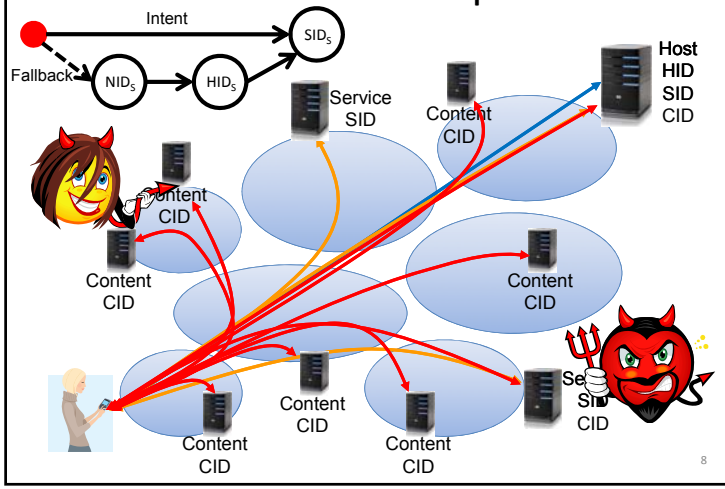
6

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
- Useful for bootstrapping e-e security solutions
- Intrinsic security is specific to the principal type:
  - Content XID: content is correct
  - Service XID: the right service provided content
  - Host XID: content was delivered from right host

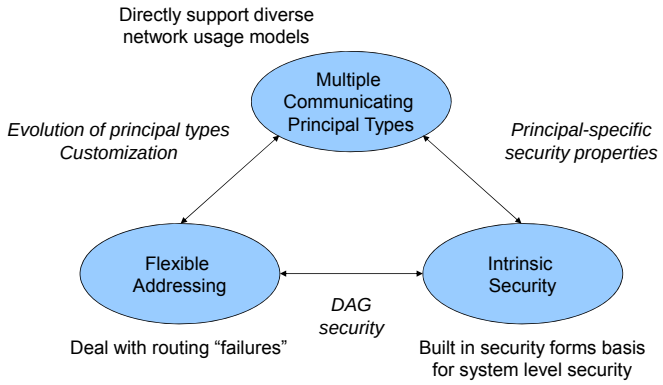
7

XIA: An Example



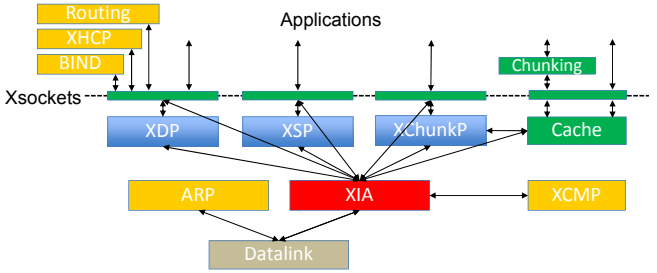
8

Ideas are Complementary



Open Source XIA Release

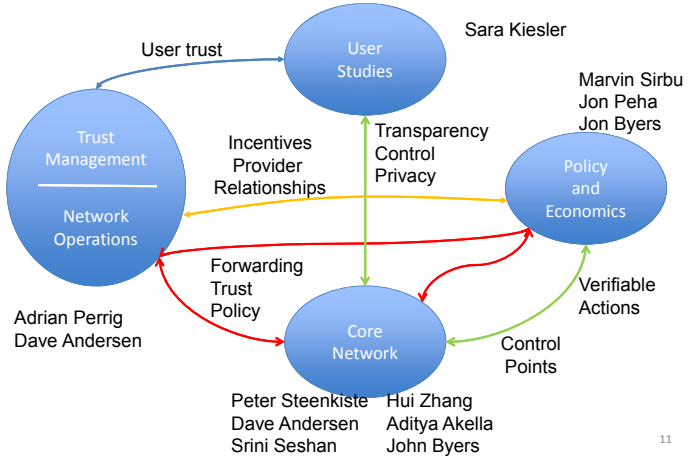
https://github.com/xia-project/



- 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

10

Broader XIA Research Agenda



11

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; extensibility
- Design of a network control plane
- 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

12

Outline

- XIA overview
- Research nuggets
  - Architecture
  - Controlling paths
  - Evolvability everywhere
  - Users and providers
- Next phase directions

13

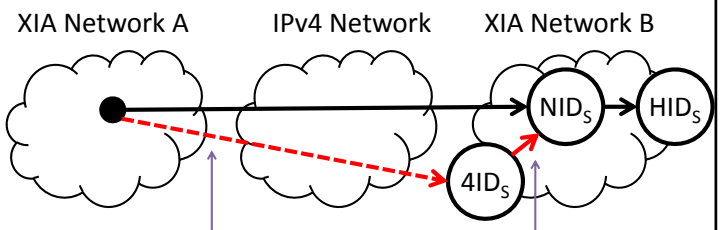
Architecture Nuggets

Examples of how XIA features can help address various network challenges

- Evolvability
- Mobility
- Incremental deployment
- Accountability versus privacy
- eXtreme evolvability

14

4ID in Action: Dealing with Legacy Networks



Entering IPv4 network: Encapsulate XIA packet with IP header

Entering XIA network: Remove IP header for native XIA packet processing

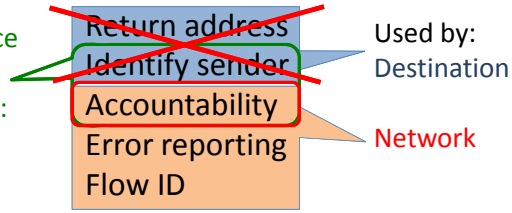
Works for arbitrary pairs of XIA networks

15

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?

Hard to balance Privacy and Accountability: Tor versus AIP



16

Accountability and Privacy

- View source addresses as accountability addresses
  - "Service" that takes responsibility for packet
    - Accountability can be delegated
  - Return address can be inside packet
  - Uses AIP style accountability
- Many "details": nature of delegate, faith sharing, …

17

XIA as a Platform of Architectural Exploration

- Evolvability is hard to quantify
- Our approach: port alien designs
  - Push evolvability to the extreme
  - Realize pluralism through inclusiveness
- Recurrent porting questions
  - How to best map Y's identifiers to XIDs?
  - When can we reuse XID types?
  - How to break Y into principals?
  - Are there interesting alternative interpretations?

How Alien Designs Pushed XIA

- Serval: service-centric architecture
  - multiple classes of identifiers
- NDN: content-centric architecture
  - evolution stress test

- IP: migration/deployment plan
- ANTS: active network
  - Proof/demonstration of generality

Outline

- XIA overview
- Research nuggets
  - Architecture
  - Controlling paths
  - Evolvability everywhere
  - Users and providers
- Next phase directions

20

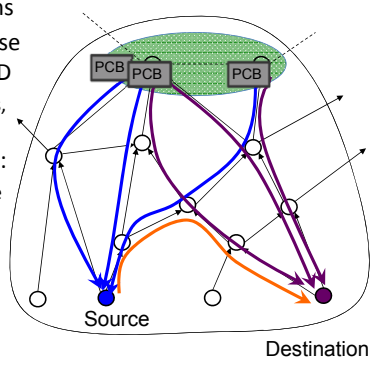
SCION Architectural Goals

- High availability, even in presence of malicious parties
- Explicit trust for network operations
- Minimal TCB: limit number of entities that need to be trusted for any operation
  - Strong isolation from untrusted parties
- Operate with mutually distrusting entities
  - No single root of trust
- Enable route control for ISPs, receivers, senders
- Simplicity, efficiency, flexibility, and scalability

21

Path Selection in SCION Architecture Overview

- Split network in trust domains
- Source/destination can choose from up/down hill paths in TD
  - 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



22

Richer Interfaces - Tussle

- How do we control relationship between users, service providers, ISP, etc. – "choice points":
- Choice of XID type, i.e. how is communication operation performed involving different tradeoffs
  - Choices for both end-points and providers: XIDs to use or support
- DAGs add flexibility: fallback, services, …
  - Input from destination, sources, and providers
  - Different options for supporting binding, mobility, …
- Scion offers some control over path selection
  - Can balance control between end-points and providers
  - Opens doors for service differentiation

23

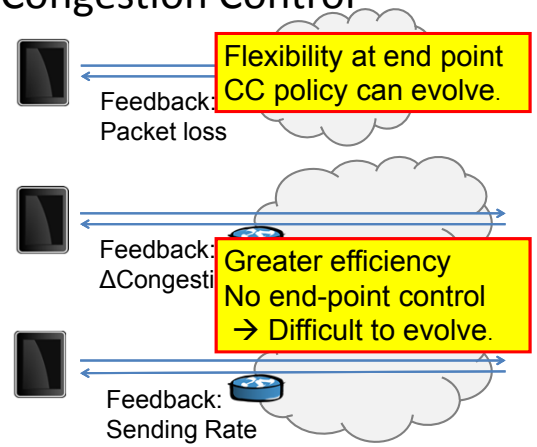
Outline

- XIA overview
- Research nuggets
  - Architecture
  - Controlling paths
  - Evolvability everywhere
  - Users and providers
- Next phase directions

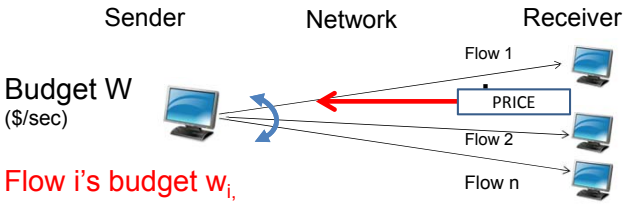
24

Evolvability Everywhere Congestion Control

- TCP and friends
- XCP
- RCP



Can we achieve both?



Flow i's budget w_i, subject to $W \geq \Sigma w_i$

Flow i's price: P_i ($/Byte)

Flow i's rate: R_i = budget/price = w_i / P_i (Byte/sec)

Questions/Challenges
- Can we achieve high efficiency?
- Can we implement different CC policies?
- How to deal with feedback errors due to delay?

26

Outline

- XIA overview
- Research nuggets
  - Architecture
  - Controlling paths
  - Evolvability everywhere
  - Users and providers
- Next phase directions

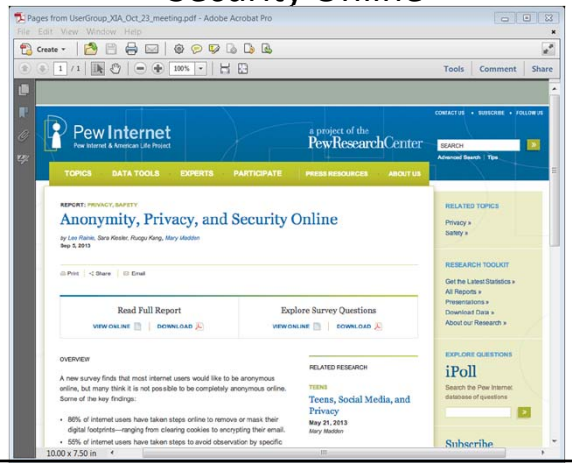
27

User Perspective

- Research questions
  - What do people know about the Internet?
  - Does informing them change their behavior?
- User study on user perspective on anonymity and privacy online (Ruogu Kang)
  - Users care about privacy for some sessions
  - User concerns are very diverse (really)
  - Users do not have clear picture of who gets access to what information as a result of specific actions
    - E.g., network versus application level threat

28

Pew Study on Anonymity, Privacy and Security Online



29

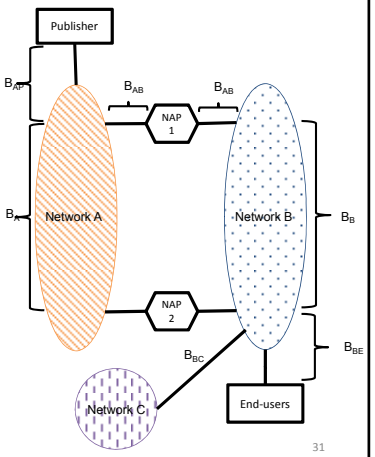
Must "Empower" Users

- Having network-level mechanisms to deal with various threats is not sufficient
- How do users know what information is visible to observers inside the network?
  - Tell them!
  - Course project in HCI defined sample interface
- How do users control privacy for individual sessions?
  - Need to have model of what the threat is: source, destination, different points in the end-to-end path

30

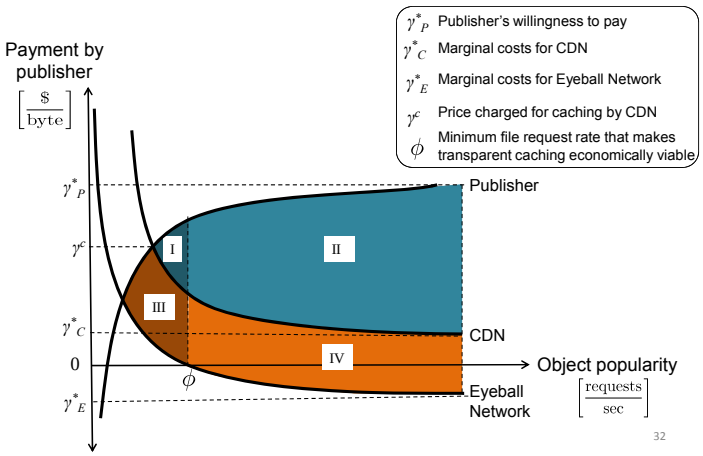
When Should ISPs Cache?

- Many FIA proposals support app-independent caching, e.g., CIDs
  - ISP can subsume role of CDNs
- Consider transparent and "for pay" caching
  - Payment requires billing/ accountability services
- Eyeball networks have the most to gain



31

When is caching viable?



32

Outline

- XIA overview
- Research nuggets
- Next phase directions
  - Evaluation of network architectures
  - Network environments
  - Control plane architecture
  - Building and using XIA networks
  - Privacy, anonymity, and accountability

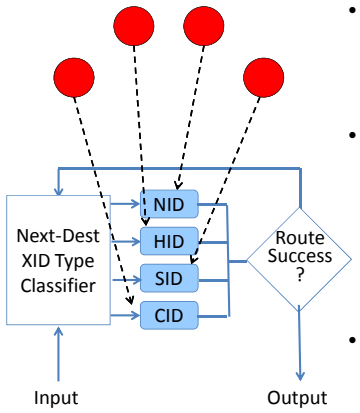
33

Control Plane Architecture

- Today's internet does not have a real control plane
  - Ad hoc collection of independently developed control protocols, e.g., BGP, ICMP, …
- What would an architecture for a internet control plane look like?
  - What functions can be shared across protocols?
  - Can it evolve? Incremental protocol deployment?
  - How do we secure it?
- Use routing for our initial focus
  - More on this later

34

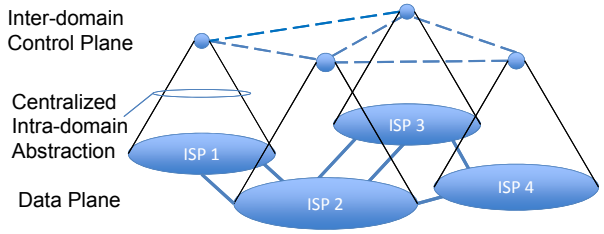
XIA Packet Processing Pipeline



- Principal-independent processing defines how to interpret the DAG
  - Core architecture
- Principal-dependent processing realizes forwarding semantics for each XID type
  - Logically: one forwarding table per XID type
  - Reality: anything goes, e.g., no forwarding table
- Control plane sets up forwarding for each principal type

35

Control Plane
The 10K Mile View



- Domains present a single point of control at inter-domain level
- Matches logically centralized intra-domain control
  - But actual implementation can be anything

36

Building and Using an XIA Network

- Looking at various network challenges and they can be addressed within XIA
  - Internet congestion control
  - Multicast and mobility
- Deploying and managing XIA networks
  - Multihoming, multipath
  - Service discovery, binding and routing
  - Fast XIA
  - Establishing and controlling session

37

Questions?