XIA: An Architecture for a Trustworthy and Evolvable Future Internet

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

GENI Engineering Conference 10
March 16, 2011

Carnegie Mellon

BOSTON UNIVERSITY

THE UNIVERSITY of WISCONSIN MADISON

Outline

- Vision
- Getting real
- The real world

2

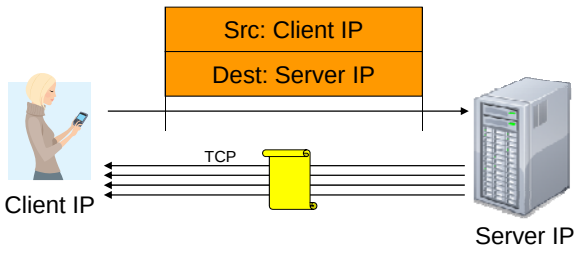
Vision

We envision a future Internet that:

- Is trustworthy
  - Security broadly defined is the biggest challenge
- Supports long-term evolution of usage models
  - Including host-host, content retrieval, services, …
- Supports long term technology evolution
  - Not just for link technologies, but also for storage and computing capabilities in the network and end-points
- Allows all actors to operate effectively
  - Despite differences in roles, goals and incentives

3

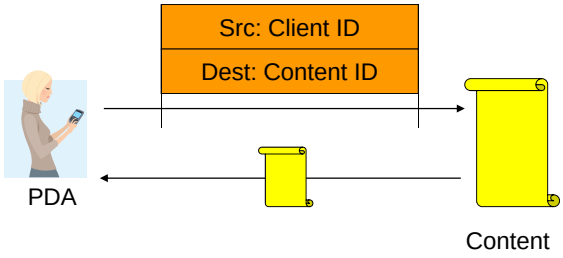
Today's Internet



- 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!

4

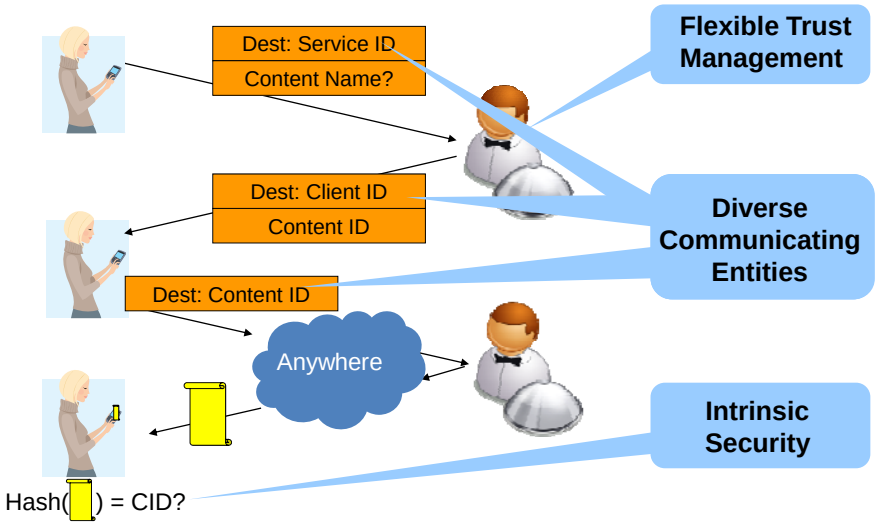
eXpressive Internet Architecture



- 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

5

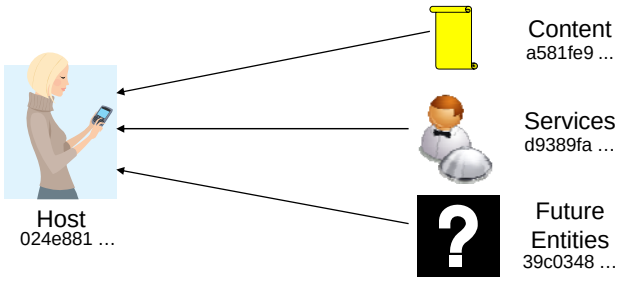
A Bit More Detail …



6

P1: Evolvable Set of Principals

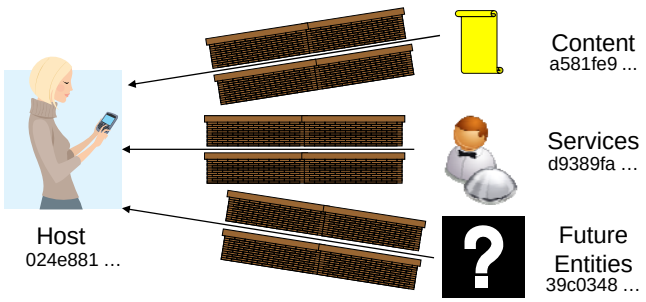
- Identifying the intended communicating entities reduces complexity and overhead
  - No need to force all communication at a lower level (hosts), as in today's Internet
- Allows the network to *evolve*



7

P2: Security as Intrinsic as Possible

- Security properties are a direct result of the design of the system
  - Do not rely on correctness of external configurations, actions, data bases
  - Malicious actions can be easily identified



8

Other XIA Principles

- Narrow waist for trust management
  - Ensure that the inputs to the intrinsically secure system match the trust assumptions and intensions of the user
  - Narrow waist allows leveraging diverse mechanisms for trust management: CAs, reputation, personal, …
- Narrow waist for all principals
  - Defines the API between the principals and the network protocol mechanisms
- All other network functions are explicit services
  - XIA provides a principal type for services (visible)
  - Keeps the architecture simple and easy to reason about

9

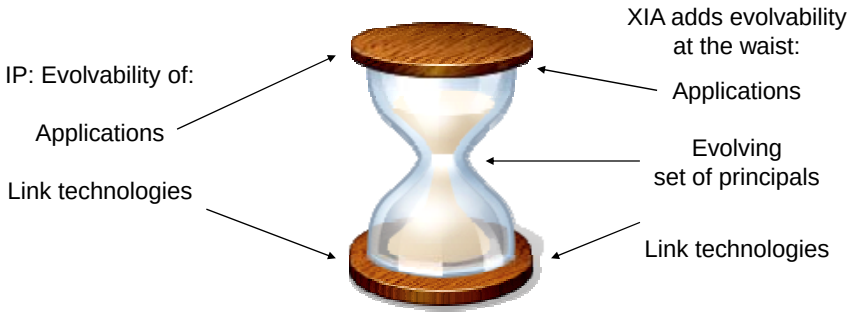
XIA: eXpressive Internet Architecture

- 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

10

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



11

Developing XIA v0.1

- Principles do not make a network!
- Meet the core XIA team:

Five happy professors cheering:
John Byers, Aditya Akella, Dave Anderson, Srini Seshan, Peter Steenkiste


Fahad Dogar


Dongsu Han


Hyeontaek Lim


Ashok Anand


Michel Machadoy


Boyan Li


Wenfei Wu

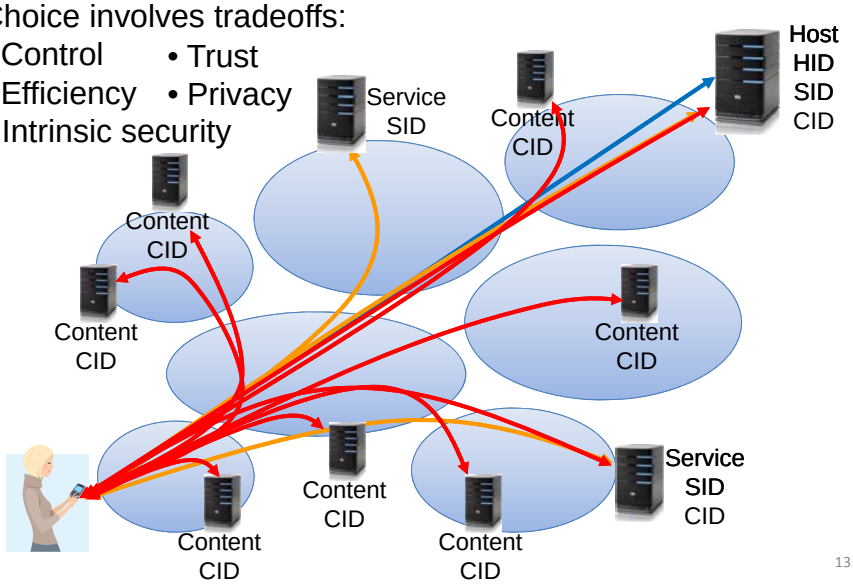
- Next: quick look at multiple principals, intrinsic security, and evolvability

12

Multiple Principal Types

Choice involves tradeoffs:

- Control
- Trust
- Efficiency
- Privacy
- Intrinsic security



13

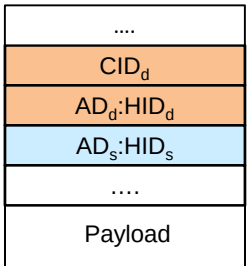
Intrinsic Security in XIA

- 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
  - Important – guarantees depend on 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

14

Evolvability

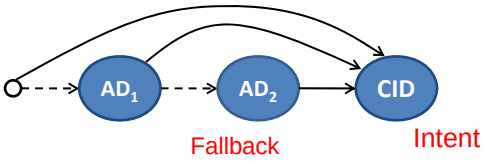
- Introduction of a new principal type will be incremental – no "flag day"!
  - Not all routers and ISPs will provide support from day one
  - No universal connectivity
  - Some ISPs may never support certain principal types
- Solution is to provide an *intent* and *fallback* address
  - Intent address allows in-network optimizations based on user intent
  - Fallback address is guaranteed to be reachable



15

Generalizing Evolvable Address Format

- Use a directed acyclic graph to represent address
  - Router traverses the DAG
  - Priority among edges

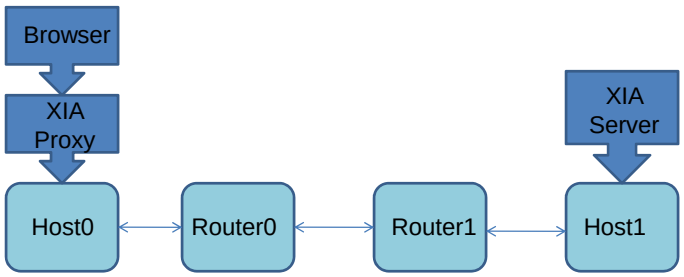


- DAG format supports many addressing styles
  - Shortcut routing, binding, source routing, infrastructure evolution, ..
- Packet processing combines basic and principal specific processing

16

Prototype Implementation

- Click implementation of XIA router
- Python API for sending/receiving packets
- Implemented a web service using XIA
- Ran simple tests over ProtoGeni



It Is Not Just About Architecture!

- End-to-end transport over heterogeneous networks and for mulitple principals
  - Error control, congestion control, …
  - How to better support wireless mobile users, insertion of services, vehicular, DTNs, …
- Trustworthy network operations
  - Improve “security” broadly defined by leveraging the intrinsic security properties of XIA
  - Focus on availability and systematic approaches to trust management

18

What About the Real World?

- Policy and economic viability
  - Impact of multiple principals on economic incentives
  - Net neutrality, audit trails for billing purposes, …
- Interfaces for applications and users
  - Value of network depends on whether users are willing to use all its capabilities - User trust is key
  - User studies to evaluate impact on user's attitude
- Rich interactions with core network, security

19

Conclusion

- XIA supports evolution, expressiveness, and trustworthy operation.
  - Multiple principal types and intrinsic security
- But research has just started!
  - Protocols that take advantage of in-network caches and services
  - Trustworthy protocols that fully utilizes intrinsic security of XIA
- More information on

  http://www.cs.cmu.edu/~xia