XIA: An Architecture for a Trustworthy and Evolvable 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

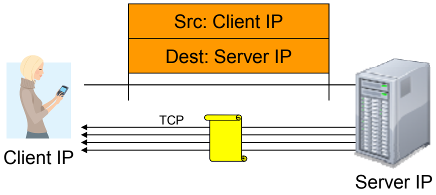
Network Seminar
Stanford University, April 21, 2011

Outline

- The eXpressive Internet Architecture – a proposal
  - Example and concepts
  - Research thrusts
- Tapa: supporting mobile users
  - Concepts
  - Applications
  - Tapa as an XIA transport

2

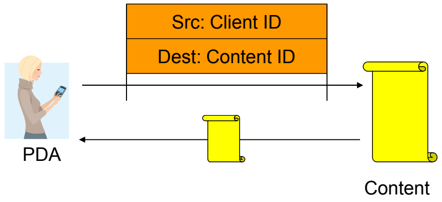
Today's Internet



- 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!

3

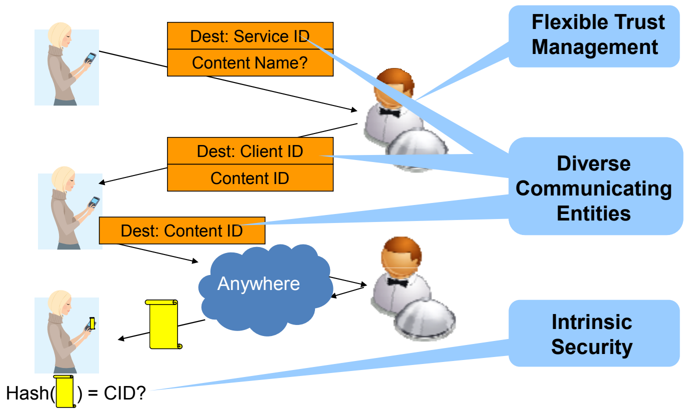
eXpressive Internet Architecture



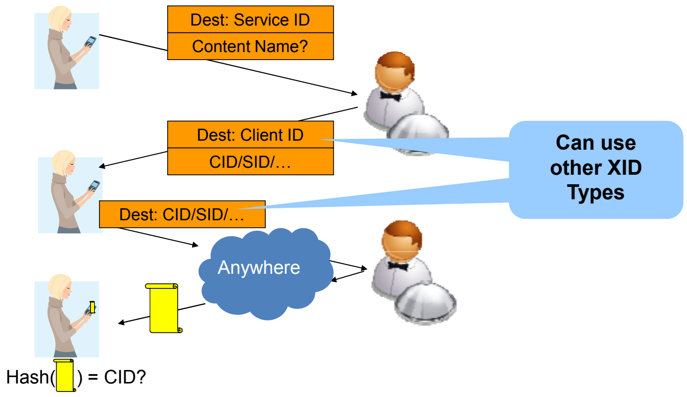
- Client expresses communication intent for content explicitly
  - Network uses content identifier to retrieve content from appropriate location
- How does client know the content is correct?
  - Intrinsic security! Verify content using self-certifying id:
    hash(content) = content id
- How does source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

4

A Bit More Detail …

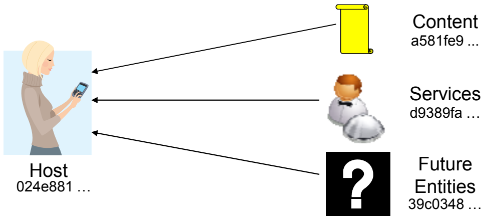


What About Dynamic Content?



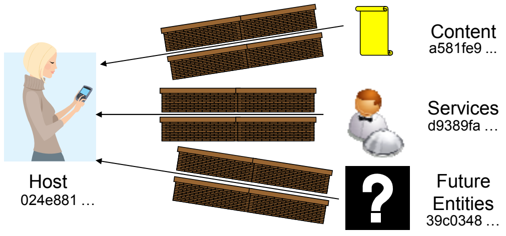
P1: Evolvable Set of Principals

- 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*



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



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

XIA: eXpressive Internet Architecture

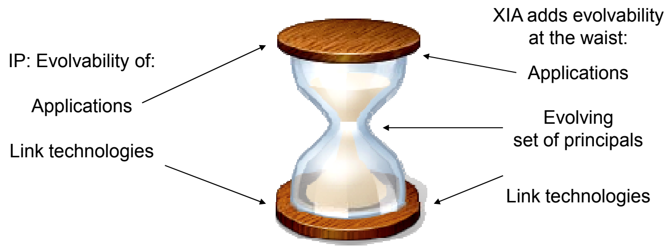
- Each communication operation expresses the intent of the operation
  - Also: explicit trust management, APIs among actors
- XIA is a single inter-network in which all principals are connected
  - Not a collection of architectures implemented through, e.g., virtualization or overlays
  - Not based on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

What Applications Does XIA Support?

- Since XIA supports host-based communication, today’s applications continue to work
  - Will benefit from the intrinsic security properties
- New applications can express the right principal
  - Can also specify other principals (host based) as fallbacks
  - Content-centric applications
  - Explicit reliance on network services
  - Mobile users
  - As yet unknown usage models

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



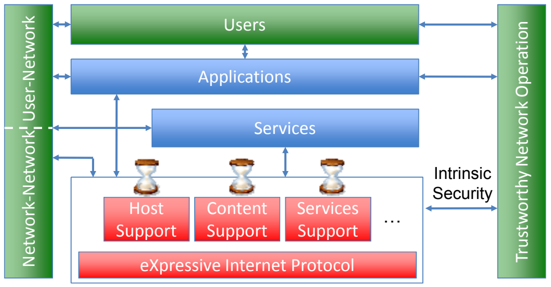
It Is Not Just About Architecture!

- End-to-end transport over heterogeneous networks
  - – TCP works well over wired segments
  - – 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 systematic approaches to trust management and availability

What About the Real World?

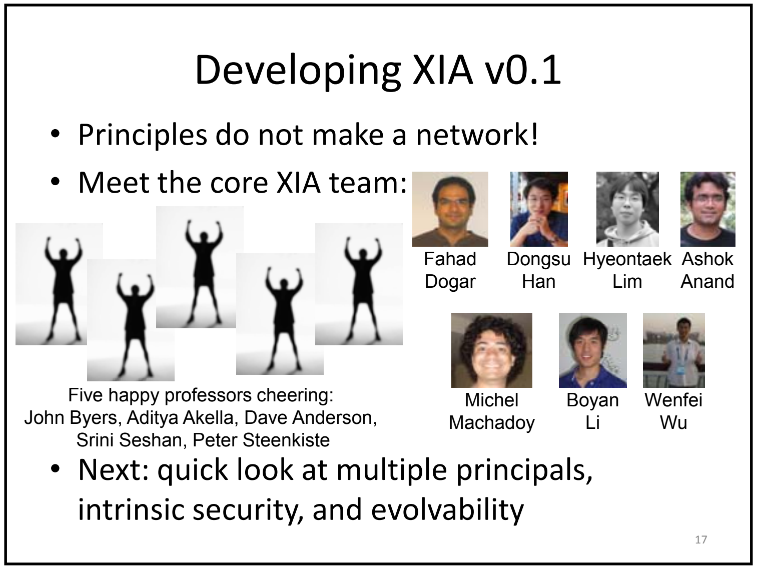
- Relationship among providers
  - – Impact of multiple principals, new routing paradigms, etc. on economic incentives
  - – Net neutrality, audit trails for billing purposes, …
- Interfaces for applications and users
  - – Why would users trust data that can come from "anywhere"; why would they make data available?
  - – Focus is on an audit trail capability both at the network and user level
  - – User studies to evaluate impact on user's attitude

XIA Components and Interactions


Network-Network | User-Network
Users
Applications
Services
Host Support
Content Support
Services Support
…
eXpressive Internet Protocol
Intrinsic Security
Trustworthy Network Operation

Outline

- Background
- The eXpressive Internet Architecture – a proposal
  - – Example and concepts
  - – Research thrusts
- XIA building blocks:
  - – AIP
  - – Tapa



Developing XIA v0.1

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

Fahad Dogar

Dongsu Han

Hyeontaek Lim

Ashok Anand

Michel Machadoy

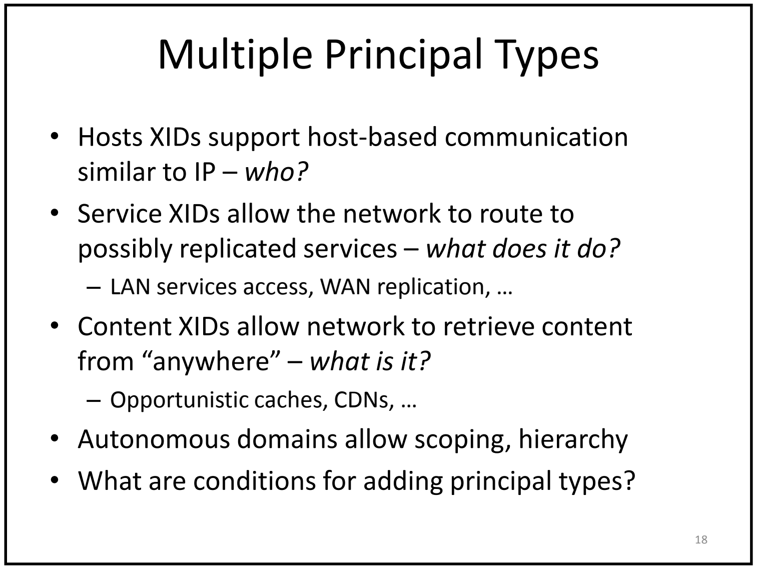
Boyan Li

Wenfei Wu

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

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

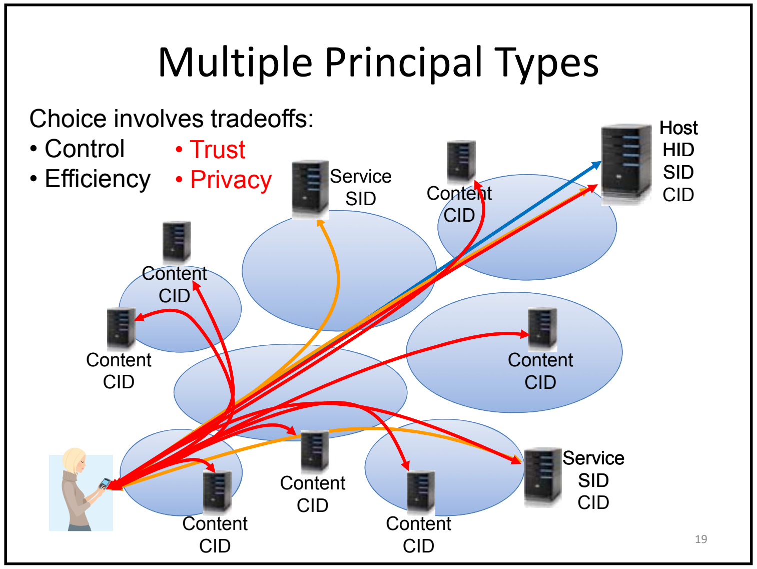
17



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
- What are conditions for adding principal types?

18



Multiple Principal Types

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

Service
SID

Content
CID

Host
HID
SID
CID

Content
CID

Content
CID

Content
CID

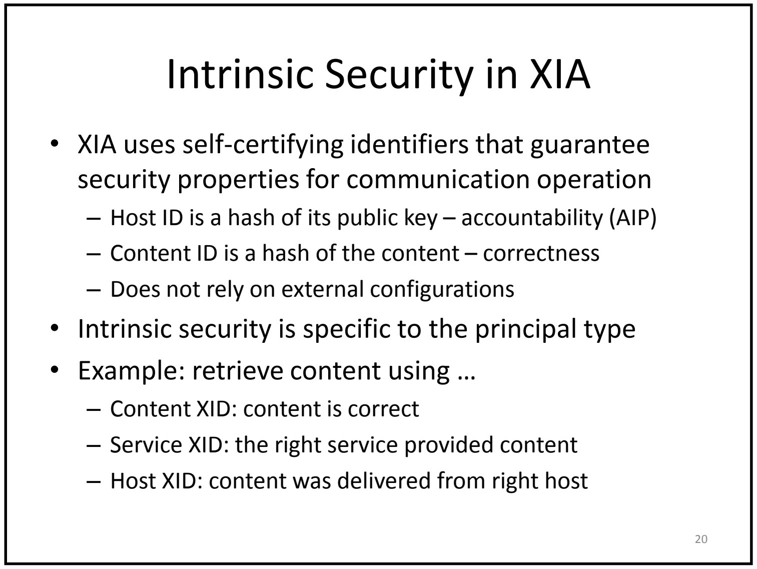
Content
CID

Content
CID

Content
CID

Service
SID
CID

19

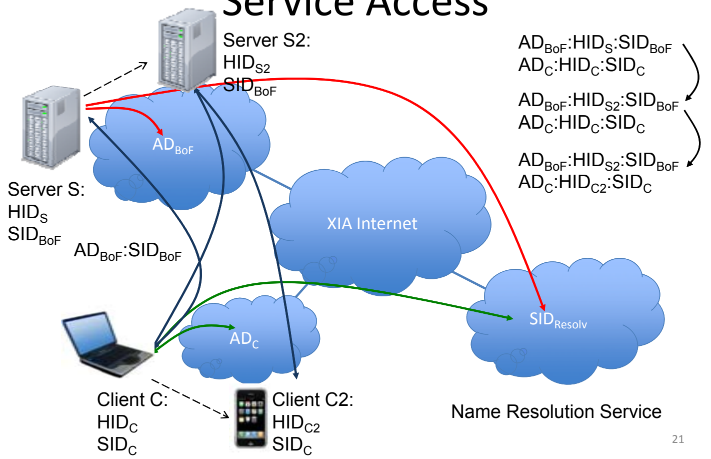


Intrinsic Security in XIA

- 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

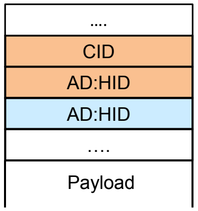
20

Example of Secure Mobile Service Access



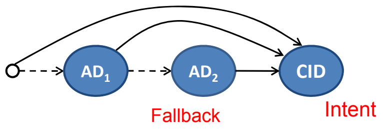
Evolvability

- 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



Generalizing Evolvable Address Format

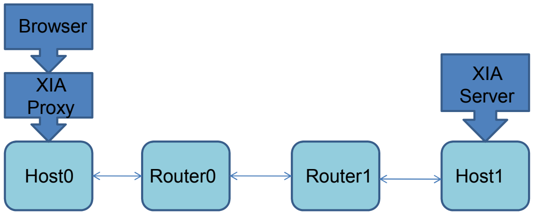
- Use a directed acyclic graph to represent address
  - Router traverses the DAG
  - Priority among edges



- DAG format supports many addressing styles
  - Shortcut routing, binding, source routing, infrastructure evolution, ..
  - Common case: small dag, most routers look at one XID

Prototype Implementation

- Click implementation of XIA router
- Python API for sending/receiving packets
- Implemented a web service using XIA
- User-level version runs over ProtoGeni


Browser
XIA Proxy
XIA Server
Host0
Router0
Router1
Host1