15-744: Computer Networking

L-19 Future Internet Architecture

Readings

- Required:
  - eXpressive Internet Architecture
  - 2 sections of Mobility First
  - 2 sections of Nebula
- Relevant earlier meeting:
  - CCN -> Named Data Network

Outline

- Motivation and discussion
- Some proposals:
  - CCN
  - Mobility First
  - Nebula
  - XIA

The "Next" Internet: More of the Same?

Performance — **Diverse Service, QoS** — **"-ilities"**

Internet 2	Next Generation Internet	Integrated Services Networks	Future Internet Architecture

Internet Architecture Fixed

Change Me!

Four “FIA” Projects

- Mobility First
  - Mobility as the norm rather than the exception – generalizes delay tolerant networking
- Named Internet Architecture
  - Content centric networking - data is a first class entity
- Nebula
  - Internet centered around cloud computing data centers that are well connected
- eXpressive Internet Architecture
  - Focus on trustworthiness, evolvability

5

Key Internet Features

But maybe there are better ways …

What we learned about the current Internet:

- Simple core with smart endpoints
- The IP narrow waist supports evolution
- Addresses have topological meaning
- 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

6

Outline

- Motivation and discussion
- Some proposals:
  - CCN
  - Mobility First: slides …
  - Nebula: slides …
  - XIA

7

CCN Discussion

- Simple core with smart endpoints
- The IP narrow waist supports evolution
- Addresses have topological meaning
- 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

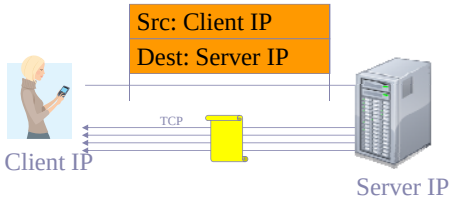
8

Outline

- Motivation and discussion
- Some proposals:
  - CCN
  - Mobility First: slides Jun Han
  - Nebula: slides Guangyu
  - XIA
    - Overview
    - Multiple principal types
    - Addressing
    - Intrinsic security and AIP

9

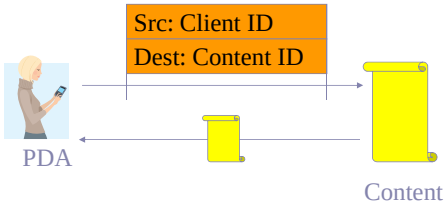
Today's Internet



- 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!

10

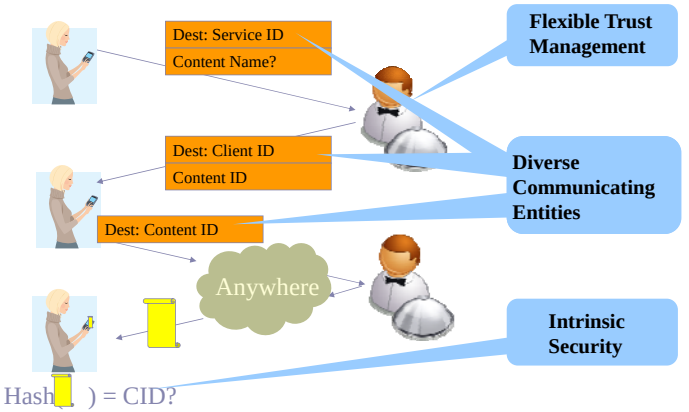
eXpressive Internet Architecture



- 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

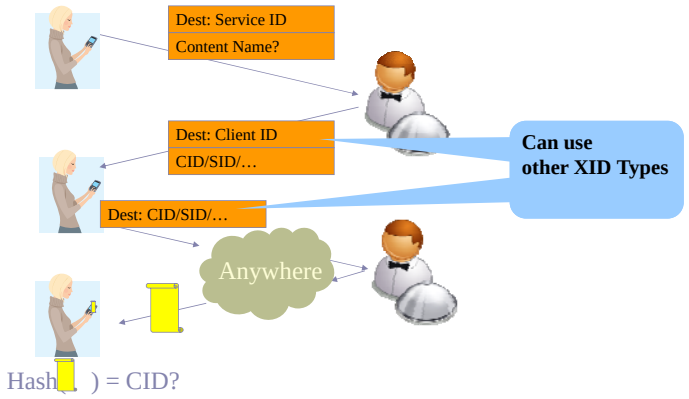
11

A Bit More Detail …



12

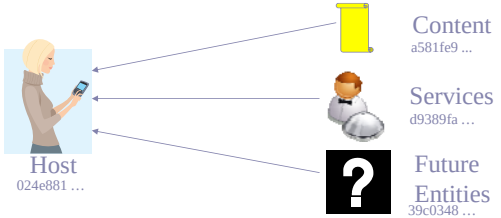
What About Dynamic Content?



13

P1: Evolvable Set of Principals

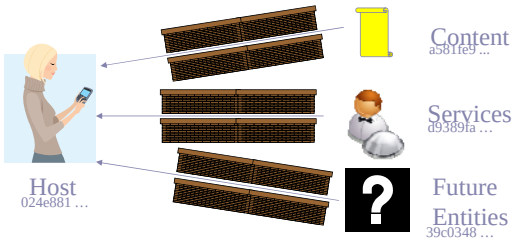
- Identifying the intended communicating entities reduces complexity and overhead
  - No need to force all communication at a lower level (hosts), as in today's Internet
- Allows the network to *evolve*



14

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



15

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, easy to reason about

16

XIA: eXpressive Internet Architecture

- Each communication operation expresses the intent of the operation
  - Also: explicit trust management, APIs, …
- 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

17

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, using network services, mobile users, as yet unknown usage models
- Performance of applications will improve as support in the network increases

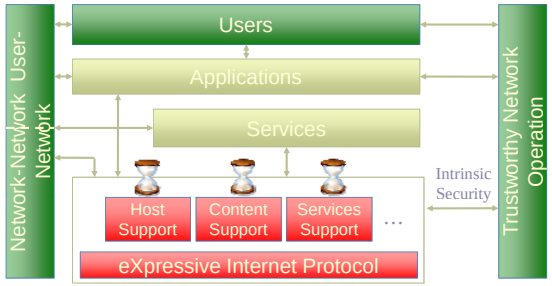
18

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

19

XIA Components and Interactions



20

Multiple Principal Types

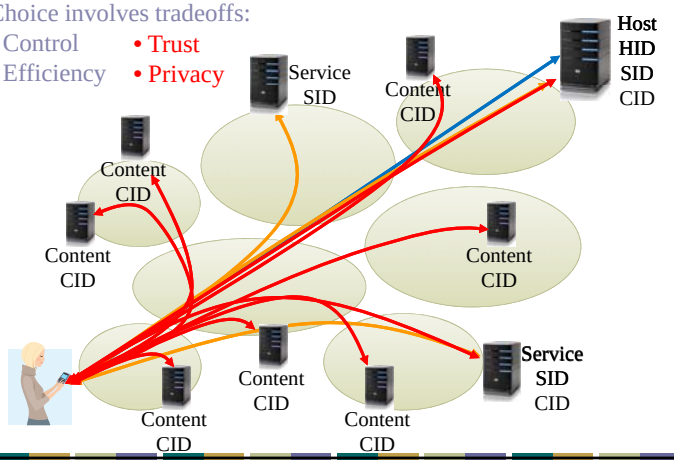
- Hosts XIDs support host-based communication similar to IP – *who?*
- Service XIDs allow the network to route to possibly replicated services – *what does it do?*
  - LAN services access, WAN replication, …
- Content XIDs allow network to retrieve content from "anywhere" – *what is it?*
  - Opportunistic caches, CDNs, …
- Autonomous domains allow scoping, hierarchy
- What are conditions for adding principal types?

21

Multiple Principal Types

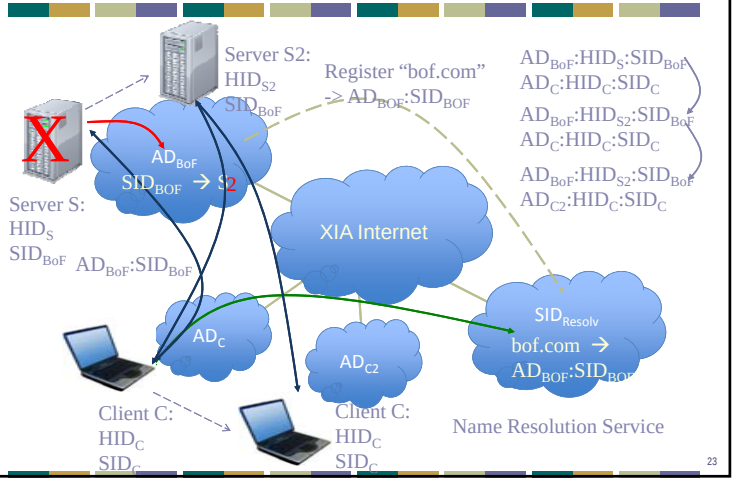
Choice involves tradeoffs:

- Control
- Efficiency
- Trust
- Privacy



22

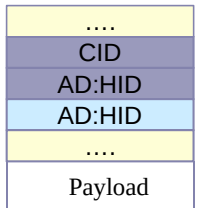
Example: Secure Mobile Service Access



23

Evolvability

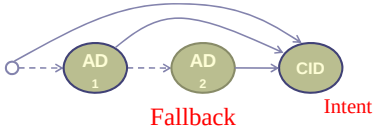
- Introduction of a new principal type will be incremental – no "flag day"!
  - Not all routers/ISPs will offer support from day one
  - No universal connectivity
  - Some ISPs may never support certain principal types
- Solution is to provide an *intent* and *fallback* address
  - Intent address allows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



24

General Evolvable Address Format

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

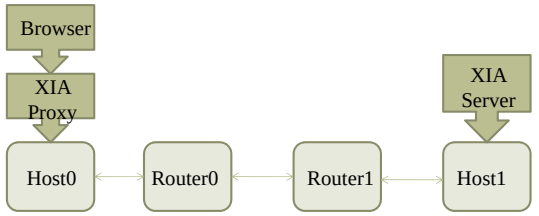


- DAG format supports many addressing styles
  - Shortcut routing, binding, source routing, infrastructure evolution, ..
  - Common case: small dag, most routers look at one XID

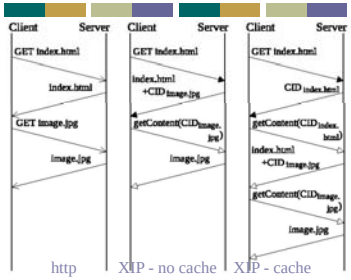
25

Prototype Implementation

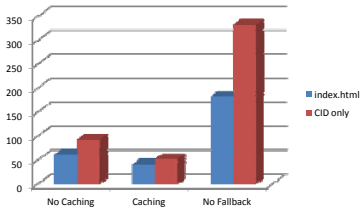
- Click implementation of XIA router
- Python API for sending/receiving packets
- Implemented a web service using XIA
- User-level version runs over ProtoGeni



Simple Web Example



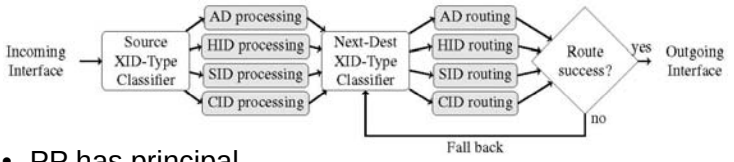
- Web page with one embedded image
- Three-hop path hops
  - 5ms/hop; gigabit links



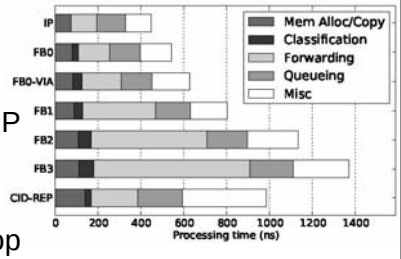
- Caching clearly helps
- Sending initial page helps (fast network)
- Fallback avoids timeouts

27

Packet Processing



- PP has principal dependent and independent element
- Processing costs seem manageable relative to IP
  - Fallbacks, source processing add time
  - In software on desktop



28

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

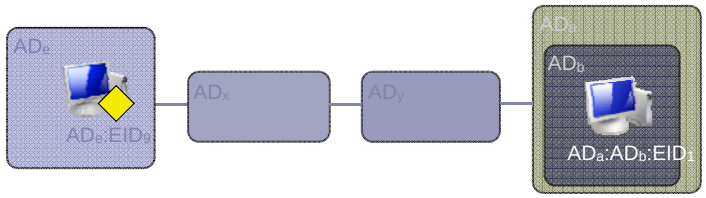
29

AIP Motivation

- Many security challenges are a result of not being able to unambiguously determine who is responsible for a specific action
  - Source spoofing, denial-of-service 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

30

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

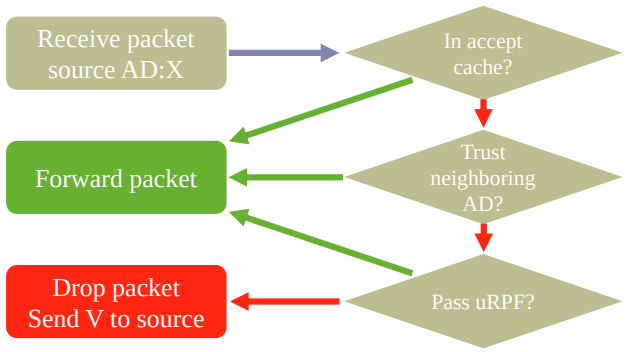
31

Self-Certifying Identifiers

- Identifier of object is public key of object
  - Convenient to use hash of key (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

32

Example: AD verification



33

Verification Packet

- Router sends a packet 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 send 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

34

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

35

Looking Ahead

- Next lecture: QoS and ideo distribution
- Friday: Data Center networks
  - Lecture starts at 3:30

36