XIA: eXpressive Internet Architecture - A Proposal for a Future Internet Architecture

15-441: Computer Networking

Lecture 25: What is Next?

Peter Steenkiste

Fall 2010

www.cs.cmu.edu/~prs/15-441-F10

Outline

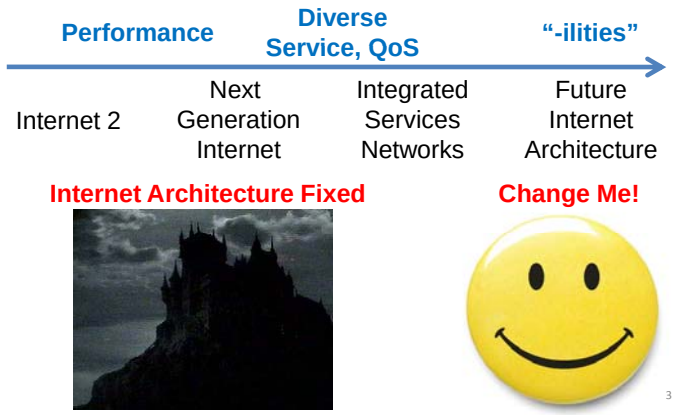
- Background
- The eXpressive Internet Architecture – a proposal
  - Example and concepts
  - Research thrusts
- XIA building blocks:
  - AIP
  - Tapa

NOTE: this lecture describes a research project

This material will not be on the final exam

2

The "Next" Internet – More of the Same?



3

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

4

Key Internet Features

What we learned about the current Internet:

- Simple core with smart endpoints
- The IP narrow waist supports evolution
- 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

But maybe there are better ways …

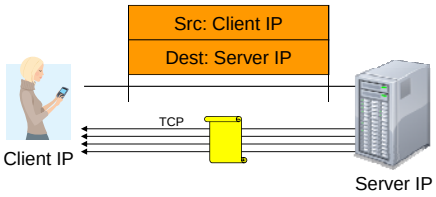
5

Outline

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

6

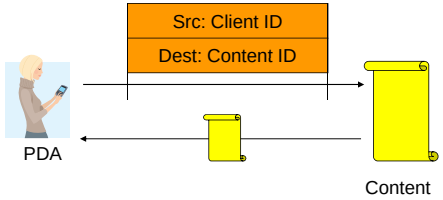
Today's Internet



- 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!

7

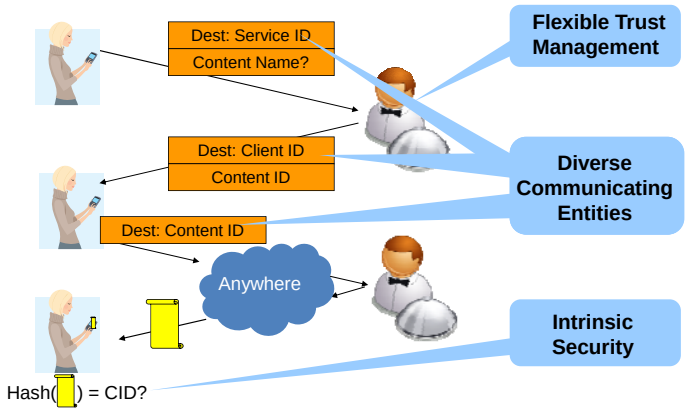
eXpressive Internet Architecture



- 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

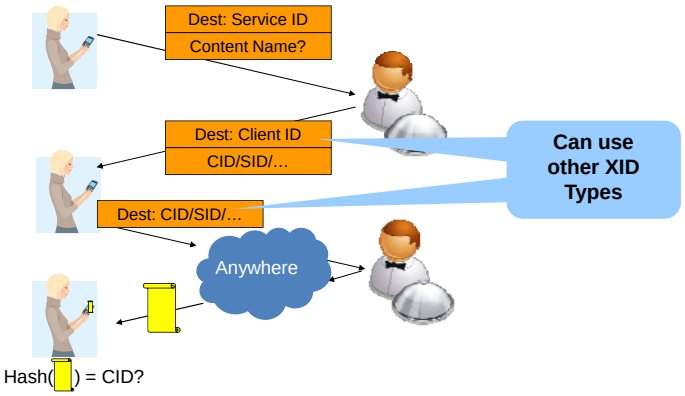
8

A Bit More Detail …



9

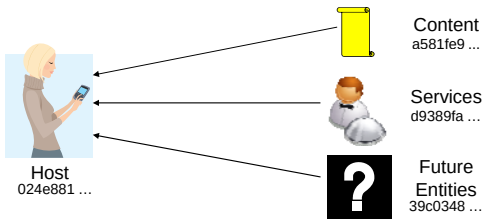
What About Dynamic Content?



10

P1: Evolvable Set of Principals

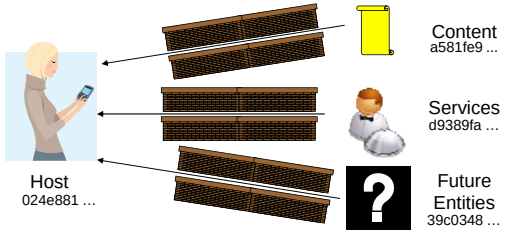
- Identifying the intended communicating entities reduces complexity and overhead
  - No need to force all communication at a lower level (hosts), as in today's Internet
- Allows the network to *evolve*



11

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



12

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

13

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

14

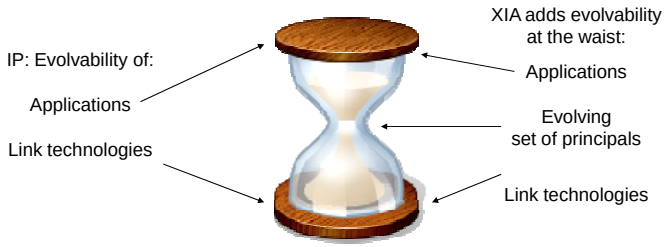
What Applications Does XIA Support?

- 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

15

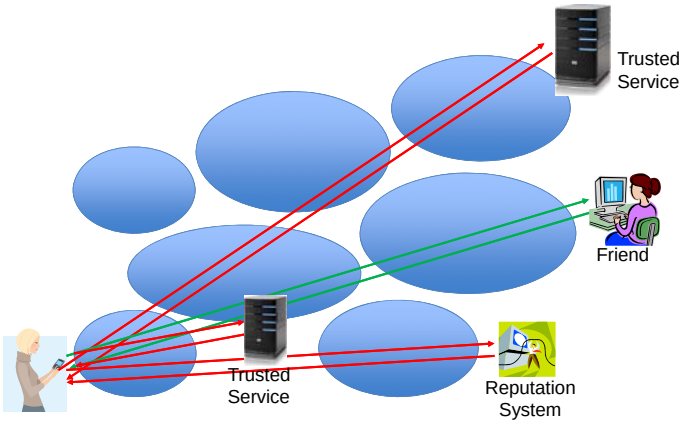
What Do We Mean by Evolvability?

- 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



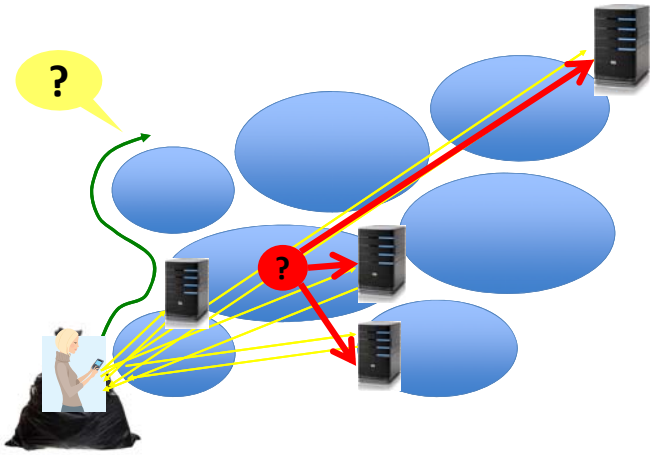
16

Revisit Our Example



17

Revisit Our Example



18

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

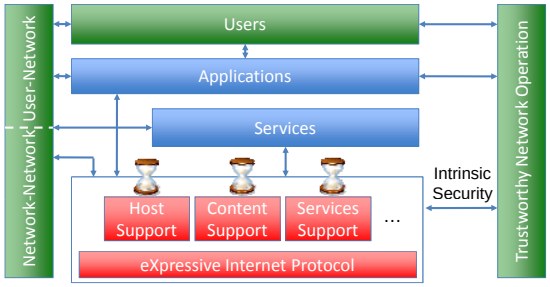
19

What About the Real World?

- Relationship among providers
  - Impact of multiple principals 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

20

XIA Components and Interactions



21

Outline

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

22

A Couple of XIA Building Blocks

- The Accountable Internet Protocol
  - Accountable Internet Protocol (AIP). David Andersen, et al, ACM *SIGCOMM* 2008
  - Example of intrinsic security for host-based communication
- The Transport Access Point Architecture
  - Segment based Internetworking to Accommodate Diversity at the Edge, Fahad Dogar, Peter Steenkiste, CMU CSD technical report, CMU-CS-10-104, February 2010
  - Transport services for mobile and wireless users
  - Not part of the architecture, but can leverage many of its features

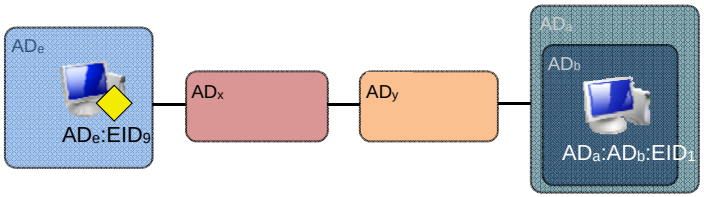
23

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

24

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

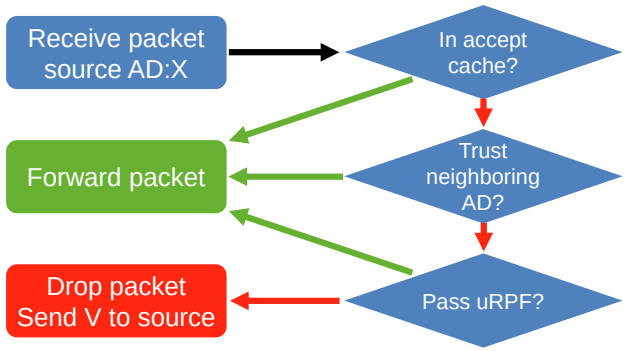
25

Self-Certifying Identifiers

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

26

Example: AD verification



27

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

28

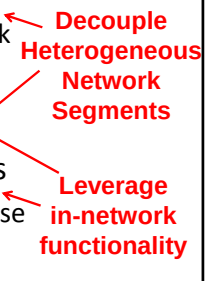
AIP Discussion

- 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

29

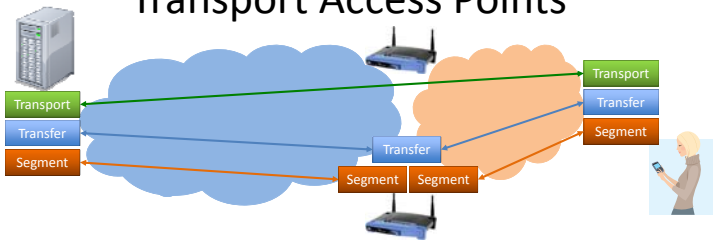
Wireless and Mobile Challenges

- Network and device heterogeneity
  - "Wired" protocols stack may not work
- Diverse network services
  - Content retrieval, mobility services
- Relaxed synchronization end-points
  - Intermittent connectivity common case
- Topology control
  - Handoff, multi-path



30

Transport Access Points



- Tapa supports visible middleboxes (TAPs) that break up e-e connections in segments
- Each segment uses custom solutions for congestion, error, and flow control
- Transfer, transport layers glue segments into e-e path
  - Operate on self-certifying chunks of data (ADUs)

31

Unbundling the Transport Layer

- Tapa unbundles the "thick" Internet transport layer
  - Motivated by the "dumb middle" idea
- Segments support best effort delivery of "chunks"
  - Must support congestion, flow, and some error control in way that is appropriate for that segment
  - Chunks are a few KB and self-certifying
- Transfer layer supports best effort end-to-end delivery of chunks by stitching segments together
  - Naturally supports insertion of network services
- Thin end-to-end transport supports e-e semantics
  - Also flow, error, congestion control across segment path

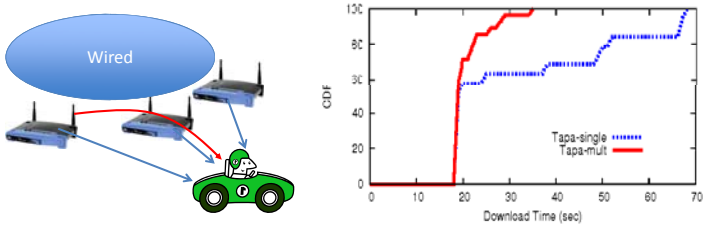
32

Tapa Prototype

- Leverages Data-Oriented Transport (DOT)
  - Uses self-certifying chunks of data
  - Supports application-independent caching
- Uses diverse protocols for wireless segment
  - TCP is convenient solution for wired backbone
- Intelligent end-end transport intelligence is implemented on mobile host and TAP
  - Vehicular communication
  - Catnap battery savings

33

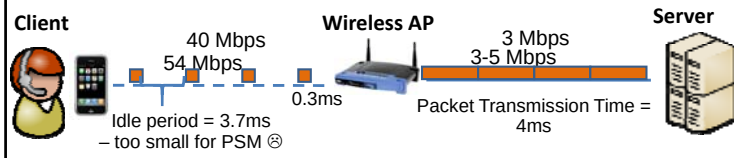
Vehicular Example



- Vehicle-infrastructure suffers from frequent interruptions, short periods of connectivity
- Vehicle optimizes transfers by explicitly managing server-TAP and TAP-vehicle transfers
  - Leverages self-certifying content identifiers

34

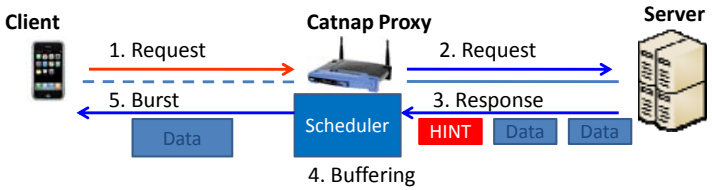
BW Discrepancy in typical end-to-end transfers



Catnap leverages this opportunity to provide up to 2-5x energy savings during data transfers

35

Catnap Design Overview



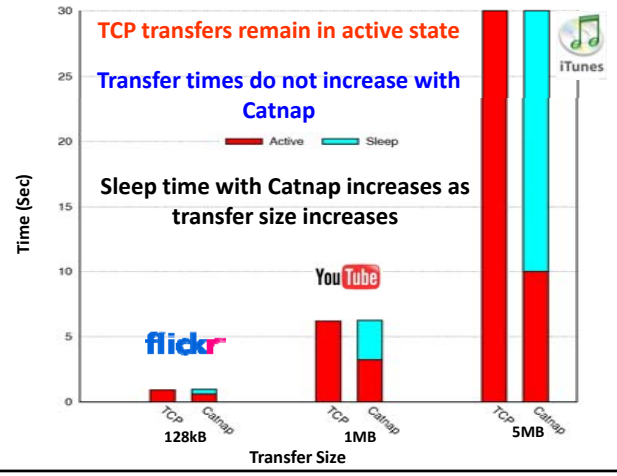
1. Decoupling of Wired and Wireless Segments

2. ADU Hint -- Length of ADU

3. Scheduler – Decides when to send data to client

36

How much can the NIC sleep?



37

Tapa and XIA

- Content-centric optimizations in Tapa can be pushed "into the network"
  - Tapa can use content XIDs rather than host XIDs
  - Old APs can be listed as hints (rather than server)
- Tapa needs support from services on/near APs
  - Simple "decoupling services", content optimization, Catnap, higher level services
- Tapa will benefit from intrinsic security properties

38

Summary

- XIA changes Internet architecture by supporting communication between multiple principals, while offering intrinsic security properties
  - Improve support for new usage models, evolvability, and trustworthiness
- Project is also studying how the XIA features help improve key components of the Internet
  - Both in the network, and interactions with/between actors
- XIA is based on a number of existing building blocks
  - AIP, Tapa, DOT, trust management, …

39

XIA Project

- More information:
  - http://www.cs.cmu.edu/~xia
- XIA faculty
  - Peter Steenkiste, CS/ECE, Carnegie Mellon
  - Dave Andersen, Dave Feinberg, Srini Seshan, Hui Zhang, CS, Carnegie Mellon
  - Sara Kiesler, HCII, Carnegie Mellon
  - Jon Peha, Marvin Sirbu, EPP, Carnegie Mellon
  - Adrian Perrig, ECC, Carnegie Mellon
  - CS, Carnegie Mellon
  - Aditya Akella, CS, University of Wisconsin
  - John Byers, CS, Boston University

Carnegie Mellon BOSTON UNIVERSITY THE UNIVERSITY of WISCONSIN MADISON