eXpressive Internet Architecture
Security Architecture

Dave Andersen, Adrian Perrig, Peter Steenkiste
David Eckhardt, Sara Kiesler, Jon Peha, Srini Seshan,
Marvin Sirbu, Hui Zhang
Carnegie Mellon University
Aditya Akella, University of Wisconsin
John Byers, Boston University

FIA PI meeting
Oakland, May 25-26, 2011

Carnegie Mellon BOSTON UNIVERSITY THE UNIVERSITY OF WISCONSIN MADISON

Outline

- Brief XIA overview
- Security architecture
  - Requirements
  - XIA principles and concepts
  - Supporting basic security properties
- Security research overview

XIA Vision

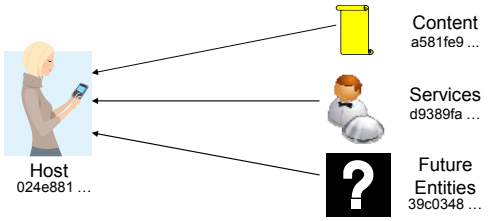
We envision a future Internet that:

- 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

Security central to all four aspects!

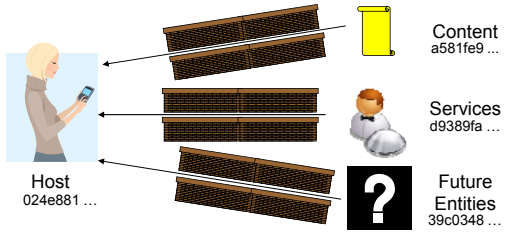
P1: Evolvable Set of Principals

- Specifying intent allows future network support to optimize performance, efficiency
  - 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



5

Other XIA Principles

- Narrow waist for trust management
  - Intrinsically secure identifiers must match the user's trust assumptions and intensions
  - Narrow waist allows leveraging diverse mechanisms for trust management: CAs, reputation, personal, …
- Narrow waist for all principals
  - Defines the API between principals and 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

6

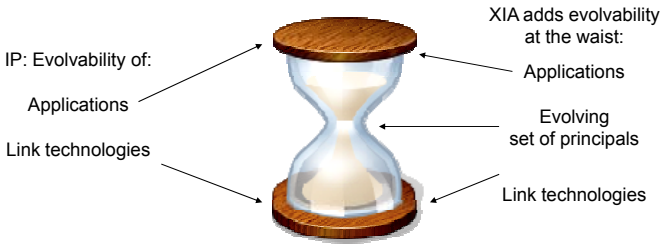
XIA: eXpressive Internet Architecture

- Each communication operation expresses intent of operations
  - 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

7

What Do We Mean by Evolvability?

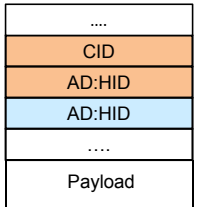
- Narrow waist of the Internet has allowed the network to evolve significantly
- But need to evolve the waist as well!
  - Can make the waist smarter



8

Evolvability

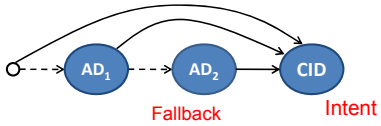
- Introduction of a new principal type must be incremental – no "flag day"!
  - Not all routers and ISPs will provide support from day one
  - No universal connectivity
  - Some ISPs may never support certain principal types
- Solution is to provide an *intent* and *fallback* address
  - Intent address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



9

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

10

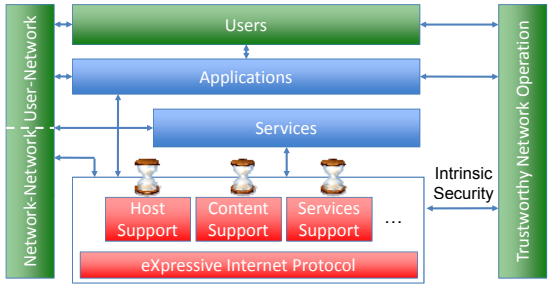
XIA Security in the Real World?

- 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
  - User's trust in "the network" affects what tasks they are willing to use it for:

    What makes people trust information they obtain?
    Why would they make data available?
    What about privacy?

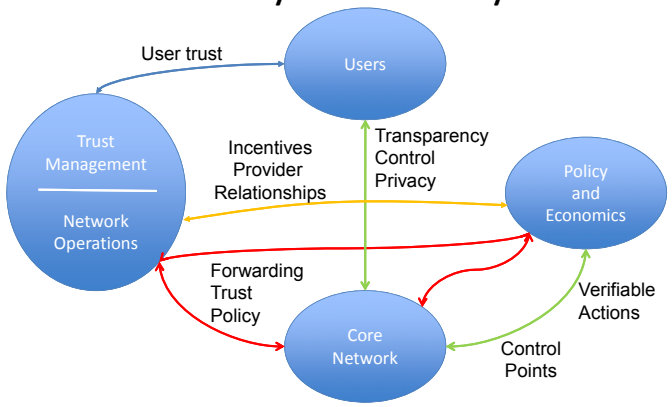
11

XIA Components and Interactions



12

Cross-Cutting Themes are Heavy on Security



13

Outline

- Brief XIA overview
- Security architecture
  - Requirements
  - XIA principles and concepts
  - Supporting basic security properties
- Security research overview

14

XIA Security

- A key feature of XIA is flexibility, thus, the architecture can be extended in ways we cannot anticipate
- XIA security depends on
  - Underlying architecture
  - XIA extension principals and mechanisms
  - Specific extensions future designers choose
- Consequently, detailed security analysis depends on specific principal types

15

XIA High-Level Security Goals

- Support today's Internet-style host-to-host communication with drastically improved security
- Provide improved security for two classes of communication we anticipate being important: content retrieval & accessing services
- Provide groundwork for future extensions to make good decisions w.r.t. security and availability

16

Main Security Properties

- Availability
  - Communication availability (hosts and services)
  - Finding nearby contents and services
  - Defenses against DoS attacks
- Authenticity / integrity
  - Authentication of user, host, domain, service, content
- Authentication and Accountability
  - Both authorization and deterrence, respectively
- Secrecy of identity, anonymity, privacy
  - Sender / receiver privacy if desired
- Trust management
  - How to set up trust relations, roots of trust

XIA Security Design Principles

- Well-foundedness: Identifiers, associations match user's intent
- Fault isolation: Good design reduces dependencies, insulates correct portions of network operation from incorrect/malicious
- Fine-grain control: Allow users to specify their intent
- Explicit chain of trust: Allow users to understand the basis for trust, underlying assumptions

18

Security-relevant XIA Mechanisms

- Multiple principal types
- Intrinsically secure identifiers
- Flexible trust management

19

Security-Relevant XIA Mechanisms

Multiple Principal Types

- Hosts XIDs support host-based communication (like IP)
  - W*ho is talking?*
- Service XIDs route to (possibly replicated) services
  - *Identify what the service does and who provides it*
- Content XIDs specify specific chunks of content
  - Identify what the content is
- Autonomous domains allow scoping, hierarchy

Intrinsically Secure Identifiers

Flexible Trust Management

20

Security-Relevant XIA Mechanisms

Multiple principal types

Intrinsically secure identifiers

- Self-certifying or self-verifiable identifiers
- Guarantee security properties *once you know the ID*
  - e.g., Host XID is hash(public key)
    - Knowing host ID, can validate public key, and bootstrap signatures & encryption
  - Content ID is a hash of the content – correctness
- Does not rely on external configuration
- Key question: Bridging from "human ID" to intrinsic ID ..

Flexible trust management

21

Security-Relevant XIA Mechanisms

Multiple principal types

Intrinsically secure identifiers

Flexible trust management

- Name resolution: Name -> secure XID
- Trust bootstrapping between communicating entities
- Should support many sources of trust: CAs, DNSSEC-like mechanisms, PGP model, "perspectives"-like trust models, physical interaction, etc.
  - Goal: Create a "Narrow waist" - minimal / flexible API for trust management
  - Needs to involve users; how to communicate relevant information and decisions?

22

Integrity	Availability	Secrecy	Accountability

Design Principles

- Allow verification of integrity at *the highest semantic level possible*
- Make integrity *intrinsic* so that it's easy for any component in the system to verify

Integrity	Availability	Secrecy	Accountability

XIA Mechanisms

- Multiple principal types
  - Allow users to express highest-level intent
- Intrinsically secure principals
  - Verify that your intent was actually met
- Flexible trust management
  - Allow many ways to bootstrap trust from human-level ID to intrinsically secure ID

Integrity	Availability	Secrecy	Accountability

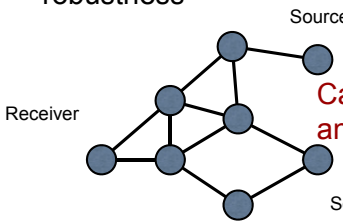
Per-principal integrity

- IP expresses: Packet P from host A to B
- IPSec can sign contents of packet
- XIA expresses:
  - Content! ID = hash(content)
    Integrity: Verify hash
  - Services & hosts! ID = hash(service public key)
    Integrity: Verify signature
  - Future types! ID = <your idea here>

Integrity	Availability	Secrecy	Accountability

Design Principle

Choice of path, source + replication provide robustness



Can survive failure/DoS of any one link or server

(More on resource isolation later in talk)

Integrity	Availability	Secrecy	Accountability

XIA Mechanisms

- Multiple principal types
  - Any source that has the capability to satisfy your intent *can* do so.
- Intrinsically secure principals
  - Satisfy intent even from untrusted sources
- Flexible trust management
  - Fallback mechanisms for trust establishment, e.g., out-of-band via cellphone, etc.

Integrity	Availability	Secrecy	Accountability

Content Example

- Express intent: Content ID *CID*
- Retrieve from any cache, Akamai replica, origin server, or your neighbor
  - Your intent is content, not a particular source...
- Use of replication require integrity: Detect fake source by checking the hash
  - Need mechanism to then avoid that source for the next request is valid

Integrity	**Availability**	Secrecy	Accountability

Next few years question: Service Replication

- Hash(service public key)
  - Any replica that knows private key can provide service
- Easy step: Accessing already-replicated services
  - Future: Combine with trusted computing to create a TrustedCDN for wide-area, mutually isolated service replication?

Integrity	Availability	**Secrecy**	Accountability

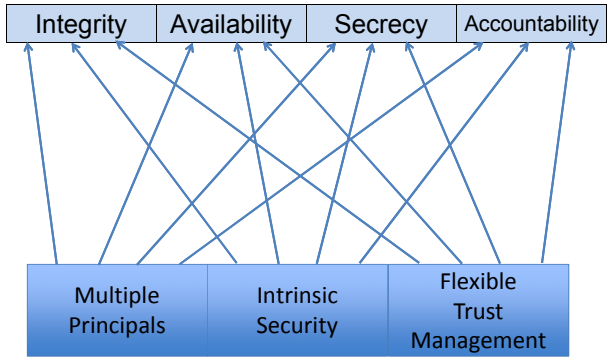
XIA Mechanisms

- Multiple principal types
  - Expresses user's intent
  - Expressiveness versus revealing intent
- Intrinsically secure principals
  - If you know the sender/receiver ID, you know a key to use for encryption
- Flexible trust management
  - Provide many ways to reliably *obtain* that ID

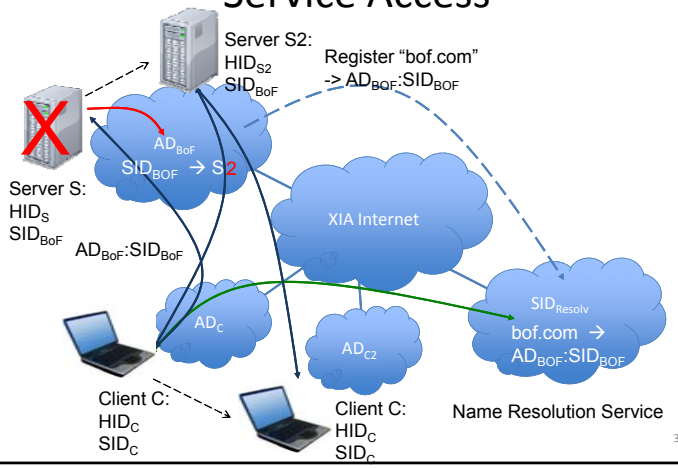
Integrity	Availability	Secrecy	**Accountability**

XIA Mechanisms

- Multiple principal types
  - Higher semantic level may provide stronger level of accounting
- Intrinsically secure principals
  - Authentication per principal type
  - Provides a basis for irrefutable, verifiable statements, e.g., audit trails
- Flexible trust management
  - Scope which IDs we trust and how



Example of Secure Mobile Service Access



33

Outline

- Brief XIA overview
- Security architecture
  - Requirements
  - XIA principles and concepts
  - Supporting basic security properties
- Security research overview

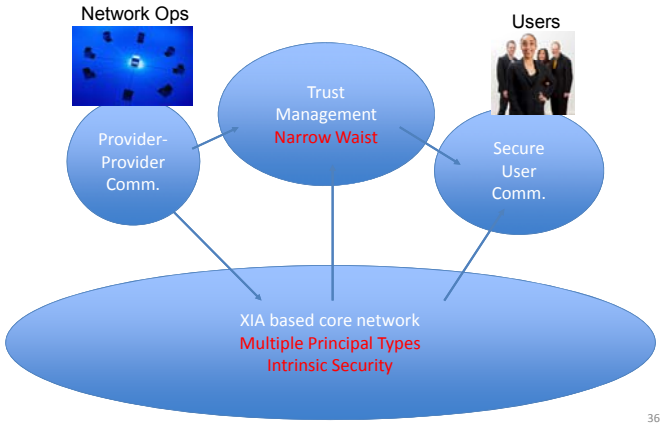
34

Security Focus for XIA

- Important network security aspects
  - Core network security properties
  - Trust management
  - Trustworthy network operations, provider-provider relations, public policy
  - User trust in the network
- Deemphasized areas: host security, DRM
  - Hope to learn from teams working on these topics

35

XIA Security-related Research



36

Initial Results
XIA Security in the Real World

- Trust management
- User trust in the network
- Enable content delivery
- SCION: network level resource isolation and path selection

37

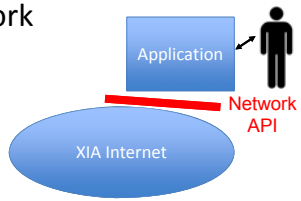
Flexible Trust Management

- How can users establish trust in Internet entities and resources?
  - Service, data, content provider
  - Individuals (email address, Twitter data, etc.)
- Flexible approaches
  - Leverage existing PKI mechanism
  - Perspectives: age-based trust
  - Usage-based trust: social network-based trust
  - Local trust establishment between users

38

Who is the User?

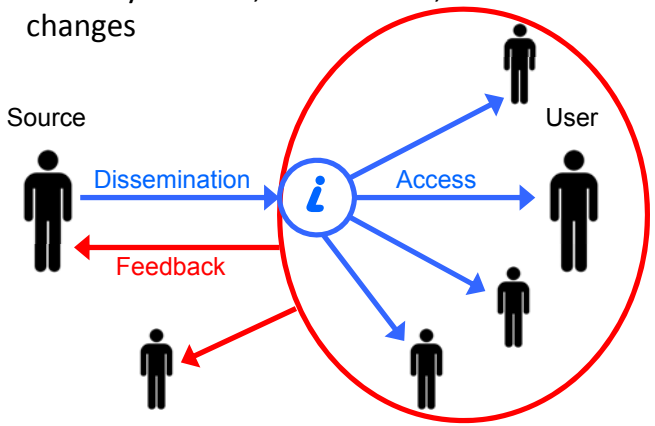
- Traditional focus of network API is to support robust application development
- Users do not directly interact with network
  - Separate user view from application API
- A broader perspective on what people know about Internet behavior at different levels
  - Network, other users, third parties, etc.



39

How Users See Information Dissemination

- Visibility of users, transactions, and content changes



Trust Management Example

- Users are interested in common identities across sites, services, organization, etc.
  - However, anonymity important in some contexts
- Can improve trust in content
  - E.g., Wikipedia article authored by a NYT journalist
- Also of interest to service providers
  - Can simplify tracking interests, managing joint promotions, etc.
  - But may be perceived differently by users

41

Supporting Content Delivery

- Today's CDNs are based on contracts between CDN and a relatively small number of customers
  - Contract is basis for trust
- CIDs open the door for widespread use of caches, but …
- what are the economic incentives for deploying caches in different types of networks?
  - Reducing cost
  - Potentially new revenue streams: publisher payments
- What security protocols are needed to support economically viable deployment?
  - Tracking cache hits in verifiable way
  - How to scale contract establishment to XIA distribution model

42

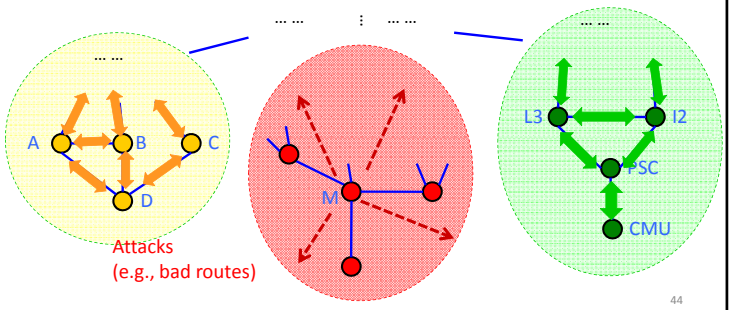
SCION Architectural Goals

- Scalability, Control, and Isolation on Next-generation networks (SCION)
- High availability, even for networks with 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

43

Wish List (1): Isolation

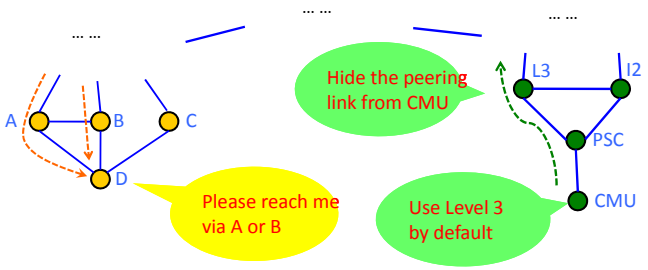
- Localization of attacks
- Scalable and reliable routing updates
- Operate with mutually distrusting entities without a global single root of trust



44

Wish List (2): Balanced Control

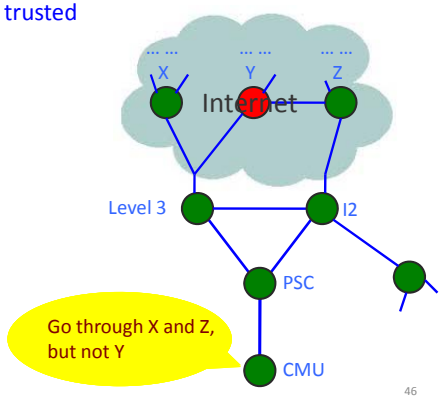
- Source: select paths to send packets
- Destination: select paths to receive packets
- Transit ISPs: select paths to support
- Support rich policies and DDoS defenses



45

Wish List (3): Explicit Trust

- Know who needs to be trusted
- Select whom to trust
- Confidence in selected paths
- Enforceable accountability



46

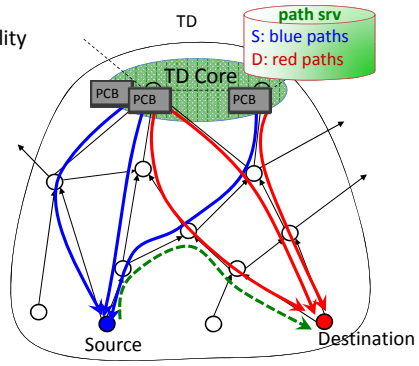
SCION Architectural Goals

- High availability, even for networks with 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

47

SCION Architecture Overview

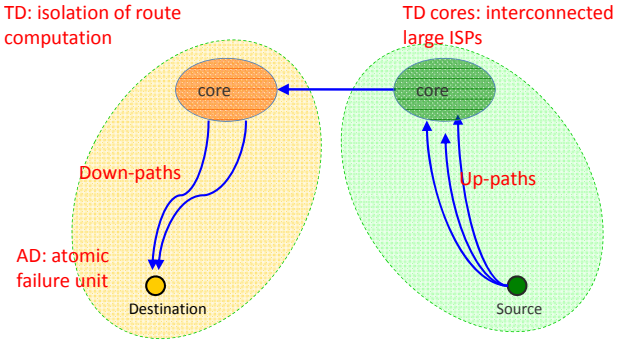
- Trust domain (TD)s
  - Isolation and scalability
- Path construction
  - Path construction beacons (PCBs)
- Path resolution
  - Control
  - Explicit trust
- Route joining (shortcuts)
  - Efficiency, flexibility



48

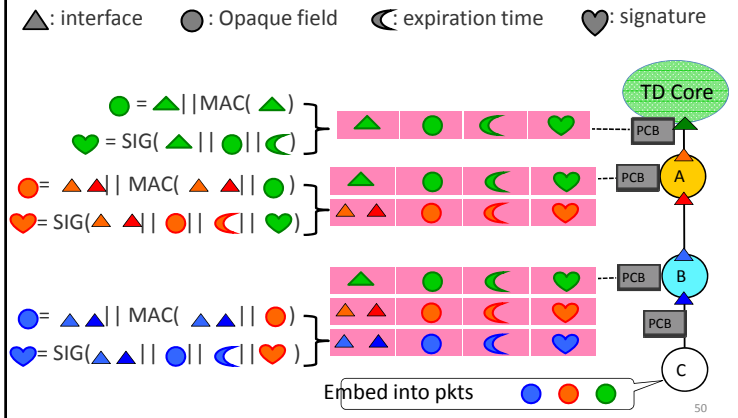
Hierarchical Decomposition

❖ Split the network into a set of trust domains (TD)



49

Path Construction



50

SCION Security Benefits

		S-BGP etc	SCION
Isolation	Scalability, freshness		
	Path replay attack	☹	☺
	Collusion attack		
	Single root of trust		
Trusted Computing Base		Whole Internet	TD Core and on-path ADs
Path Control	Source	End-to-end control	Only up-path
	Destination	No control	Inbound paths
	DDoS	Open attacks	Enable defenses

51

Ongoing and Future Work

- Study security interactions among principal types
- Availability for content and service types
- Accountability for content origin
- Mechanisms for trust management
- Support transparency for users
- Privacy / anonymity: in-network, overlay, …

52

Conclusions

- Core XIA security mechanisms …
  - Intrinsically secure identifiers
  - Multiple principal types
  - Flexible trust management
- … help support basic security properties
  - Integrity, secrecy, availability, accountability
- Used as the basis for security protocols supporting trustworthy network operations and to improve user trust
  - SCION, caching, improving user trust, …

53