

XIA: eXpressive Internet Architecture

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

NSF PI Meeting– November 15, 2010

Carnegie Mellon

BOSTON
UNIVERSITY

THE UNIVERSITY
of
WISCONSIN
MADISON

Outline

- Vision and architectural principles
- Research overview and status
- Project organization
- Outreach and broader impact
- NSF questions and discussion

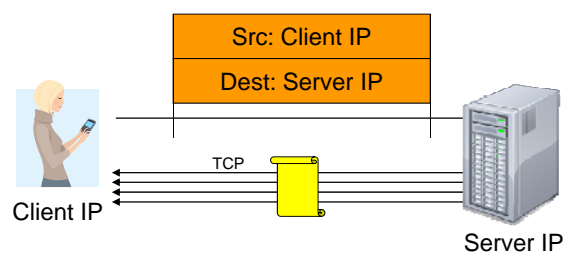
Vision

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

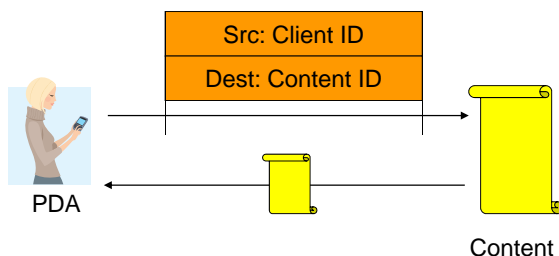
Today's Internet



- 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

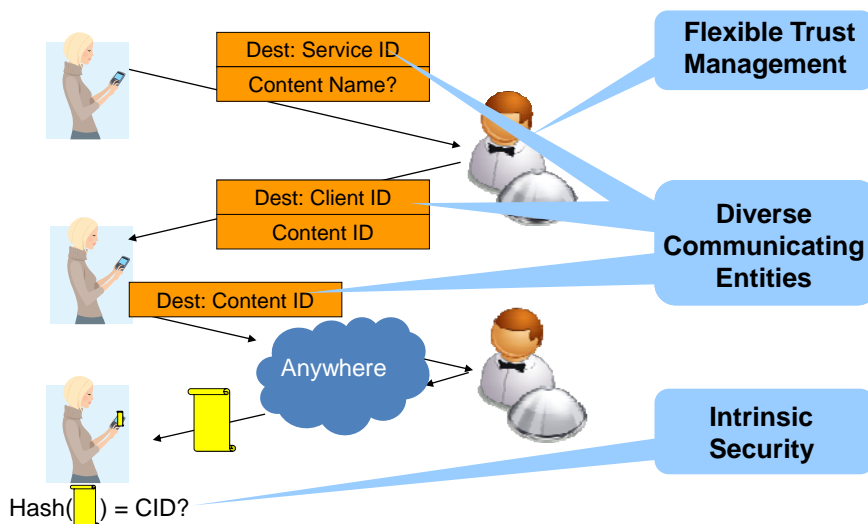
eXpressive Internet Architecture



- 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

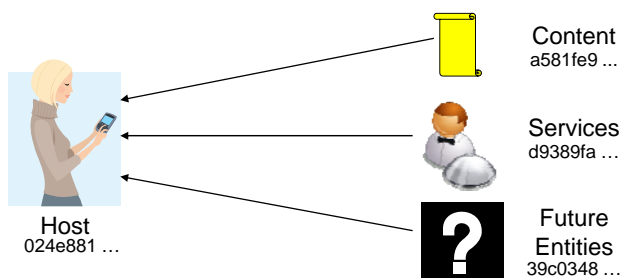
A Bit More Detail ...



6

P1: Evolvable Set of Principals

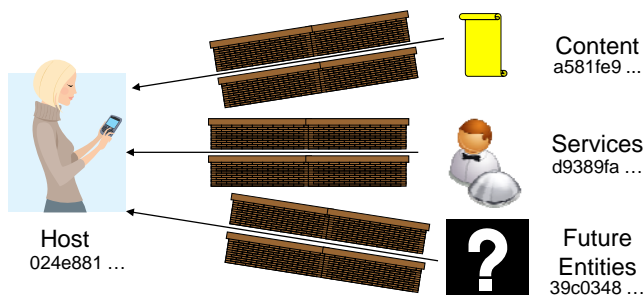
- Identifying the intended communicating entities reduces complexity and overhead
 - No need to force all communication at a lower level (hosts), as in today's Internet
- Allows the network to *evolve*



7

P2: Security as Intrinsic as Possible

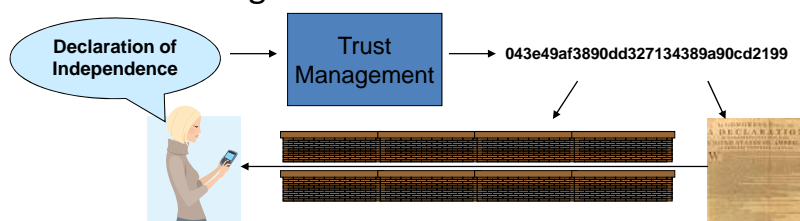
- Security properties are a direct result of the design of the system
 - Do not rely on correctness of external configurations, actions, data bases
 - Malicious actions can be easily identified



8

P3: Narrow Waist for Trust Management

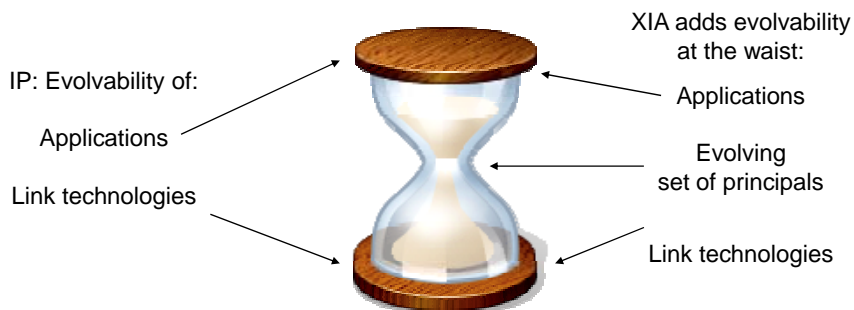
- Ensure that the inputs to the intrinsically secure system match the trust assumptions and intensions of the user
 - Certificate authorities, reputation, personal, ...
- Narrow waist allows leveraging diverse mechanisms for trust management



9

P4: Narrow Waist for All Principals

- Extends today's host-based narrow waist to all principals: hosts, services, content, ...
- Defines the API between the principals and the network protocol mechanisms



10

P5: All other Network Functions are Explicit Services

- DNS, firewalls, ...
 - Causes problems in IP
 - Covers all functions not part of the narrow waist
- XIA provides a principal type for services
- Keeps the architecture simple and easy to reason about

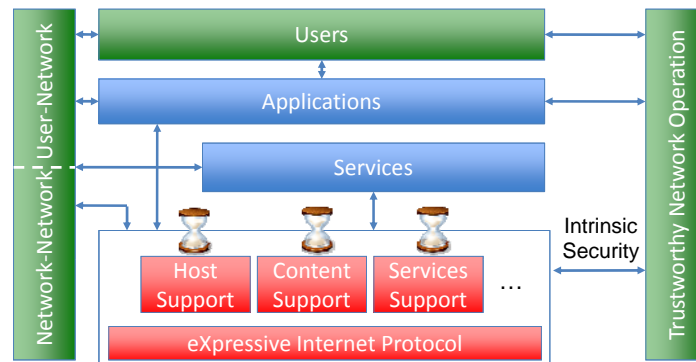
11

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, overlays
 - Not based on a “preferred” principal (host, content), that has to support all communication

12

XIA Components and Interactions



13

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

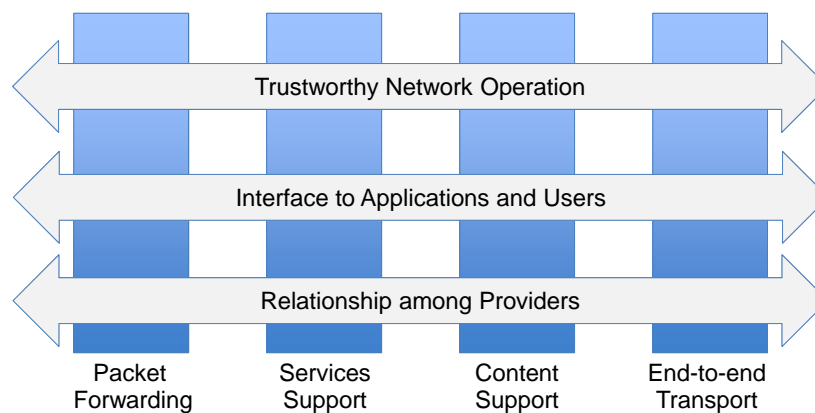
14

Outline

- Vision and architectural principles
- Research overview and status
- Project organization
- Outreach and broader impact
- NSF questions and discussion

15

Research Agenda



16



Intrinsically Secure Identifiers

- Inspired by AIP, the Accountable Internet Protocol
- XIA host identifiers are self-certifying: hash of public key of domain/endhost
 - Similar to AIP
- Basis for intrinsic security properties
 - Example is source accountability
- XIA expands this idea to an evolving set of principals
 - All principals have self certifying XIDs
- *XIA supports direct communication among all principals while offering intrinsic security properties*

17



XIA Addressing and Packet Processing

- Direct communication among principals offers many benefits
 - Reduced complexity: no translation to host-based comm.
 - Evolvability: network can be smarter over time
 - Optimizations: “late binding” to device: caches, failures, ...
 - Security: intrinsic security for communication with principals
- XIDs are the interface between principals, network – networks do not have to support all XIDs natively
 - API does not specify mechanism used by network
 - Depends on technology, scale, role, ... of the network
 - Distinguish between guaranteed reachable and optional

18

XIP Packet Processing – Research



- Packet formats and packet processing
 - E.g. ordered XID tuples, XID stacks, etc.
 - Rules for interpretation?
 - Scalability: fast look up, hierarchy, ...
- Routing based on XIDs
 - Can adapt existing protocols: IP prefix → domain id
 - Multiple XID types has big influence on routing policy
- Use of intrinsic security for authentication of control and verification of data
 - Quantify specific intrinsic security properties
 - Creates basis for trust management and availability

19

XIA Support for Content



- Accessing and publishing content likely to be predominant forms of communication
 - Tweets, blog posts, multimedia, news feeds etc.
- Consumer and publishers more interested in timeliness and integrity than source or format
- Existing approaches not attractive
 - Overlays: additional layers of complexity
 - Content-centric: very constraining for other communication forms
- XIA supports content as a principal intrinsically alongside other principals

20



Building Blocks and Approach

- Data-Oriented Transport (DOT)
 - Separates content negotiation from specifics of content transport; application agnostic
 - Supports “content from anywhere” notion
 - Self-certifying content XIDs to label content
- Caching and Redundancy Elimination (RE)
 - Router-level scheme to cache/suppress duplicate content
 - Provides mechanisms for cache coordination and management
 - Improves content availability and end-to-end performance

21



Content Support – Research

- Many forms of self-certifying content XIDs, each suited to specific scenarios
 - Hierarchical: bind additional information (e.g., creator) to content
 - Presentation-independent: same multimedia content in different forms → identical content XIDs
- Granularity and chunking support in content XIDs
 - Crucial to resolving tension between representing small objects and high network overhead
- Narrow waist for caching
 - Transparent vs. application-controlled

22

XIA Support for Services

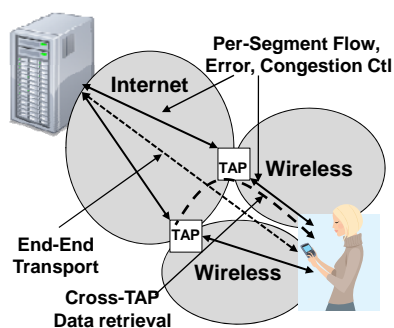
- In contrast to hosts, service XIDs lack unique binding
 - I.e. many places on the network provide the same service
- Routing: how do we deliver packets to a service XID?
 - Role of network versus host, e.g. late versus early binding
 - Scalability, e.g. many devices will offer many services
- Delegation: how do we manage uses of “delegates”?
 - Name resolution of destination can provide address stack
 - Role of network, source(s), destination(s)?
- Intrinsic security: what does service XID bind to?
 - Diverse services: global (DHCP), local (Local LPD), replicated (CDN), unique (CNN)
 - Must manage secrets bound to XIDs differently in each case

23

Building Block: Tapa

Network Support for Mobile Users

- Many challenges:
 - Link, device heterogeneity
 - In network services
 - E2E synchronization
- Move some transport functions to homogeneous network segments
 - Optimized solutions
- TAPs create end to end paths
 - Reduced end-to-end synchronization
 - Optimization of data transfer using DOT-style self-certifying content XIDs



24

Transport over Heterogeneous Networks - Research

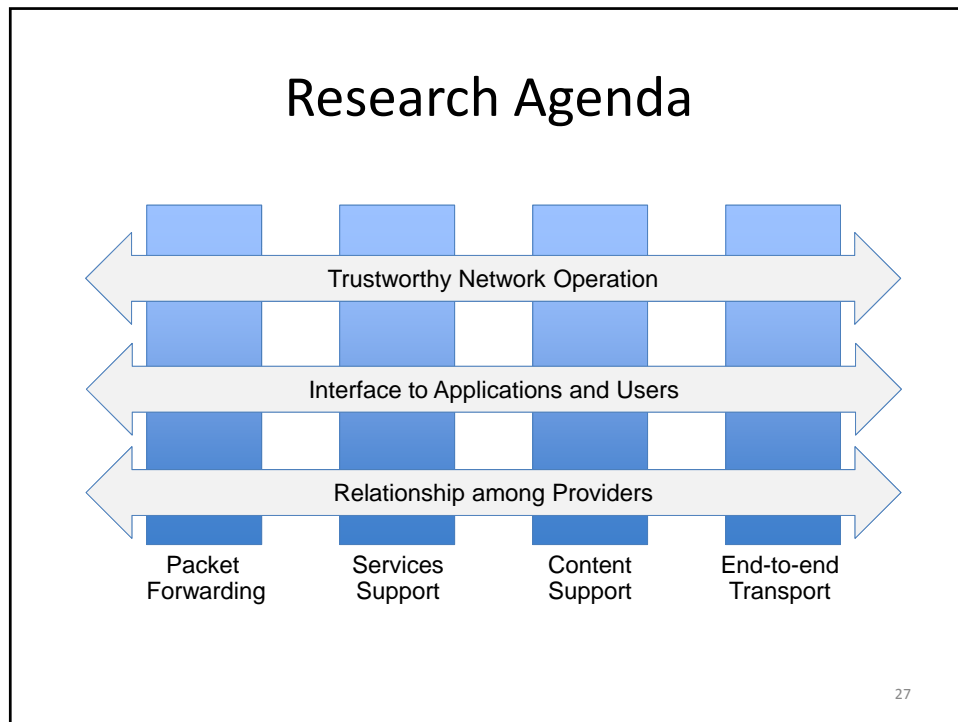


- Leverage XIA service principals on TAPs
- Maintain intrinsic security properties in mobile environment
 - Wireless technologies, mobility optimizations
- Use Tapa over more diverse wireless technologies
 - Cellular technologies, cognitive/DSA networks, vehicular, and extensions to DTN
- Exploring end-to-end transport semantics
 - Expand scope of semantics and include role of intermediaries, e.g., with respect to failure modes, security, and content


25

Core Networking Research Status

- Team of ~5 faculty and ~8 students defining the interface for the various XIA principals
 - Focus on content as a new principal, but must also consider hosts and services
- Look at efficient ways of supporting transport functionality on top of XIP
 - Error control, flow control, congestion control, etc.
 - Consider caching, replicated services, mobility, ...
- Planning first XIA prototype



Three Principles of Trustworthy Design



- Well-foundedness
 - Identifiers, associations match user's intent
 - Trust management
- Fault isolation
 - Good design reduces dependencies, insulates correct portions of network operation from incorrect/malicious
 - Intrinsic security
- Active defense (attack neutralization and recovery)
 - Shared resources = cannot always isolate
 - Availability (network resilience & DDoS defense)

28

Research Agenda



- Trust management: develop a practical suite of trust bootstrap mechanisms that can interoperate
 - Replace current stove pipe design
 - Social nets, direct contact, notaries and registries
 - “API” for providing evidence to support trust
 - Quantifiable metrics, systematic composition
- Ensure the availability of alternatives / mitigation mechanisms even under attack
 - Leverage greater accountability, easy redundancy, ...
- Defend any new attack surfaces exposed by XIA
 - Content caches, service provision, user interfaces

29

The User-Network Interface



- In today’s infrastructure, principals have:
 - Minimal control over exposure of private information
 - No information on how data is sourced, changed, used, copied, forwarded to others
 - Limited means to access useful diagnostic information
- In XIA, options are to be explicit and well-defined
 - Expose and formalize available network capabilities
 - Provide secure audit trails
 - Variants useful for not only content provenance, but also network diagnostics, commercial use (e.g. ad tracking), ..

30

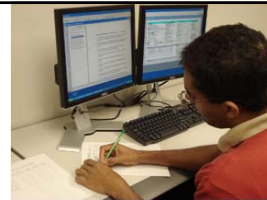
User-Network Interface – Research



- Audit capabilities at the network layer:
 - Session-level audit trails in an advisory capacity
 - Self-certifying names enable principals to assert e.g., it cached a document, or forwarded a packet
 - Prior work on packet sampling, network monitoring
- Similar methods apply at the application layer:
 - Secure content provenance: where did content originate? Who has modified it and how?
 - Key concern is how it affects the user's trust and overload
 - Study user experience and impact on user behavior

31

User Studies



- Prototype network will support experimental apps and interfaces, e.g., audit trails (early studies can be Wizard-of-Oz type)
 - Conduct empirical field experiments
- Example - multi-organizational collaboration
 - Such collaborations often face inadequate information sharing and problem solving (intelligence analysis across agencies is one example domain)
 - Paradigm at CMU for testing collaboration behaviors under different levels of trust with audit trails and other apps
 - Builds on prior and ongoing NSF-funded HCI research

32

Policy and Economic Feasibility

- A future architecture should align the technical decisions by individual actors with their incentives
 - Should promote effective and efficient system operation
 - Otherwise, adoption is difficult or even infeasible, e.g. QoS
- Our research will explore
 - The potential incentives created by XIA design principles
 - How technical design and public policy might be changed to constructively alter those economic incentives
- Example: What is the economic incentive for ISPs to cache content?
 - Reduce upstream bandwidth costs
 - Garner payments from publishers
 - Latter may require architectural support (audit mechanism)

33

Relationships Between Actors -

Research

- Relationship between the XIA architecture and the organizational structure of service providers
 - Organizational structure should conform to clean interfaces
- Potential revenue flows
 - Who will pay for storage in content-centric approaches?
- Viability of competition among providers
 - Is competition sustainable for naming? Caching? Others?
 - Implications for antitrust and regulation
- Potential for individual actors to become gatekeepers
 - “net neutrality” issue for storage function? Cryptography?
- Monitoring and auditing as it relates to ..
 - privacy and security protection, lawful wiretapping, ...

34

Research Status

- Policy group's initial focus on incentives for providers to deploy content caches
 - Provider bandwidth savings vs payments from publishers
 - Asymmetric incentives across NAPs
- The security group is focusing on diverse approaches for trust management that share an interface
 - Social networks for trust communication
 - Perspectives style trust management
- User group is evaluating for applications that leave a "trail" and use it internally
 - Also interacting with trust management researchers

Outline

- Vision and architectural principles
- Research overview and status
- Project organization
- Outreach and broader impact
- NSF questions and discussion

Team Expertise

- | | | |
|---|------------------|---------------|
| • Diverse background | Peter Steenkiste | Networking |
| • Cohesive team | Aditya Akella | Nets, Content |
| – Geographically concentrated | Dave Andersen | Networking |
| – XIA has lots of shared ideas | John Byers | Algs., Nets |
| • Long track record of collaboration | Dave Feinberg | Education |
| • Industry and government experience | Sara Kiesler | HCI |
| – Startups, FCC | Jon Peha | Policy, Nets |
| – Manufacturers, services, operator, policy | Adrian Perrig, | Security |
| | Srini Seshan | Networking |
| | Marvin Sirbu | Policy |
| | Hui Zhang | Nets, Content |

37

How are We Organized?

- Four “focus” groups concentrating on specific aspects of the project
 - Core network, providers, users, trust management
- Maintaining synergy is key!
 - Overlap in membership of the groups
 - Regular joint/project meetings
 - Make sure students benefit from project breadth
- Reevaluate structure periodically
 - Both nature of the groups and their interactions

Our Kickoff Meeting!



- The XIA team met at CMU on Oct 28-29
 - Get students engaged
 - Jumpstart cross-thrust collaboration



Outline

- Vision and architectural principles
- Research overview and status
- Project organization
- Outreach and broader impact
- NSF questions and discussion

Broader Outreach

- To policy makers through DC workshops
 - Yearly workshop involving staff from Congress, FCC, FTC, Commerce Department, White House, NSF, ...
- To diverse Internet users for interface evaluation and prototyping
 - Diverse population of college and high school students
- To network operators at PSC and WiscNet
 - Trial deployments, experiments, and operator input
- To the research community
 - By making prototype available for use and feedback
- Activities designed to be of mutual benefit

41

Integration Education and Research

- Training and mentoring of students at all levels
 - Long track record of REUs, MS thesis projects, PhDs
- Create larger projects that look at FIA problems that are not the focus of XIA
 - Applications and services, transport protocols, energy efficiency, inter-domain routing, QoS, rural, ...
 - Teams of UG or MS students; summer or semester long
- Courses with a FIA focus at grad and undergrad level
 - Both existing and new courses
- Provides another opportunity for feedback, e.g.
 - Evaluation of XIA interfaces for application developers
 - Integrated use of XIA features in a social networking appl.

42

Outline

- Vision and architectural principles
- Research overview and status
- Project organization
- Outreach and broader impact
- NSF questions and discussion

43

NSF Questions

- Articulate the overview of your architectural approach.
- Articulate your approach to dealing with security.
- Identify the hard problems—the issues that have to be resolved to reduce risk in the project. What do you worry about?
- What problems have you had to set aside or defer? Why?
- What do you imagine will be the end-product?? How will you evaluate your system? What sort of demonstrations do you anticipate?

44

Risks and Risk Mitigation

- Aggressive time line of the FIA program
 - Cohesive team, past collaboration
- Integration risks
 - Cohesive building blocks, system building experience
- Testbed and prototyping capabilities
 - Internal capabilities but will require external resources for large scale tests
- Very hard to evaluate the ability to support uses and requirements that do not yet exist
 - Many activities in application and service development
- Transition to any new architecture is difficult
 - Considering policy, economics, user requirements up front

45

Hard Problem: Evaluation of a Network Architecture

- Evaluation plan for XIA includes
 - Development and use of an XIA prototype
 - Use standard techniques for components: analytical methods, simulation, ...
 - Critique by the diverse stakeholders
- But is this good enough?
 - Evaluate architecture, not an implementation
 - E.g., evaluating evolvability is crucial
 - Also important to get research published
- Good topic for FIA wide discussion

46

What Problems Did We Decide Not to Focus On?

- Network management
- Quality of service
- Generic routing topics
- Many non-core-networking issues
 - Legal, economics, usable privacy, ...
- And I am sure many others ...

... although all of these topics are touched on

End-Product

- Design of an architecture plus a prototype implementation of XIA
 - Combined with studies documenting impact on providers , users, and trustworthiness
- Heavy emphasis on using the prototype
 - Mobile users, applications, audit trails for various uses, etc.
 - Important part of the evaluation of the architecture and the interfaces

In Conclusion

- The key principles for XIA include:
 - A diverse, evolving set of communicating principals
 - Intrinsic security properties
 - A narrow waist for all key functions
- XIA is a single inter-network in which all principals are connected
- The XIA building blocks exist and are based on a coherent set of ideas
- The XIA team is very cohesive with
 - A long history of collaboration
 - A strong track record in networking, policy, HCI, and education
 - Experience in academia, industry and government
- The project includes a broad outreach program and strong integration of education and research
 - Activities designed to be mutually beneficial

49