XIA: An Evolvable, Expressive, and Secure Internet Architecture

Multiple Principal Communication Types

What is a principal type?
A principal type is a set of identifiers and the semantics of communicating with one of these IDs. Specific semantics allow endpoints to directly express the intent of a packet. Varying semantics are achieved through type-specific per-hop processing.

Example Principal Types
We introduce the host, service, and content principals. New types can be added in the future to provide native network support for new modes of communication, making XIA networks evolvable.

Flexible Addressing
Addresses in XIA are represented as directed acyclic graphs (DAGs), which allows for graceful implementations of mechanisms like fallbacks, iterative refinement, and session binding.

Example: Fallbacks and Iterative Refinement
- Provide backwards compatible paths
- Facilitate endpoint evolution
- Allow incremental deployment in the network

Example: Session Binding
Some communication sessions must be bound to a particular server (e.g., an online banking session).

Intrinsically Secure Identifiers
- IP is hard to secure, as security was not a first-order consideration in its design
- XIA aims to build into the architecture a means for bootstrapping secure communication
- The exact meaning of “secure communication” varies by principal type

- Hosts
  Host IDs (HIDs) are the hash of a host’s public key
  \[ \text{HID} = \text{hash}(\text{Pub}) \]

- Services
  Service IDs (SIDs) are the hash of a certifying authority’s public key
  \[ \text{SID} = \text{hash}(\text{Cert}) \]

- Content
  Content IDs (CIDs) are the hash of the content itself
  \[ \text{CID} = \text{hash}() \]

A prototype implementation of XIA is publicly available at http://www.cs.cmu.edu/~xia

XIA is funded by NSF under awards CNS-1040757, CNS-1040800 and CNS-1040801