Carnegie Mellon

CyLab

CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
www.cylab.cmu.edu

Future Internet Projects @ CMU

XIA & SCION

Adrian Perrig

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

Carnegie Mellon

BOSTON UNIVERSITY

THE UNIVERSITY of WISCONSIN MADISON

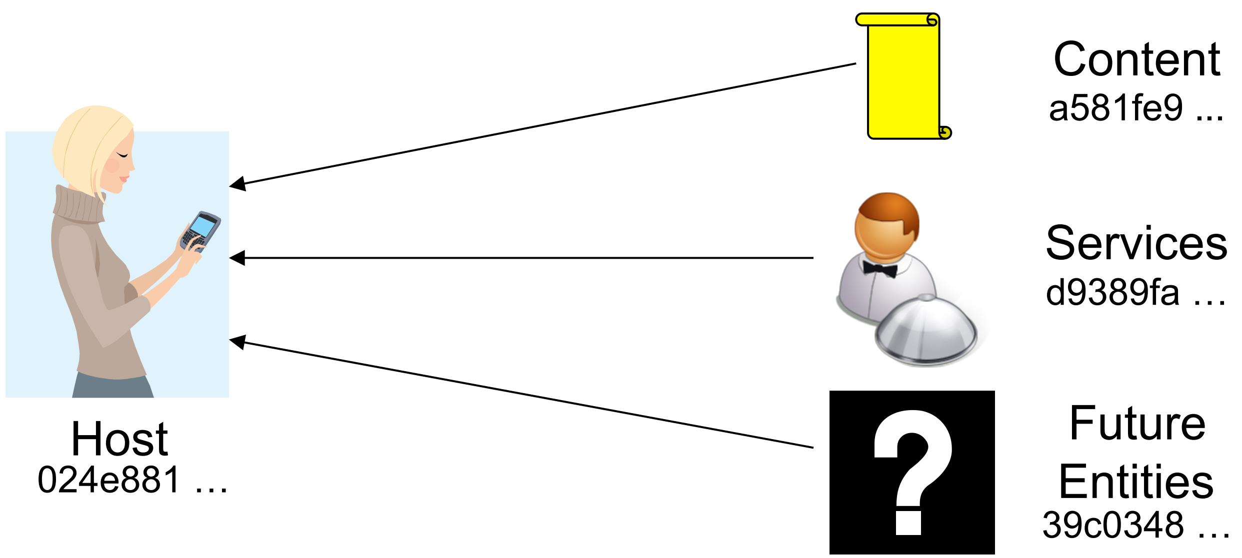
XIA Vision

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

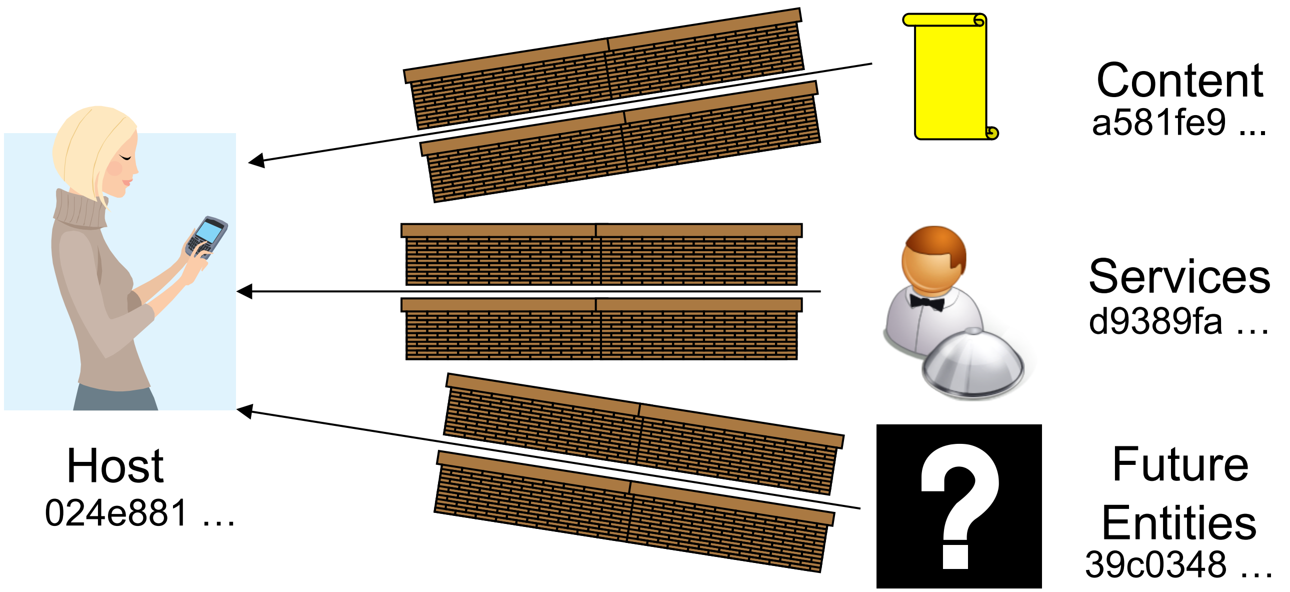
P1: Evolvable Set of Principals

- 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



Other XIA Principles

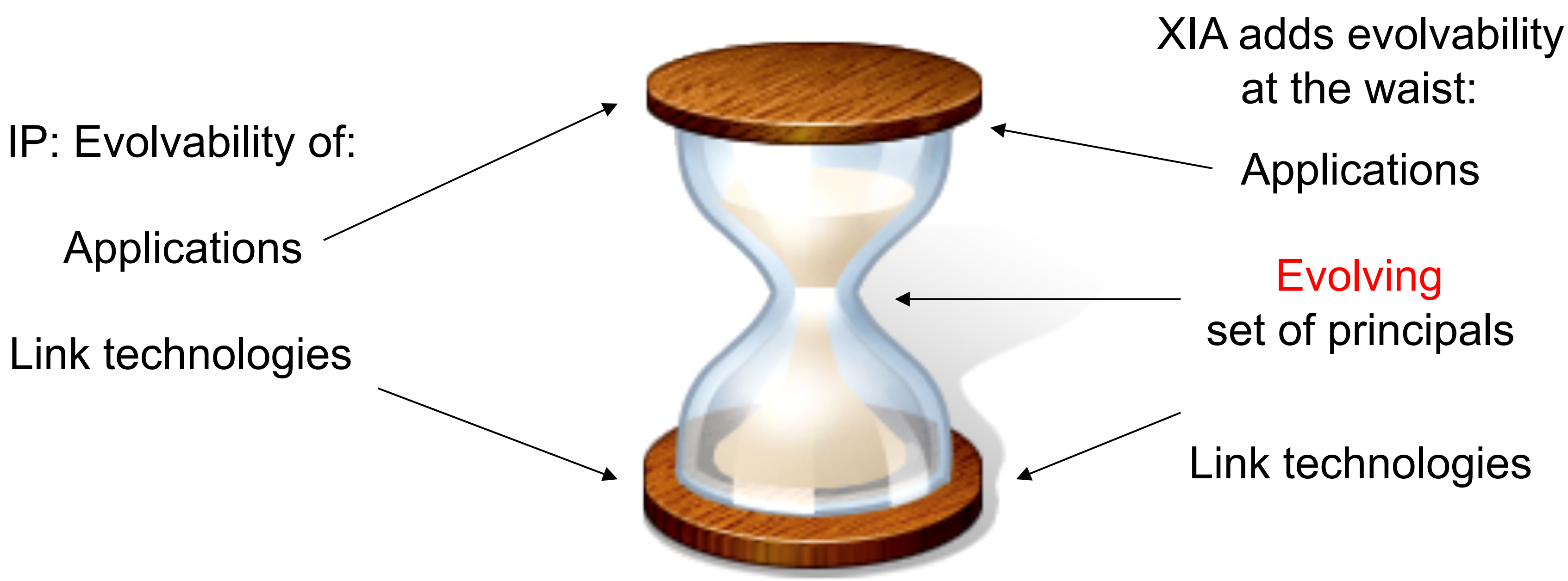
- Narrow waist for trust management
  - Intrinsically secure identifiers must match the user's trust assumptions and intensions
  - Narrow waist allows leveraging diverse mechanisms for trust management: CAs, reputation, personal, …
- Narrow waist for all principals
  - Defines the API between principals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

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

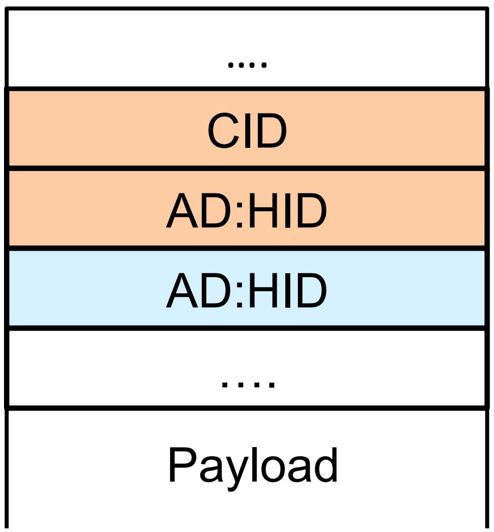
What Do We Mean by Evolvability?

- 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



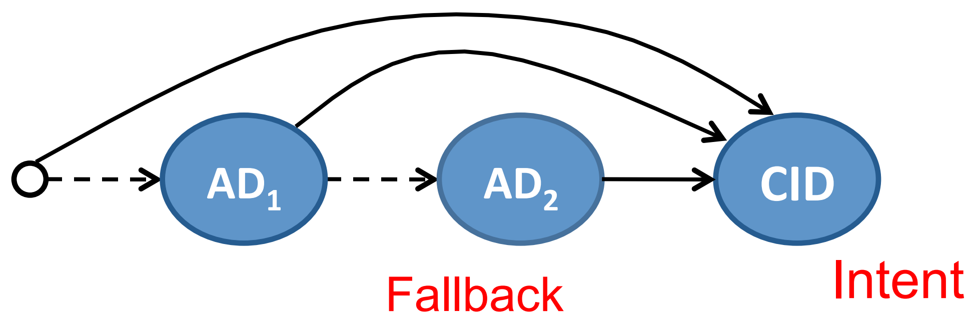
Evolvability

- 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



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

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

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

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-grained control: users can specify their intent
- Explicit chain of trust: Allow users to understand the basis for trust, underlying assumptions
- Intrinsically secure identifiers

Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
www.cylab.cmu.edu

SCION:

Scalability, Control and Isolation On Next-Generation Networks

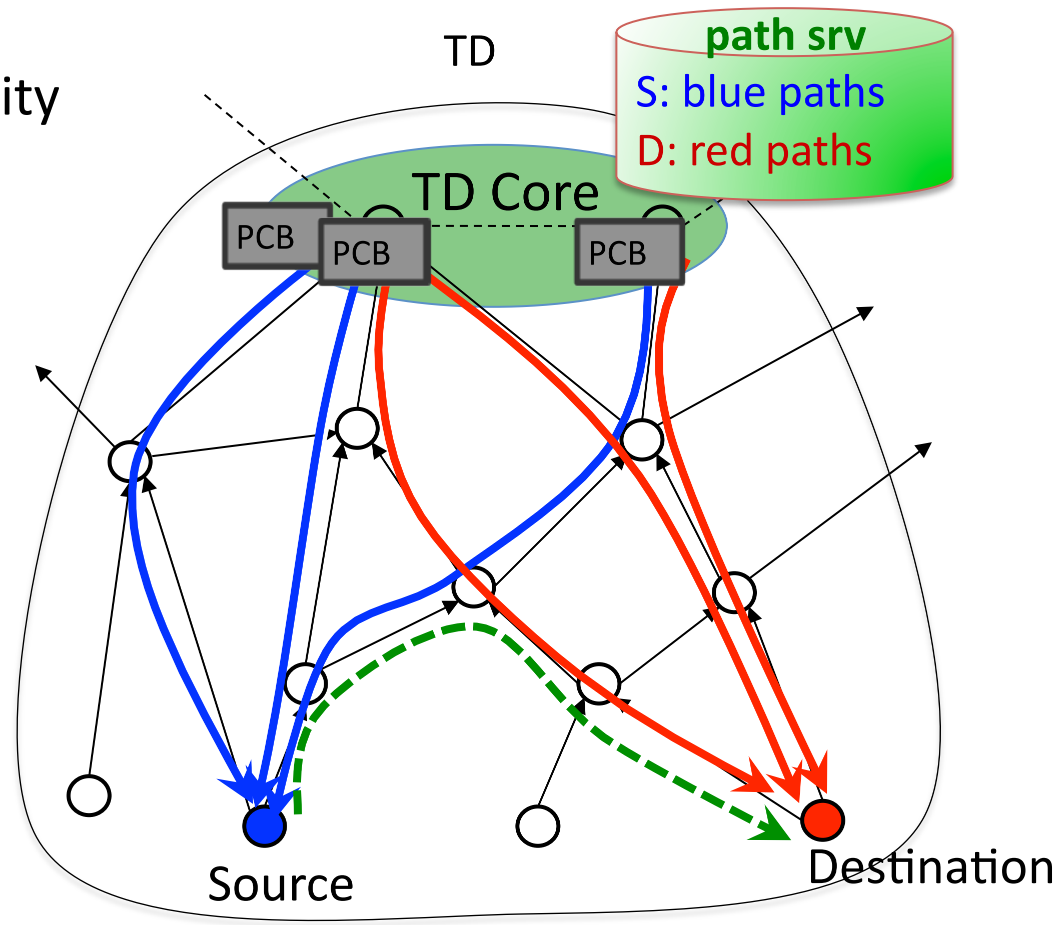
Xin Zhang, Hsu-Chun Hsiao, Geoff Hasker,
Haowen Chan, Adrian Perrig, David Andersen

SCION Architectural Goals

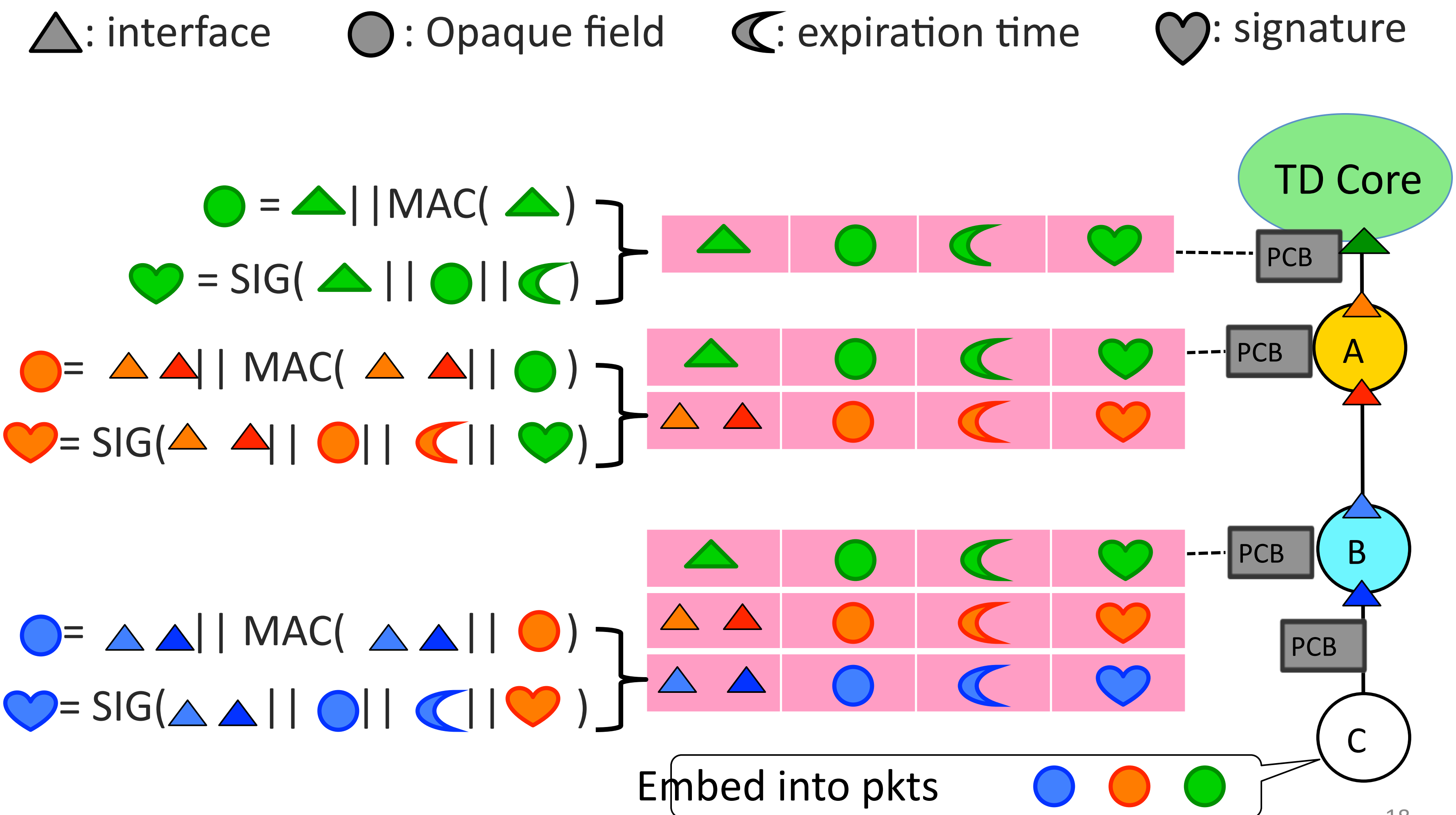
- High availability, even for networks with malicious parties
- Explicit trust for network operations
- Minimal TCB: limit number of entities that need to be trusted for any operation
  - Strong isolation from untrusted parties
- Operate with mutually distrusting entities
  - No single root of trust
- Enable route control for ISPs, receivers, senders
- Simplicity, efficiency, flexibility, and scalability

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



Path Construction



Discussion

- Incremental Deployment
  - ✓ Current ISP topologies are consistent with the TDs in SCION
  - ✓ ISPs use MPLS to forward traffic within their networks
  - ✓ Only edge routers need to deploy SCION
  - ✓ Can use IP tunnels to connect SCION edge routers in different ADs

- Limitations
  - ✗ ADs need to keep updating down-paths on path server
  - ✗ Increased packet size
  - ✗ Static path binding, which may hamper dynamic re-routing

BGP / Control Plane Issues

- Lack of fault isolation
  - Error propagation, potentially to entire Internet, disruption of flows outside domain
  - Can attract flows outside domain
  - Black art to keep BGP stable, manual rule sets, unanticipated consequences
- Instability propagates, when link/router goes down, remainder of the network has much more work to find new routes
  - Increased number of routing updates during DDoS attacks
  - Path changes need to be sent to entire Internet
  - Much more work required during times of instability
- Lack of scalability, amount of work by BGP is O(N), where N is number of destinations
- S-BGP requires single root of trust for AS and address certificates
- Lack of freshness for BGP update messages
- Slow route convergence
  - Convergence attack
  - Network may require minutes if not tens of minutes for convergence
- Other specific attacks
  - Blackhole attacks
  - Wormhole attack

IP / Data Plane Issues

- Complex route table lookup for each packet
- Lack of predictability for path availability
- Lack of route choice/control by senders and receivers
- Bursting routing tables

IP / BGP / Misc. Issues

- No path predictability due to inconsistency between routing table and BGP updates
- No isolation between control and data planes (routing and forwarding)
    - By attacking routing, prevent forwarding to work correctly
- Huge TCB (entire Internet)
- Single root of trust for DNSsec

Performance Benefits

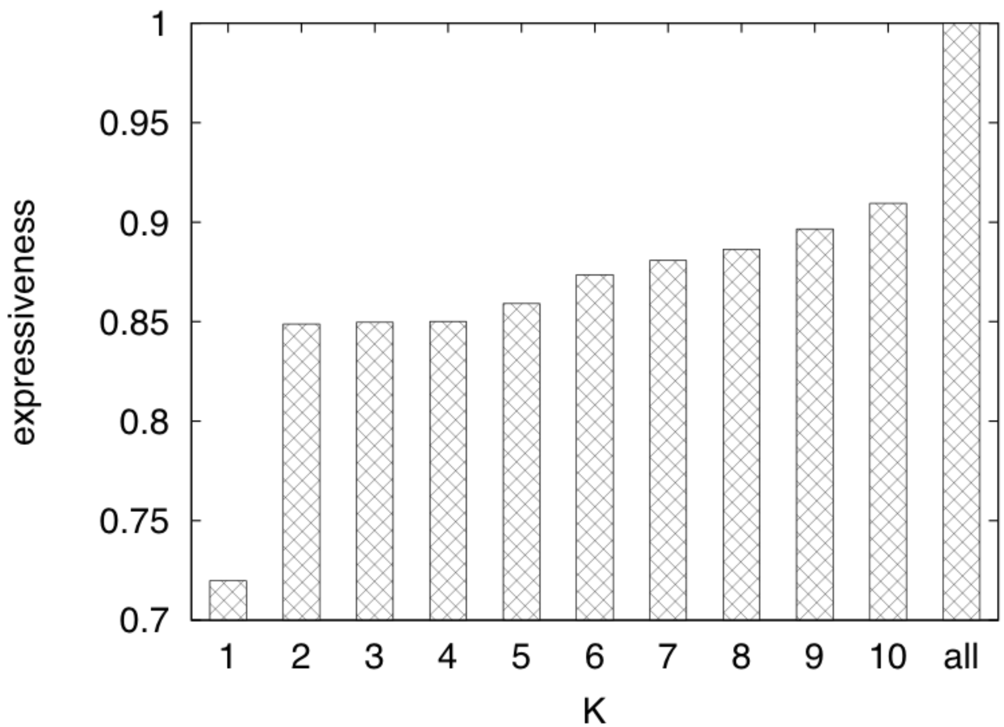
- Scalability
  - Routing updates are scoped within the local TD
- Flexibility
  - Transit ISPs can embed local routing policies in opaque fields
- Simplicity and efficiency
  - No interdomain forwarding table
    - Current network layer: routing table explosion
  - Symmetric verification during forwarding
  - Simple routers, energy efficient, and cost efficient

Evaluation

- Methodology
  - Use of CAIDA topology information
  - Assume 5 TDs (AfriNIC, ARIN, APNIC, LACNIC, RIPE)
  - We compare to S-BGP/BGP
- Metric 1: additional path length (AD hops) compared to BGP
  - *Without* shortcuts: 21% longer
  - *With* shortcuts:
    - 1 down/up- path: 6.7% longer
    - 2 down/up- path: 3.5% longer
    - 5 down/up- path: 2.5% longer

Evaluation (cont'd)

- Metric 2: Expressiveness
  - Fraction of BGP paths available under SCION



Summary

- Availability is fundamentally most important security property
- Core design mechanisms to provide maximum availability in XIA / SCION
  - XIA: Intrinsic security, user-specified intent, user-understandable trust, fault isolation, designed for extensibility
  - SCION: Isolation, explicit trust, control, no single root of trust

- Check us out at: http://www.cs.cmu.edu/~xia/