ICN+SCION: A global name-based network service

Thanks: NSF CNS-2512457
EAGER: NDN+SCION: Toward a global name-based network service
Also: ETH

Jeremiah S. Davis

Jakob Duerstock, Ken Calvert

University of Kentucky

Agenda

I. Overview
II. Motivations
III. Background
   - SCION
   - RHINE
IV. ICN+SCION Initial Design & Status
V. Summary and Q&A

Overview

ICN+SCION

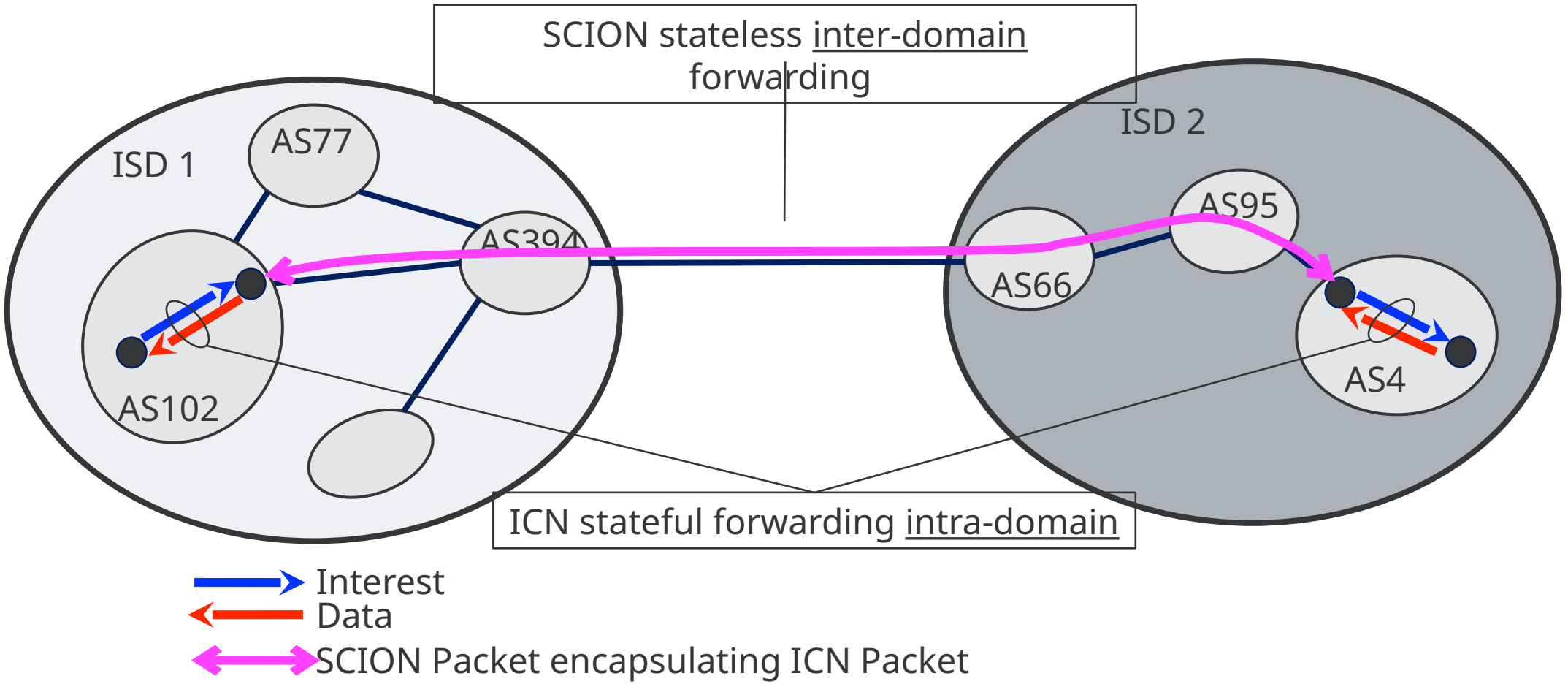
…combines existing network-layer protocols/services

- NDN/CCNx
- SCION inter-domain routing/forwarding system
  - Secure, path-oriented replacement for BGP
  - Packets carry path indicating domains to traverse

…Goal: create an end-to-end network (layer 3) service, that:

- has trustworthiness of data as a fundamental, built-in feature
- is compatible with existing Internet ecosystem
- supports heterogeneous trust structures at network and application layers
- supports multipath transmission natively
- does not depend on IP at any level
- scales to provide global connectivity

Inter-domain Interest-Data Exchange



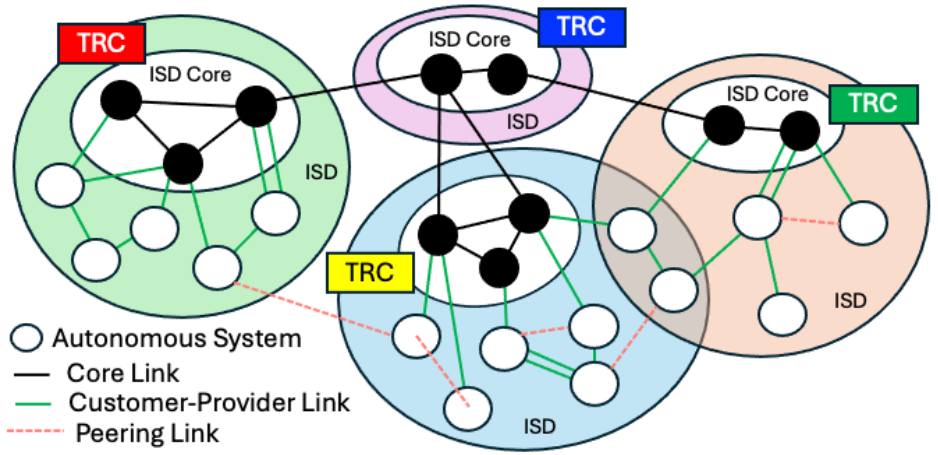
Motivations

- Synergy between the protocols
  - Security as a primary design goal of both ICN and SCION
  - SCION systematizes inter-AS trust
  - ICN helps to reflection and other spoofing based attacks
- Control plane solution to problem of namespace authority
  - Competing claims to same prefix can lead to cache poisoning and network congestion
  - Producers must prove to their AS that they have the authority to publish
- Today's Internet is a highly-tuned monoculture
  - Escaped lab experiment – now critical infrastructure
- Goal: Proof of concept for a global network layer with those properties

Background: SCION

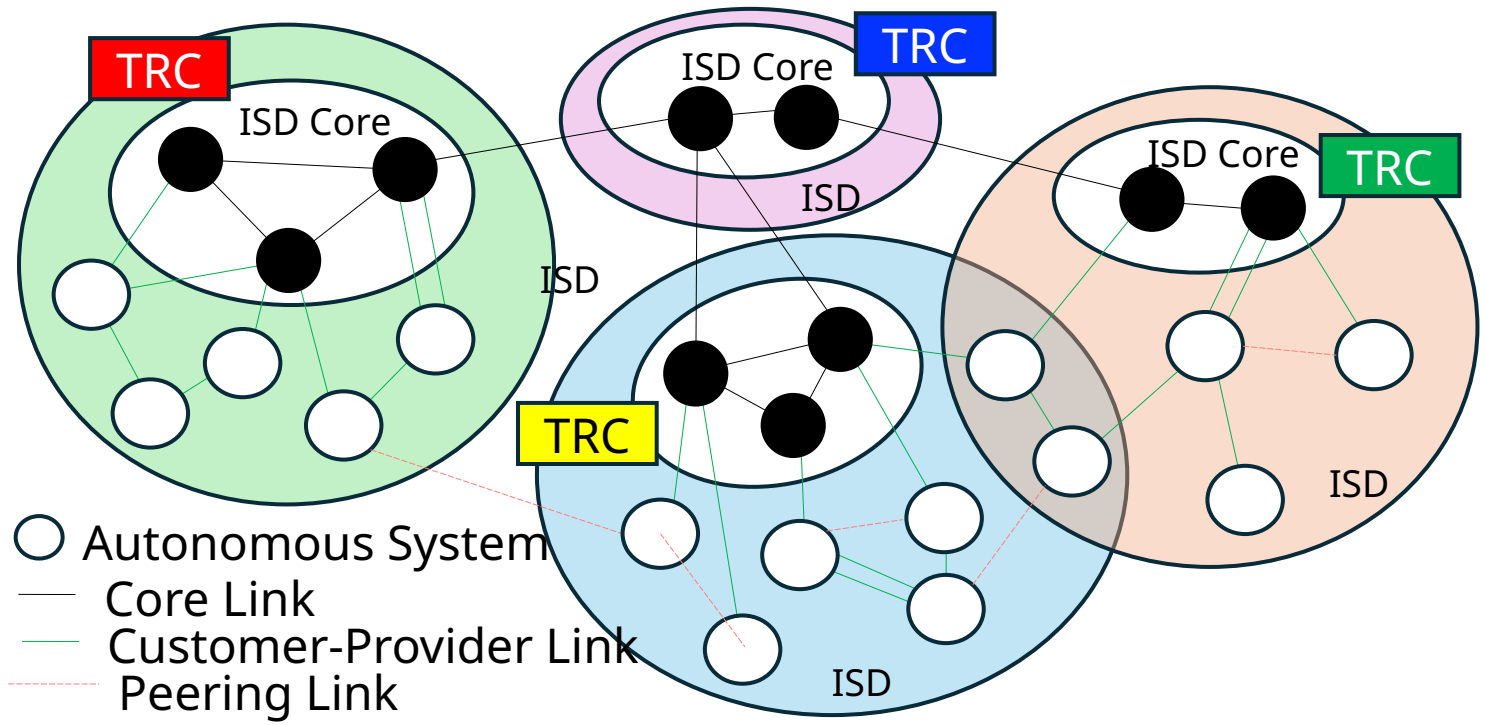
The Complete Guide to SCION. Adrian Perrig *et al*, Springer, 2022.

- Path-aware inter-domain routing/forwarding system
  - From Adrian Perrig's group at ETH Zurich
- Secure replacement for BGP
  - Internet-drafts being discussed in the IRTF/IETF (panrg)
- Designed for security "from the ground up"
  - Consistent with existing provider ecosystem
- Forwarding information carried in packets, not Routing Tables
  - Each packet carries the (cryptographically secured) AS path to follow
- Being commercially developed by Anapaya Systems (anapaya.net), and in real world production networks



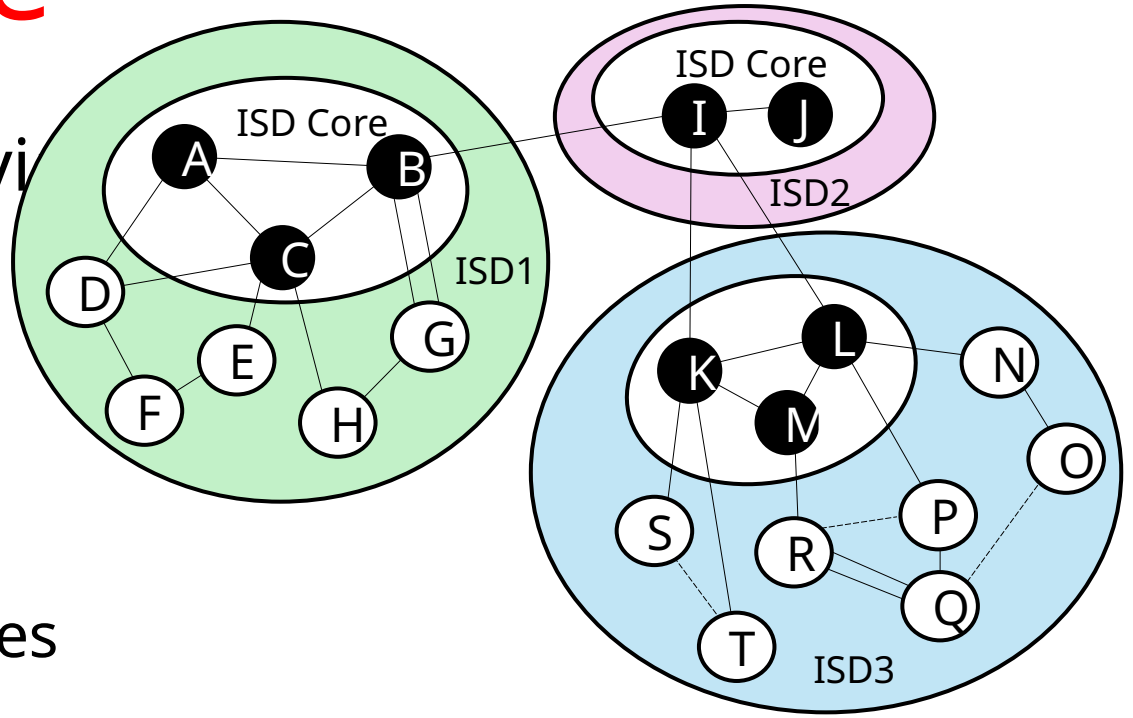
SCION Trust Structure

- Isolation Domain (ISD): group of ASes with common trust structure
  - TRC = trusted root config =
- CA keys + metadata for ISD
  - Think ISP customer cone
- ISDs connect via Core ASes



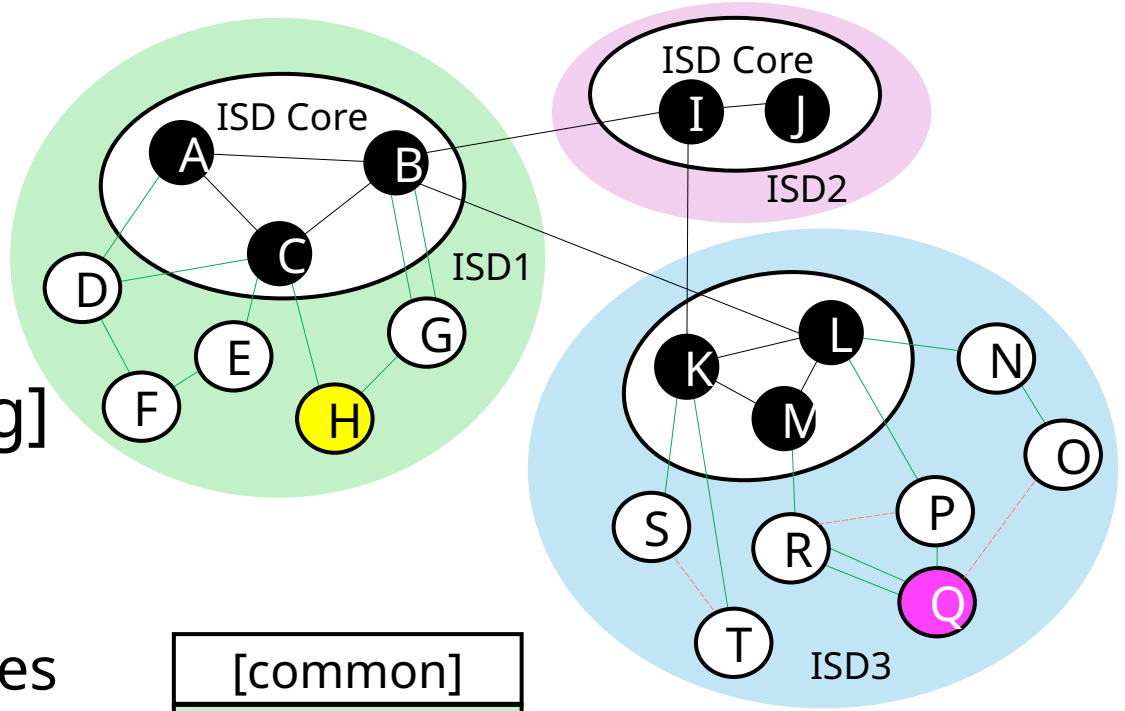
SCION Control Plane

- AS path segments constructed via beaconing within ISDs
  - Protected cryptographically
  - Beacons emitted from Core ASes, propagate away from Core
  - Applying policy along the way
  - Cores beacon across ISD boundaries
- Path segments are oriented
  - Down Segments, e.g.: M→R, K→S→T
  - Core Segments, e.g.: C→A, B→I→L
  - Up Segments, e.g.: F→E→C, T→S→K



SCION Data Plane

- Packets carry AS Path
  - Sequence of ASes to be transited
  - Optional: E2E HMAC covers path
- Path: [up-seg][core-seg][down-seg]
- Paths collected by AS's Control Service
  - Endpoints request paths to other ASes
  - Source selects path to place in packet
- Paths are reversible



[common]
H→G→B
B→I→L
L→P→Q
payload

Key Components of the ICN+SCION Design

ICN+SCION Gateway

- Responsible for finding prefix-to-ASN mappings
- Allows ICN applications to be unaware of SCION topology and path

RHINE Name Service

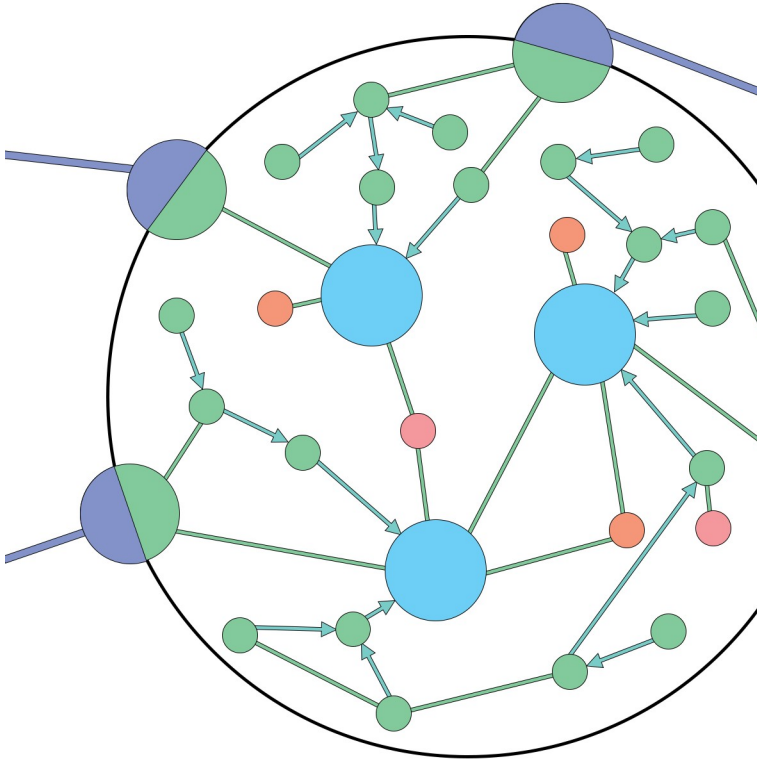
- Improves on DNSSEC
- Holds prefix-to-ASN records, ICN public signing key records

ICN+SCION Border Routers

- "Speak" both ICN and SCION
- Responsible for encapsulating Interests in SCION packets Gateway
- Reflexive forwarding allows ICN+SCION Gateway to set up necessary state in Border Routers

Verification of Namespace Authority

- Publishing authority is always in a defined context
- Producers must prove authority to AS before advertisement
- ScopeID: a 4-byte typed name component defining the namespace authority type



Background: RHINE

RHINE: Robust and High-performance Internet Naming with E2E Authenticity
Huayi Duan, Rubén Fischer, Jie Lou, Si Liu, David Basin, and Adrian Perrig, *NSDI 2023*

- Name Resolution System
- Designed to replace and solve problems with DNS
  - E.g., uky.edu can override netlab.uky.edu even with DNSSEC
- More flexible and secure trust/delegation system
  - Separate mechanisms to secure delegation status vs zone data
  - Leverage WebPKI-type CAs to certify binding between Name prefixes and keys
  - Multiple roots of trust ("assertion contexts")

Why use RHINE?

- Traditional DNS has well-known insecurities:
  - Lack of Data Authentication
  - Attackers can tamper with DNS responses
- DNSSEC also suffers from design flaws:
  - Zone data is authenticated via its parent zone (chain of trust)
  - Rogue parents can:
    - Overwrite children's zone data
    - Delegate more rogue child zones without challenge
- RHINE mitigates attacks from a rogue system:
  - Authentication is directly backed by trusted Certificate Authorities
  - Zone delegations are verified against a well-known global state

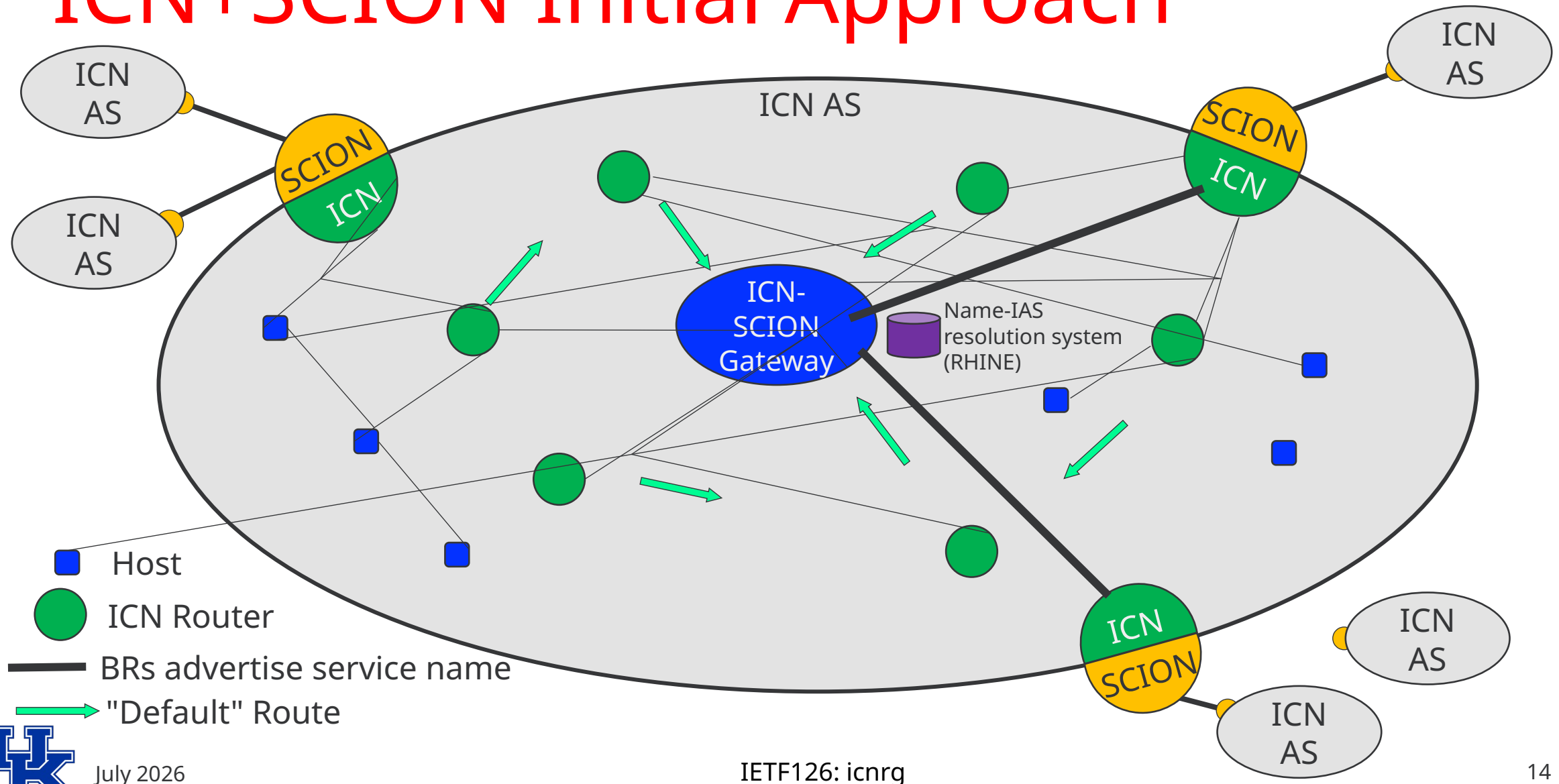
Sidebar: Reflexive Forwarding

Reflexive Forwarding for CCNx and NDN Protocols (Workgroup: ICNRG, Internet Draft)

David R. Oran, Dirk Kutscher, Hitoshi Asaeda, Ken Calvert.

- Facilitates multi-exchange handshakes in ICN **without** resorting to persistent consumer names and/or push semantics
- *Trigger Interest* establishes temporary forwarder state (PIT entries), permitting one or more *Reflexive* Interest-Data exchanges
- Final *Trigger Data* packet tears down temporary state

ICN+SCION Initial Approach



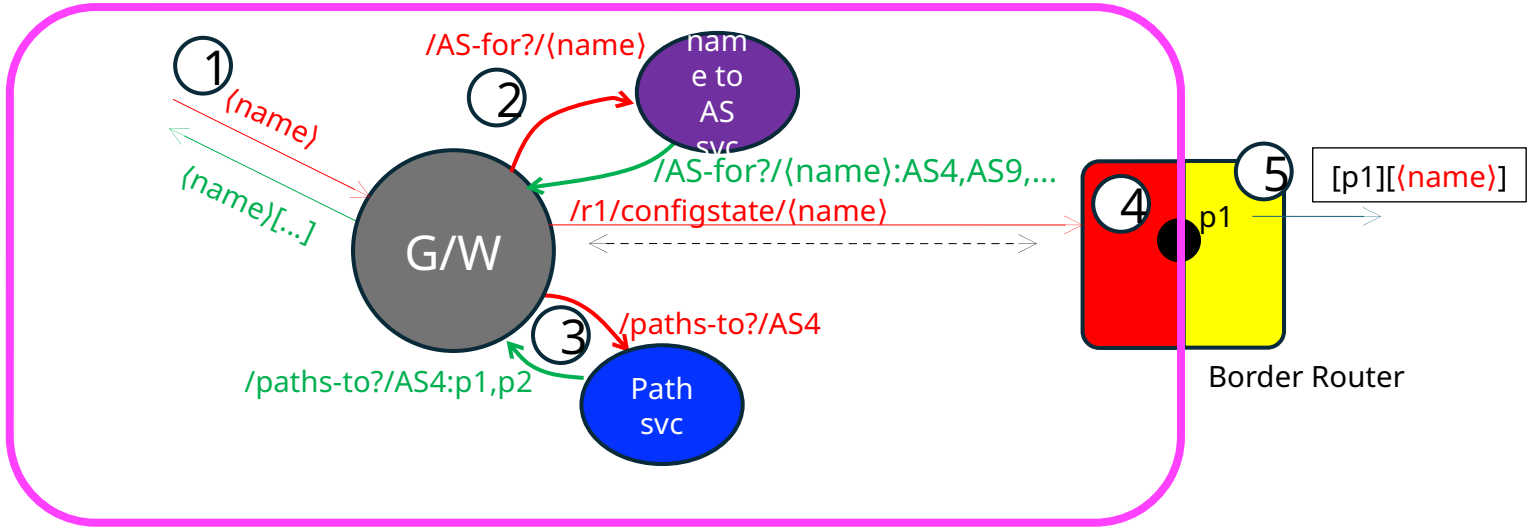
Locating Data with RHINE

- An application may request data from another AS:
  - The application knows the full name of the ICN object
  - The application may not know which AS contains the data

- The Gateway (or application) can query the resolution service:
  - Gateway queries the resolver with the ICN full name
  - Resolver queries external ASes' nameservers to find data owner
  - Resolver sends producer's ASN to client
  - Gateway sends ICN interest together with remote ASN and SCION path information to the Border Router

ICN-SCION Interoperation

1. Interest for ⟨name⟩ finds no match in FIB, forwarded to ICN-SCION Gateway (G/W)
2. G/W gets ASes that contain authorized sources for ⟨name⟩ from RHINE name-to-AS mapping (AS4, AS9)
3. G/W gets paths p1, p2 to AS4 from SCION path service
4. G/W sets up state in border router (via reflexive forwarding), associating p1 with PIT entry for ⟨name⟩
5. Border router encapsulates Interest, adds SCION path header, forwards along path p1

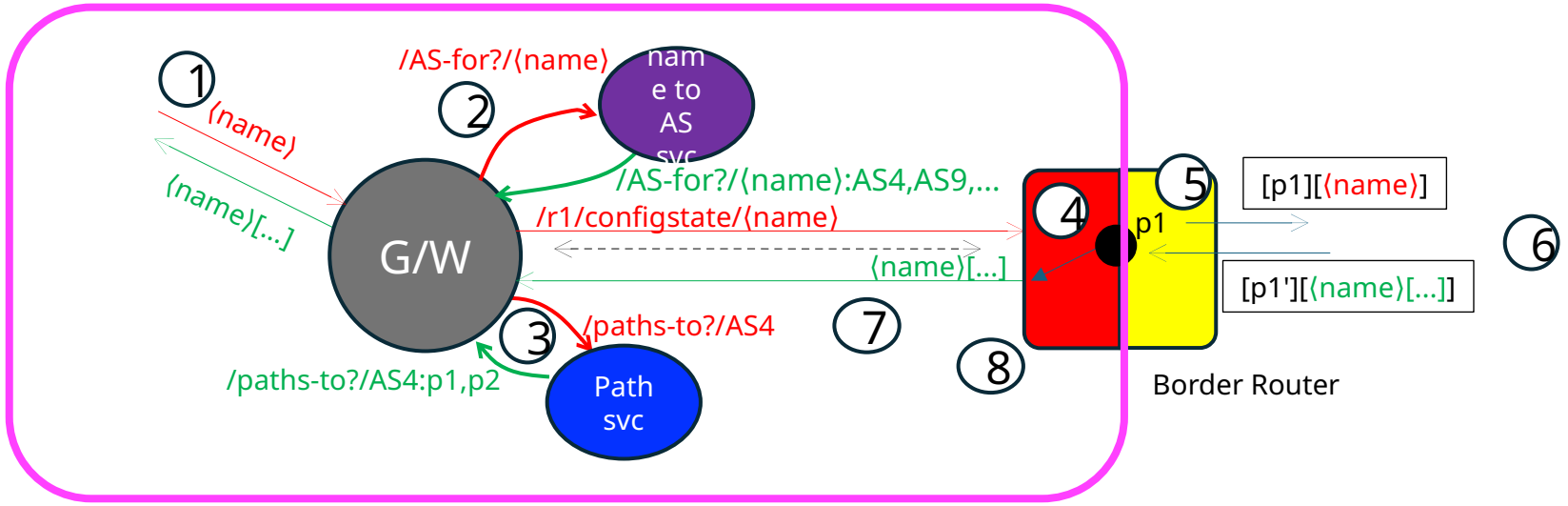


ICN-SCION Interface

6 At AS4, routing system forwards Interest to source for ⟨name⟩ and returns Data via reverse path (including reversed AS path)

7 At ingress router, Data packet is decapsulated and and matched to PIT entry ⟨name⟩, forwarded back to G/W and thence to source

8 Border router eventually advertises availability of ⟨name⟩ in intra-domain routing system



Ongoing Work

- Component protocols running in FABRIC
  - Cefore implementation of CCNx
  - SCION's open-source implementation
  - RHINE's open-source implementation
- ICN-SCION Gateway and Border Routers under development
- FABRIC facility port for connection to SCIERA research network

ICN+SCION Research

- Producer verification protocol
- How to find authoritative name servers for given Name
- Scalability of ICN-SCION Gateway and Border Router functions
- Namespace design for SCION control functions to use ICN
  - Initially: UDP/IP

Summary

1. Combining "mature" research implementations is not straightforward
2. Building on ICN/SCION/RHINE, can we do better than IP?
   - Security-first design
   - Multipath capability
   - Policy & trust flexibility
3. Long-term goal: off-the-shelf ICN, SCION, RHINE capabilities