PLA and PSIRP

Dmitrij Lagutin, Dmitrij.Lagutin@hiit.fi
Helsinki Institute for Information Technology HIIT

15.03.2010

Part of the material is based on lecture slides by prof. Sasu Tarkoma and Kari Visala

Contents

- Securing the Internet with Packet Level Authentication (PLA)
- Clean-slate networking design: PSIRP
- Summary

Packet Level Authentication (PLA)

- Internet was not designed to be secure against internal attacks
  - It was assumed that attacker only will try to destroy the infrastructure by physical means
- Security related problems on the current Internet
  - Denial-of-service attacks (DoS, DDoS)
  - Unsolicited mail (SPAM)
  - Phishing, etc.
  - Inflexible user authentication
- Firewalls can block traffic only near its destination
  - Firewalls are often so restrictive that normal communication becomes difficult

Packet Level Authentication (PLA)

- Traditional end-to-end security solutions such as IPSec and HIP are not enough, they are not effective if the network infrastructure is attacked
- We assume that per packet public key cryptography operations are feasible in Internet's scale because of new digital signature algorithms and advances in semiconductor technology
- PLA is a novel solution for protecting the network infrastructure against various attacks (e.g., DoS) by providing availability
  - The network should be able to fulfill its basic goal: to deliver valid packets of valid users in reliable and timely manner in all situations

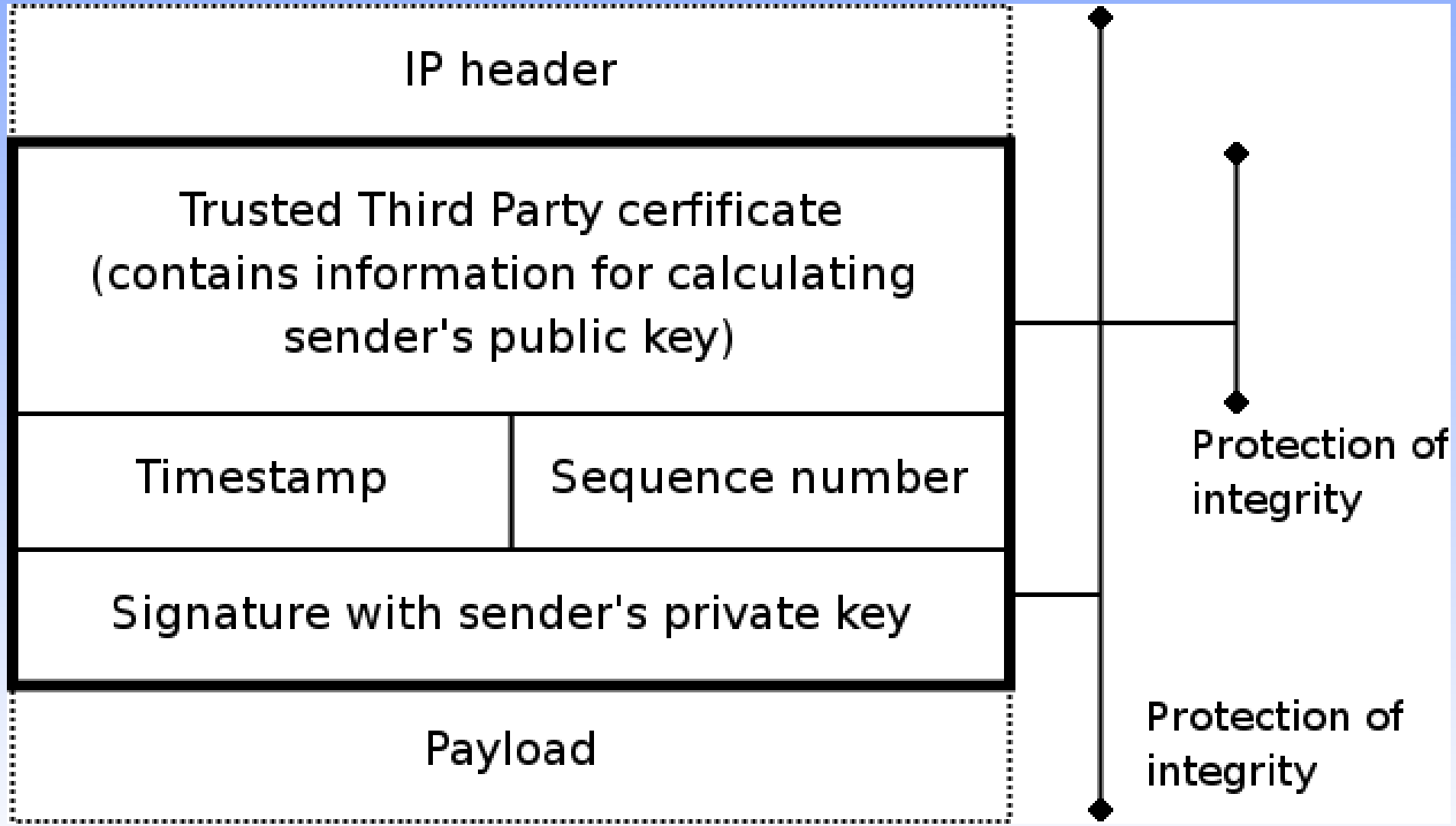
PLA continued

- The main aim of PLA is to make it possible for any node to verify authenticity of every packet without having previously established trust relation with the sender of the packet
  - Malicious packets can be detected and discarded quickly before they can cause damage or consume resources in the rest of the network
  - Good analogy for PLA is a paper currency: anyone can verify the authenticity of the bill by using built-in security measures like watermark and hologram, there is no need to contact the bank that has issued the bill

PLA continued

- PLA accomplishes its goals by using public key digital signature techniques. PLA adds an own header to the packet using standard header extension technique
- Using the PLA header information any node on the path can independently verify authenticity and validity of the packet
  - Is the packet an original and unique?
  - Has it been sent by an authorized sender?
- PLA complements existing security solutions instead of replacing them. PLA can work together with other security solutions such as HIP and IPSec
- Originally PLA was designed for IP networks, however it can be used with any network layer protocol

PLA Header


IP header
Trusted Third Party cerfificate
(contains information for calculating
sender's public key)
Timestamp
Sequence number
Signature with sender's private key
Payload
Protection of
integrity
Protection of
integrity

PLA Header

- Signature by sender's private key together with a sender's public key are used to check authenticity of the packet
- Trusted third party (TTP) authorizes the sender through the certificate
- Timestamp is used to detect delayed packets which may be a sign of a replay attack
- Monotonically increasing sequence number is used to detect duplicated packets

PLA: Trusted Third Parties

- Simply signing packets is not enough by itself
  - Attacker may generate a large amount of identities
- Trusted Third Party (TTP) provides higher layer protection
  - Authorizes the user's public key, i.e., permission to use the network
  - Binds the cryptographic identity to the real one
  - Allows more efficient trust management, no need to trust in individual users, trusting in a TTP is enough in most cases
  - Various organizations (operator, company, country) may have an own TTP

PLA: Cryptographic Solutions and Performance

- PLA uses elliptic curve cryptography (ECC) due to its compact keys
  - 163-bit ECC key is as strong as 1024-bit RSA key
  - The total size of the PLA header is about 1000 bits
- A dedicated hardware is necessary for verifying signatures at wire speed
  - FPGA based proof-of-concept accelerator can perform 166,000 verifications per second
  - Hardcopy based 90nm ASIC can verify 850,000 packets/s, corresponding to 5 Gbps of average traffic
  - Power consumption is only 26µJ/verification (less than the cost of wireless communication)

PLA: Other Applications

- Having strong per-packet signatures allows PLA to be used for several other applications
- Sequence number can be used for secure per-packet and per-bandwidth billing
- Securing higher level protocols such as MIH (media independent handover) without excessive signalling
- Controlling incoming connections: no data connection can be established without an explicit permission from the receiver
- PLA is a natural solution for securing the future publish/subscribe and data-oriented approaches, such as PSIRP

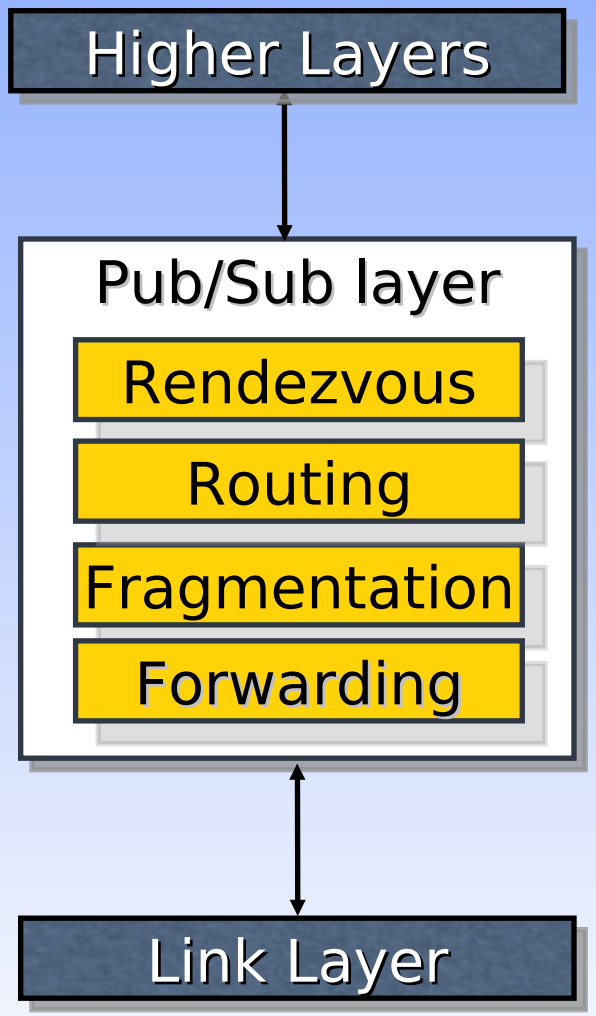
PLA: Wireless Authentication

- User authentication and roaming, especially useful in wireless networks, for example:
  - Network bootstrapping messages are protected by PLA. Base stations would check if the user is authorized by a trusted TTP (e.g. TKK's TTP)
  - Authentication is done at the bootstrapping phase. Afterwards, a symmetric session key can be used to secure further traffic.
  - No manual intervention, such as entering passwords or credit card information, is needed from users
  - No signalling to the external authentication server is necessary if the TTP is known by the base station

PSIRP (Publish/Subscribe Internet Routing Paradigm)

- We propose a future clean slate network design that
  - gives more **trust** and more **anonymity** to Internet
  - ensures network and data **availability**
  - ensures **rapid** and **accurate** dissemination of crucial information
- The **publish/subscribe** model
  - Subscribers and publishers
  - Many-to-many communication
  - End-points described in terms of data and local links
  - Incorporating support for end-point identification
    - Flat self-certifying labels
  - **Data-centric** routing, forwarding, rendezvous

PSIRP



Observations

No topological addresses, only labels

Security enhanced using self-certification

End-to-end reachability, control in the network

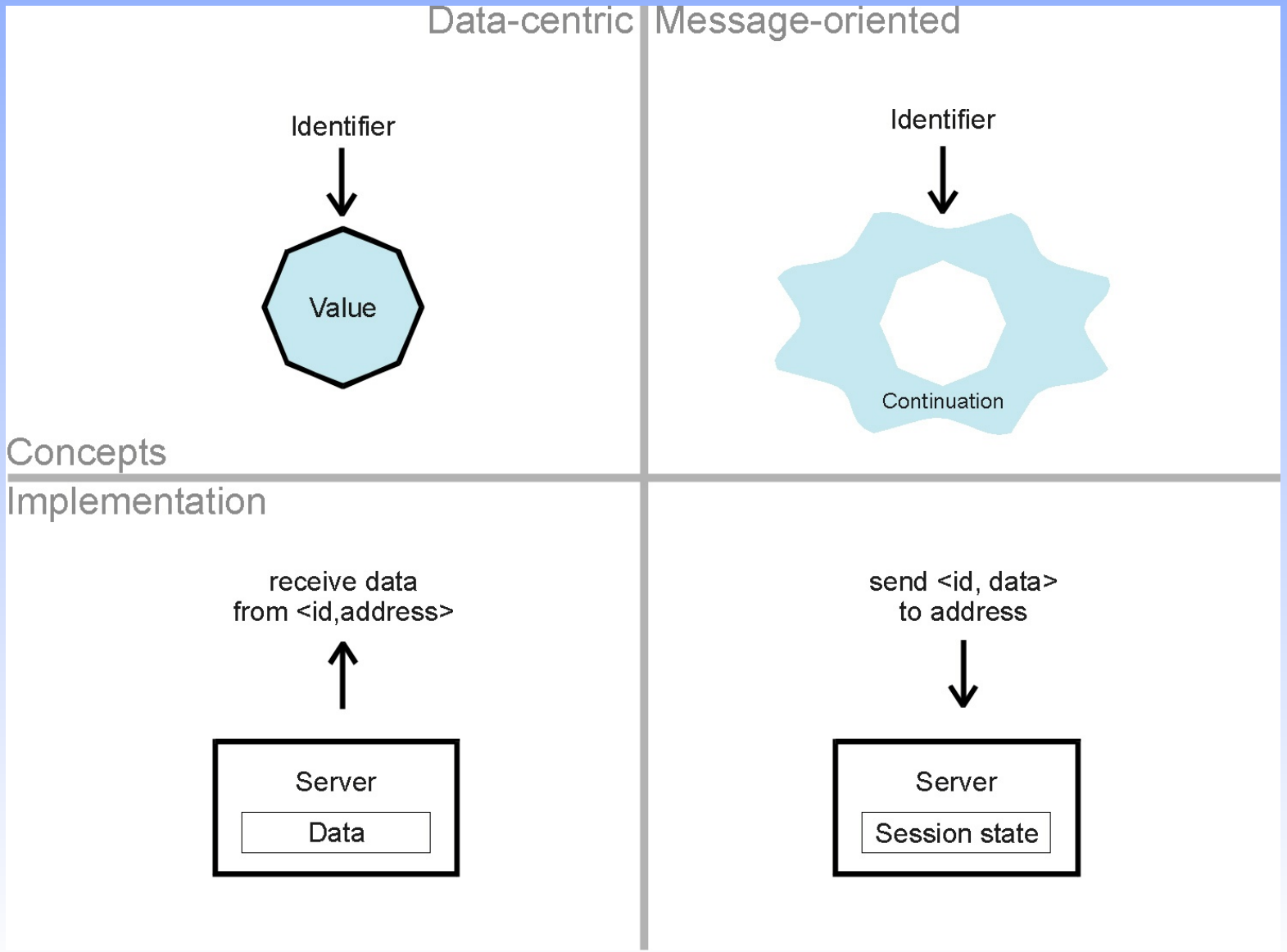
Natural support for multicast, it is the norm

Support for broadcast and all-optical label-switching technologies

Dynamic state is introduced into the network

How do we make it scale?

Data-centric publish/subscribe vs connections



Advantages of clean-state data-sentric routing

- Large amount of the current network traffic is already data-centric in nature (Youtube, P2P, software updates, etc.)
- A data-centric network layer would have many advantages:
  - Lower latency and higher efficiency because of caching
  - Native asynchronous multicast → efficiency, no flash crowd bottleneck
  - No unwanted traffic, since no data is transferred without an explicit request
- Peer-to-peer overlays have efficiency, incentive, and security problems
  - Often traffic does not go through the most efficient path
- Content delivery networks (CDNs) are also inflexible

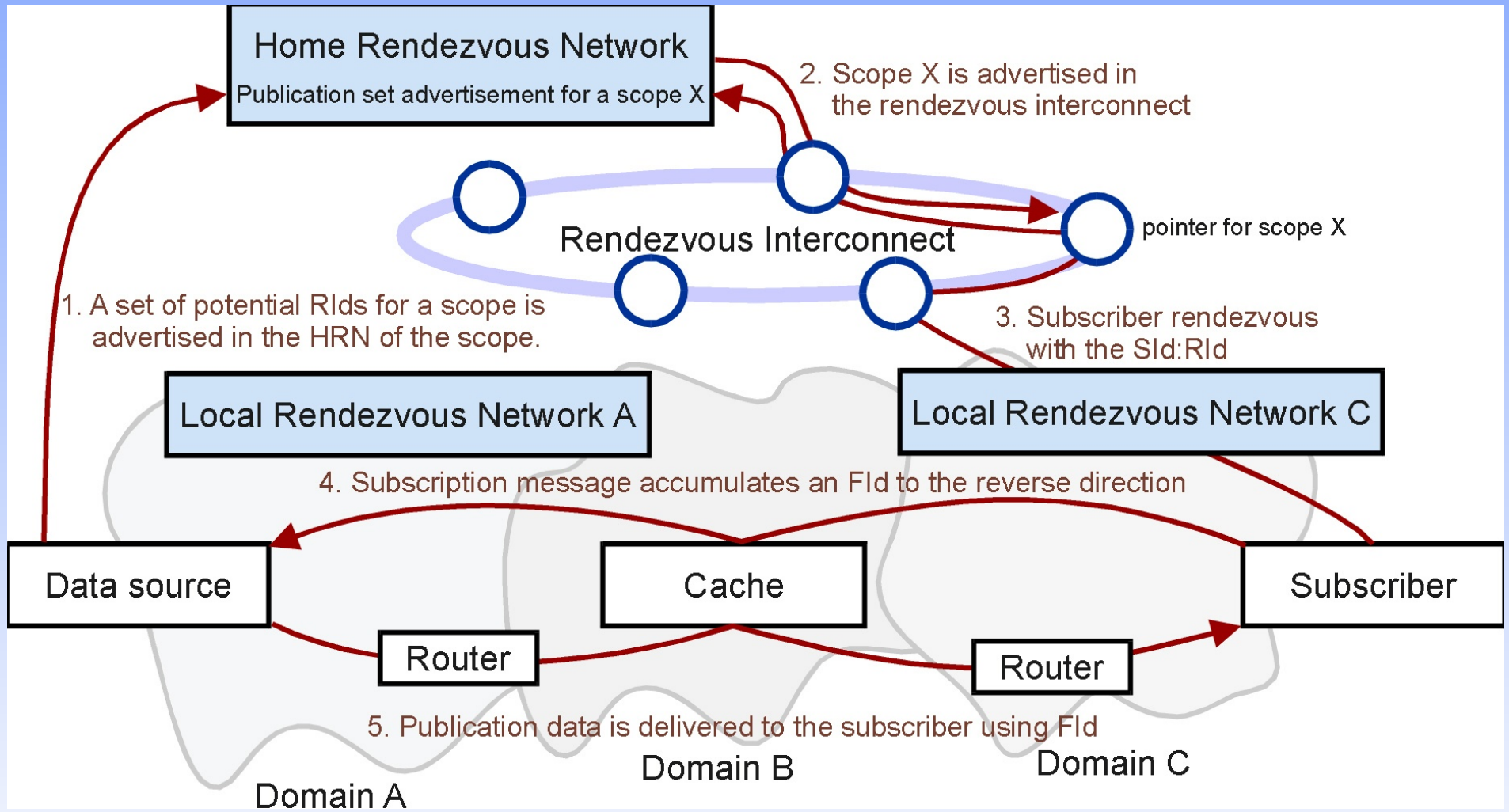
PSIRP: Concepts

- *Namespace owner* manages the namespace for publication identifiers, it also authorizes publishers to use part of the namespace for their publications.
- *Publisher* creates the actual publication, which is delivered to interested *subscribers*
- *Data source* host the actual publication data
- *Scopes* controls how publications are disseminated
- *Rendezvous system* acts as a middleman between publishers, subscribers and scopes

PSIRP: Identifiers

- PSIRP utilizes several types of identifiers
- On higher layers, application use Application identifiers (Aid)
- Publications are identified by Rendezvous identifiers (Rid) on the network layer, while scope identifiers (Sid) identify scopes
  - Publications are immutable
- Information is forwarded using forwarding identifiers (Fid)
- Rids and Sids utilize <P:L> structure, where the P is the namespace owner's public key, and L is the hash over some label
  - PSIRP utilizes ECC, therefore the whole public key can fit into a 256-bit Rid and Sid

PSIRP: Example flow



PSIRP: Forwarding

- PSIRP utilizes Bloom-filter based forwarding (zFilter)
  - Bloom filter is a probabilistic data structure, in which a simple *AND* operation can be used to test whether the element is present in a set
- Instead of naming nodes, links are named using Bloom filters
  - Paths are defined by using *OR* operations over multiple links
- Example: Link A: 0 0 1 0 0 1, B: 0 1 0 0 0 1, C: 1 0 0 0 0 0
  - Bloom filter: 1 1 0 0 0 1 would forward packet to both B and C, but not A
- No false negatives, but false positives are possible (packets are forwarded to unwanted destinations)

Summary

- PLA aims to bring availability on the network layer through cryptographic signatures
  - Malicious and unwanted traffic can be detected and dropped quickly
  - Strong network layer security mechanisms also benefit higher layer applications
- PSIRP is a clean-slate publish/subscribe based network architecture
  - Aims to solve problems of the current message-oriented Internet
  - Especially useful for data-oriented communication

Security and Trust

- We are going towards identity-based service access
  - A number of identities per host
  - Pseudonyms, privacy issues
  - Delegation and federation are needed
- Decentralization: the user has the freedom of choosing who manages identity and data
- Solutions for authentication
  - Below applications: HIP, PLA
  - Web-based standard (top-down)
    - ID-FF
  - Web-based practice (bottom-up)
    - OpenID and oAuth
  - Web services
    - SAML 2.0

Summary of Future Internet Developments

- Incremental using overlays and middleboxes
  - Short term solutions
  - HIP
  - Difficult to introduce new protocols
    - Connectivity and reachability problems
    - A lot of issues are solved in application layer
- Radical with clean-slate
  - Impossible to deploy?
  - Long haul development
  - PLA, PSIRP

Thank You