NPLA: Network Prefix Level Authentication

Ming Li,Yong Cui,Matti Siekkinen,Antti Ylä-Jääski
Aalto University, Finland
Tsinghua University, China

FutureNet III

IEEE 2010 GLOBECOM
GLOBAL COMMUNICATIONS CONFERENCE, EXHIBITION & INDUSTRY FORUM

Structure

- Motivation
- Objective
- Architecture overview
- Implementation
- Overhead
- Conclusion and future work

Motivation

- IP addresses spoofing
- Lack of accountability
- DoS, vulnerability scanning,...
- Ruin noval applications in practice
- ...

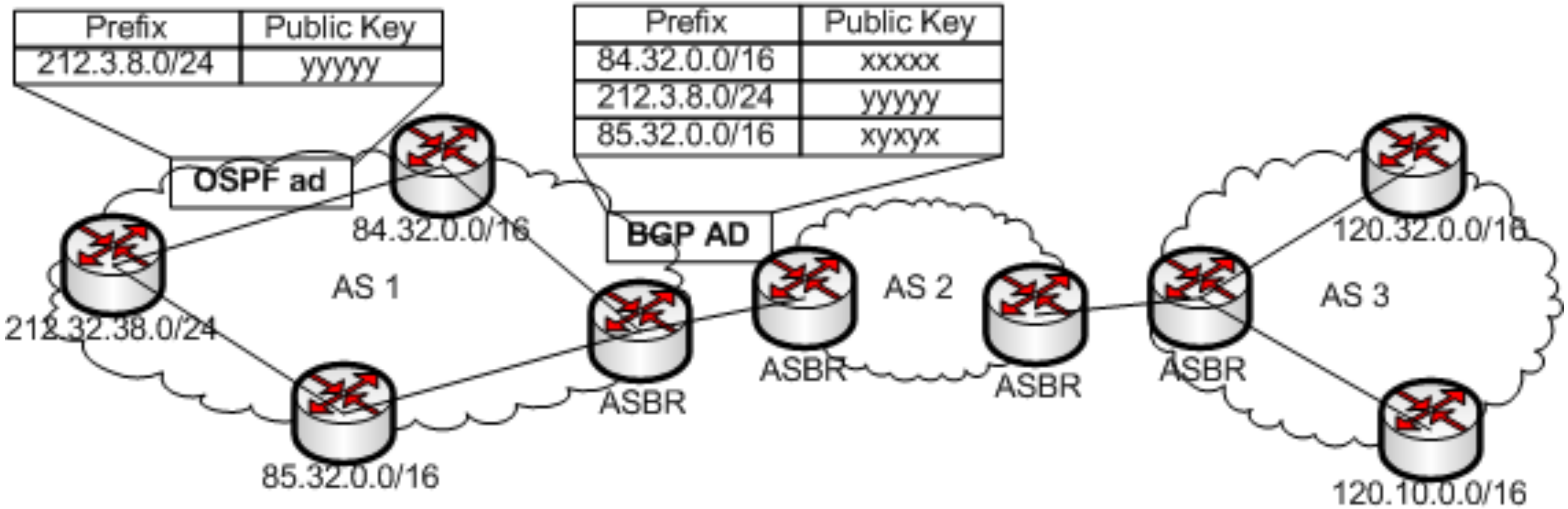
Objective

- Our Goal
  - Provide packet level authentication on the Internet
- Basic Approach
  - Digital signatures on packets

Objective

- Accountability is the responsibility for one's actions
  - Link actions to their actors
  - Punish misbehavior
- Packet Authentication
  - Eliminate/mitigate source spoofing based attacks
  - Target for existing Internet not clean slate solution

Architecture overview (NPLA)



Implementation

- How to implement if we intend to for partial deployment in today's Internet
  - What kind of key
  - Which protocol layer
  - Signature size
  - Crypt. security
  - Key distribution
  - Granularity
  - Inject/verify entities
  - Interact with legacy entities
    - Host, router, NAT, prefix aggregation...
  - Overhead
  - Effectiveness

Requirements->Implementation

- Strong identitifier/on route entities could verify the packets -> key type
  - ✓ Asymmetric key
- Compatibility -> protocol layer
  - ✓ Shim layer between IP and TCP

Requirements->Implementation...

- Key distribution
  - Public key infrastructure (PKI)
  - ✓ Routing protocols (BGP)
  - Offline
- Signature size and security
  - ✓ ECC public key cryptography algorithm
  - ✓ Security: 163-bit ECC key = 1024-bit RSA key

Requirements->Implementation...

- Security level/key management overhead -> authentication granularity
  - Host/personal level
  - ✓ Network prefix level (intra-domain)
  - AS level (inter-domain)
- Signature injection and verification entities
  - ✓ Prefix border router
  - ✓ AS border router

Requirements->Implementation

- Partial/incremental deployment, interact with legacy entities
  - Legacy host (strip off before arriving)
  - Router (compatible)
  - NAT (update)
  - Prefix aggregation (known to the administrator)
  - Incentive deployment
  - IP fragmentation

Overhead and performance

- The overhead must be affordable
- Computation overhead (FPGA crypt hardware)
  - Generate 645K/s and verify 283K/s signatures
  - Generate 3.8G/s and 1.7G/s traffic
- Traffic overhead (%6-10%)
- Memory overhead
  - 13MB for prefix level authentication

Overhead and Performance

- Delay
  - ~16us per generation
  - ~24us per verification

Conclusion and Future Work

- Authenticate packets to its claimed network prefix
- Implementation challenges
  - How to make it work in practice?
- Future work
  - Implementation in real networks