Accountable Internet Protocol (AIP)

David G. Andersen, Hari Balakrishnan,
Nick Feamster, Teemu Koponen,
Daekyeong Moon, and Scott Shenker

SIGCOMM'08

Presented by Gaspar Modelo-Howard

Outline

1. Introduction
2. AIP Design
3. Uses of Accountability
4. Routing Scalability with AIP
5. Key Management
6. Conclusion

1. Introduction

- The Internet is rife with vulnerabilities at the IP layer
  - Misconfigured routers disrupt packet delivery
  - Route spoofing
  - Denial of Service
  - Source addressing spoofing
- There is no shortage of proposed fixes. But often come with one or more problematic requirements
  - Complicated mechanisms
  - External sources of trust
  - Operator vigilance

1. Introduction

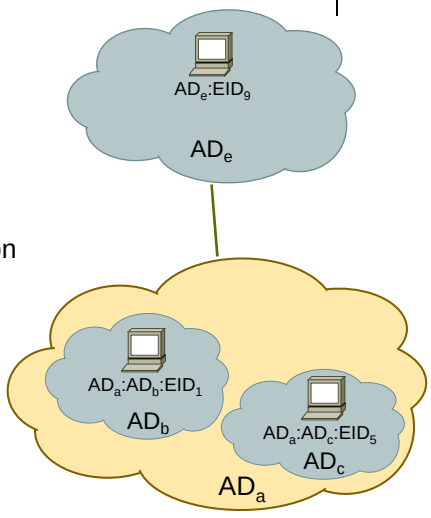
- **What changes to the architecture would provide a firmer foundation for IP-layer security?**
- Many of the vulnerabilities are due to lack of *accountability*
  - Internet has no fundamental ability to associate an action with the responsible entity
- Solution: replace IP with AIP

2. AIP Design

- Addressing structure: 2 or more levels of flat addressing
  - Closer to Internet's original incarnation than CIDR-based
  - Carefree attitude towards scaling
- Self-certifying addresses for domains and hosts
  - Includes imposter detection mechanisms to deal with key compromises
- Considers long-term technology trends

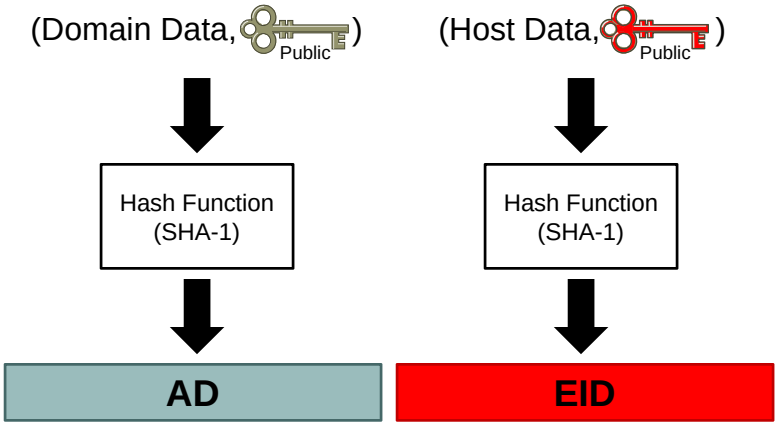
2. AIP Design

- Addressing structure:
  - Accountability domains (AD)
  - End-point identifier (EID)
- AD corresponds to BGP prefix
  - Allows hierarchical organization
- Self-certifying address
  - Name of object is public key (or hash) of object
  - AS is hash of public key of domain
  - EID is hash of public key of host



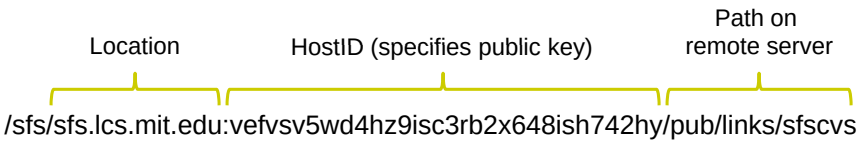
2. AIP Design

- Self-certifying addresses



Self-Certifying Addresses: An Example

- In [MAZ99]
  - No one controls the global namespace
  - HostID = SHA-1("HostInfo, *Location, Public Key,* "HostInfo, *Location, Public Key*)



[MAZ99]: Mazieres, D., et al. *Separating key management from file system security*. SOSP, 1999.

2. AIP Design

- Eliminates use of prefixes and CIDR-style addresses
- Returns to hierarchical addressing format

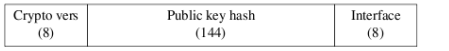


Figure 1: The structure of an AIP address. For AD addresses, the interface bits are set to zero.

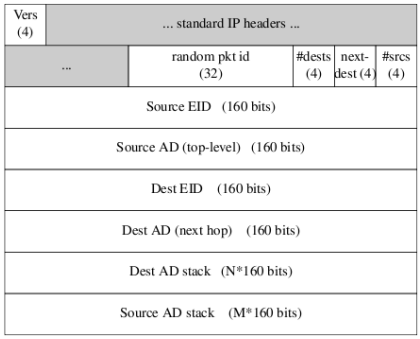


Figure 2: The AIP packet header.

Interaction with internetwork architecture: *Routing*

- Until packet reaches destination AD, intermediate routers use only destination AD to forward packet
- Upon reaching destination AD, forward based on EID
- BGP advertisements are for ADs
  - AIP routing tables map AD numbers to “next hop” locations
- Routers should also use interior routing protocol to maintain routes to EIDs
- AIP supports notion of autonomous system
  - Organizations might not want to advertise internal AD structure
  - BGP Path descriptors don’t have to include EIDs, also are 160-bit self-certifying AIP addresses

Interaction with internetwork architecture: *DNS and Mobility*

- DNS would include an AIP-record with AIP address(es) for each hostname in domain
- AIP requires a secure DNS variant to prevent unauthorized DNS modifications
- Mobility support based on self-certifying EID
  - Mobility transport protocols can bind to EIDs while hosts roam between ADs
  - Self-certificates allow for dynamic DNS update

3. Uses of Accountability: Source Accountability

- AIP mechanism extends “unicast reverse path forwarding” (uRPF)
  - Automatic filtering mechanism that accepts packets only if route to packet’s source address points to same interface on which packet arrived
  - Mechanism doesn’t require configuration or interaction by users
- Aims to protect against
  - Using spoofed address at which can’t received packets
  - Malicious host uses address at which can received packets
  - Address minting: ability to create large number of addresses for itself (attacker)

3. Uses of Accountability: Source Accountability

- Source address validation performed with AD and EID components
  - Each first-hop router verifies directly-connected hosts are not spoofing
  - Each AD thru which packet passes verifies previous hop is valid for specified source address

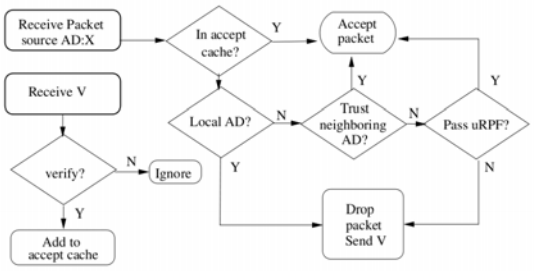


Figure 3: Process for verifying a packet's source address.

3. Uses of Accountability: Source Accountability

- R send packet *V* to S if it has not verified recently the source host
- Requires implementation in network switches or linked to some switch-level ARP security mechanism
- Routers bound size of *accept cache* by accepting AD-wildcards if threshold *T* is reached for particular AD

Let:

rs = Per-router secret, rotated once per minute

$\text{HMAC}_{\text{key}}\langle \text{M} \rangle$ = Message authentication code of M

$H\langle P \rangle$ = Hash of P

iface = Interface on which packet arrived

Source $S_{AD} : S_{EID} \rightarrow$ **Dest** $D_{AD} : D_{EID}$
Packet P.

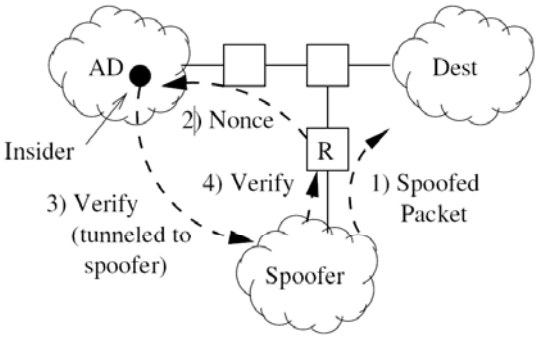
Router R1 $\rightarrow$ **Source**:
Verification packet V =
$\text{HMAC}_{rs}\langle S_{AD} : S_{EID} \rightarrow D_{AD} : D_{EID}, H\langle P \rangle, \text{iface} \rangle$

Source $\rightarrow$ **R1**:
$\{\text{accept}, K_{S_{EID}}, V\}_{K^{-1}_{S_{EID}}}$

Figure 4: Source address verification protocol.

3. Uses of Accountability: Source Accountability

- Protocol admits insider attack against source AD
  - Requires many compromised hosts to create *V*s and cause route to upgrade to wildcard entry
  - But DoS reflector attack can only be launched on "fully" compromised victim
  - Other remedies
    - Require AD domain signature on *V*
    - Router verification of interface on which *V* arrives



3. Uses of Accountability: Shut-off Protocol

Zombie → Victim: Packet P.

Victim → Zombie:
$\{\text{key} = K_{\text{victim EID}}, \text{TTL}, \text{hash} = H\langle P\rangle\}_{K^{-1}_{\text{victim EID}}}$

- Mechanism to throttle unwanted traffic
  - Victim sends explicit "shut-off" to sender
- Requires "smart-NIC" to suppress or rate-limit packet transmission
  - Accepts shut-off packets (SOPs) within 30 sec of packet tx'd
  - Records transmitted packet hashes using Bloom filter
- Requires out-of-band mechanisms to stop determined attackers to prevent
  - Firmware tampering thru physical security
  - Preemptive shut-off with SOPs at low rate
  - Replay prevention with 32-bit random packet ID
- Protocol should be disable for servers (tx: >50k pkts/seg)

3. Uses of Accountability: Securing BGP

- AIP could simplify task of deploying mechanisms similar to S-BGP
  - No need for external trusted registries (public keys)
- Uses mechanisms similar to S-BGP
  - Operators configure a BGP peering session
  - BGP routers sign their routing announcements
  - Each router must be able to find public key to corresponding AD

4. Routing Scalability with AIP

- Technology trends suggest that routing scalability with respect to memory consumption, CPU overhead, and network bandwidth are all manageable
- According to paper, neither the continued growth of Internet nor introduction of AIP should impose undue scaling burden
  - Based on industry (semiconductor, networking) growth trends studies
  - Crypto costs of AIP similar to those for S-BGP

5. Key Management

- As with any system relying on public key crypto, AIP faces three general problems:
  - Cryptographic algorithm compromise
    - Versioning address to support phasing new algorithms
    - Two or three crypto versions will be present on network st any given time
  - Key discovery
  - Individual key compromise

Key Discovery

- Key is automatically obtained once the address is known
  - Any (secure) lookup service could be used
  - Peering ADs can identify each other out-of-band for initial setup

Key Compromise

Protecting against compromise | Detecting compromise | Dealing with compromise

- First and third are relatively straightforward
  - Domains/hosts should follow established policies
  - Hardware solutions may assist
  - If host key is compromised, adopt new key and publish it into DNS record (might involve out-of-band mechanism)
  - If domain key is compromised, revoke it thru interdomain routing protocol and via public registries
    - Key revocation must propagate down every path that carries route for AD

Key Compromise

- How to detect when attacker is impersonating a victim? (stolen private key)
- Answer: maintain a public registry of peers for each AD and ADs to which each EID bound
- Registry only stores self-certifying data
  - No need for central authority to verify correctness of content
  - Registry can be populated mechanistically by entities involved (no operator vigilance)

Public Registry

- Principals can register various cryptographically signed assertions
- It exists per-domain, housed by ISPs
- Classes of assertions
  - Keys: $\{X,K_x\}$
  - Revoked keys: $\{K_x, \text{is\_revoked}\}K_x^{-1}$
  - Peerings: $\{A, K_A, B, K_B\}K_A^{-1}$ $\{A, K_A, B, K_B\}K_B^{-1}$
  - ADs of EID X: $\{A,X\}K_A^{-1}K_X^{-1}$
  - First hop router of X: $\{\text{Router}, X, MAC_X\}K_{router}^{-1}K_X^{-1}$

Public Registry

- Maintain the domain registry
  - Responsibility should lie with AD (not EIDs)
  - Should force domain to sign A : X entries before DNS servers accept them as result of DNS resolution
- Using the registries
  - Shared or used by both domains and hosts to check for compromise
  - Domain can recognize whenever an imposter has established a peering arrangement with some other domain
  - Host can recognize whenever an imposter has estalished itself in another domian or same domain

7. Conclusion

- AIP attempts to solve accountability requirement in network layer
- Enables solutions to source spoofing, (certain kinds of) DoS attacks, and secure BGP
- Possible concerns (route scalability, traffic engineering, key compromise) don't appear to be show-stoppers for AIP adoption

Are the security (accountability) requirements strong enough to convince parties involved to replace IP?

Questions

- Impact of AIP on protocols in the upper layers
- Study considers 2048-bit keys
- What would happen if we need to change the crypto algorithm?