Origin Authentication in Interdomain Routing

CSE598K/CSE545 - Advanced Network Security
Prof. McDaniel - Spring 2008
Interdomain routing …

• The internet consists of a large number of autonomous systems (ASes)
  › E.g., AT&T, Pennsylvania State University, …

• At the highest layer, the Internet routes from AS to AS, rather than from host to host
  › Scale
  › Policy
  › Resilience
BGP address use (refresher)

BGP UPDATE: AS 1 -> 192.168.27.0/24

192.168.27.1

1

BGP UPDATE: AS 1 -> 192.168.27.0/24
Problem Statement

• How do we ensure that addresses are associated with only those ASes that have the right to service (originate) them?

• This is a question of delegation and authentication or simply “Origin Authentication”

But first ....
Outline

• Delegation Semantics
• Cryptographic Proofs
• Current Address Delegation
• Approach Performance
• Future of Security
How is address space really delegated?

• Principally, address space is delegated to registries, then to ISPs, then to customers
• “Bellovin exception”: you went directly to IANA (now ICANN) to get address space
• How space was retrieved, by whom, when, and who owns it now is not very well documented
  ▸ Logistical nightmare to untangle
  ▸ Some are trying … (DHS folks, for example)
Address delegation

Diagram showing the delegation of address space from IANA to AT&T, ARIN, BETA, Modus, AS11521, and AS7018. The arrows indicate the direction of delegation and assignment of IP addresses.
Semantics: Preliminaries

• A prefix is: $y/k$
  
  Where $y = \{0,1\}^k$ and $k = \{0 \ldots g\}$, $g = 32$ for IPv4

• Other definitions
  
  $\text{ASN} = \{ 1 \ldots K \}$, where $K = 2^{16}$
  
  $O = \text{organizations, IANA, registries}$
  
  $\text{ASN}(C) = \text{set of ASes assigned to } C \in O$
Semantics: Delegation

An organization \( C \in O \) delegates/assigns \( y/k \) by

\[(C, y/k, C'), C' \in O, \text{ (organization delegation) or}
(C, y/k, n), n \in ASN \text{ (AS assignment) or}
(C, y/k, R), R \text{ (RESERVED) or}
(C, y/k, \bot), \bot \text{ (UNAUTHENTICATED)}\]

Note: Non-assignments have subtree semantics

Note: \( P(C) = \) delegations made by \( C \in O \)
Delegation Graph

A directed delegation graph $G = (V,E)$

Where $V = O \cup ASN \cup \{R\} \cup \{\perp\}$

$E = \{(x,y/k,z) \in P(O)\}$

Example:

- (IANA, 12.0.0.0/8, AT&T)
- (AT&T, 12.1.245.0/24, MODUS)
- (MODUS, 12.1.245.0/24, AS11521)
Validity

A delegation path for \( y/k \) is valid iff

a) The ownership source is IANA
b) Path is monotonic
c) Path is acyclic
d) Assignment edge is labeled \( y/k \) and is ASN respecting

\( C \in \mathcal{O} \) is faithful if no two \((x, y/k, z) \in \mathcal{P}(\mathcal{O})\) conflict.
Advertisement validation

• Assume we know the delegation graph for the Internet (or at least enough of it)

• Address validation algorithm:
  ‣ Check the validity of the delegation path
  ‣ Check faithfulness of all $C \in O$ on path

• Q: How do we securely and efficiently validate these properties?
Authenticated delegation graph?

- **Attestations** are proofs of edges in the graph
  - In-band: S-BGP [Kent et. al.]
  - Out-of-band: IRV [McDaniel et. al.]
  - ID model: soBGP [Weis et. al.]

- **Assumption**: certificate infrastructure (PKI)

- **Origin Authentication Tags (OAT)**
  - Proof of AS ownership (Origin <-> ASN map)
  - Collection of delegation proofs (path)
    - We are concerned with the latter
Simple Delegation

• Signed delegation

\[ \{(C, \ y/k, x)\}_{S(C)} \]

• Where \( S(C) \) is the signature using the private key associated with of \( C \)‘s well known public key certificate

• A proof is generated by \( C \) for each prefix delegation
Authenticated Delegation List

- Each $C$ signs a single statement of all delegations and assignments it makes

\[
\{ (C, y/k, x_1),
(C, y/k, x_2), \ldots
(C, y/k, x_m) \} \subseteq (C)
\]

- An **AS Authenticated Delegation List** creates a list of all delegations (assignments) made to a single organization or registry (AS)
Authenticated Delegation Tree

- Merkle hash tree (Hash function $H$)

- Proof: root and siblings on path to root

- $((C, y/k, x_1) : \{H(L_{12}, R_{34})\}_{S(C)}, H(L_3, R_4), (C, y/k, x_2))$
Authenticated Del. Dictionaries

- 2-3 tree with Merkle hashing

\[ H(L, M, R) \]

\[ H(proof) \]

\[ H(proof_1|proof_2) \]

- Advantage: attestations and faithfulness proofs
Current Address Delegation

- What does the delegation graph look like?
  - How are addresses used?
  - How many delegators?
  - How many delegations?
  - How are delegations distributed?
  - How stable is the IP address delegation graph?
Address Usage

- 0.0.0.0
- 12.0.0.0/8 (AT&T)
- 128.0.0.0/2 (128.0.0.0-191.255.255.255)
- 255.255.255.255
Address Usage

- **Multicast**: 224.0.0.0/4
  - Reserved
  - Assigned but unadvertised (publicly)
- **Class E (experimental)**: 240.*-255.*
Approximating the IPv4 Delegation Graph

- Sources: IANA, BGP updates
- (bgpaddr) approximate delegation graph by looking at who is advertising addresses
  - Assumption: delegation artifacts are present in BGP updates
  - E.g., AT&T 12.0.0.0/8 -> 923 prefixes by other ASes
  - Tie addresses to organizations at root at all nodes in the tree, add AS delegation
Approximation Example

12.1.2050.0824

UPDATES
Prefix    | ASN
----------|----
12.0.0.0/8 | 7018
12.1.83.0/24 | 14787
12.1.96.0/24 | 23306
12.1.226.80/29 | 2386
12.1.241.128/26 | 2386
12.1.245.0/24 | 11521
Findings

- 1 RIB 14,912 ASes, 129,731 prefixes
- 2,112 out of 14,912 are delegators (14.1%)
More findings

- **Very** dense
  - 16 organizations do 80% of the delegation
  - 122 organizations do 90% of the delegation
  - 1220 organizations do 99% of the delegation

- Factoid: big delegators
  - ARIN (30%), Various (15%), APNIC (12%), RIPE NCC (8%), RIPE (4%), LACNIC (3%), AT&T (2%), UUNET (1%), ARIN Cable (1%), Sprint (1%)
## Delegation Stability

<table>
<thead>
<tr>
<th>Class</th>
<th>Jan-May 03 (max)</th>
<th>Jan-May 03 (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stable</td>
<td>128350 (89.6%)</td>
<td>103397 (72%)</td>
</tr>
<tr>
<td>Added</td>
<td>6977 (4.8%)</td>
<td>19001 (13.2%)</td>
</tr>
<tr>
<td>Removed</td>
<td>7052 (4.9%)</td>
<td>15770 (11.0%)</td>
</tr>
<tr>
<td>Moved</td>
<td>836 (0.5%)</td>
<td>5047 (3.5%)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>143215</strong></td>
<td><strong>143215</strong></td>
</tr>
</tbody>
</table>
Evaluation

• OK, swell, but is real time OA realistic?
Evaluation: trace-based sim

- **OASIM**: origin authentication tool
  - Simulates BGP speaker
  - Reads time-stamped traces of BGP updates
  - Calculates bandwidth, computational costs

- **Dataset**
  - Traces obtained from RouteViews
  - 24 hour period on April 2nd, 2003
  - Approximated delegation graph

- **Q**: How does OA perform on the Internet?
Computational Costs

many attestations from same org/AS
Origin Authentication

- Origin authentication issue for interdomain routing
- Formalization establish address semantics
  - Generalize address delegation as proof system
- Delegation study
  - Dense (16 orgs delegate 80% address space)
  - Static (10-30% movement in 5 Months)
- Consider OA approaches performance
  - Tree-based proof systems has best computation/bandwidth trade-offs