How Secure are Secure Internet Routing Protocols?

Sharon Goldberg
Boston University

Michael Schapira
Princeton

Pete Hummon
AT&T

Jennifer Rexford
Princeton
How Secure is Internet Routing Today? (1)
April 2010: China Telecom intercepts traffic

This packet is destined for Verizon.

I am Verizon
69.82.0.0/15
(and 50k other IP prefixes)

Verizon
69.82.0.0/15

London Internet Exchange

China telecom

‘The Internet’

UK ISP
February 2008: Pakistan Telecom hijacks Youtube.
How Secure is Routing on the Internet Today? (4)

Here’s what should have happened....

“The Internet”

Drop packets going to YouTube

IP 208.65.153.0 / 22

I’m YouTube: IP 208.65.153.0 / 22

Block your own customers.
How Secure is Routing on the Internet Today? (5)

But here’s what Pakistan ended up doing...

“The Internet”

Pakistan Telecom

I’m YouTube: IP 208.65.153.0 / 22

No, I’m YouTube! IP 208.65.153.0 / 24

Draw traffic from the entire Internet!
Today, Internet routing is surprisingly insecure
• Decade of research on secure routing protocols
• With RPKI we can finally consider deploying one.

Our Goal: Compare the effectiveness of these protocols.
• Each has a different set of security properties.
• How well do they prevent attacks?

Our approach: Evaluate via simulation on network data.
• Data: Map of Internet & business relationships
• … from [CAIDA] and [UCLA Cyclops]
• To compare protocols, we must find worst-case attacks
This talk

Pakistan Telecom hijacks YouTube

How Internet Routing Works
(and why economics matter)

Secure Routing Protocols and Attacks

Theory Interlude

Results!

Implications & Deployment Challenges
A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.

The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.
The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses. A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
The Border Gateway Protocol (BGP) sets up paths from Autonomous Systems (ASes) to destination IP addresses.

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.
This talk

Pakistan Telecom hijacks YouTube

How Internet Routing Works
(and why economics matter)

Secure Routing Protocols and Attacks

Theory Interlude

Results!

Implications & Deployment Challenges
Traffic Attraction Attacks on:

BGP
Origin Authentication
Secure Origin BGP
Secure BGP
Defensive Filtering
Traffic Attraction Attacks on BGP

Attacker wants max number of ASes to route thru its network. (For eavesdropping, dropping, tampering, …)

Simulations show he attracts 62% of ASes!

A model of routing decisions:
- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.
Proposed Security Mechanism: Origin Authentication

RPKI: A secure database that maps IP Prefixes to owner ASes.

Simulations show he attracts 58% of ASes!

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors.
**Proposed Security Mechanism:** secure origin BGP

**RPKI:** A secure database that maps IP Prefixes to owner ASes.

**soBGP:** A database of all the links in the AS-level topology.

---

**Smart Attack Strategy:** Announce the shortest path I can get away with to all my neighbors.
Proposed Security Mechanism: “Secure BGP” [KLS98]

Secure BGP:
Cannot announce a path that was not announced to you.

Origin Authentication +

Public Key Signature
Anyone who knows v’s public key can verify that the message was sent by v.
Are attacks still possible with Secure BGP? (1)

**Smart Attack Strategy:** Announce the shortest path I can get away with to all my neighbors!
Are attacks still possible with Secure BGP? (2)

**Smart Attack Strategy:** Announce the shortest path I can get away with to all my neighbors!
Are attacks still possible with **Secure BGP?** (3)

**Smart Attack Strategy:** Announce the shortest path I can get away with to all my neighbors!

Simulations show he attracts 16% of ASes!
Wait! Why is this an “attack”? 

**Smart Attack Strategy:** Announce the shortest path I can get away with to all my neighbors!

A stub is an AS with no customers. A stub should only announce paths to its own prefixes.
Security Mechanism: **Defensive Filtering (of Stubs)**

**Defensive Filtering:** The provider drops announcements for prefixes not owned by its stubs.

Defensive filtering thwarts all attacks by stubs!

In the data, **85%** of Ases are stubs.
This talk

Pakistan Telecom hijacks YouTube

How Internet Routing Works
(and why economics matter)

Secure Routing Protocols and Attacks

Theory Interlude

Results!

Implications & Deployment Challenges
Wait! Is this the “best” attack strategy?!?

Can’t lie about my business relationship with a2, so I might as well announce the shortest path I can.

But Not Optimal!

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Sometimes announcing to fewer neighbors is better!

Sometimes longer paths are better!

Theorem: It’s NP hard to find the optimal attack strategy.

Smart Attack Strategy underestimates damage.
Sometimes longer paths are better?!?

Announce 3-hop path to a2, a3: 16% of ASes
Announce 4-hop path to a1: 56% of ASes
Attack on insecure BGP: 62% of ASes

Key Observation: Who you announce to is as important as what you announce.
This talk

Pakistan Telecom hijacks YouTube

How Internet Routing Works
(and why economics matter)

Secure Routing Protocols and Attacks

Theory Interlude

Results!

Implications & Deployment Challenges
We ran multiple experiments

- For each, randomly chose (attacker, victim) pair, and
- … simulate Smart Attack on each security protocol.

In the following graph:

- An attacker is “successful” if it attracts 10% of ASes.
- What fraction of pairs have a successful attacker?
Probability* Smart Attack attracts 10% of ASes

*Probability is taken over random choice of attacker and victim.

Recall that the Smart Attack Strategy underestimates damage.
Probability* **Smart Attack** attracts >x% of ASes (1)

*Probability is taken over random choice of attacker and victim.

Recall that the **Smart Attack Strategy** underestimates damage.

Recall that 15% of Ases are not stubs!
Probability* Smart Attack attracts $>x\%$ of ASes (2)

- Probability is taken over random choice of attacker and victim.
- Recall that the **Smart Attack Strategy underestimates** damage.

> UCLA Cyclops Nov 20, 2009

> 15% of ASes are not stubs!
The Importance of Aggressive Export Policies

Probability* of Attracting >x% of the Internet

*Probability is over random victim and attacker with > 25 customers.

Key Observation: Who you announce to is as important as what you announce.
Tier 2’s are the most effective attackers

Probability* of Attracting \( >x\% \) of the Internet Attack on BGP (i.e. Originate victim prefix to all neighbors)

*Probability is over random victim and attacker from different classes
Pakistan Telecom hijacks YouTube

How Internet Routing Works
(and why economics matter)

Secure Routing Protocols and Attacks

Theory Interlude

Results!

Implications & Deployment Challenges
WHO you announce to is as important as WHAT you announce

Defensive filtering is as effective as Secure BGP.

• Each mitigates a different attack strategy
• Secure BGP limits path-shortening attacks
• Filtering prevent stubs from announcing paths too widely

Why is it so hard to implement these things in practice?
Implementing **Defensive Filtering**?

**Today:** The provider locally keeps a list of the prefixes that its stubs own.

**Issues:**
1) Relies on altruism & trust.
2) Maintaining prefix lists is hard.

**But, some good news:**

**Origin Authentication:** A secure database that maps IP Prefixes to their owner ASes.

(For past few months?) prefix lists can be derived from RPKI!
What if only large ASes implement prefix lists? (1)

CAIDA Nov 20, 2009

If ISPs with > 10 customers filter, 56% of attacks stopped.
What if only large ASes implement prefix lists? (2)

If ISPs with > 10 customers filter, 55% of attacks stopped.