Issues in Routing Security

Steven M. Bellovin
http://www.cs.columbia.edu/~smb
Columbia University

March 24, 2008

Introduction

What is Routing Security?

- Bad guys play games with routing protocols.
- Traffic is diverted.
  - Enemy can see the traffic.
  - Enemy can perform traffic analysis.
  - Enemy can easily modify the traffic.
  - Enemy can drop the traffic.
  - Enemy can steal prefixes
- End-to-end cryptography can mitigate the effects, but not stop them.

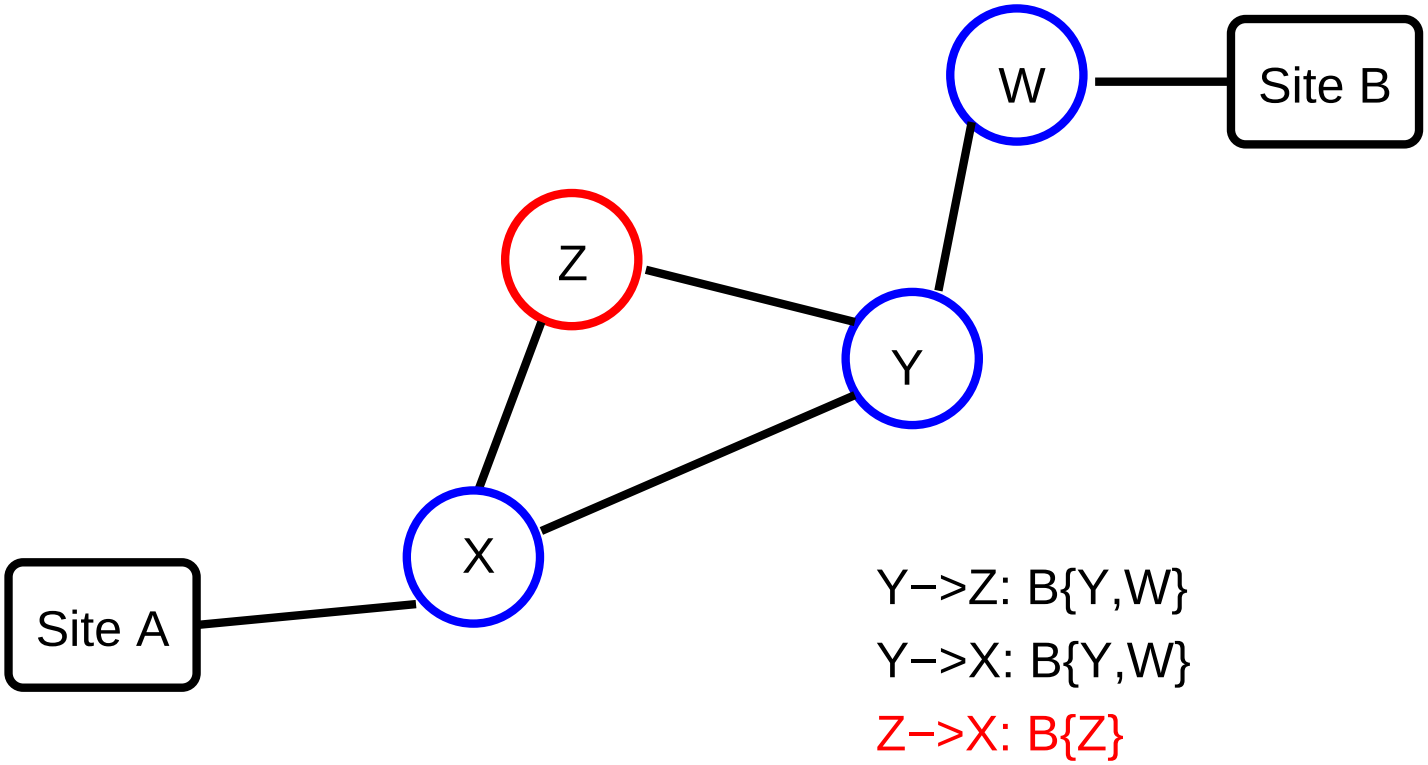
Why is this Threat Different?

- Most communications security failures happen because of buggy code or broken protocols.
- Routing security failures happen despite good code and functioning protocols. The problem is a dishonest participant.
- Hop-by-hop authentication isn't sufficient.

The Attack

- The attacker generates a false advertisement: an improper prefix, a fake AS path, etc.
- The false advertisement has a lower metric for that prefix than the legitimate path
- The victim believes the fake path instead of the legitimate one, and routes some traffic towards the attacker
- To reinject traffic — after inspecting or modifying it — set up a tunnel to somewhere close enough to the victim that it isn't affected by the fake route

The Attack



Z is lying, so the path through it looks shorter.

Who's Launching Routing Attacks?

- Spammers (though they've mostly switched to bots of late)
- DoSers — vandals, extortionists, etc.
- Industrial spies
- Governments
- Sometimes it happens by accident

Spying on or Modifying Traffic

- A lot of traffic that should be encrypted isn't
- Most secure web pages are invoked via links from unprotected pages
- The attacker can modify these — think phishing on steroids
- (Who checks certificates?)
- Most email isn't encrypted

Denial of Service

- Attract traffic, but don't forward it
- Better yet, forward most but not all of it
- Selectively drop TCP packets to slow things down
- Selectively drop DNS packets
- But pings and traceroutes will show that everything looks fine

Stealing Prefixes

- Connect to a clueless ISP
- Claim you have PI space
- Start using your stolen (or black market, or abandoned) prefixes
- Will someone three hops upstream check the routing registry?

Traffic Analysis

- See who is talking to whom
- Monitor connection length
- Doesn't look at (possibly encrypted) content
- Frequently used by law enforcement and intelligence agencies
- Very hard to disguise

History

Earliest Mentions

- Radia Perlman's dissertation: *Network Layer Protocols with Byzantine Robustness*, 1988.
- Gregory Finn, *Reducing the Vulnerability of Dynamic Computer Networks*, 1988.
- Steve Bellovin, "Security Security Problems in the TCP/IP Protocol Suite", 1989.
- Accidental routing problems were what got me interested in Internet security in the first place...

Defenses

- A few early attempts in the mid-1990s
- Notable effort: RFC 2154 (Murphy, Badger, and Wellington), 1997.
- Not taken seriously by most

The Interdomain Case

- AS 7007
- AT&T Worldnet taken off the air by a routing error in 1999
- National Academies report *Trust in Cyberspace* called routing one of the two ways to take down the Internet
- Pakistan Telecom versus YouTube
- Kenya versus Above.net

Current Status

NanoBGP Tutorial

- An *Autonomous System* (AS) x emits a $\langle\{\mathrm{AS}_x\}, \text{prefix}\rangle$ sequence
- Neighboring AS hop y applies *policy* to decide which advertisements to accept or forward
- It prepends its AS# and emit $\langle\{\mathrm{AS}_y, \mathrm{AS}_x\}, \text{prefix}\rangle$
- AS z emits $\langle\{\mathrm{AS}_z, \mathrm{AS}_y, \mathrm{AS}_x\}, \text{prefix}\rangle$
- AS path length is one possible policy to apply

Securing BGP

- IRR
- SBGP (Kent et al.), 2000
- soBGP (Ng et al.), 2002
- Many more proposals since then

Internet Routing Registry

- Register your prefixes
- Register your policies
- Filter incoming announcements against their policies and what you know
- Strictly local; doesn't deal with corruption from more than one hop away

SBGP: Oversimplified Design

- Digitally sign advertisements
- Receiving AS hops sign the entire signed path
- AS x emits a signed statement of the path it announces to neighbor y:

$$\boxed{\langle \mathrm{AS}_x, \mathrm{prefix}, y \rangle}_x$$

- AS y sends to AS z:

$$\boxed{\langle \mathrm{AS}_y, \boxed{\langle \mathrm{AS}_x, \mathrm{prefix}, y \rangle}_x, z \rangle}_y$$

- Many signatures, many verifications

More Details

- Each AS has a certificate for its AS #
- Each AS has a certificate for each of its prefixes
- Prefix certificates can be obtained from an RIR or an upstream AS that delegated address space

soBGP: Secure Origin BGP

- Originating AS signs the prefix origination message:

$$\boxed{\langle \mathrm{AS}_x, \mathrm{prefix} \rangle}_x$$

- Policy certificates describe connectivity policies
- Subsequent hops are not signed:

$$\mathrm{AS}_z, \mathrm{AS}_y, \boxed{\langle \mathrm{AS}_x, \mathrm{prefix} \rangle}_x$$

- Fewer signatures and verifications; weaker protection

Many Other Proposals

- Neither SBGP nor soBGP has been accepted by the ISPs
- Cost and deployability are among the reasons
- Many other proposals have been published
- None of these have gained much support, either

Issues

Issues

- Capital cost
- Operational cost
- Deployability
- Expertise needed
- Failure modes
- Data cleanliness
- Operability

Capital Cost

- Routers will need to be upgraded to support any of these schemes
- Some (especially SBGP) will require crypto accelerators
- New servers and databases must exist

Operational Cost

- Each RIR must run a CA to assign prefixes
- Each ISP must run a CA to delegate prefixes
- Both must run a 24×7 help desk to handle certificate issues

Deployability

- What is the incentive for deployment?
- How do we deal with partial deployment, within an AS or between ASs?
- How can an upgraded router tell that a path should have been protected?
- When do we start reaping the benefits?

Expertise Needed

- This is a new function for RIRs and ISPs
- Do they have the staff that understands the issues?
- Is their staff trained to deal with failures in a security mechanism?

Failure Modes

- If a secured BGP message fails authentication or authorization checks, the announcement *must* be discarded
- Failure modes include expired certificates or bogus CRL entries
- Neighboring ISP can't simply accept the bad data; the next hop will discard it
- Securing BGP creates new ways to kick someone off the net
- (Might certificates be revoked for political reasons? Think `www.ciaocuba.com` and `www.fitnathemovie.com`)

Data Cleanliness and PKI

- All proposals require authoritative knowledge of who owns which prefixes and AS #s
- Do we have such knowledge, especially for "swamp" space?
- Who is authoritative? A hierarchical PKI? With what root?
- Web of trust? What about collusion? Who owns which AS?

CS @CU

Operability

- Is the cost of any such solution greater or less than the cost of cleaning up after occasional mistakes and attacks?
- Will security-induced denial of service accidents impact more or fewer users than accidental or intentional prefix hijacks?
- Is securing BGP a net benefit to the Internet, the ISPs, and the users?