

# Routing Security Economics

Steven M. Bellovin

<http://www.cs.columbia.edu/~smb>

Columbia University

January 18, 2007

# What is Routing Security?

## What is Routing Security?

How is it Different?

Lying Routers

Problems Caused

Costs

Cost of Defenses

Deaggregation

Economic Choices

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

# How is it Different?

What is Routing Security?

How is it Different?

Lying Routers

Problems Caused

Costs

Cost of Defenses

Deaggregation

Economic Choices

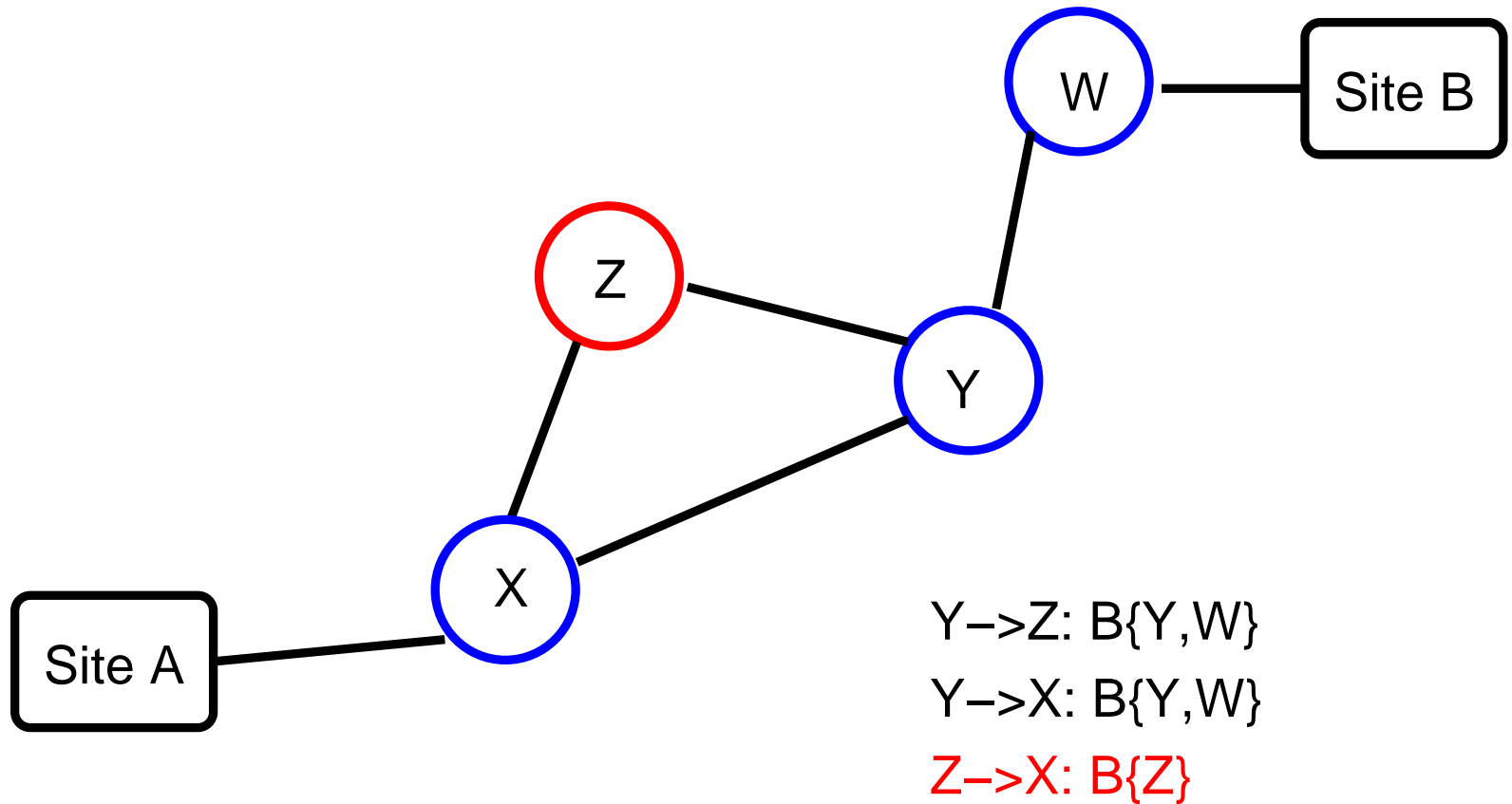
- Most communications security failures happen because of buggy code or broken protocols.
- Routing security failures happen despite good code and functioning protocols. The problem is a dishonest participant.
- Hop-by-hop authentication isn't sufficient.

# Lying Routers

What is Routing Security?  
How is it Different?

## Lying Routers

Problems Caused  
Costs  
Cost of Defenses  
Deaggregation  
Economic Choices



# Problems Caused

What is Routing

Security?

How is it Different?

Lying Routers

Problems Caused

Costs

Cost of Defenses

Deaggregation

Economic Choices

- Reachability
- Spoofing
- Denial of service
- Spam or other attacks
- Traffic analysis

- Cost of dealing with the attacks (what is traffic privacy worth?)
- Cost of clean-up
- Cost of route advertisement filtering

# Cost of Defenses

- All proposed defenses involve lots of cryptography, and frequently public key cryptography
- This implies capital expenditures for router upgrades: memory, CPU power, modular exponentiation hardware, etc.
- Most Internet users get IP address ranges from their ISPs; this means that ISPs need to
  1. Obtain certificates for their own address ranges
  2. Operate (or outsource) a CA and help desk to issue address-based certificates to their customers

# Deaggregation

- Routers use a “longest prefix” match to select a routing table entry
- Some sites are advertising redundant, longer prefixes to forestall (inadvertent?) attacks
- Example: AT&T currently advertises 12.0.0.0/8, 12.0.0.0/9, and 12.128.0.0/9
- Result: three RIB entries instead of one; more importantly, two FIB entries instead of one (Note: this was the direct consequence of a routing incident in 2005.)
- What if they need to switch to 256 /16s? (Some of that already for traffic engineering and multihoming.)



**Do nothing** Continue to absorb the cost of attacks — low thus far, except for spam, but the spammers currently favor botnets.

**Full-scale crypto** ISPs spend a lot — can they recover their costs? None of the proposed solutions provide economic incentives for early adopters. (Of course, without ISP demand, vendors haven't built any hardware.)

**Deaggregation** The cost of deaggregating is low for the originator, but it increases everyone else's costs. Furthermore, we are seeing increasing pressure on router FIB sizes for other reasons.