Routing Threats

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

April 10, 2006

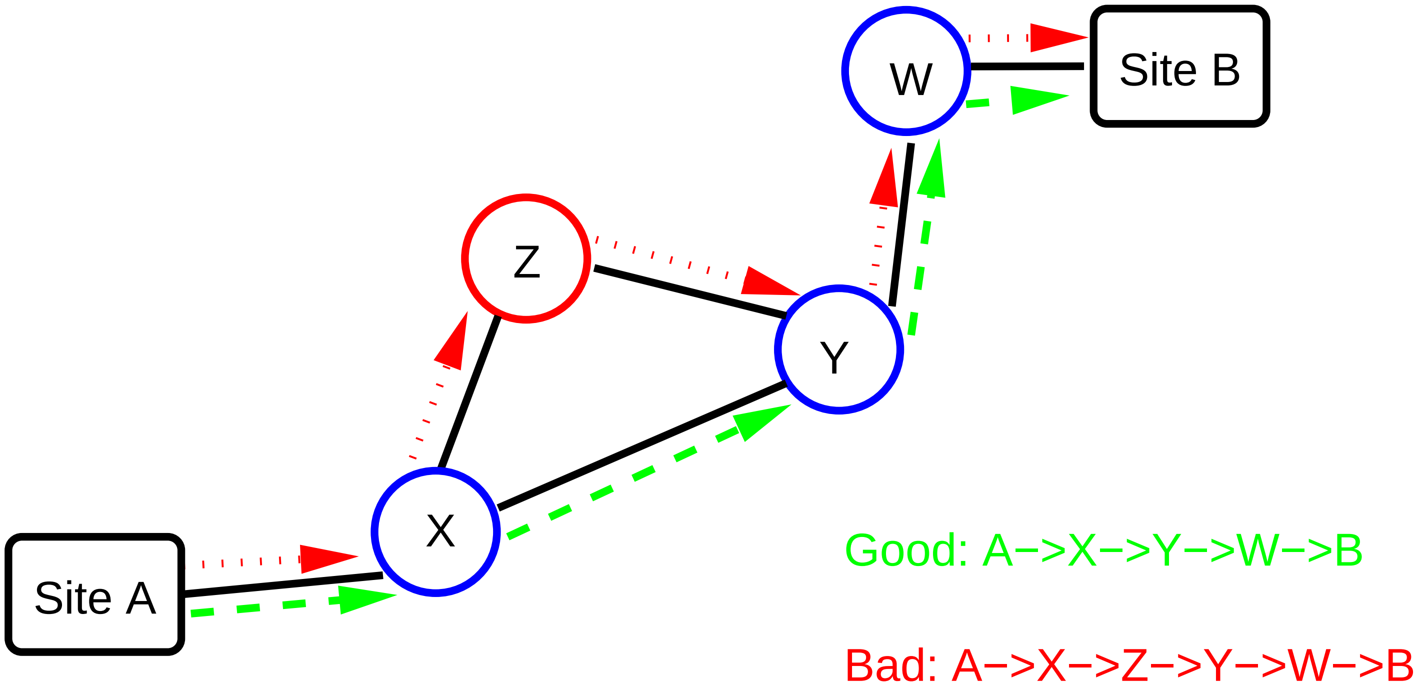
What is Routing Security?

- 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.
  - 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 Enemy's Goal?

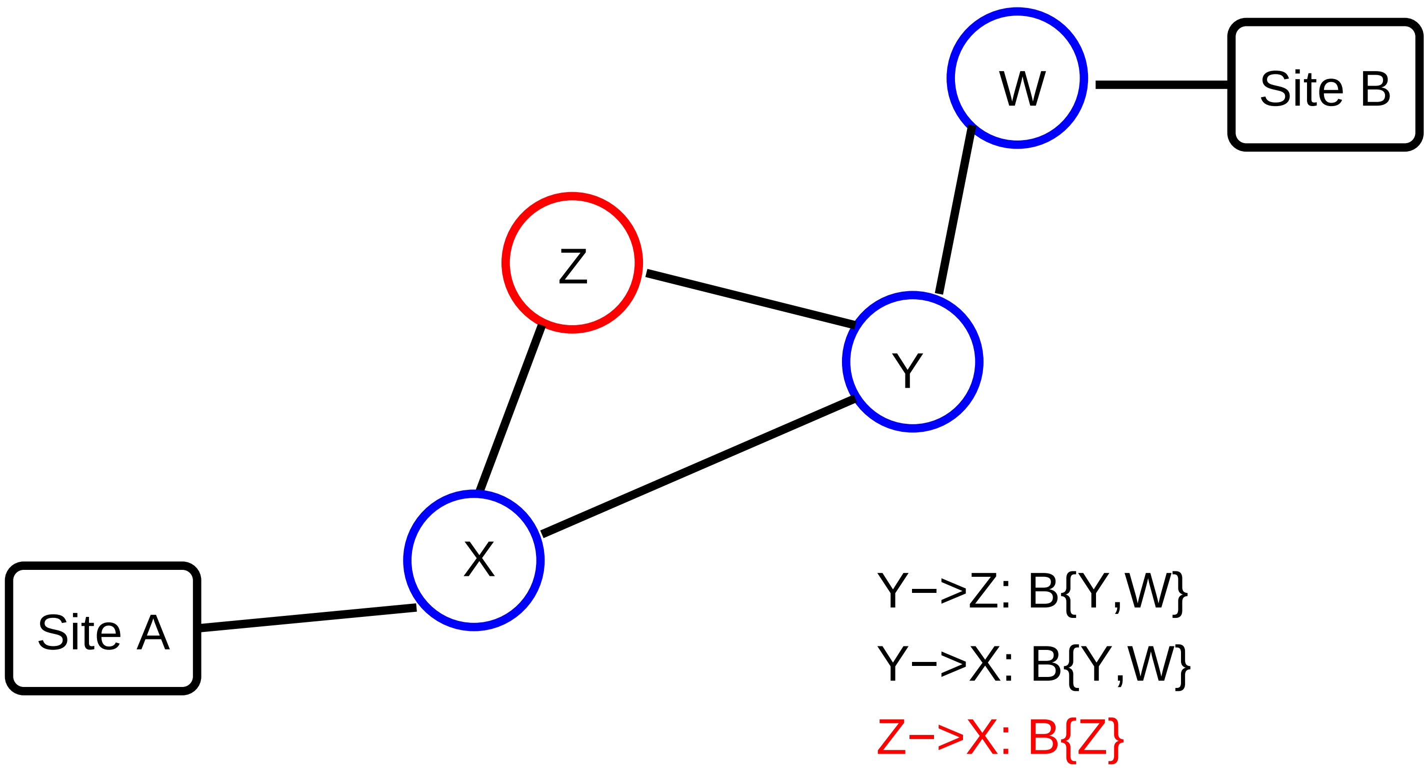


But how can this happen?

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.

Why is the Problem Hard?

- X has no knowledge of Z's real connectivity.
- Even Y has no such knowledge.
- The problem isn't the link from X to Z; the problem is the information being sent. (Note that Z might be deceived by some other neighbor Q.)

CS@CU

Who's Launching Routing Attacks?

- Spammers (though they've mostly switched to bots of late)
- DoSers — vandals, extortionists, etc.
- Industrial spies
- How to phrase this? Umm, "Others"

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?

If We Don't Fix Routing?

- We will see more attacks
- As other attack vectors are closed, the bad guys will pay more attention to routing
- Anyone not using end-to-end encryption will be susceptible to eavesdropping and/or packet modification
- Everyone will be vulnerable to highly-tunable denial of service

Fixing the Problem

- We need digital signatures, to permit verification of a message without knowing a secret
- We need certificates, to bind resources — AS numbers and prefixes — to public keys
- Many details, but all solutions must rest on those two points