Routing Protocol Security
CS 239
Advanced Topics in Network Security
Peter Reiher
April 12, 2004

The Problem

- Routing protocols control how packets flow through the Internet
- If they aren't protected, attackers can alter packet flows at their whim
- Most routing protocols were not built with security in mind

Routing Protocol Security Threats

- Threats to routing data secrecy
  - Usually not critical
- Threats to routing protocol integrity
  - Very important, since tampering with routing integrity can be bad
- Threats to routing protocol availability
  - Potential to disrupt Internet service

What Could Really Go Wrong?

- Packets could be routed through an attacker
- Packets could be dropped
  - Routing loops, blackhole routing, etc.
- Some users' service could be degraded
- The Internet 's overall effectiveness could be degraded
  - Slow response to failures
  - Total overload of some links
- Many types of defenses against other attacks presume correct routing

Where Does the Threat Occur?

- At routers, mostly
- Most routers are well-protected
  - But . . .
  - Several recent vulnerabilities have been found in routers
- Also, should we always trust those running routers?

Different Types of Routing Protocols

- Link state
  - Tell everyone the state of your links
- Distance vector
  - Tell nodes how far away things are
- Path vector
  - Tell nodes the complete path between various points
- On demand protocols
  - Figure out routing once you know you two nodes need to communicate

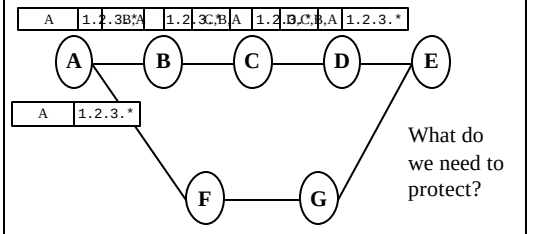
Popular Routing Protocols

- BGP
  - Path vector protocol used in core Internet routing
  - Arguably most important protocol to secure
- RIP
  - Distance vector protocol for small networks
- OSPF
- Ad hoc routing protocols

Fundamental Operations To Be Protected

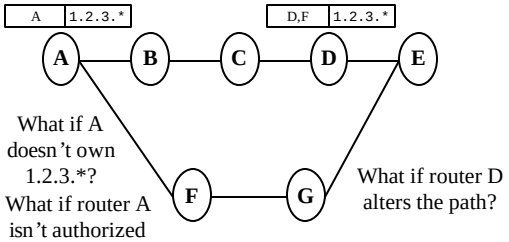
- One router tells another router something about routing
  - A path, a distance, contents of local routing table, etc.
- A router updates its routing information
- A router gathers information to decide on routing

Basic BGP Routing Issue



A wants to tell everyone how to get to 1.2.3.*

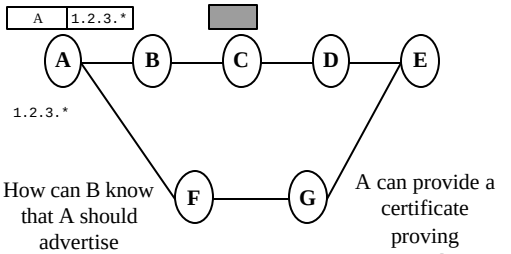
Well, What Could Go Wrong?



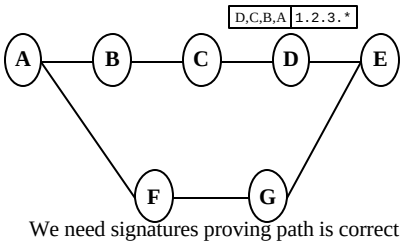
How Do We Solve These Problems?

- Advertising routers must prove ownership and right to advertise
- Paths must be signed by routers on them
- Must avoid cut-and-paste attacks
- S-BGP addresses these issues

An Example



How About Verifying Paths?



We need signatures proving path is correct
Who must sign?
What does each entity sign?

Some Questions for Discussion

- Partial deployment?
- Feasibility?
- Necessity?
- What do these measures fail to protect in routing?
- Interoperation between different protocol styles?