Issues with existing Cryptographic Protection Methods for Routing Protocols

Joel Jaeggli

11/9/09

History

- Draft as been floating around in less consolidated form since 2006
- Found a home in the reconstituted OPSEC WG
- Rehabilitated
- Believed to be headed for informational
- Major Contributors
  - Vishwas Manral – IP Infusion
  - Manav Bhatia – Alcatel Lucent
  - Russ White – Cisco Systems
  - Joel Jaeggli - Check Point Software

Goals / Application

- Declare for the sake of argument the issues that we know we live with in existing IGP cryptographic protection mechanism.
- Uses:
  - The router originating this packet is:
    - Authorized via the shared key mechanism to peer with the local router, and exchange routing data.
    - The implicit trust of routing protocol exchange protected by a shared secret is intended to protect against the injection of falsely generated routing data being injected into the routing system by unauthorized systems.
  - Assert that the data has not been altered in transit between two neighboring routers.

Goals / Limitations

- Limitations:
  - Manual configuration of shared secret keys, especially in large networks and between networks, poses a major management problem. In many cases it is challenging to replace keys without significant coordination or disruption.
  - In some cases, when manual keys are configured, some forms of replay protection are no longer possible , allowing the routing protocol to be attacked though the replay of captured routing messages.
  - The MD5 digest algorithm was not designed to be used in the way most routing protocols are using it. which has potentially serious future implications.

Getting out ahead of MD5

- Discrete PDUs are not trivially vulnerable to pre-image or hash collision attacks
- That said, taking the tool out of the Box is probably the right thing to do.
- Some external requirements driving replacement of MD5 as well.
- Security Area ADs agree.
- Concluding that it's hard to exploit is not an excuse to not deprecate an existing approach

Replay protection still a problem

- E.G. OSPF sessions with can be replayed if an adjacency is brought down
- OSPF, multiple packets with the same sequence number.
- Multiple opportunities to DOS OSPFv3 adjacencies through replay use to ESP use of manual keying
- ISIS has similar issues.

IP addresses not covered by the MAC

- E.G. in OSPF adjacencies between two neighbors can be brought down by replacing an authenticated hello having changed the source address.

Rekeying...

- You can do that?
  - In practice, not so often.
  - Some shims such as BGP daemons temporarily accepting bad digests up to the hold interval represent further opportunities for DOS
  - The possibility of more than two parties requiring the shared secret caused us avoid inclusion in the past.

IGPs and BGP (of course) are now deployed in fairly hostile environments

- Are all the devices participating in the same administrative domain with an enterprise or ISP?
  - Exchange point fabrics
  - DMZs
  - Split between security, network operations, hosting
- Never mind the question of what routing information to accept or propagate
- The authorization and protection assumptions built into our existing protocols feel a little dated.

These are all problems.. What do we do about them?

- Well there's KARP...
- Overall desire to not be caught short.
- BGP ttl hack and rapid tcp MD5 deployment for control plane protection being obvious and rapid responses to control plate exposure.
- When the tools are deployed before they're needed then transition from one to the other at least has the possibility of being orderly.
- Orderly is nice.
- Our track record both in the IETF and operationally is not great.

Issues with existing Cryptographic Protection Methods for Routing Protocols

- OPSEC can socialize the problem.
- Ops is not going to solve them.