KMART BOF

Issues with existing Cryptographic Protection Methods for Routing Protocols,

Requirements

and

Deployment Considerations

David Ward

What is this talk about?

- Introduce drafts in the routing area surrounding crypto auth in IGPs and deployment considerations
  - First is meant to give an overview of what we know and don't know about our IGP security. Mostly showing the clumsy use of cryptography
    - draft-manral-rpsec-existing-crypto-05.txt
  - Second is perspective on requirements
    - draft-bhatia-manral-igp-crypto-requirements-00.txt
  - Third draft on how protocols are deployed and why certain practices are (not) observed - more than just security
    - draft-white-rppract-00.txt

What is existing-crypto draft about?

- Routing protocols are designed to use cryptographic mechanisms to authenticate data being received from a neighboring router to ensure that it has not been modified in transit, and actually originated from the neighboring router purporting to have originating the data.
- There are some issues in how we use authentication currently with the routing protocols, leaving them vulnerable to attacks, despite using authentication mechanisms described in the standards - this draft discusses these issues.

What is existing-crypto draft about? (contd)

- The goal is to identify the weak points (make the community aware of the issues).
- The draft discusses the management and the technical issues with the existing cryptographic authentication schemes for protecting the routing protocols.
- Because of lack of time the presentation only discusses some of the technical issues with each of the routing protocols OSPF, IS-IS and RIP.

- Refer to the draft for more issues and a detailed explanation for each one of these.

Issues with OSPFv2

- Sequence Num initialized to 0 when nbr comes up/goes down. Can replay OSPF pkts from the previous session if key isn't regularly changed.
  - Seq Num frequently derived from a clock to shrink window/solve
- Current specs use MD5 - MUST upgrade to HMAC-SHA.
- Key is shared between all routers in the broadcast domain and possession of the key is used as an identity check.
  - X can masquerade as Y and send packets to Alice without the latter ever knowing about this.
  - Neighbors on broadcast/NBMA/p2mp networks are identified by the IP address in the IP header. Cryptographic Auth scheme from RFC 2328 does not cover this in the MAC. An attack can exploit this and bring down the adjacency between X and Y.

- Refer to the draft for more issues and a detailed explanation for each one of these.

Issues with OSPFv3

- Replaying Hellos with an empty neighbor list can cause all the neighbor adjacencies with the sending router to be reset.
- Replaying Hellos from early in the designated router election process on broadcast links can cause all the neighbor adjacencies with the sending router to be reset, disrupting network communications.
- Replaying Database description packets can cause all FULL neighbor adjacencies with the sending router to be reset, disrupting network communications.

- Refer to the draft for more issues and a detailed explanation for each one of these

Issues with OSPFv3 con't

- The issue is due the use of manually keyed AH, where replay protection can't be used.
- So the problem isn't really AH, it is due to a lack of an IPsec group key management solution suitable for use with OSPF.
  - It is the broadcast link problem that keeps us from using IKEv2 with OSPFv3.
- There are IETF group key management protocols, but the applying them to OSPF is problematic since they rely on a key server.

- Refer to the draft for more issues and a detailed explanation for each one of these

Issues with IS-IS

- Possible to replay IS-IS PDUs as there is no crypto sequence number in the PDUs.
- An IIH PDU containing a digest within a TLV, and an empty neighbor list, could be replayed, causing all adjacencies with the original transmitting IS to be restarted.
- Old CSNP packets can be replayed to trigger an LSP storm when a large number of LSPs are flooded.
- Current specs use MD5 - MUST upgrade to HMAC-SHA or something stronger.
  - Being addressed in current drafts

Issues with IS-IS (contd)

- IS-IS does not have the notion of a Key ID. During Key rollover, each message received has to be checked for integrity against all keys that are valid. This can be exploited to launch a DOS attack on the IS-IS router.
- Lifetime is not covered in the authentication. This can be exploited to force the IS-IS router to flood all its segments again.
  - Under certain scenarios an attack can force the IS-IS process to shut down for around 20+ minutes (MaxAge + ZeroAgeLifetime).

- Refer to the draft for more issues and a detailed explanation for each one of these.

Issues with RIPv2

- RIPv2 cryptographic Authentication does not cover the IP and the UDP headers.
- RIP uses the IP header to determine the neighbor its learnt the RIP update from. Since there is no protection provided to the IP header, an attacker can exploit this and disrupt the RIP routing sessions.
- An attacker can reply an earlier RIP packet and by modifying the IP header, can deceive the receiver in believing the packet came from a different source.

- Refer to the draft for more issues and a detailed explanation for each one of these.

Requirements draft

- Support one or more auth schemes and algorithms in common
- Keys used must be changed periodically and implementations MUST be able to store and use more than one key at the same time
- Solve fundamental protocol issues over time if possible or hide them

- Refer to the draft for more issues and a detailed explanation for each one of these.

Deployment draft

- The focus is not to describe how routing protocols should be deployed, but rather how they are generally deployed
  - provide those working on specifications which impact the operation of routing protocols with guidance in what will likely be deployed, or what will likely not be deployed.
  - Configuring routing/signaling protocols is like writing assembly language
    - All hand crafted, fine tuned
  - Enterprise operator view
- Network Growth
  - State changes are often hidden at various points within the network.
  - Topology information is often reduced from a fine grain view of the network to a single point of reachability.

- Refer to the draft for more issues and a detailed explanation for each one of these.

Deployment draft.2

- Deterministic Behavior
  - Link metrics are normally ***manually*** engineered to select a primary and alternate path through the network for any given source/destination pair
    - Rather than allowing the routing protocol to naturally process the paths, and build paths which might fail over in non-deterministic ways.
  - Trees for routing multicast routing may be ***manually*** configured throughout a network, to control the paths and backup paths available to certain classes of traffic
- Extreme convergence (< 100 ms) and stability
  - Pushing detection as close to the hardware as possible.
  - ***Manually*** configure L2 and L3 and protocols to converge AFAP
  - Using exponential backoff and other dampening mechanisms to prevent a positive feedback loop from forming
- Refer to the draft for more issues and a detailed explanation for each one of these.

Deployment draft.3

- Policy section
- RIB management
- Aggregation
- Common Peering practices
- Routing protocol security
  - Auth keying not always deployed
    - Due to convergence impact (more cycles)
    - Operational Complexity

- Refer to the draft for more issues and a detailed explanation for each one of these.

Thanks to Ran Atkinson, Tony Li, Manav Bhatia, Vishwas Manral, Russ White, Ahbay Roy, Acee Lindem, Mike Shand, Les Ginsberg, Stefano Previdi

Questions?