Security Requirements for Routing Protocols

draft-puig-rpsec-generic-requirements-01.txt

Jean-Jacques Puig
Emanuele Jones
Danny McPherson

IETF 58 - RPSEC Working Group
Wednesday, November 12, 2003
Hilton, Minneapolis, MN, USA

How many folks here have read
draft-puig-rpsec-generic-requirements-01.txt?

Not sure I believe most of you
-- we've only received
comments from <10!

Goals ?

- *Requirements on the (inner-)security of routing protocols*
- *Requirements in the secure operation of routing protocols (through the device)*

- These are not requirements on forwarding security
- Section ‘2’ states goals of the document.

Relation with Threats doc

- [Section 3] divides threats into 2 categories
  - Elected for mitigation -> Strong requirements (MUSTs & SHOULDs)
  - Other Threats -> weak requirements (MAYs & CANs) or no requirements at all.
- [Appendix B] reserved for a verbose description of how requirements address each particular threat.
- Within the document, references to particular threats addressed by a requirement. List of threats {,,,} addressed by a particular requirement.
- Threats doc and Requirements doc should be considered as companion documents.

A Model for Routing Protocols ?

- Planes division
  - Control Plane
  - Data Plane
  - Management Plane?
- Functional Approach (from threats draft)
  - Transport Subsystem
  - Neighbor State Maintenance
  - Database Maintenance
- Data presentation (Path, Attributes, Reachability Information)

Requirements

- Feedback needed on requirements granularity
- It is useless to consider requirements without proper agreement on stated goals and on which threats are most important
- Future formulation shall lay emphasis on short, straight-forward requirements
- Coherence with other drafts or docs (e.g., IRTF RRG) where practical

Related Considerations

- Transport Subsystems (includes neighbors and addressability)
- Cryptography side-effects

Active Participation to Overall Security

- Detection of failures (active/passive checks, error messages, auditable events)
- Reactions (Graceful degradation, fail-back procedures, filtering, corrections).

- Failing participants which were excluded should be offered occasions to participate again

Local Resource Exhaustion

- Hardware Considerations
  - Buffers/Queues
  - CPU Cycles
  - Bandwidth
- Logic Considerations
  - Checks before commits to underlying database
  - Appropriate persistence of routing information wrt trust
  - Tips in order to avoid database overflows
- Does this even belong here?

Inter-Domain

- Added Complexity
- A lot of work needs to be done in this area!

Editorial Tags

- *[OLD]* precedes the old version of the next paragraph
- *[TBD]* To Be Discussed/Decided

Specific Issues (TBDs)

[2.1] Should route attributes require as much protection as routes themselves. - Probably yes.

[2.2] Need to better define document scope

[3.2] Should confidentiality of routing information be a requirement? To what level? (e.g., hide topologies, relationships, etc..)?

[4.] *Routing functions* comes directly from threats draft, need to evolve into requirements - or remove.

[4.1] Is the *Routing Protocol Components* section useful?

[5] Method in which routes are presented has implications on security (e.g., full path v. next hop, etc..).

Specific Issues (TBDs)

[6.1.1] Adjacency Section Needs Expansion

[6.1.2] Byzantine Section Needs Polishing

[6.2.2] Legitimacy -- use of tokens or other? Needs lots of work.

[6.2.4] Underclaiming and overclaiming -- should probably remove? Threats removed the latter, former is mostly addressed by Legitimacy -- or is it?

[6.3.1] Interaction with Transport Layer/Subsystem needs work.

[7.1] Producers, consumers and forwarders and relays. Who must perform what functions and what functions must be performed by which components?

Specific Issues (TBDs)

[7.2.3] Key Strength & Lifetime; IGP v. EGP

[7.3] Considerations of other data stored in NV memory? Does out-of-band management present new vulnerabilities

[10.3.1] Legitimacy for advertising routes/updating information. Is using authorization paradigm sufficient?

[10.3.2] Ways to prove the right to advertise a prefix. Where will we find the appropriate victim for the administration of these databases?

Specific Issues (TBDs)

- What's a path?
- What portions should be secured/verified/authenticated?

All we need is YOU!

1. Agree on stated goals
2. Agree on threats selection
3. Feedback on routing protocols parts (functions, route descriptions); granularity
4. Express your opinion on requirements
5. General feedback