BGP Security: Current IETF work

Tony Tauber

1/31/2005

Routing Protocol Security WG

- Choice charter excerpts:

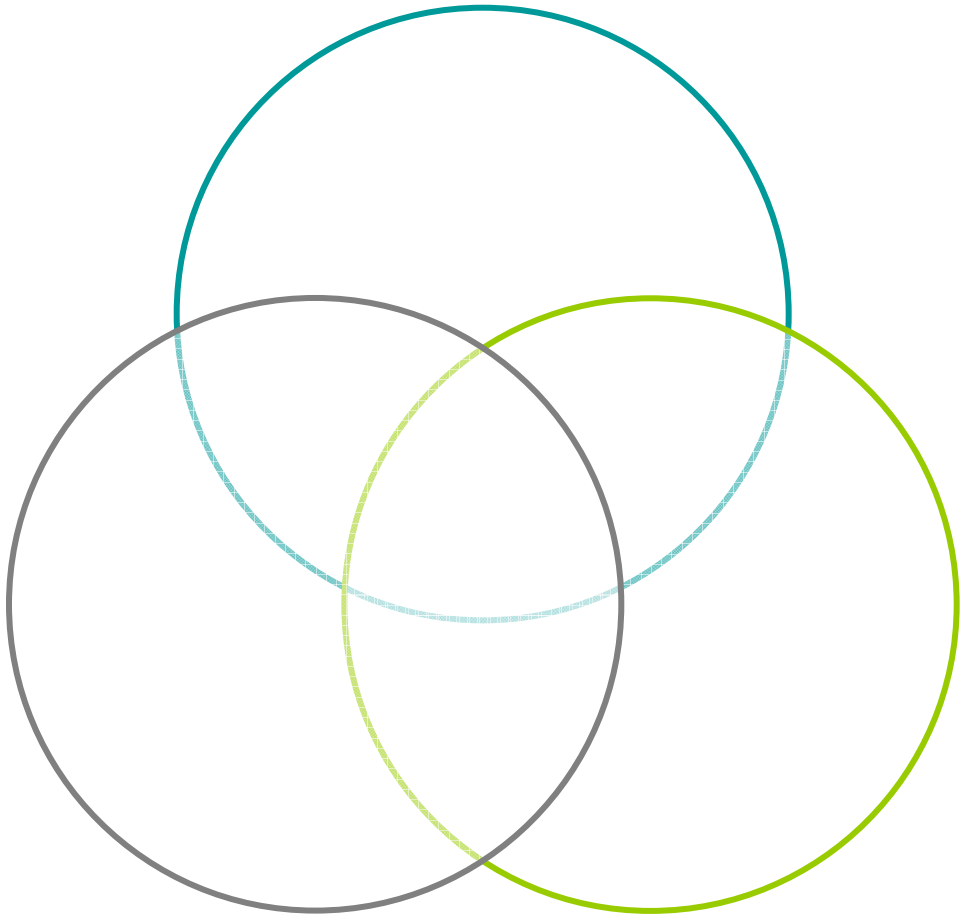
  (www.ietf.org/html.charters/rpsec-charter.html)

  "... The products of this working group will be used by routing protocol designers to ensure adequate coverage of security in the future, including well known and possible threats.

  - Document security analysis and requirements for specific routing protocols (e.g., OSPF, BGP)
  - Provide a common area for discussion between security and routing experts on the topic of securing the routing system" [*Also Operations experts!*]

You are here:

Operations

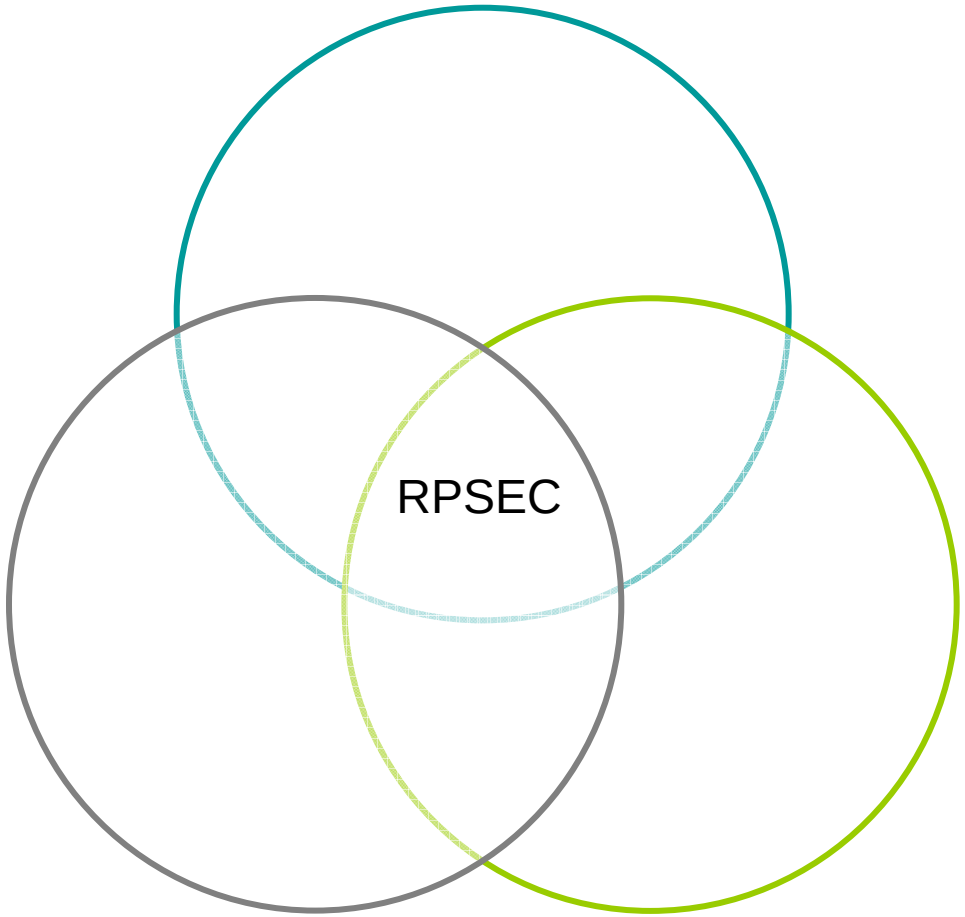


Security

Routing

You are here:

Operations

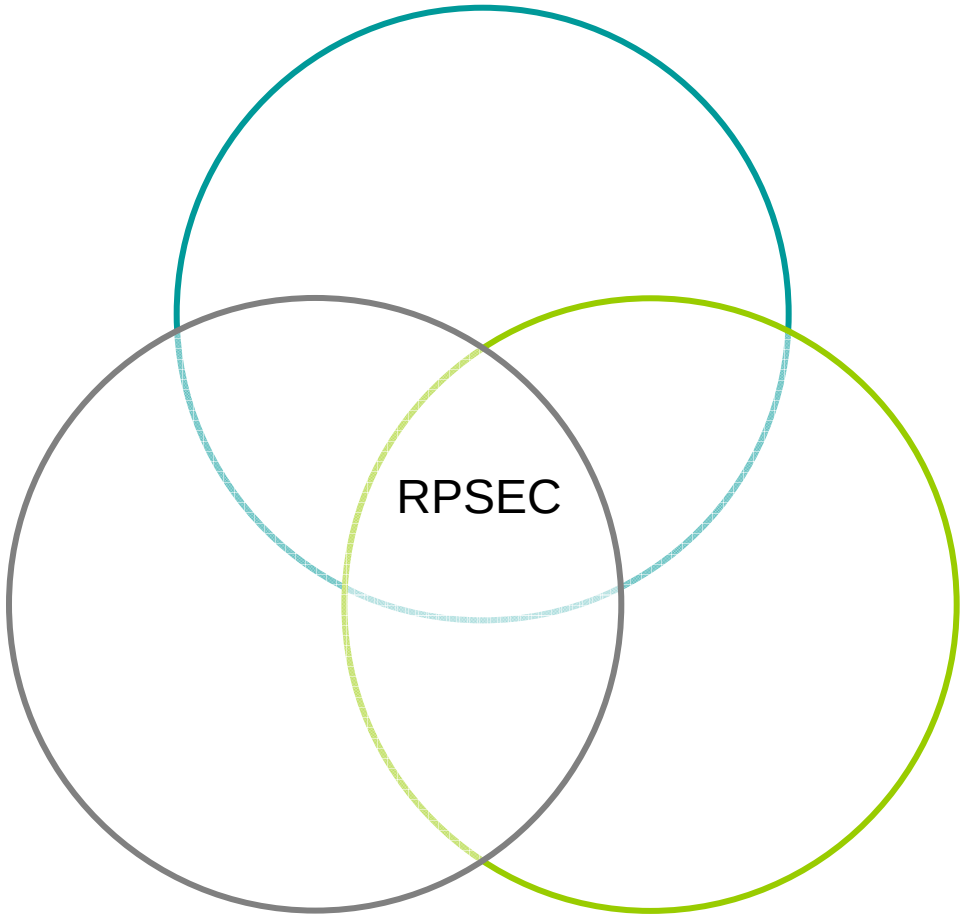


Security

Routing

You are here:

Operations



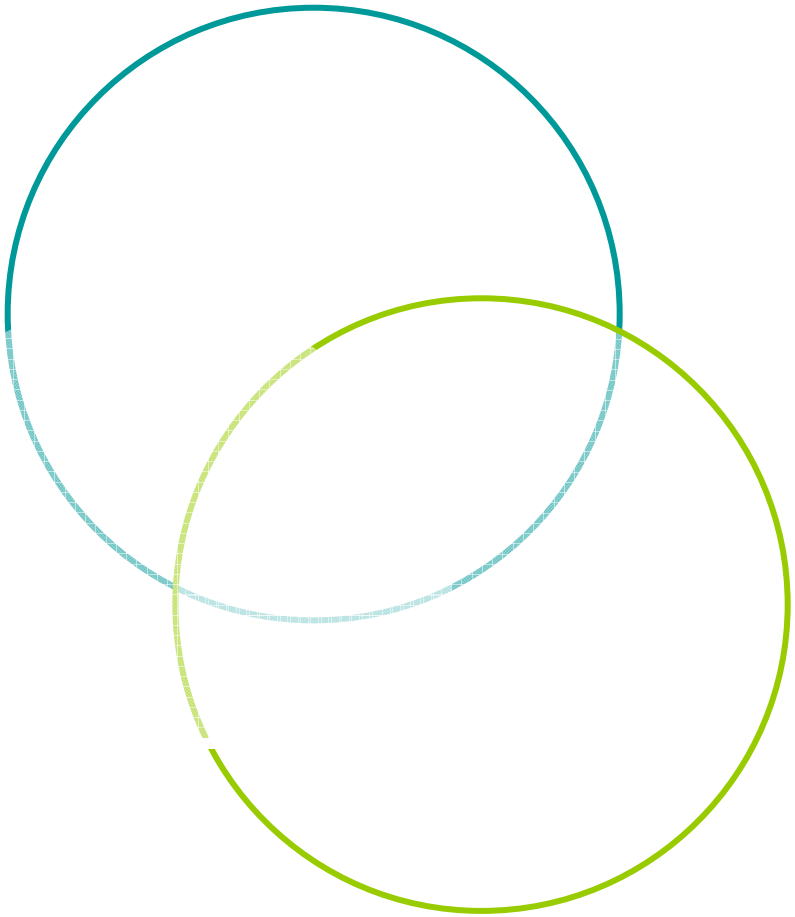
Security

Routing

"It won't work."

You are here:

Operations



Routing

"It won't work."

BGP Security

- Worked on since at least 1997
- Some different solutions posed
  - S-BGP (Secure BGP)
  - so-BGP (secure origin BGP)
  - IRV (Interdomain Route Validation)
  - SPV (Secure Path Vector)
- All have (somewhat) differing sets of received requirements

BGP Security Requirements (1)

- Try to go back and derive an agreed-upon set of requirements
- Then, go and analyze any proposed solutions against the requirement
- Not quite so easy after all....

BGP Security Requirements (2)

- So far, lively exchange among people with routing and security backgrounds, but...
- Operators are needed to provide balance!
  - Everyone needs to *talk* and *listen* !!!

Known Operational Problems

- Improper route origination or propagation
  - Accidental and naïve
    - 18.0.0.0/8
    - AS 7007
  - Malicious
    - Antagonistic or competing announcements
    - "Pop-up" hacking using un-announced space
      - advertise, hack or spam, disappear
- Is route filtering really the solution?
  - How do we check who's authorized, really?

Projected Operational Problems

- Session resets, data injection/corruption
  - Blind attacks
- TCP-MD5: solution or other problems?
  - Key management (How to get keys around?)
  - Rogue employees (Who wants some keys?)
  - Compromised routers (Who needs keys?)
- GTSH (Generalized TTL Security Hack)?
  - As above for bad routers/employees

Sticky Bits

- Need to agree on taxonomy
  - Route, path, routing, forwarding, update
  - Signature, certificate, hash, key, encrypted
  - Neighbor, peer, AS
- Need to identify operational practices which aren’t necessarily reflected in any specification or other IETF document
  - Some really essential
  - Some just hacks?

Trust and Authority

- Issue of how trust is established is generally considered beyond scope of protocol requirements
  - Is this approach wrong?
  - How do we leverage what exists without replicating problems?
- Current {route, numbering} registry info?
  - Too inaccurate?
  - What's the alternative?

Standards

- Can these goals be accomplished without standards?
- How do you know what you’re getting or whether it’s being done right otherwise?

More Operator Involvement

- Please!!
- Others welcome, too
- Subscribe:
  - rpsec-request@ietf.org
- Archive:
  - http://www.ietf.org/mail-archive/web/rpsec/index.html
  - Don’t feel like you have to catch up to jump in.
- Document:
  - http://ietf.org/internet-drafts/draft-ietf-rpsec-bgpsecrec-00.txt

Panelists

- Blaine Christian – KMC Telecom
- Doug Montgomery – NIST (not with us…)
- Danny McPherson – Arbor Networks
- Sandy Murphy – Sparta (last minute!)
- Tony Tauber – MIT Lincoln Laboratory