Keying and Authentication for Routing Protocols (karp)

IETF 78

Agenda

- **Administrivia** (5 minutes)
  - Scribes (Meeting Minutes & Jabber)
  - Blue Sheets
- **Welcome** - Chairs (5 minutes)
- **NANOG Report** - Joel Halpern (10 minutes)
- **Cryptographic Authentication Algorithm Implementation Best Practices for Routing Protocols** - Joel Jaeggli (10 minutes)
- **Status of Design Guide, Framework, and Threat Analysis I-Ds**
  - Gregory Lebovitz (10 minutes)
- **Database of Long-Lived Cryptographic Keys** - Tim Polk (20 minutes)
- **Analysis of OSPF Security According to KARP Design Guide**
  - Sam Hartman (30 minutes)
- **Operations Model for Router Keying** - Sam Hartman (10 minutes)
- **Analysis of Security Association for Current Routing Protocol**
  - Yinxing Wei (10 minutes)
- **Open Discussion**
  - Other urgent items for KARP?
  - What design teams should be spun up?

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

A reminder of why we are here ….

Black Hat USA 2010

Las Vegas, 24-29 July 2010

Burning Asgard - What happens when Loki breaks free

Speakers: Daniel Mende, Rene Graf

I personally remember the release of Yersinia at Black Hat Europe 2005. It was a ground breaking experience: a number of Layer 2 attacks regarded purely theoretical until then, was suddenly available in a mostly automated way. And those guys even showed some forays completely unbeknownst to me at the time. We plan to do the same in Vegas, with a new tool called Loki (after the giant from Norse mythology associated with cunning, trickery and evil). It's a Python based framework implementing many packet generation and attack modules for Layer 3 protocols, including BGP, LDP, OSPF, VRRP and quite a few others.

After outlining Loki's inner architecture we'll give insight into several modules and discuss some particularly interesting attacks in the routing protocol space (e.g. cracking OSPF MD5 keys, injection of routes into OSPF and EIGRP environments etc.). Furthermore we'll describe vulnerabilities in lesser known protocols like VRRP. Every attack we mention will be shown in a practical demo and - of course - Loki will be released right after our talk.

Document Status

- Three KARP WG I-Ds have been published
  - draft-ietf-karp-design-guide-00
  - draft-ietf-karp-framework-00
  - draft-ietf-karp-threats-reqs-00
- They're still -00, and need more review by the WG in order to be progressed.
- Pay attention to today's presentations to catch which ones are asking to become WG I-Ds
  - But don't lose track of the fact that we need to progress the current doc's!