RFC3552bis

New Guidelines for Writing RFC Text on Security Considerations

Magnus Westerlund (magnus.westerlund@ericsson.com)

Yoav Nir (ynir.ietf@gmail.com)

RFC 3552 (BCP 72)

- Published July 2003 – 13 years ago – as an IAB document.
- Follows RFC 2223 which required a Security Considerations section for all RFCs.
- Has extensive sections about the goals of security and the Internet Threat Model.
- Has a very extensive section (13 pages) about common issues both in security requirements and security solutions.

Updating RFC 3552

- Some outdated information
  - Protocols, algorithms.
- Evolved concept of Privacy
- Changes in Internet environment
  - Pervasive monitoring
- Add draft-gont-numeric-ids-sec-considerations?
- Add something about Opportunistic Security?
- Guidance for common special cases:
  - Extension documents.
  - Usage documents for specific applications of generalized frameworks.

Examples – Outdated Information

- Section 4.5.2 recommends using “SSL” or TLS 1.0. SNI is described as “too new to have seen wide deployment”.
- Section 4.5.1 recommends AH; states that AH & ESP are mandatory for IPv6.
- No mention of algorithm selection, algorithm agility, or AEADs.
- Stuff that never happens: “Non-repudiation”, secure purchases over S/MIME.
- Section 3.2.2 on password sniffing mentions telnet, PoP, and NNTP, but not HTTP or OAuth.

Examples - Privacy

- Most of this is just referencing RFC 6973.
- Some issues that were not considered at the time:
  - Stored data compromise
  - Correlation
  - Identification
  - Secondary Use
  - Anonymity / Pseudonymity
  - Data Minimization

Example – Changes in Environment

- Pervasive Monitoring:
  - RFC 3552 distinguishes off-path vs on-path attackers, and passive vs active attacks.
  - On-path attackers are described as capable of both active and passive attacks. It is assumed (though not explicitly stated) that on-path attacks are rare and targeted.
  - Pervasive monitoring invalidates those assumptions. On-path attacks can be performed at scale, although they are limited to passive attacks.
  - Does it matter? That is up to the protocol or the deployment, so it is something to consider. Something to add to the security considerations.
- Death of the Perimeter
- UDP-based protocols; DTLS

The Plan

- Submit a -00 draft by September
- Have extensive discussion on SAAG
  - Already started. Thanks Christian and others.
  - This is not Magnus and Yoav writing this, we hope for a lot of community input.
  - Comments are silver, text is gold.
  - If the discussion volume gets too high, we'll ask for a special list.
- Revise the examples; make them more modern.
- More discussion at IETF 97.
- Hopefully IETF LC early next year.

Questions? Comments?