Security Considerations Issues for RFC 2821bis
draft-klensin-rfc2821-security-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 9, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

RFC 3552 is a useful analysis and presentation of recommendations for Security Considerations Sections. Part of its content is an extensive analysis of, and proposed replacement for, the Security Considerations section of RFC 2821. In important respects, the proposed replacement text may not be appropriate for this type of document. It also raises some specific issues that may not be consistent with the consensus community of email experts about best practice. Given the way it is worded, and the fact that it was published as a BCP document, it is plausible to consider it as an

Update to RFC 2821 and to consider its "example" to be normative for any future revision of RFC 2821 such as the work that has been started in [7]. Those perceptions should be definitively evaluated and corrected if necessary. This document is a first step in doing so and also makes some specific additional suggestions about the handling of Security Considerations material.

Table of Contents

1. Introduction

RFC 3552 [2] is a useful analysis and presentation of recommendations for Security Considerations Sections. Part of its content is an extensive analysis of, and proposed replacement for, the Security Considerations section of RFC 2821 [1] (SMTP). In important respects, the proposed replacement text may not be appropriate for the type of document that RFC 2821 represents, namely a unified description and collection of clarifications to a widely-deployed and very established protocol. This document suggests that RFC 3552 should have made a distinction between the intent of Security Considerations sections for a new protocol at or before early stages of deployment and a mature and widely deployed protocol. For early-stage protocols, the activity of constructing a Security Considerations section and working through the issues involved may result in significant improvements to the protocol itself. By contrast, for a protocol as well-established and widely deployed as SMTP, the security issues are, to paraphrase a discussion with one of RFC 3552's authors, essentially what they are: the construction and review of a Security Considerations section is unlikely to have any significant impact on how the protocol is designed or operates, although a security analysis may be helpful in making operational decisions.

The proposed replacement text may also not reflect consensus of the community of email experts about best practice, especially in the area of address-based blacklist filtering for spam. That document can be interpreted as suggesting that it is reasonable to expect that a document specifying email transport should be required to contain an analysis of at least a very large fraction, and perhaps even a comprehensive listing, of the ways in which email could be attacked or misused, or how one might (reasonably or otherwise) defend against those attacks.

This author believes that level of analysis would be extremely useful. Considerable analysis is, however, required. Moveover, the security environment for Internet applications often evolves much more rapidly than the applications, especially the more mature ones, do themselves. This combination suggests that, at least for mature and widely-deployed protocols, the analysis is better prepared separately and placed in a document separate from the protocol specification itself.

Put differently, there is unquestionably a place for complete security analyses of a protocol and its applications and implementations. Such work is certainly valuable when it can be produced, but expecting such an analysis, or even a near approximation to it, as part of a "security considerations" section

-- the adequate completion of which is prerequisite to approval and publication of any document that comes through the IETF process-- is probably unwise when the base document reflects clarifications and document unification for a mature protocol. A statement of known risks in the design and use of the protocol --or even a statement that the protocol is sufficiently insecure that it should be used only in a highly-protected and isolated environment -- is certainly reasonable and appropriate. But a normative presentation and analysis of suggestions of some subset of ways to resist certain misuses of the protocol by end users might reasonably be the subject of other documents, and even standards, but it is inappropriate to require it as part of the "security considerations" section of the base protocol.

Given the way RFC3552 is worded, and the fact that it was published as a BCP document, it is plausible to consider it as an update to RFC 2821 (i.e., replacing the Security Considerations section of that document) and to consider its "example" to be normative for any future revision of RFC 2821. Those perceptions should be definitively evaluated and corrected if necessary. This document is a first step in doing so and also makes some specific additional suggestions about the status, in practice, of RFC 3552 and the handling of Security Considerations material for mature and deployed standards.

2. Practical Application of RFC 3552

The author has extracted a convenience sample of a dozen, specifications whose principal focus was not security, approved as Proposed Standards in the two years since RFC 3552 was published. If the documents examined were representative, they would suggest that RFC 3552 has been generally ignored, with few if any of those documents meeting all of its requirements for identification of possible threats and discussion of proposed threat-protection mechanisms that would not work. Perhaps it would be reasonable to conclude from this that it should be ignored in constructing the replacement for RFC 2821 as well. However, since RFC 2821 is singled out as an example, that seems unwise and this document is supplied to initiate a specific discussion in the context of unfolding work up an update to RFC 2821 [7]. (Cf. Section 5.)

3. Mail Principles and Security

It is a long-standing principle of email on the Internet and elsewhere, and, indeed, of most postal mail systems, that the mail should, if at all possible, go through and that, if it does not go through, the failure should be indicated through established and standardized mechanisms. As RFC 2821 points out, it is entirely

rational for mail systems to make operational exceptions to that principle and to, e.g., drop mail without making great efforts to return it, if they know they are under attack. But the principle remains: rejecting, discarding, or blocking mail that cannot be positively identified as hostile or otherwise unwanted is generally considered extremely undesirable. Indeed, doing so can create a security risk, since it is possible that an incorrectly-discarded message might contain information that was critical to the intended recipient.

Consequently, while feelings often run very high about where the lines should be drawn, any system for mail filtering and rejection for other than undeliverability or known inaccessibility to the intended recipient must be considered a tradeoff between improved safety or convenience and the risk of incorrect rejections.

4. Section by Section Analysis of the Replacement Section

Section 5 of RFC 3552 requires identifying, as a strong requirement (i.e., with "MUST" language as defined in [4]) the range of attacks that are possible on a protocol, those that are not relevant ("out of scope"), and what attacks it protects against. Perhaps only because of the differences between new protocols and those that are mature and widely deployed, these requirements may not, as written be appropriate for SMTP. With a protocol as old and established as SMTP, the security issues are generally well understood, much more so than with a protocol that has not yet been extensively tested by experience. One way to look at this is that, for a newer protocol, we have Security Considerations and their influence on the design or applicability of the protocol itself. For SMTP, a security analysis is useful and important. Such an analysis might include suggestions about, e.g., the configuration of an SMTP implementation for use under various circumstances but is necessarily somewhat different from one written to describe risks and issues in a new protocol.

Familiarity with RFC 3552 section 5, and the SMTP-specific material in section 6.1, is assumed in the material that follows. The section numbers cited are in RFC 3552.

4.1 Section 6.1.1.1: Discussion of IDENT

IDENT [3] is a Proposed Standard. If one agrees with the analysis in 3552, the appropriate action would be to deprecate IDENT, or generate an appropriate applicability statement about it, not to simply insert comments into the SMTP specification. The text and examples of 3552 can be read to suggest is a requirement to discuss every unfortunate or ineffective approach to SMTP security. If that were to be the goal, then discussions on the IETF-based SMTP and anti-spam mailing

lists during the year preceeding July 2005 present a legion of opportunities, most of them more problematic than IDENT. The IDENT material probably does not belong in RFC 2821, although a pointer to a discussion if IDENT, and a number of ideas with similar intent, would be entirely appropriate.

4.2 Section 6.1.1.3: Security value of disabling VRFY

RFC 3552 suggests adding a note indicating that disabling VRFY may not have much security value since the same information may be available from RCPT TO. If this is going to be said, it should be associated with a more complete discussion of when VRFY does actually produce more information that RCPT TO, e.g., when address processing is deferred for the latter, as the mail specifications have permitted for years. The text in the initial draft of 2821bis has been modified to reflect that point. The statement and recommendation in RFC 3552 appears to be too simplistic in this area. So, if a subsection of a Security Considerations were to discuss issues with VRFY, it would presumably need to pick up (or point to), considerable material that already appears elsewhere in RFC 2821 and avoid some of the pitfalls identified there.

4.3 Section 6.1.1.8: Spam

RFC 3552 recommends including an extended discussion of spam-fighting issues in the SMTP specification, citing and expanding on [6]. The email-expert portion of the IETF community has repeatedly reached rough consensus that the base email transport and message headers and body specifications should be kept free of operational considerations, particularly those concerned with spam-fighting and spam-resistance, other than to note areas of the specifications in which exceptions can be made when operationally necessary. The various efforts in the IETF and IRTF to develop anti-spam specifications and techniques have generally been instructed to stay away from modifications to the base email specifications (although they may, and have, created compatible extensions to them). Yet RFC 3552 proposes to override that consensus and those agreements to include a spam-fighting discussion in RFC 2821 and its successors.

Worse, the text proposed in 3552 appears to recommend "blacklisting" techniques of various sorts, going so far as to identify particular sources of blacklists. While they were more popular a few years ago than they are today, it would be a significant understatement to suggest that these techniques are controversial in the email community and that there is no IETF consensus to recommend them as appropriate.

4.4 Section 6.1.2: Communications Security

In the opinion of this author, this material is quite good. It belongs somewhere, but probably not in the SMTP specification. For that specification, it goes fairly far into message header issues (normally the provence of other specifications), it explores difficulties in other protocols, such as the use of IPSEC, and so forth. In addition, it suffers from some of the same difficulties discussed above in Section 4.2: if one is going to go into these areas in the context of SMTP, some of the discussion is insufficient and incomplete.

4.5 6.1.3: Denial of Service

Again, while there is nothing wrong with this new material, it is not clear that it is adequate in the SMTP context. Singling out one specific implementation for one of its idiosyncracies seems particularly inappropriate. If one is going to examine DoS attacks in the SMTP context, perhaps the most important issue --certainly an important issue-- involves tuning of the various SMTP timeouts. That is a hot topic on many discussion lists, especially those concerned with spam fighting, and has been for years. Additionally, there are specific, standards-track, SMTP extensions (including [5], a Full Standard) that can be used to manage some of the issues this section raises (in the case of RFC 1870, the excessive disk usage problem) but are not mentioned in the discussion that RFC 3552 supplies. Where is it appropriate for the security considerations material of RFC 2821 us stop, given the level of detail provided in other subsections?

4.6 Additional Material for 2821bis

Interestingly, there are a wide range of topics that might appropropriately be covered in a security analysis of SMTP that the RFC 3552 analysis odes not cover. They include a more comprehensive treatment of approrpriate and inappropriate actions in dealing with mail that is presumed to be hostile, the among and type of logging and reporting that should be maintained for mesages that are dropped, various authentication frameworks and the problems they do and do not solve, and so on. The likely extent of that material again suggests that it would be better placed in a separate "mail security analysis" document than forced into the SMTP specification.

5. Conclusion and Recommendations

The tone and several of the requirements imposed by RFC 3552 are dubious, especially when applied to documents describing mature and widely-deployed protocols. For such protocols, the most likely

impact of strict application of 3552 as written would be to further discourage applicability statements, standards that consolidate prior work (in the case of SMTP, much of it already at a full Standard level), and documents created to raise the maturity level of the specifications, by imposing a burdensome analysis and documentation requirement. We have too few of such documents as it is; they should be made more burdensome to create only after careful consideration by the community. It is also problematic to require, as RFC 3552 can be interpreted as requiring, that the security considerations section of every protocol specification either contain a discussion of every other protocol that might be used with it or point to a discussion of that protocol that was adequate under 3552's rules. Security analysis of collections of protocols is probably better left to stand-alone documents that can be referred to from individual members of the collection.

Perhaps fortunately, the IESG has apparently ignored the requirements of RFC 3552 in a number of specifications it has approved for the standard track subsequent to 3552's publication. Of course, that creates a different problem, one of having procedural BCPs that are approved by the IESG and then ignored (either globally or selectively). It is hard to argue that such documents are BCPs at all, and their approval is probably indicative of a systemic problem in the IETF.

At least in this author's opinion, the discussion in RFC 3552 is quite useful and the suggestions it makes should be given serious consideration. The difficulties arise when its text --all of its text-- are considered normative for other specifications, especially specifications that describe mature and widely-deployed protocols. Its BCP status, and the use of strong normative requirement language from RFC 2119, certainly implies that it should be considered normative in that way and that situation probably requires some clarification.

6. Security Considerations

This document is about an effort to refine the specification for security considerations sections, especially in the context of updated descriptions for mature and widely-deployed protocols. It does not, itself, have any impact on protocol security.

7. Acknowledgements

Thanks to Ted Hardie and a brief discussion during an Applications Area meeting that led to the suggestion that a document like this one was the right way to pursue this problem. Thanks also to the several people who encouraged me to not just write off 2821bis in the light

of the discovery of the provisions of 3552. And thanks especially to Eric Rescorla for his extensive and helpful discussion of issues in RFC 3552 and an earlier version of this document.

8. References

8.1 Normative References

[1] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[2] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

8.2 Informative References

[3] Mindel, J. and R. Slaski, "FTP-FTAM Gateway Specification", RFC 1415, January 1993.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Klensin, J., Freed, N., and K. Moore, "SMTP Service Extension for Message Size Declaration", STD 10, RFC 1870, November 1995.

[6] Lindberg, G., "Anti-Spam Recommendations for SMTP MTAs", BCP 30, RFC 2505, February 1999.

[7] Klensin, J., "Simple Mail Transfer Protocol", July 2005.

Author's Address

John C Klensin
1770 Massachusetts Ave, #322
Cambridge, MA 02140
USA

Phone: +1 617 491 5735
Email: john-ietf@jck.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.