Independent Submission
Internet Draft
Intended status: Informational
Expires: December 2019

M. McFadden
internet policy advisors ltd

June 27, 2019

Methodology for Researching Security Considerations Sections
draft-mcfadden-smart-rfc3552-research-methodology-00.txt

Status of this Memo

Copyright Notice

Abstract

RFC3552 provides guidance to authors in crafting RFC text on Security Considerations. The RFC is more than fifteen years old. With the threat landscape and security ecosystem significantly changed since the RFC was published, RFC3552 is a candidate for update. This draft proposes that, prior to drafting an update to RFC3552, an examination of recent, published Security Considerations sections be carried out as a baseline for how to improve RFC3552. It suggests a methodology for examining Security Considerations sections in published RFCs and the extraction of both quantitative and qualitative information that could inform a revision of the older guidance.

Table of Contents

1. Introduction

RFC 2223 requires that all RFCs have a Security Consideration section. The motivation of the section is both to encourage RFC authors to consider security in protocol design and to inform readers of relevant security issues. RFC 3552 was published in July of 2003 to give guidance to RFC authors on how to write a good Security Considerations section. It is structured in three parts: a tutorial and definitional section, then a series of guidelines, and finally a series of examples.

It is possible to observe that the Internet security landscape has changed significantly since the publication of RFC 3552. Rather than an immediate attempt to draft and discuss a revision to the older RFC, it may be prudent to learn from the experience of nearly fifteen years of documents published since RFC 3552 was approved for publication.

It is possible that an examination of published Security Considerations sections of existing documents could give both quantitative and qualitative insight on how to proceed with a newer version of the Security Considerations guidelines. The motivation is to inform any discussion of a revision with quantitative and qualitative data gleaned from years of published RFCs.

This document proposes a methodology for such research.

This scope of this proposal is for the research itself. Discussion of relevant issues, document organization and revised content for a revision of RFC 3552 is out of scope. Instead, the motivation is to guide a piece of research that would later form part of the foundation for a discussion of a revision to RFC 3552.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119.

3. Motivation

Since 1998, all RFCs have been required to have a Security Considerations section. The authors of RFC 3552 observed that "historically, such sections have been relatively weak." The motivation for RFC 3552 was, in part, to improve the quality of Security Considerations sections.

Today the Internet threat model, the landscape of attacks, and our understanding of how to craft protocols that are more robust and resilient has changed significantly. Experience in both protocol design and implementation has greatly improved our understanding of the security implications of choices made during protocol design.

It is possible that a revision of RFC 3552, reflecting the changes to the Internet and our understanding of the evolved security landscape and threat model, is appropriate.

If a revision were to be contemplated, it would be useful to learn from the body of experience of crafting Security Considerations sections in recent years. That body of experience could inform the discussion of what makes up a good Security Considerations section by collecting real-world data from existing RFCs. It would be possible to have a survey of the existing Security Considerations sections in published RFCs. The data collected from that survey could provide one source of information for discussion of how to improve upon RFC 3552 in the current environment.

For such a survey to be successful, an outline of some basic goals and a methodology would be required. This document provides those goals and methodology. The intent is that individuals or organizations could then carry out such a survey, publish te results and use that data to inform any discussion of a potential 3552bis.

3.1. Non-goals and scoping

This document specifically does not make suggestions for changes to RFC 3552. It also does not identify changes to the Internet threat model or the general security landscape that has changed since that RFC has been published.

The scope of this document is to provide a basic set of goals for research on existing Security Considerations sections and establish a methodology for conducting that research.

3.2. Research Group

This original research work was inspired by the themes in the proposed Stopping Malware and Researching Threats (smart) research group in the IRTF to survey current and historic IETF material to discover existing deliberations on attack defense. This work could also be conducted independently and submitted as an Independent Submission in the IETF.

4. Goals for Surveying Existing Security Considerations Sections

A cursory examination of recent years' Security Considerations sections shows that authors publish a wide variety of these sections. This is natural since the RFC series has a diverse set of purposes and readership.

However, even a cursory examination shows that published Security Considerations sections have some clear characteristics. Identifying useful characteristics and then surveying the existing base of published RFCs may provide a useful base of information for a later discussion of revising RFC 3552.

The goal of surveying existing Security Considerations sections is to provide quantitative and qualitative data, from existing, published RFCs, that can be used to inform a discussion of revising RFC 3552.

5. Methodology

5.1. Methodology Overview

The survey of existing Security Considerations sections would examine a subset of RFCs published since the publication of RFC 3552. RFCs obsoleted by later publications, RFCs that are reports from IAB activities and IETF, IRTF, and IESG administrative RFC are omitted from consideration.

Documents other than RFCs are also omitted: the RFC Series is, as a permanent repository of protocol development and guidance to implementors, the series of documents most likely to be read for security considerations.

The survey should select a specific timeframe, across which, all RFCs published in that period are examined.

The examination proceeds in two parts: a quantitative examination of the Security Considerations sections and then a qualitative examination.

As an example, the quantitative examination might survey and collect data on the source of the RFC (e.g. Security Area, Routing Area, Transport Area), whether the RFC extends the Security Considerations section of a previously published document, the wordcount of the section, and the existence of specific keywords.

The qualitative analysis might group Security Considerations sections by particular characteristics - those characteristics being discovered, in part, during an initial examination of the published documents.

5.2. Quantitative Methodology

Once the set of RFCs (where the size of the set is said to be n-set) to be considered is established, the quantitative analysis proceeds as follows for each item in the set:

- recording the date of publication
- recording the source of the original draft
- recording the category of the RFC (e.g. Informational, etc.)
- recording the size of the Security Considerations section in words and paragraphs
- recording whether or not the section updates or extends the Security Considerations section of a previously published document
- record whether or not examples exist in the Security Considerations section
- record whether or not example code appears in the Security Considerations section
- extracting the text and creating a new text removing the 100 most common English words
- against the new text created in the step above, perform text analytics - for instance, create a count of the number of occurrences of expected keywords

The result would be a series of metrics for n-set that establish certain characteristics of the Security Considerations sections of published RFCs. Once the quantitative data was gathered, further analysis of the data could be conducted (for instance, finding relationships between certain features of the RFCs).

5.3. Qualitative Methodology

The documents could also be assigned qualitative characteristics as a result of the survey. For instance, based on characteristics of the document, the Security Considerations could be characterized as "extensive" or "limited."

It is also clear that analysis of the Security Considerations could lead to other groupings. For instance, an analysis of recent RFCs shows that those documents which focus on cipher suites have quite

different security considerations sections compared to those that extend and existing protocol. Identification of those characteristics might be possible during an initial survey. In another case, those characteristics might emerge during the survey execution.

5.4. Implications of the Size of n-set

Since part of the execution of the survey has to be done via human intervention, the size of n-set has an effect on whether or not volunteers or organizations take on the effort. While it would be helpful to have as large a sample size as possible for the collection of data to support the analysis. It may be necessary to limit the size of n-set in practice.

One way to do this is to limit the range of dates for the RFCs being analyzed. A cursory, initial examination of Security Considerations sections seems to indicate that, in recent years, a clear set of prototypical security considerations sections has emerged and that there are distinct type of sections. By limiting the RFCs for the set of considered document to a specific, recent timeframe the goal is to focus the analysis on recent practice in crafting Security Considerations sections and moving them through the document approval process.

Another approach to solving the potential problem of the size of n-set is to incorporate a sampling regime for the selection of RFCs to be examined. This would be a meaningful approach in the event where the timeframe was extended, but where it was still desirable to reduce the size of n-set.

A third approach is to attempt to cluster the sample sets based on particular metrics (e.g. source working group, date, or the existence of certain keywords. Clustering might be a mechanism where correlations might be found to exist between certain characteristics of the RFCs and the quality of the security consideration section.

This proposal suggests to use the timeframe limitation but not incorporate sampling.

6. Security Considerations

This document describes goals and a methodology for surveying the existing body of Security Considerations in published RFCs. It does not create, extend or modify any protocols. Its intent is to provide a foundation for a data-driven discussion of the guidelines for writing a Security Considerations section in an RFC.

7. IANA Considerations

Upon publication, this document has no required actions for IANA.

8. References

8.1. Normative References

To Do.

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

[2] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

8.2. Informative References

To Do.

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A. Document History

[[To be removed from the final document]]

-0

Initial Internet Draft

Authors' Addresses

Mark McFadden
Internet policy advisors ltd
Madison Wisconsin US

Email: mark@internetpolicyadvisors.com