Network Working Group
Internet Draft

R. Atkinson,
Editor
2 June 1997

Guidelines for Writing RFC Text on Security Considerations

Status of this Memo

1. INTRODUCTION

This memo provides guidelines on how to write a useful "Security Considerations" section for an RFC. It is intended to provide information for RFC Authors and Editors in the hope of making their job easier.

Participants at the recent IAB Security Workshop came to consensus that any new protocol must not worsen the overall security of The Internet. The act of writing the "Security Considerations" section for a new protocol or technology should cause the editor of that document to reflect on the security issues and clearly document those issues.

A future version of this draft might be published as a Best Current Practice (BCP) RFC by the IESG or Informational RFC by the IAB.

2. OBJECTIVES

The "Security Considerations" section of an RFC is a mechanism via which the authors/editors of an RFC communicate to the reader the security issues (including threats) of the RFC topic and discuss mechanisms for mitigating or eliminating those threats. Each risk reduction mechanism not documented directly in that RFC should cite another RFC or document which describes the risk reduction mechanism.

The "Security Considerations" should be readable and focused on the matters discussed in that particular RFC.

After reading the "Security Considerations" of an RFC, the reader should have a clear understanding of the threats, methods for mitigating those threats, and the residual risks of deploying or using the procedures, technology, or protocol described in that RFC. The reader should be able to use the citations to further investigate the potential risk reduction mechanisms.

[outline for the Security Section needed here]

Cyfi

3. DEFINITIONS

Access Control
: The security service that protects against unauthorised use of system resources.

Active Attack
: An attack that is not a "passive attack".

Applicability Statement
: A formal statement of the operational environment in which a particular procedure, protocol, or technology is reasonable to use. This statement should also clearly indicate which operational environments are unreasonable or inappropriate for that procedure, protocol, or technology to be used.

Attack
: A threat action that results from an intelligent threat. An attack is an intentional act involving a means or method of exploiting a vulnerability. Attacks might be either passive or active.

Attacker
: A malicious or hostile adversary with the motivation and means to carry out an attack.

Authentication
: The security service that verifies an identity claimed by an entity. Note that in some situations, a particular mechanism that provides authentication might also provide integrity as an intrinsic by-product. Despite this,

authentication and integrity are conceptually separate services.

Availability
: The service ensuring that the network is accessible and usable upon demand by an authorised entity.

Confidentiality
: The security service that protects data from disclosure to unauthorised entities.

Countermeasure
: Something that reduces a threat or vulnerability by eliminating or preventing it, by minimising the harm it can cause, or by discovering and reporting it so that corrective action can be taken. For example, the vulnerability of a Cyclic Redundancy Check (CRC) can be reduced by suitable cryptographic techniques.

Critical
: A communications service is critical if its denial would jeopardize its user's ability to perform a primary mission function.

Denial of Service
: A kind of attack where the adversary seeks to deny a legitimate user access to some resource or service. For example, disrupting routing could cause packets to be lost or misdelivered, thus denying use of the network to legitimate users.

Gateway
: Usually a synonym for "router".

Hosts
: Computers that run full Internet protocol stacks and support application protocols. Hosts range from small personal computers to large supercomputers. In some communities these are considered 'end systems'.

Infrastructure
: The Internet infrastructure includes networks, relays, routers, and any necessary support hosts (e.g. those hosts that provide DNS service).

Integrity
: The security service that protects data from unauthorised alteration or destruction.

Non-repudiation
: The service that protects against false denial of a communication. For example, this service would prevent the sender of a signed email message from being able to falsely deny sending that message.

Passive Attack
: An attack that only observes the operation of network elements to learn about them or observes data and data traffic characteristics to learn the data's semantic content.

Principle of Least Privilege
: TBD

Risk
: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Analysis
: A systemic identification of valuable resources, threats, and countermeasures along with quantification of the loss exposures based on estimated frequencies and costs. [NBS79, HR91] The analysis then lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first.

Sensitive
: Data is sensitive if its disclosure, alteration, or destruction would adversely affect the interests or business of its owner or user. There can be different degrees of sensitivity. For example, compromise of some sensitive data might cause a death while compromise of other sensitive data might merely cause a brief disruption to normal operations.

Threat
: A potential violation of security. A threat exists when there is a circumstance, capability, or event that could breach security and cause harm. Threats might be either accidental or intentional. CERT Advisories document threats, though not all threats are documented in CERT Advisories.

Vulnerability
: A flaw or weakness in a system's security. A characteristic that could be exploited to cause harm by disclosing, modifying, or destroying functions or resources, or by denying service to authorised users. Existence of a vulnerability creates

a threat.

4. MINIMAL THREAT ENVIRONMENT

[This section seems mis-organised]

This section describes the minimal threat environment applicable to every RFC. Alternately put, any RFC written should have a Security Considerations section that assumes the following threats (at a minimum) exist.

Any class of attack described in a CERT Advisory or equivalent is considered to be a legitimate potential threat. CERT Advisories are quite predictable given knowledge of the threat. Hence, CERT Advisories are considered an existence proof of the threat, but do not constitute a threat analysis.

Other known kinds of attacks (e.g. from published magazine articles, from conference papers) are also considered to be legitimate potential threats. For example, many of the recently seen attacks on the Internet use techniques and exploit vulnerabilities described in the literature some years ago. [Bellovin89]

5. GUIDELINES

There should be a clear description of the kinds of threats on the described protocol or technology. This should be approached as an effort to perform "due diligence" in describing all known or foreseeable risks and threats to potential implementers and users.

The methods via which those some or all of those threats are mitigated or eliminated (e.g. firewalls, packet filtering, encryption, cryptographic authentication) should be described along with an indication of the extent to which the particular method mitigates the risk. If external mechanisms (e.g. IPsec) are identified for risk reduction, the relevant RFCs or other documents should be cited so the reader knows where to obtain more information.

The threat environment addressed by the Security Considerations section MUST at a minimum include deployment across the global Internet across multiple administrative boundaries without assuming that firewalls are in place. It is not acceptable to only discuss threats applicable to LANs and ignore the broader threat

environment. All IETF standards-track protocols are considered likely to have deployment in the global Internet. In some cases, there might be an Applicability Statement discouraging use of a technology or protocol in a particular environment. Nonetheless, the security issues of broader deployment should be discussed in the document.

There should be a clear description of the residual risk to the user or operator of that protocol after threat mitigation has been deployed. Such risks might arise from compromise in a related protocol (e.g. IPsec is useless if key management has been compromised), from incorrect implementation, compromise of the security technology used for risk reduction (e.g. 40-bit DES), or might be risks that are not addressed by the protocol specification (e.g. denial of service attacks on an underlying link protocol).

There should also be some discussion of potential security risks arising from obvious potential misapplications of the protocol or technology described in the RFC. This might be coupled with an Applicability Statement for that RFC.

6. EXAMPLES

An RFC discussing TCP should mention the SYN flooding denial of service attacks and possible implementation strategies for reducing that risk. [CERT96]

An RFC discussing HTTP should discuss the potential for eavesdroppers to obtain credit card or other personal data when security techniques are not in use. Such an RFC should also recommend use of appropriate security techniques (e.g. SET, SSL, SHTTP) to mitigate that threat. [SHTTP,SSL,SET]

An RFC discussing a security protocol might discuss common implementation flaws so that implementers know how to avoid those. [Atk95]

7. DESIGN SUGGESTIONS

When a protocol uses cryptography to provide some security service, the protocol should be designed in a manner independent of any particular cryptographic algorithm. This permits future substitution of a new cryptographic algorithm for the originally specified cryptographic algorithm if the original is broken. This property is often referred to as "algorithm-independence".

Also, when a protocol relies on the randomness of some number, it should clearly indicate what level of randomness is required. If cryptographic randomness is required, it would be reasonable to help implementers by citing a reference or two (e.g. ECS94) on how to obtain such randomness.

REFERENCES

[Bellovin89] Stephen M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, No. 2, ACM, New York, NY, March 1989.

[CERT96] US DoD Computer Emergency Response Team, "TCP SYN Flooding Attacks", CERT Advisory CA-96.21, 19 September 1996. ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding

[NBS79] US National Bureau of Standards, "Guideline for Automatic Data Processing and Risk Analysis", Federal Information Processing Standard (FIPS) 65, National Bureau of Standards, Gaithersburg, MD, USA, 1 August 1979.

[SSL]
[SHTTP]
[SET]

[SK] Robert W. Shirey & Stephen T. Kent, "Security Principles for Internet Architecture".

[HR91] P. Holbrook, J. Reynolds, "Site Security Handbook", RFC-1244, 23 July 1991.

[ECS94] D. Eastlake, S. Crocker, J. Schiller, "Randomness Recommendations for Security", RFC-1750, 29 December 1994.

[Atk95] R. Atkinson, "IP Security Architecture", RFC-1825, July 1995.

ACKNOWLEDGEMENTS

This note was written after the IAB Security Workshop held in early 1997. Everyone at that workshop has contributed to this document, either via email or in the discussions at that workshop. Some of the specific text above is taken from an email message written by Fred Baker. Virtually all of the definitions in Section 3 are excerpted with permission from a document "Security Principles for Internet Architecture" by Robert W. Shirey and Stephen T. Kent [SK].

Any errors are the responsibility of the editor.

Editor's Addresses:

Randall Atkinson <rja@home.net>

@Home Network
385 Ravendale Drive
Mountain View, CA 94043

Voice: +1 (415) 944-7200