Network Working Group
Request for Comments: 3365
BCP: 61
Category: Best Current Practice

J. Schiller
Massachusetts Institute of Technology

August 2002

Strong Security Requirements for Internet Engineering Task Force Standard Protocols

Status of this Memo

Copyright Notice

Abstract

It is the consensus of the IETF that IETF standard protocols MUST make use of appropriate strong security mechanisms. This document describes the history and rationale for this doctrine and establishes this doctrine as a best current practice.

Table of Contents

1. Introduction

The purpose of this document is to document the IETF consensus on security requirements for protocols as well as to provide the background and motivation for them.

The Internet is a global network of independently managed networks and hosts. As such there is no central authority responsible for the operation of the network. There is no central authority responsible for the provision of security across the network either.

Security needs to be provided end-to-end or host to host. The IETF's security role is to ensure that IETF standard protocols have the necessary features to provide appropriate security for the application as it may be used across the Internet. Mandatory to implement mechanisms should provide adequate security to protect sensitive business applications.

2. Terminology

Although we are not defining a protocol standard in this document we will use the terms MUST, MAY, SHOULD and friends in the ways defined by [RFC2119].

3. Security Services

[RFC2828] provides a comprehensive listing of internetwork security services and their definitions. Here are three essential definitions:

* Authentication service: A security service that verifies an identity claimed by or for an entity, be it a process, computer system, or person. At the internetwork layer, this includes verifying that a datagram came from where it purports to originate. At the application layer, this includes verifying that the entity performing an operation is who it claims to be.

* Data confidentiality service: A security service that protects data against unauthorized disclosure to unauthorized individuals or processes. (Internet Standards Documents SHOULD NOT use "data confidentiality" as a synonym for "privacy", which is a different concept. Privacy refers to the right of an entity, normally a person, acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.)

* Data integrity service: A security service that protects against unauthorized changes to data, including both intentional change (including destruction) and accidental change (including loss), by ensuring that changes to data are detectable.

4. Some Properties of the Internet

As mentioned earlier, the Internet provides no inherent security. Enclaves of networking exist where users believe that security is provided by the environment itself. An example would be a company network not connected to the global Internet.

One might imagine that protocols designed to operate in such an enclave would not require any security services, as the security is provided by the environment.

History has shown that applications that operate using the TCP/IP Protocol Suite wind up being used over the Internet. This is true even when the original application was not envisioned to be used in a "wide area" Internet environment. If an application isn't designed to provide security, users of the application discover that they are vulnerable to attack.

5. IETF Security Technology

The IETF has several security protocols and standards. IP Security (IPsec [RFC2411]), Transport Layer Security (TLS [RFC2246]) are two well known protocols. Simple Authentication and Security Layer (SASL [RFC2222] and the Generic Security Service Application Programming Interface (GSSAPI [RFC2743]) provide services within the context of a "host" protocol. They can be viewed as "toolkits" to use within another protocol.

One of the critical choices that a protocol designer must make is whether to make use of one of the existing protocols, engineer their own protocol to use one of the standard tools or do something completely different.

There is no one correct answer for all protocols and designers really need to look at the threats to their own protocol and design appropriate counter-measures. The purpose of the "Security Considerations" Section required to be present in an RFC on the Internet Standards Track is to provide a place for protocol designers to document the threats and explain the logic to their security design.

6. The Danvers Doctrine

At the 32cd IETF held in Danvers, Massachusetts during April of 1995 the IESG asked the plenary for a consensus on the strength of security that should be provided by IETF standards. Although the immediate issue before the IETF was whether or not to support "export" grade security (which is to say weak security) in standards the question raised the generic issue of security in general.

The overwhelming consensus was that the IETF should standardize on the use of the best security available, regardless of national policies. This consensus is often referred to as the "Danvers Doctrine".

Over time we have extended the interpretation of the Danvers Doctrine to imply that all IETF protocols should operate securely. How can one argue against this?

Since 1995 the Internet has increasingly come under attack from various malicious actors. In 2000 significant press coverage was devoted to Distributed Denial of Service attacks. However many of these attacks were launched by first compromising an Internet connected computer system. Usually many systems are compromised in order to launch a significant distributed attack.

A conclusion we can draw from all of this is that if we fail to provide secure protocols, then the Internet will become less useful in providing an international communications infrastructure, which appears to be its destiny.

One of the continuing arguments we hear against building security into protocols is the argument that a given protocol is intended only for use in "protected" environments where security will not be an issue.

However it is very hard to predict how a protocol will be used in the future. What may be intended only for a restricted environment may well wind up being deployed in the global Internet. We cannot wait until that point to "fix" security problems. By the time we realize this deployment, it is too late.

The solution is that we MUST implement strong security in all protocols to provide for the all too frequent day when the protocol comes into widespread use in the global Internet.

7. MUST is for Implementors

We often say that Security is a MUST implement. It is worth noting that there is a significant different between MUST implement and MUST use.

As mentioned earlier, some protocols may be deployed in secure enclaves for which security isn't an issue and security protocol processing may add a significant performance degradation. Therefore it is completely reasonable for security features to be an option that the end user of the protocol may choose to disable. Note that we are using a fuzzy definition of "end user" here. We mean not only the ultimate end user, but any deployer of a technology, which may be an entire enterprise.

However security must be a MUST IMPLEMENT so that end users will have the option of enabling it when the situation calls for it.

8. Is Encryption a MUST?

Not necessarily. However we need to be a bit more precise here. Exactly what security services are appropriate for a given protocol depends heavily on the application it is implementing. Many people assume that encryption means confidentiality. In other words the encryption of the content of protocol messages.

However there are many applications where confidentiality is not a requirement, but authentication and integrity are.

One example might be in a building control application where we are using IP technology to operate heat and vent controls. There is likely no requirement to protect the confidentiality of messages that instruct heat vents to open and close. However authentication and integrity are likely important if we are to protect the building from a malicious actor raising or lowering the temperature at will.

Yet we often require cryptographic technology to implement authentication and integrity of protocol messages. So if the question is "MUST we implement confidentiality?" the answer will be "depends". However if the question is "MUST we make use of cryptographic technology?" the answer is "likely".

9. Crypto Seems to Have a Bad Name

The mention of cryptographic technology in many IETF forums causes eyes to glaze over and resistance to increase.

Many people seem to associate the word "cryptography" with concerns such as export control and performance. Some just plain do not understand it and therefore shy away from its use. However many of these concerns are unfounded.

Today export control, at least from most of the developed world, is becoming less of a concern. And even where it is a concern, the concern is not over cryptography itself but in its use in providing confidentiality.

There are performance issues when you make use of cryptographic technology. However we pride ourselves in the IETF as being engineers. It is an engineering exercise to figure out the appropriate way to make use of cryptographic technology so as to eliminate or at least minimize the impact of using cryptography within a given protocol.

Finally, as to understanding cryptography, you don’t have to. In other words, you do not need to become a cryptographer in order to effectively make use of cryptographic technology. Instead you make use of existing well understood ciphers and cipher suites to solve the engineering problem you face.

One of the goals that we have in the Security Area of the IETF is to come up with guides so that protocol implementers can choose appropriate technology without having to understand the minutiae.

10. Security Considerations

This document is about the IETF’s requirement that security be considered in the implementation of protocols. Therefore it is entirely about security!

11. Acknowledgements

The author would like to acknowledge the participation of the Security Area Advisory Group and in particular Rob Shirey, Ran Atkinson, Steve Bellovin, Marc Blanchet, Steve Kent, Randy Bush, Dave Crocker, Stephen Farrell, Paul Hoffman, Russ Housley, Christian Huitema, Melinda Shore, Adam Shostack and Kurt D. Zeilenga.

12. References

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

[RFC2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[RFC2411] Thayer, R., Doraswamy, N. and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1.", RFC 2743, January 2000.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

13. Author's Address

Jeffrey I. Schiller
MIT Room W92-190
77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA

Phone: +1 (617) 253-8400
EMail: jis@mit.edu

14. Full Copyright Statement

Acknowledgement

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