Network Working Group D. Crocker
Internet Draft Brandenburg InternetWorking
draft-crocker-mime-security-00.txt October, 2002

Expires: <4/03>

Mandatory MIME Security Considered Harmful

STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

(IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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.

ABSTRACT

MIME is the preferred Internet mechanism for labeling and aggregating bulk data objects, such as for email and the web, and it is essential to have useful, MIME-based mechanisms. Indeed, two standards have existed for some years: OpenPGP and S/MIME. A current IESG policy for new application protocols requires that they mandate conforming implementations to support a single security mechanism. For applications using MIME security, this means that the specification is required to choose between S/MIME and OpenPGP. Although well-intentioned, the policy is at least useless and at worst counter-productive. This note discusses the problem and suggests returning to the previously acceptable policy that better reflects the lack of market resolve for MIME security.

INTRODUCTION

Most uses of the global Internet can benefit from having universal security mechanisms, such as for authentication and privacy. Certainly the success of SSL/TLS for commerce over the Web is an example of that benefit. Identity spoofing and unauthorized disclosure do occur without such protection, and the problem only gets worse as the Internet gets larger.

Transfer-level mechanisms provide only hop-by-hop protection and there are times that an end-to-end mechanism is necessary. This is achieved by encapsulating the data object in a security wrapper. For the Internet protocols, by far the most common method of labeling and aggregating bulk data is with [MIME1, MIME2]. The focus on providing end-to-end security has therefore been through MIME-based security. This note considers the problems in the current IESG policy for MIME-based security in new application protocols.

The IETF has two, competing specifications for secure object wrapping: [S/MIME] and [OpenPGP]. In terms of basic security capabilities, they are equivalent. They have existed for some years and each has achieved a modicum of use. What is noteworthy is that neither has gained large-scale popularity. In a network of at least 100 million users, "large-scale" needs to mean at least tens of millions. A protocol that is popular with a small fraction of the Internet well might be useful, but it cannot claim the type of Internet-scale adoption that IETF standards typically seek. Certainly most users of MIME-based applications would say that they want and need security. And most Internet users use MIME, the requirement for MIME-based security really does need an Internet-scale solution..

The reasons for this sustained lack of market acceptance and use of a MIME-based security are varied. The basic algorithms work. Products implement them. Some users make effective use of these mechanisms. Still, regular use of OpenPGP or S/MIME is minimal. Contributing causes include difficult user interfaces, complex public key certificate mechanisms that have yet to scale well, as well as usage and intellectual property legal barriers. Of these causes the IETF certainly should focus on the technical factors within its skillset. The other factors require the IETF to wait for resolution elsewhere.

Until very recently, the IESG has approved application protocol specifications that contained security text of the form:

> Implementations may choose to offer MIME-based security services for message authentication, integrity and confidentiality, through OpenPGP or S/MIME.

The current IESG policy, requires re-writing this text to be:

> Implementations MUST offer OpenPGP MIME-based security services for message authentication, integrity and confidentiality.

or:

> Implementations MUST offer S/MIME MIME-based security services for message authentication, integrity and confidentiality.

There is strong IETF consensus that strong security mechanisms need to be available to users. Hence the bias towards requiring its specification in IETF protocols is extremely well-founded, and there is no reasonable basis for arguing that application protocol security is a secondary concern.

The question is precisely what details of MIME-based security should be included in IETF standards? What is practical, within the realities of current security technology and current market behavior?

IESG POLICY

As demonstrated above, the IESG currently requires new application protocols to mandate that conforming implementations support a specific security mechanism. That is, the specification is required to use RFC 2119 keyword MUST [KEY] and specify a single, specific choice for the security mechanism to be offered by all implementations.

For applications using MIME-based security, the IESG now requires a specification to choose between S/MIME and OpenPGP. This requirement is problematic.

There are a number of arguments in favor of mandating that protocols using MIME must support a single MIME-based security mechanism. For example:

* The market will not demand security until it is too late and security can not be retro-fitted. Therefore the IETF is assisting the market -- in effect, making the decision for the market, before it is too late. If this effort does not succeed, what is the harm?

* The requirement for interoperability means that two independent implementations of the same specification need to interoperate with reasonable security. This cannot be achieved unless there is a common security mechanism to use.

These represent valid concerns. However there are several reasons the resulting policy is ill-advised with respect to MIME security:

* Mandating a technology that has so far failed to achieve popularity will not make it popular. The IETF does technical engineering, not behavioral engineering. OpenPGP and S/MIME are already on the standards track. Having a new application protocol specification arbitrarily choose one of the two, and mandate its use, provides no further technical detail.

* When two applications have the same operational characteristics, and they have the same security requirements, then it is counter-productive to have each of them specify their own security details. First it is more likely that one of them will contain an error in the specification, especially when the function involves the complexity and subtlety of a networking security mechanism. Second it encourages divergence when there is no technical basis for it and no market pressure for it. Given that the competition between S/MIME and OpenPGP has gone on for some years, and that there is still no clear winner, any application that mandates one over the other does so arbitrarily. Besides lacking objective merit such an arbitrary choice means that different applications will make different choices. This only servers to further fragment the market.

* In reality the IESG (IETF) still has not decided on a specific MIME security solution. Instead, the IESG is attempting to swap disagreement between individuals (in the market) for disagreement between IETF working groups. Even so, the market disagreement remains.

* When an application chooses one alternative over the other, it forces wasteful implementation effort for services wishing to use the other. In order for that service to claim that it is "conformant" with the application protocol specification, then it must implement the mandated security choice, even though it will not be used. (The IETF would do well to remember back to that peculiar time in history, when purchasing departments for customers of networking products would mandate that the product support OSI, even though the product was going to be used exclusively in a TCP/IP network. We should be careful not to replicate that bit of pro forma expense.)

THE DILEMMA OF IAB GUIDANCE

The recent IAB Internet-Draft [SECCONS] is an excellent tutorial on the security concerns that a protocol should specification to consider. Section 5 gives explicit guidance for writing the Security Considerations section of a specification and is particularly helpful. Internet-Draft [SECMECH] highlights the difficulties in devising security mechanisms for Internet Protocols and in noting that "Internet scale" service is quite different from "LAN scale".

Note that Section 4.7 of [SECCONS] treats S/MIME and OpenPGP equally. It gives no guidance to protocol authors about differences between the two that justify choosing between them. In Section 5.8 of [SECMECH] MIME Security Multiparts [SECMULT] is recommended generically, although Multipart/Encrypted is used only by OpenPGP. S/MIME uses an opaque MIME Application content-type.

Section 5.10 of [SECMECH] gives an excellent discussion of the differences between S/MIME and OpenPGP. However the discussion makes quite clear that neither has yet proved adequate for the large-scale Internet. How, then, can an application protocol writer choose between them?

A MODEST PROPOSAL

As [SECCONS] directs, the specification of an application protocol must include a careful review of the threats that are a realistic concern and they must provide mechanisms for satisfying those concerns. However a specification cannot ignore established market behaviors and pretend to mandate a choice that the market has, so far, firmly refused to agree to.

In order to find a productive path that responds to these competing constraints, a number of actions would be helpful:

* The IETF should develop a standard framework for MIME-based integrity, authentication, confidentiality and signed receipt, and it should specify profiles of existing Internet standards, to provide those functions.

* The IETF must be constructive in dealing with the reality of having two, competing, equivalent standards for a security function -- or any other function -- but no clear technical basis for choosing between them. Other specifications that need the function can do no more than cite the choice, until the market demonstrates a clear preference for one. The IETF can, and should, strongly encourage use of these standards, but it cannot force the new protocol to choose between them.

* Were there a single choice for object security, there would still a choice between object security and transfer-based (hop-by-hop) security. [SECMECH] provides a helpful step towards developing a clear sense of the basis for making that choice. Until this has reasonable consensus, it is not possible for a working group to mandate one over the other, except arbitrarily. In the matter of security services, such arbitrary choices seem to confuse more than they help. Hence, IETF applications need to cite when security requirements can be satisfied through either approach, recommend that a service use at least one of them, but refrain from requiring a particular choice. An example of this approach is in [SFAX].

* The IETF should formulate a clear sense of the reason(s) that MIME object security has not become popular yet. If the reasons are technical, the IETF should then remedy the deficiency.

REFERENCES

[MIME1] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[MIME2] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046 November 1996.

[S/MIME] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[OpenPGP] M. Elkins, D. Del Torto, R. Levien and T. Roessler. , "MIME Security with OpenPGP", RFC 3156, August 2001

[SFAX] H. Ohno, J. Murai and D. Wing, "A Simple Mode of Facsimile Using Internet Mail", RFC: 2305, March 1998

[KEY] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[SECCONS] E. Rescorla and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", draft-iab-sec-cons-01.txt, October 2002

[SECMECH] S. Bellovin and J.Schiller, "Security Mechanisms for the Internet", draft-iab-secmech-01.txt, June 2002

[SECMULT] J. Galvin, S. Murphy, S. Crocker, and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, Oct. 1995