Network Working Group
INTERNET-DRAFT
draft-uusitalo-sipping-algorithm-agreement-00.txt
Expires: August 2002

J. Arkko
V. Torvinen
I. Uusitalo
Ericsson

February 2002

Requirements for SIP Security Mechanism Agreement

Status of this Memo

1. Abstract

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution and multimedia conferences. SIP has a number of security mechanisms used for hop-by-hop or end-to-end protection. In this document we discuss requirements concerning SIP security mechanism agreement.

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].

3. Table of contents

4. Introduction and Motivation

SIP has a number of security mechanisms for hop-by-hop and end-to-end protection. Some of the security mechanisms are built-in to the SIP protocol, such as variants of HTTP authentication and secure attachments such as S/MIME. SIP can also use underlying security protocols such as IPSec/IKE [7] and TLS [6]. Some of the built-in security protocols have alternative algorithms and parameters. A way to negotiate the used mechanisms, and parameters used within them, is needed. Without a secure negotiation method SIP is vulnerable to certain attacks. For example, HTTP authentication is known to be vulnerable to so called Bidding-Down attacks. There a Man-In-The-Middle attacker modifies messages in such a way that communicating parties believe the other side only supports weaker algorithms than they actually do. In small workstation networks these issues might not be very relevant, but the deployment of hundreds of millions of small devices with little or no possibilities for coordinated security policies, let alone software upgrades makes these issues much worse. You either deny connections from large amounts of older equipment or risk losing the benefit of new algorithms through attacks that are trivial to attackers.

The need for a security mechanism agreement is also supported by the fact that deployment of a large number of SIP-based consumer devices such as 3GPP terminals requires all network devices to be able to accommodate both current and future mechanisms. There is no possibility for instantaneous change since new solutions are coming gradually as new standards and product releases occur. It isn't even possible to upgrade some of the devices without getting completely new hardware.

The conclusions above are supported by the requirements from 3GPP [2] and discussed in more detail in [5].

This document is an effort to define requirements for secure algorithm agreement used with SIP protocol. Most of the requirements

are discussed also in "3GPP Requirements on SIP" [2], but we consider them to be beneficial also to infrastructures other than 3GPP. Therefore they've been separated into this new draft that's easier to deal with.

The requirements of this document address attacks discussed in chapter 22.1.3 and mechanisms discussed in chapter 22.2 of SIP-draft [1].

5. Definitions

MITM: Man-In-The-Middle

6. Requirements

Some of the built-in SIP security functions like HTTP Digest have alternative algorithms and other parameters. Different algorithms are suitable for different situations. Also, security holes might be found from old algorithms and new algorithms will evolve. Without a secure method to choose between algorithms and their parameters SIP is vulnerable to certain attacks, for example the MITM attack described above and in [5].

>> Req 1: It MUST be possible for a SIP node to select message protection algorithms and parameters within security mechanisms.

Also new security mechanisms will evolve and existing ones, like HTTP Digest or TLS, might be used in parallel depending on the situation. In order to achieve interoperability and backward compatibility, it would be beneficial if a SIP node could choose the security mechanism used.

>> Req 2: A SIP node MUST be able to select a SIP security mechanism among supported alternatives.

The negotiation methods must not be vulnerable to so called Bidding-Down attacks. In such an attack a MITM attacker modifies messages in such a way that parties believe the other side supports weaker security methods than they actually do.

>> Req 3: The negotiation mechanism MUST protect against attackers who do not have access to authentication credentials. In particular, it must not be possible for man-in-the-middle attackers to influence the negotiation result such that services with lower or no security are negotiated.

7. Discussion

Bidding-down protection is needed between different security schemes. It will not be sufficient to do bidding-down protection just for e.g. Digest. In SIP [8], only Digest is required, and most

3GPP terminals will also apply Digest. Hence a very large number of devices supporting only Digest will be deployed, and these devices

will probably be used for long in the future. Now, assume that in the future other mechanisms, for example S/MIME or TLS, are used in parallel with Digest. The new devices capable of these additional security mechanisms could offer to run e.g. TLS, but without protection against bidding-down attacks an attacker could make parties believe that the device on the other end does not support TLS. Therefore TLS would not be used even if both devices supported it.

Algorithms can be agreed upon with basic SIP features, such as OPTIONS request and Require, Supported headers. They are capable of informing parties about various capabilities including security mechanisms. However, using these features in a straightforward manner does not guarantee the security of an agreement. In their basic form these methods are vulnerable to for example bidding-down attacks. At least some kind of integrity protection for the methods is needed.

Draft "Security Mechanism Agreement for SIP connections" [5] proposes a secure solution for algorithm agreement. There the security features are represented as regular option tags in SIP. The client announces a list of supported option tags in its first message, and the server returns its selection in the second message. The agreement is secured by simply repeating the client's original list of option tags in the client's first protected request (protected with a lower layer protocol). The solution in [5] supports both end-to-end and hop-by-hop agreement in a controllable fashion and without a large increase in roundtrips.

8. Acknowledgments

We would like to thank Allison Mankin, Dean Willis, Rohan Mahy, Bernard Aboba, Miguel Garcia, as well as numerous people at 3GPP SA3 and Ericsson for interesting discussions in this problem space.

9. References

1. Rosenberg, J., et al., "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-07.txt, February 2002, work in progress.

2. Garcia, M., et al., "3GPP requirements on SIP", draft-garcia-sipping-3gpp-regs-02.txt, November 2001, work in progress.

3. 3GPP TS 23.228: "IP Multimedia (IM) Subsystem (Stage 2) - Release 5". Version 5.3.0 is available at ftp://ftp.3gpp.org/Specs/2001-12/Rel-5/23_series/23228-530.zip

4. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call

control based on SIP and SDP". Version 1.9.0 is available at
ftp://ftp.3gpp.org/tsg_cn/WG1_mm-cc-sm/TSGN1_22/Docs/N1-

20280_24228-190.zip

5. Arkko, J., et al., "Security Mechanism Agreement for SIP Connections", draft-arkko-sip-sec-agree-00.txt, November 2001, work in progress.

6. Dierks, T., Allen, C., "The TLS Protocol, Version 1.0", RCF 2246, January 1999.

7. Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

8. Rosenberg, J., et al., "SIP:Session Initiation Protocol", draft-ietf-sip-rfc2543bis-05.txt, October 2001, work in progress.

10. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Vesa Torvinen
Oy LM Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Ilkka Uusitalo
Oy LM Ericsson Ab
Tutkijantie 2C
90570 Oulu
Finland

Phone: +358 40 7245404
EMail: ilkka.uusitalo@ericsson.fi