Effects of Security Mechanisms on the Development and Application of Testing Techniques Exemplified with Voice over IP

Annika Renz, Daniel Hartmann, Diederich Wermser, Research Group IP-based Communication Systems, Ostfalia University of Applied Sciences, Wolfenbüttel, Germany

Abstract

Even for network elements, which communicate via protocols extended by security functions, compatibility must be ensured across manufacturers. The main question is, whether and how testing techniques must be modified, extended or even newly developed to perform the required tests to ensure interoperability for secured communication protocols. To be able to answer this question, the test object of the different testing techniques must be observed. The changes caused by the additional security mechanisms must be investigated. This paper utilizes the *Session Initiation Protocol* (SIP) and the *Realtime Transport Protocol* (RTP) used with *Voice over IP* (VoIP) to explain the effects of security mechanisms on testing techniques.

This paper is based on the work with research focus „Modellbasierte Validierung zur Absicherung von automotiven Kommunikationsnetzwerken“, which is supported by the Department for Science and Culture of Lower Saxony in the context of the AGIP programme.

Keywords: Conformity Testing, Interoperability Testing, Testing Techniques, IP Multimedia Subsystem (IMS), Security Mechanisms, Voice over IP (VoIP), Session Initiation Protocol (SIP), SIP Security (SIPS), Transport Layer Security (TLS), Secure Realtime Transport Protocol (SRTP), ZRTP

1 Introduction

The usage of security mechanisms to transmit information via communication protocols allows more granular control of a person or company’s privacy. Both encoding algorithms and transport protocols to exchange keys can belong to these security mechanisms. By using an array of testing techniques, the compatibility between network elements implementing security mechanisms additional to the communication protocols, should be ensured. The validation of function and security of these security mechanisms is **not** the aim, but rather the guarantee for intercompatibility of network elements and among manufacturers.

This paper points out the effects of security mechanisms on the development and application of testing techniques exemplified with *Voice over IP* (VoIP). Firstly, the common security mechanisms for VoIP will be introduced. Next, the effects of these security mechanisms on conformity testing, interoperability testing as well as stress testing will be examined and illustrated with some practical examples.

2 Security Mechanisms for VoIP

The exchange of information within a telecommunication network involves diverse security requirements. These are: the protection against abusing a subscriber’s access to the network provider, the protection of identity (e.g. name) and personal information (e.g. whereabouts, IP address) of a subscriber, the protection against unauthorised eavesdropping/recording and the guarantee of integrity of incoming payload [18].

Security mechanisms, which are applied to fulfil these requirements, are SIP Security Agreement to negotiate a transport security mechanism, MIKEY and ZRTP to exchange keys, S/MIME to encrypt the content of individual SIP messages, SIPS and SIP over TLS to encrypt signalling and, finally, SRTP to encrypt payload [7]. Afterwards, security mechanisms will not be differentiated based on their function when talking about signalling and payload, but based on the exchange level.

3 Effects of Security Mechanisms on Testing Techniques

The usage of security mechanisms always effects testing techniques when the test object is modified (protocol, functionality, stress behaviour etc.), or when the security mechanisms themselves become test objects.

Table 1 Effects of security mechanisms for VoIP on the different testing techniques

Security Mechanism \ Effects on…		Conformity?	Interoperability?	Stress behaviour?
Signalling	SIPS [17]	Yes	Yes	Yes
	SIP over TLS [16]	No	Yes	Yes
	S/MIME [11]	No	Yes	Yes
	Sip Security Agreement [13]	Yes	Yes	Yes
	MIKEY [15]	Yes	Yes	Yes
Payload	SRTP [14]	Yes	Yes	Yes
	ZRTP [5]	Yes	Yes	Yes

Table 1 gives an overview of the security mechanisms named in section 2 and shows whether they effect conformity testing, interoperability testing and stress testing. The following sections will explain the effects on the particular testing techniques using practical examples.

3.1 Conformity Testing

Conformity testing checks whether a protocol instance correctly implements the related protocol specification [2]. Conformity test cases must be defined and applied when testing each protocol instance implemented by a network element.

If security mechanisms and communication protocols are not interdependent, i.e. communication and security are located in different protocol layers, it is sufficient to perform independent conformity tests on each element. This is the case with SIP over TLS.

3.1.1 Usage of Additional Protocols

The moment additional protocols are used to apply security mechanisms (e.g. ZRTP to exchange keys for SRTP, **Figure 1**), new test cases must be developed.

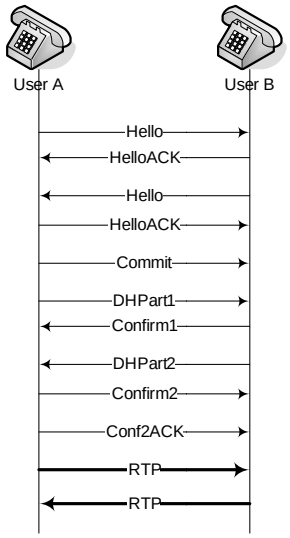

Figure 1 ZRTP handshake for key exchange

3.1.2 Additional Header Fields

The extension of SIP with additional header fields like SIP Security Agreement (**Figure 2**) changes the SIP state machine. The existing set of conformity test cases no longer matches the new state machine. Accordingly, a new set of conformity test cases must be developed, perhaps by reusing or modifying the existing test cases. It is very possible that the new set of test cases includes a subset of the existing one.

```
We define three new SIP header fields, namely Security-Client,
Security-Server and Security-Verify.  The notation used in the
Augmented BNF definitions for the syntax elements in this section is
as used in SIP [1], and any elements not defined in this section are
as defined in SIP and the documents to which it refers:

   security-client  = "Security-Client" HCOLON
                      sec-mechanism *(COMMA sec-mechanism)
   security-server  = "Security-Server" HCOLON
                      sec-mechanism *(COMMA sec-mechanism)
   security-verify  = "Security-Verify" HCOLON
                      sec-mechanism *(COMMA sec-mechanism)
```

Figure 2 Additional header fields when registering using SIP Security Agreement (excerpt from RFC 3329 [13])

3.1.3 Dependency on Header Field Contents

The SIP state machine cannot only be changed by the addition of new header fields. Changes may also occur when the contents of header fields shall affect the behaviour of network elements. The registration of a terminal device serves as an example scenario to illustrate this issue. Concerning this, **Figure 3** und **Figure 5** show excerpts from the protocol specifications for SIP (RFC 3261 [12]) and SIPS (RFC 5630 [17]).

Figure 3 shows an excerpt from RFC 3261 where the construction of a REGISTER request is described.

Figure 5 describes the behaviour of a registrar registering terminal devices using SIP and SIPS URIs. The excerpt shown extends the requirements of RFC 3261.

```
The following header fields, except Contact, MUST be included in a
REGISTER request.  A Contact header field MAY be included:

   Request-URI: The Request-URI names the domain of the location
        service for which the registration is meant (for example,
        "sip:chicago.com").  The "userinfo" and "@" components of the
        SIP URI MUST NOT be present.

   To: The To header field contains the address of record whose
        registration is to be created, queried, or modified.  The To
        header field and the Request-URI field typically differ, as
        the former contains a user name.  This address-of-record MUST
        be a SIP URI or SIPS URI.

   From: The From header field contains the address-of-record of the
        person responsible for the registration.  The value is the
        same as the To header field unless the request is a third-
        party registration.

   Call-ID: All registrations from a UAC SHOULD use the same Call-ID
        header field value for registrations sent to a particular
        registrar.

        If the same client were to use different Call-ID values, a
        registrar could not detect whether a delayed REGISTER request
        might have arrived out of order.

   CSeq: The CSeq value guarantees proper ordering of REGISTER
        requests.  A UA MUST increment the CSeq value by one for each
        REGISTER request with the same Call-ID.

   Contact: REGISTER requests MAY contain a Contact header field with
        zero or more values containing address bindings.
```

from RFC 3261 [12])

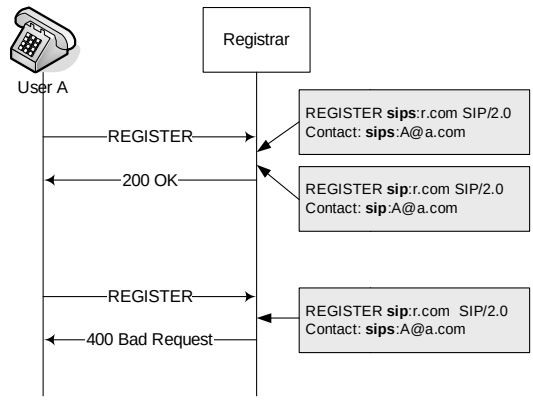

Figure 4 Registrations with different URI schemes

Figure 4 illustrates the behaviour of a registrar concerning the handling of SIP and SIPS URIs as a sequence diagram. This diagram shows that the registrar must check and compare the scheme of the request URI and the Contact header field (also Path header field, not shown). This requirement was not present in RFC 3261.

Figure 6 exemplifies the procedure of a conformity test, where the *Main Test Component* (MTC) receives a REGISTER request from the system under test, demands an authentication if required and, otherwise, confirms the REGISTER request with a 200 OK response. The MTC would also have to check the demand of RFC 3261 for the correct construction of a REGISTER request (Figure 3).

```
The UAC registers Contacts header fields to either a SIPS or a SIP
AOR.  From a routing perspective, it does not matter which one is
used for registration as they identify the same resource.  The
registrar MUST consider AORs that are identical except for one having
the SIP scheme and the other having the SIPS scheme to be equivalent.

A registrar MUST accept a binding to a SIPS Contact header field only
if all the appropriate URIs are of the SIPS scheme; otherwise, there
could be an inadvertent binding of a secure resource (SIPS) to an
unsecured one (SIP).  This includes the Request-URI and the Contacts
and all the Path header fields, but does not include the From and To
header fields.  If the URIs are not of the proper SIPS scheme, the
registrar MUST reject the REGISTER with a 400 (Bad Request).
```

Figure 5 Behaviour of a registrar registering SIP and SIPS URIs (excerpt from RFC 5630 [17])

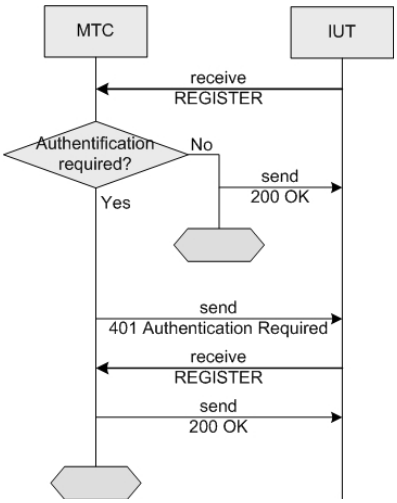

Figure 6 Conformity test procedure for a registration by RFC 3261

If a terminal device that uses SIPS is to be tested to determine whether it is compliant with the protocol specification, the test procedure shown in Figure 6 must be extended so that the requirements described in RFC 5630 (e.g. the demand for identical schemes of request URI and Contact header field, Figure 5) are also tested. This extended test procedure is illustrated in **Figure 7**.

The use of SIPS does not only affect header fields of the REGISTER request, changing the SIP state machine. The receiving of an INVITE request by a proxy, e.g., must be extended by checking the request URI, comparing it with the Contact URI that had been registered before and forwarding the request to the target or deny it with a appropriate response [17].

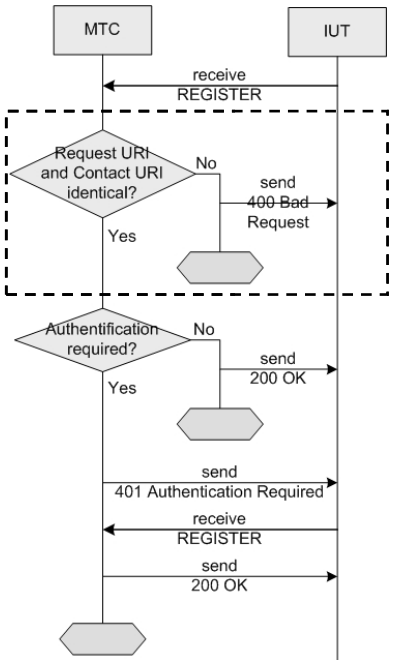

Figure 7 Conformity test procedure for a registration by RFC 5630

3.2 Interoperability Testing

Interoperability testing checks whether a function is implemented end-to-end between two or more network elements [2]. These end-to-end functions are not only comprised of pure call functions when using security mechanisms but rather one must ensure the correct operation of the used security mechanism by using interoperability testing. **Table 2** shows the test procedure checking the successful establishment of a voice call between two users.

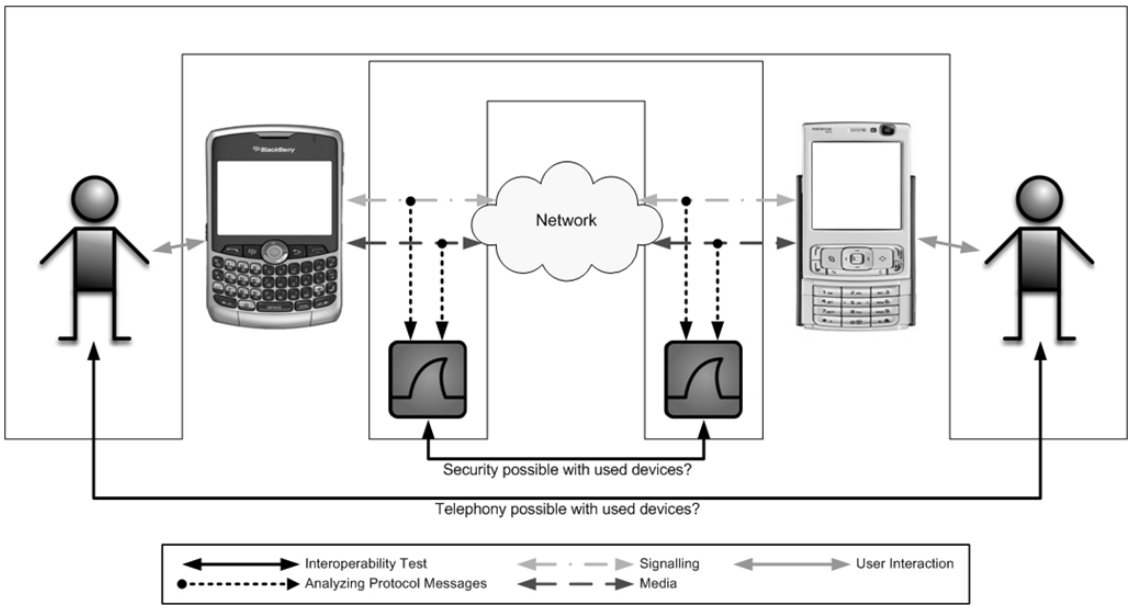

Figure 8 Interoperability testing with verification of security functionality (modified from [3])

Table 2 Interoperability test procedure to verify voice call establishment [8]

Test:	01		
Title:	Voice Call Establishment from User A to User B		
Test Purpose:	To verify that a call can be established successfully to User B by User A and that speech communication is possible between User A and User B		
Pre-test cond.:	Configure network elements to support at least codec G.711		
Step	**Test Description**	**Verdict**	
		pass	**fail**
1	Initiate a new call from User A to User B	-	-
2	A: Is dial tone heard?	Yes	No
3	B: Is the phone ringing?	Yes	No
4	User B answers the phone	-	-
5	A: Is dial tone heard?	No	Yes
6	B: Is the phone ringing?	No	Yes
7	User A talks	-	-
8	B: Can User A be heard by User B?	Yes	No
9	User B talks	-	-
10	A: Can User B be heard by User A?	Yes	No
11	Clear the call	-	-

Figure 8 shows a possible structure to perform interoperability testing, where both call and security functionality is tested. To verify the end-to-end functionality of the security, the protocol traffic is captured after each network adapter to check whether the traffic is secure according to the examined requirements. A corresponding test case is shown in **Table 3**.

Table 3 Interoperability test procedure extended by secured signalling with SIPS and its related verification (modified from [8]**)**

Test:	02		
Title:	Voice Call Establishment from User A to User B Using SIPS to Secure Signalling		
Test Purpose:	To verify that a call can be established successfully to User B by User A, that speech communication is possible between User A and User B, and that signalling is secure.		
Pre-test cond.:	Configure network elements to support SIPS and at least codec G.711		
Step	**Test Description**	**Verdict**	
		pass	**fail**
1	Start capturing protocol traffic	-	-
2	Initiate a new call from User A to User B	-	-
3	A: Is dial tone heard?	Yes	No
4	B: Is the phone ringing?	Yes	No
5	User B answers the phone	-	-
6	A: Is dial tone heard?	No	Yes
7	B: Is the phone ringing?	No	Yes
8	User A talks	-	-
9	B: Can User A be heard by User B?	Yes	No
10	User B talks	-	-
11	A: Can User B be heard by User A?	Yes	No
12	Clear the call	-	-
13	Stop Capturing	-	-
14	Analyze captured protocol traffic	-	-
15	Cap_A: Are there any SIP messages?	No	Yes
17	Cap_B: Are there any SIP messages?	No	Yes

3.3 Stress Testing

Basically, the use of security mechanisms requires additional system resources (**Figure 9**). For this reason stress tests must be modified so that, besides the performance of registrations, calls etc. security mechanisms will be used.

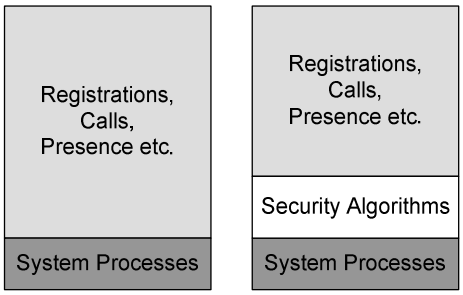

Figure 9 Required system resources with and without security mechanisms while performing stress tests

4 Conclusions

Even if communication protocols are extended by security mechanisms, the compatibility between network elements can also be ensured among different manufacturers using testing techniques. For this purpose, testing techniques must be modified depending on the effects of the applied security mechanisms.

Conformity Testing

- Subject of test is the implementation of a protocol specification of the system under test.
- Changes to the state machine require a new set of test cases.
- New protocols also require a new set of test cases.
- The state machine is also affected by dependencies on header field contents.
- Dependencies on header field contents require modifications of affected test cases.

Interoperability Testing

- Test object is the end-to-end functionality of the system under test.
- Functionality of security mechanisms must be examined in addition to call functionality.

Stress Testing

- Test object is the behaviour of the system under test while producing stress.
- Stress tests must be modified to take the processing time of security mechanisms into account for stress behaviour.

Overall this paper makes clear, that testing techniques must be extended and modified because of the multiple interdependencies between communication protocols and security mechanisms. Beyond that, the de-

velopment of new test cases is necessary. How the testing techniques must be adapted depends on the test object.

5 Future Prospects

Starting with the material described in this paper, the existing testing techniques will be modified to allow testing of network elements which utilise security mechanisms. For this purpose concrete propositions for conformity and interoperability testing will be developed. Especially with regard to testing the compliance to a protocol specification, exemplary test cases will be developed and implemented.

The investigations shall be expanded to the area of intelligent electricity grids. Their network elements also use secured IP-based communication protocols to exchange information and require testing techniques to ensure compatibility among different manufacturers.

6 Literature

[1] M. Bormann, R. Patz, D. Wermser: *Conformance Testing of Complex Services Exemplified with the IMS Presence Service*. IEEE, 2009.

[2] M. Bormann, D. Hartmann, D. Wermser: *Ensuring Interoperability between Network Elements in Next Generation Networks*. ZVEI-Elektronik, 2009.

[3] M. Bormann, D. Hartmann, D. Wermser: „Gegenüberstellung und Anwendung verschiedener Testverfahren zur Sicherstellung der Interoperabilität von Netzelementen in Next Generation Networks“. In: *Mobilkommunikation Technologien und Anwendungen*. Ed. by P. Roer et al. ITG Fachbericht 215. Berlin, Offenbach: VDE Verlag GmbH, 2009, S. 73-78.

[4] G. Camarillo und M. A. García-Martín: *The 3G IP Multimedia Subsystem (IMS)*. Second Edition. West Sussex, England: John Wiley & Sons, Ltd., 2006.

[5] Draft-zimmermann-avt-zrtp-16: *ZRTP: Media Path Key Agreement for Secure RTP*. Network Working Group, 2009.

[6] ETSI TISPAN: *IP Multimedia Subsystem (IMS); Functional architecture*. ETSI Standard ES 282 007 V2.0.0. ETSI, 2008.

[7] A. Johnston und D. Piscitello: *Understanding Voice over IP Security*. Norwood (MA): ARTECH HOUSE, INC., 2006.

[8] S. Moseley, S. Randall and A. Wiles: *Experience within ETSI of the combined roles of conformance testing and interoperability testing*. In: 3rd Conference on Standardization and Innovation in Information Technology, Oktober 2003, S. 177-189.

[9] A. Plies et al. „ePA-gestütze VoIP Authentifizierung und Verschlüsselung“. In: *Mobilkommunikation Technologien und Anwendungen*. Ed. by Peter Roer et al. ITG Fachbericht 215. Berlin, Offenbach: VDE Verlag GmbH, 2009, S. 117-122.

[10] M. Poikselkä et al: *THE IMS IP Multimedia Concepts and Services*. Second Edition. West Sussex: John Wiley & Sons, Ltd., 2006.

[11] RFC 2633: *S/MIME Version 3 Message Specification*. IETF, 1999.

[12] RFC 3261: *SIP: Session Initiation Protocol*. IETF, 2002.

[13] RFC 3329: *Security Mechanism Agreement for the Session Initiation Protocol (SIP)*. IETF, 2003.

[14] RFC 3711: *The Secure Realtime Transport Protocol (SRTP)*. IETF, 2004.

[15] RFC 3830: *MIKEY: Multimedia Internet KEYing*. IETF, 2004.

[16] RFC 5246: *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF, 2008

[17] RFC 5630: *The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)*. IETF, 2009.

[18] U. Trick und F. Weber: *SIP, TCP/IP und Telekommunikationsnetze Next Generation Networks und VoIP - konkret*. 3. Auflage. München: Oldenbourg Wissenschaftsverlag, 2007.

7 Abbreviations

IUT	Implementation Under Test
MIKEY	Multimedia Internet Keying
MTC	Main Test Component
RTP	Realtime Transport Protocol
SIP	Session Initiation Protocol
SIPS	SIP Security
S/MIME	Secure / Multipurpose Internet Mail Extensions
SRTP	Secure RTP
TLS	Transport Layer Security
URI	Unified Reform Identifier