

Call establishment delay for secure VoIP

Johan Bilien, Erik Eliasson and Jon-Olov Vatn

Telecommunication Systems Laboratory
Department of Microelectronics and Information Technology
Royal Institute of Technology, Stockholm, Sweden
bilien@kth.se, eliasson@imit.kth.se, vatn@imit.kth.se

Abstract. The IETF is developing the MIKEY and SRTP protocols to provide *end-to-end authentication* and *confidentiality* to VoIP telephone calls. We present measurements of the *call setup delay* for our own implementation of these protocols and the results show that call setup delay will not be significantly affected by introducing these security protocols.

1 Introduction

The advancement of the SIP[1] standardization process and the appearance of PDAs with WLAN support are likely to boost VoIP as a competitor to regular PSTN based telephony. However, in order for IP telephony to reach wide user acceptance it must be able to withstand spoofing and eavesdropping attacks. The IETF are designing two security protocols, MIKEY[2] and SRTP[3], to provide *end-to-end authentication* and *confidentiality* to VoIP calls. In this study we investigate whether the introduction of the MIKEY authentication handshake and the SRTP session key generation will affect *the call setup delay* significantly. For this purpose we have developed a SIP user agent (UA), minisip[4], with support for SRTP and two of MIKEY's authentication mechanisms: *shared key* and *signed Diffie-Hellman* (D-H). We have measured the *calling delay*, i.e., the time from when the caller (Alice) has dialed the callee (Bob) until she receives the SIP **Ring** message, and the *answering delay*, which is the time from when Bob picks up his phone until he has received the SIP **ACK** message **and** computed the SRTP session keys.

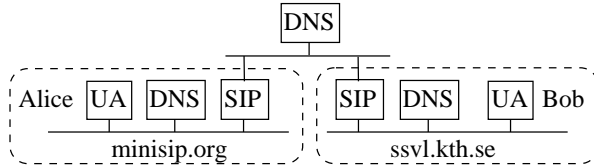
2 Test-bed and implementation

Fig. 1 shows our test-bed. Our hosts and servers are running Linux 2.4 kernels and they are connected via 10 Mb/s Ethernet links. As SIP and DNS servers we use SER[5] and BIND[6] respectively.

Fig. 2a shows (somewhat simplified) the call setup phase. The **MIKEY Response** is placed in the SIP **OK** message. In the D-H scheme we let Alice send her and her SIP provider's certificates in the **MIKEY Init** message (most of the computation for this message is done in advance). Bob has a set of root CA certificates installed, which can be used to verify the certificate chain (no certificate revocation checking done). A similar procedure is done for the **MIKEY Response** message (Bob has pre-computed D-H values for a typical configuration). To locate a SIP server a node usually performs DNS look-ups for SRV and A resource records[7]. Minisip registers an IP address and has already resolved the IP address of its SIP server during SIP registration, thus DNS look-ups are only performed in steps δ_2 and δ_{12} .

3 Measurements and results

The measurements were carried out using *tcpdump* and by adding time-stamp *hooks* to minisip. Table 1 shows the measured mean delays for 3 test-runs (DNS servers were restarted before each run to limit caching effects). The total (Tot) values show the measured calling and answering delays. The different deltas (δ) include the time to process and send the SIP messages, but no network delays (therefore Σ and *Tot* differ). In our test-bed the network delays are low and the D-H key generation exceeds the OK/ACK round-trip time ($Tot_1 > Tot_2$). If the UAs would support *reliable provisional responses*[8] it is possible to send the **MIKEY Response** in the **Ring** message (Fig. 2b). If so, the answering delay would not include any MIKEY computation. Based on the measured values in Table 1 one could estimate the corresponding answering delay to be around 10 ms (see Tot_2 for "no security"), while the ringing delay would increase about 4 ms (see δ_{11} for "D-H"). A secure call establishment using the D-H scheme will lead to some increase in network delay, as the larger packet sizes will increase the transmission time and will also require the use of TCP transport leading to additional network traversals, however, our results show that the additional computation required is insignificant for a human user.



UAs: 1.4 GHz Pentium 4 Laptops
 Root DNS and SIP servers: 1.1 GHz Celeron Desktops
 Local DNS servers: 500 MHz Pentium 3 Laptops

Figure 1. Test-bed setup.

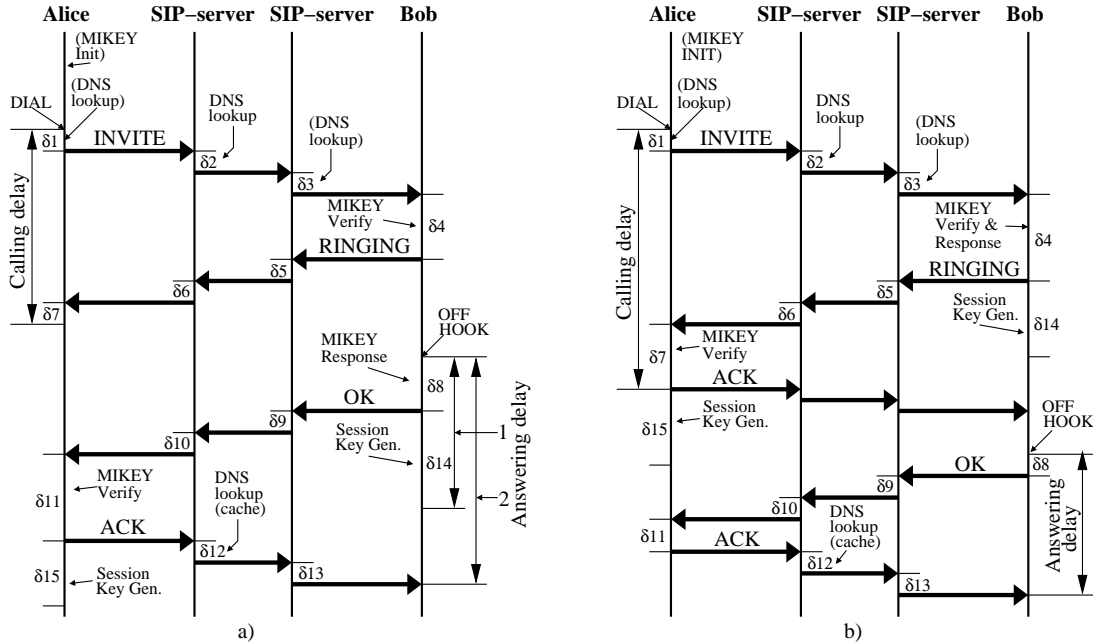


Figure 2. Secure call establishment with MIKEY Response in (a) OK message or (b) RINGING message.

Table 1. Calling and answering delays with MIKEY Response in OK message (as shown in Fig. 2a).

	MIKEY Authentication	Calling delay [ms]									Answering delay [ms]											
		δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	Σ_{1-7}	Tot	δ_8	δ_9	δ_{10}	δ_{11}	δ_{12}	δ_{13}	Σ_{8-13}	δ_{14}	(δ_{15})	Tot_1	Tot_2	
UDP	No security	1.2	9.5	0.9	4.2	0.3	0.4	0.6	17.0	19.5	0.8	0.4	0.3	1.0	3.3	0.5	6.3	-	-	-	-	9.5
	Shared key	1.9	8.9	0.6	5.3	0.2	0.3	0.7	17.8	20.9	2.4	0.2	0.2	1.3	2.5	0.3	6.9	4.6	1.1	7.0	10.5	
	Diffie-Hellman	20.2	9.7	0.7	12.3	0.2	0.2	0.6	49.8	52.5	29.8	0.3	0.4	4.5	2.7	0.4	38.1	82.6	80.4	112.5	47.6	
TCP	Diffie-Hellman	19.7	11.6	2.3	14.4	0.7	0.5	0.6	51.5	58.9	30.5	0.5	0.7	4.5	3.4	0.5	40.1	82.8	83.5	112.9	48.9	

Acknowledgments

We would like to thank the *Graduate School of Teleinformatics*, the *Wallenberg Global Learning Network* and the *Hewlett-Packard Company: Applied Mobile Technology Solutions in Learning Environments - Grant 2003* for financial support, professor Gerald Q. Maguire Jr. and professor Björn Pehrson for advice and support, and the MIKEY/SRTP design team at Ericsson Research for valuable feedback.

References

- Rosenberg, J. et al.: SIP: Session Initiation Protocol, IETF RFC3261, June 2002
- Arkko, J. et al.: MIKEY: Multimedia Internet KEYing, IETF draft (work in progress), December 2003
- Baughner, M. et al.: The Secure Real-time Transport Protocol, IETF draft (work in progress), July 2003
- Minisip SIP user agent, <http://www.minisip.org>
- SIP Express Router (SER) version 0.8.12, <http://www.ipstel.org>
- Berkeley Internet Name Domain (BIND) version 8.2, <http://www.isc.org>
- Rosenberg, J. et al.: Session Initiation Protocol (SIP): Locating SIP Servers, IETF RFC3263, June 2002
- Rosenberg, J. et al.: Reliability of Provisional Responses in Session Initiation Protocol (SIP), IETF RFC3262, June 2002