InnoSoc
Innovative ICT Solutions
for the Societal Challenges

VoIP security aspects

Marek Moravčík

marek.moravcik@fri.uniza.sk

University of Zilina
Faculty of Management Science and Informatics
Slovakia

27.4.2016, Zagreb

Agenda

- Brief VoIP description
- HTTP digest MD5
- TLS
- DTLS
- S/MIME
- Media security
  - ZRTP
  - SRTP

Voice over Internet Protocol

- Voice is transported along with data (Internet)
- Voice is digitalized, cut (approx. 20 ms) and sent as IP packets

- Two parts of VoIP:
- Signalization (SIP, SCCP, IAX, MGCP, ...)
  - Location of participants
  - Establish and tear down session
  - Agree on codec, IP addresses
- Media stream (RTP)
  - Digital voice

Why to secure VoIP?

- Signalization
  - Steal my identity
  - Calling for my money (2013 – 4.7 bilion $)
  - Modification of signalization parameters
  - Denial of Service
  - Spam
- Media stream
  - Eavesdropping

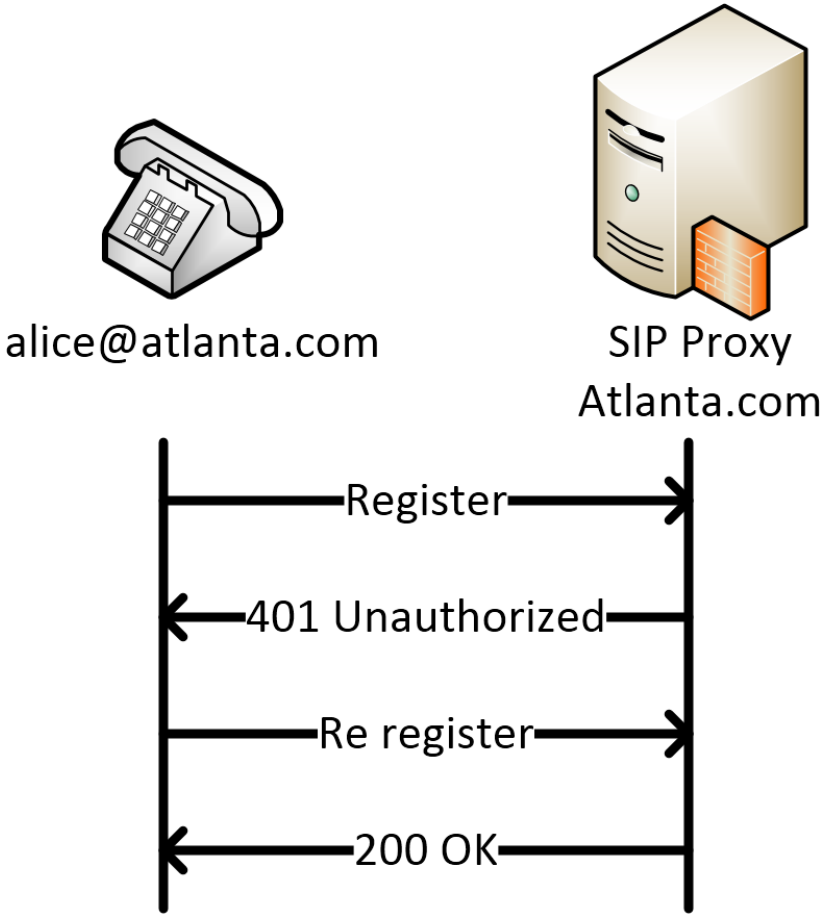
HTTP Digest authentication

- Based on HTTP authentication (RFC 7235)
- Authentication used during
  - Registration
  - Call establishment
  - Call parameters change
  - Call termination
- Messages used
  - 401 (Unauthorized)
  - 407 (Proxy Authentication Required)
  - 403 (Forbidden)

HTTP Digest principle

- When authentication enabled, SIP server requests data
- In response 401 (Unauthorized) or 407 (Proxy authentication required) SIP server adds parameters for hash function into SIP header
- Client has to include these parameters into response
  - New header Authorization + hash function computed from server and client data
  - Password is never transmitted

HTTP Digest principle



Authentication parameters

Parameter	Meaning
realm	Domain
qop	„Quality of protection“ – tells, if there is only authentication, or authentication + message integrity
nonce	Random string generated by server
cnonce	Random string generated by client
uri	sip:domain (sip:kis.fri.uniza.sk)
nonceCount	Sequence number of nonce

401 Unauthorized

```
SIP/2.0 401 Unauthorized.
From: "pepe"<sip:pepe@sipxecs.local>;tag=d70e6f7e.
To: "pepe"<sip:pepe@sipxecs.local>;tag=HZ_AcU.
Call-Id: MzFlNzRlMTk5MzBlODAxNTQ5YWFkYjk2NjVhY2IyMTc..
Cseq: 1 REGISTER.
Via: SIP/2.0/TCP 192.168.10.108:29164;branch=z9hG4bK-d8754z-8a70f357ec339608-
  1---d8754z-;rport=52090;received=158.193.152.64.
Www-Authenticate: Digest realm="sipxecs.local",
  nonce="4023dcecbf2fda7ec2f8a50233ca8c544cd13c5e", qop="auth".
User-Agent: sipXecs/4.2.1 sipXecs/registry (Linux).
Date: Wed, 03 Nov 2010 10:41:34 GMT.
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, REGISTER, SUBSCRIBE.
Accept-Language: en.
Supported: gruu, path.
Content-Length: 0.
.
```

Response computation

- Hash function – MD5
- If qop is not defined:

- response=MD5(HA1:nonce:HA2)
  - HA1=MD5(username:realm:password)
  - HA2=MD5(method:digestURI)

Response computation

- Hash function – MD5
- If qop is defined:

- response=MD5(HA1:nonce:nonceCount:clientNonce:qop:HA2)
  - HA1=MD5(MD5(username:realm:password):nonce:cnonce)
  - HA2=MD5(method:digestURI:MD5(entityBody))

Register

```
REGISTER sip:sipxecs.local SIP/2.0.
Via: SIP/2.0/TCP 192.168.10.108:29164;branch=z9hG4bK-d8754z-5b44db1b163a656b-1---d8754z-
   ;rport.
Max-Forwards: 70.
Contact: <sip:pepe@192.168.10.108:29164;rinstance=2bd3dc300ed8a123;transport=TCP>.
To: "pepe"<sip:pepe@sipxecs.local>.
From: "pepe"<sip:pepe@sipxecs.local>;tag=d70e6f7e.
Call-ID: MzFlNzRlMTk5MzBlODAxNTQ5YWFkYjk2NjVhY2IyMTc..
CSeq: 2 REGISTER.
Expires: 3600.
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO.
User-Agent: eyeBeam release 1102q stamp 51814.
Authorization: Digest
   username="pepe",realm="sipxecs.local",nonce="4023dcecbf2fda7ec2f8a50233ca8c544cd13c5e",u
   ri="sip:sipxecs.local",response="833bb9afc7b58451091273e28648f46b",cnonce="f445ef1e881bd
   6944ebeb2821d16fa8f",nc=00000001,qop=auth,algorithm=MD5.
Content-Length: 0.
.
```

HTTP Digest authentication

+	-
Password is not in plaintext	Man-in-the-Middle attacks
Server remembers nonce-s	MD5 can be compromised by dictionary attacks

TLS

- TLS and his predecessor SSL are used for data encryption
- Since august 2008 – TLS 1.2 (RFC 5246)
- Present – TLS 1.3 (draft)

- Based on certificates (asymmetric encryption)
- Encryption hop-by-hop

Intermezzo – asymmetric encryption

- Private + public key
- If encrypted by one key, can be decrypted only by the second one

- Encryption
  - Encrypt by public key
  - Decryption made only by private key owner

- Electronical signature
  - Encrypt by private key
  - Everyone can decrypt (confirm) by public key

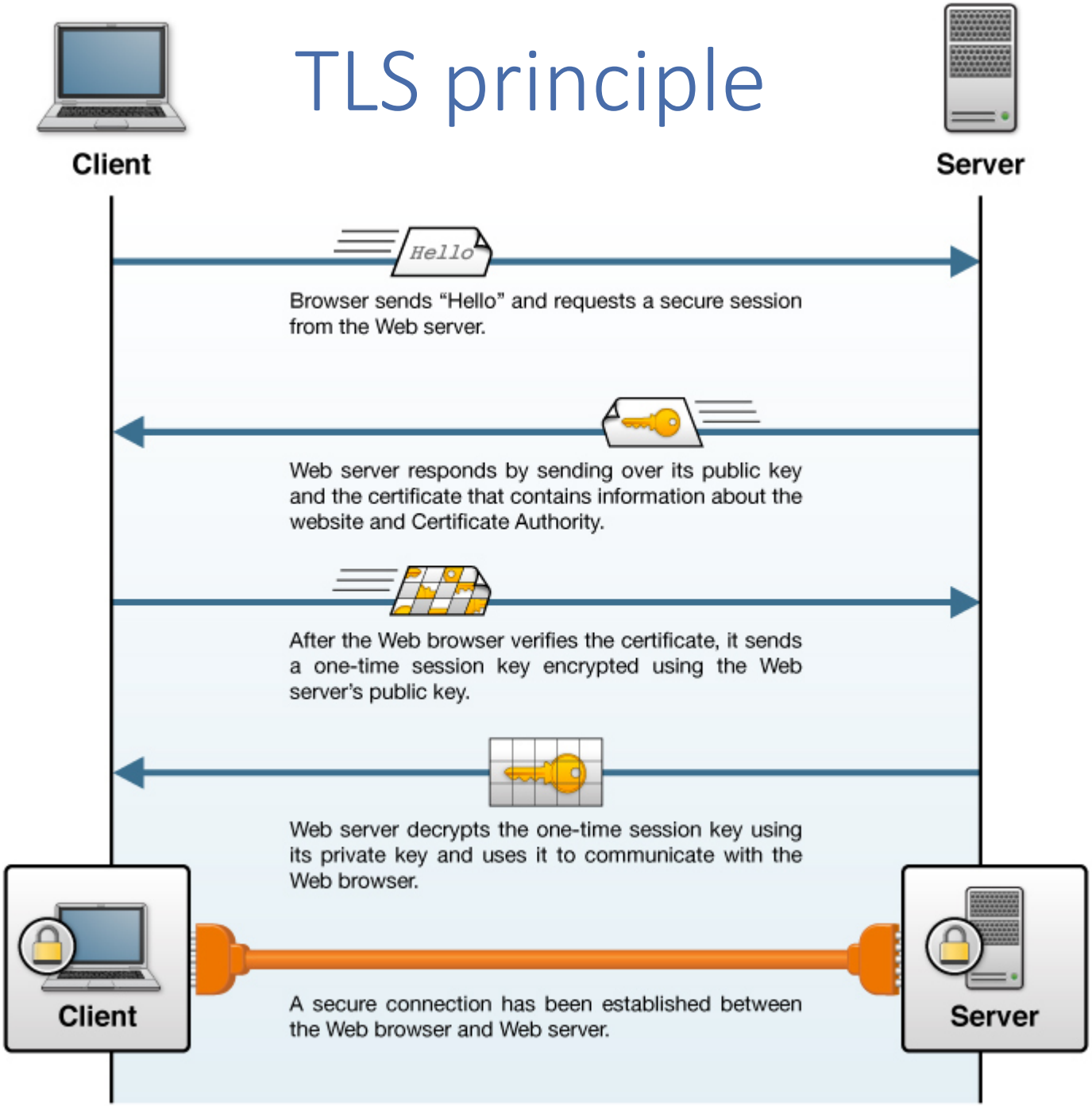
TLS handshake

- Client sends
  - Hello – Types of TLS versions, supported cipher suites, ...
- Server sends
  - Hello - Types of TLS versions, cipher algorithm, ...
  - Certificate
- Client sends
  - Certificate (if any)
  - Pre-master password encrypted by server’s public key
- Generation of shared secret (password)

TLS handshake (2)

- Client sends
  - „Change cipher spec“ - confirms cipher algorithm
  - „Client finished“
- Server sends
  - „Server finished“
- Communication is encrypted by symmetrical encryption with new shared secret

TLS principle



TLS

+	-
Communication encryption	Certificate obtaining
Sender authentication	(light) operating system load

DTLS

- Security for datagram protocols (UDP, DCCP, SCTP)
- RFC 4347, RFC 6347
- Based on TLS

Version	DTLS 1.0	DTLS 1.2
Based on	TLS 1.1	TLS 1.2

- Application must handle:
  - Datagram ordering
  - Datagram loss

DTLS handshake problems

- TLS do not allow decryption of random datagram
  - Forbiddance of stream ciphers
- TLS handshake messages are sent reliable
  - Extra timer on „ClientHello“
- Datagram can be fragmented
  - Messages are designed to be small
  - Contains „fragment offset“ and „fragment length“
- Reordering
  - Contains sequence number

DTLS

- Where can we see it?
  - Cisco AnyConnect VPN Client
  - f5 Networks Edge VPN Client
  - Chrome, Opera, Firefox – WebRTC

- February 2013 – DTLS was compromised

  http://www.isg.rhul.ac.uk/~kp/dtls.pdf

S/MIME

- Secure/Multipurpose Internet Mail Extensions
- RFC 5751
- Standard for PKI and MIME data signing
- End-To-End encryption
- Designed in RSA Data Security Inc.

S/MIME offers

- Digital signature
  - Authentication
  - Integrity
  - Non repudiation
- Encryption
  - Privacy
  - Data security

MIME

- RFC 2045-9, 4288-9
- Supports:
  - Non-ASCII charsets (also in header)
  - Non-text attachment
  - Multipart body
- MIME establishes new headers
- Goal: not to change standards
- Used in SMTP, HTTP, SIP, JPEG, GIF, ...

MIME example

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary=frontier

This is a message with multiple parts in MIME format.

--frontier

Content-Type: text/plain

This is the body of the message.

--frontier

Content-Type: application/octet-stream

Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+VGhpcyBpcyB0aGUgYm9keS BvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==

--frontier--

MIME security

- Obtain certificate (public key) of recipient
- Encrypts whole MIME message

- Problems in SIP:
  - Via headers must be readable for proxy servers (routing)

Media encryption

- RTP
- SRTP
- ZRTP

- RTCP
- SRTCP

SRTP

- RFC 3711
- Offers:
  - Encryption
  - Authentication
  - Integrity
  - Non repudiation
- Using AES cipher protocol

SRTP

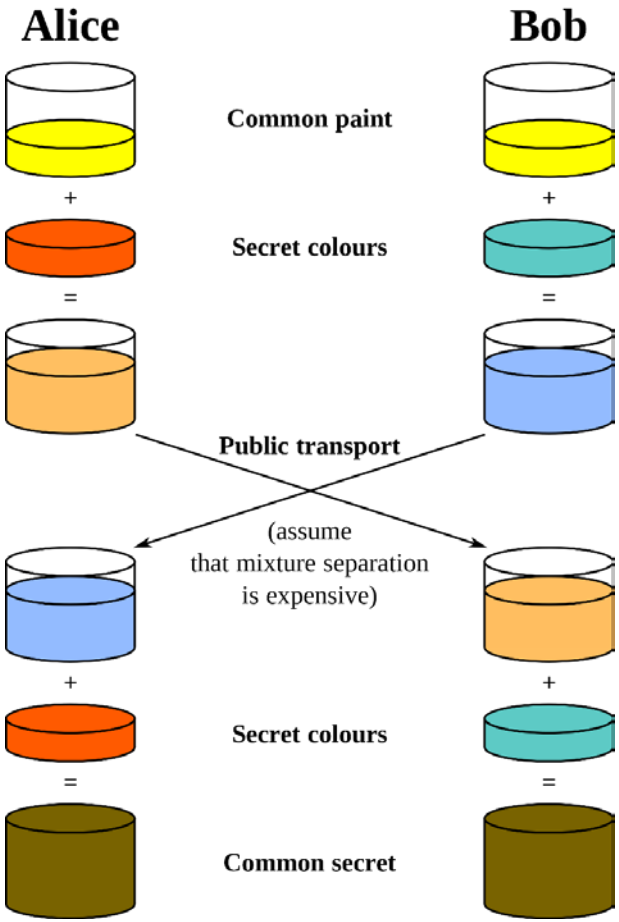
- For verification is used HMAC-SHA1
  - RFC 2104
  - 160 bit tag from header and payload
  - Attached to message
- Key deduction
  - Base key
  - Periodically deduced keys
- Relies on external key management

ZRTP

- Zimmermann RTP
- RFC 6189
- Using SRTP

- This is external key management for SRTP
- Uses Diffie-Hellman key exchange algorithm

Diffie-Hellman algorithm



Thanks for your attention

Marek Moravčík

marek.moravcik@fri.uniza.sk

KIS FRI ŽU