Zürcher Hochschule Winterthur

SIP Security

Prof. Dr. Andreas Steffen

Zürcher Hochschule Winterthur

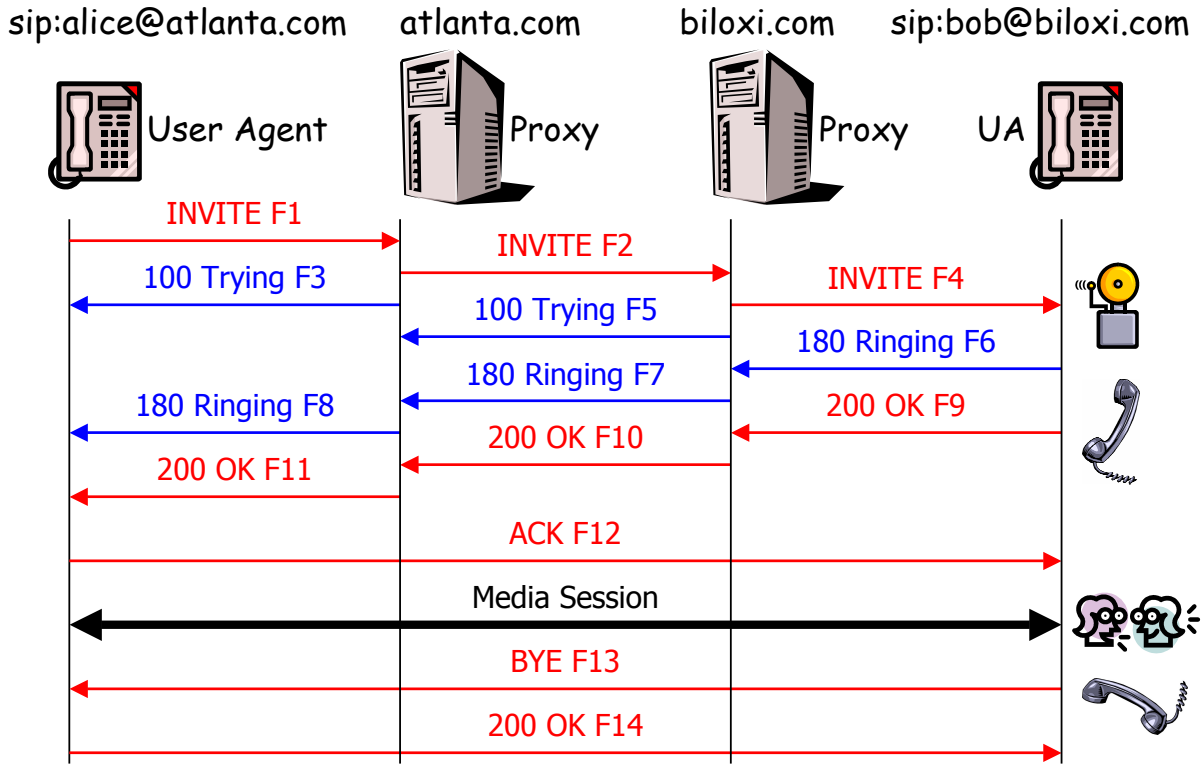
andreas.steffen@zhwin.ch

Agenda

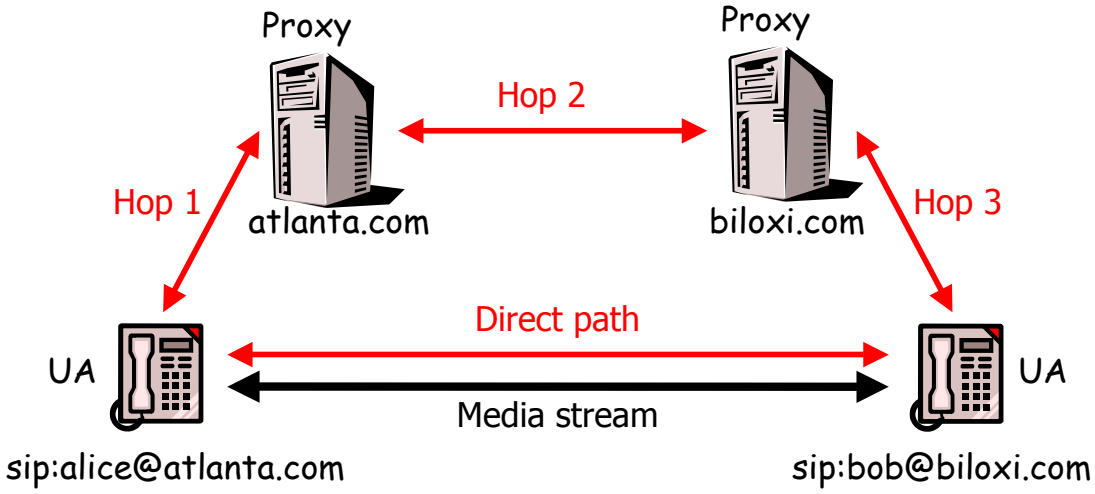
Zürcher Hochschule Winterthur

- SIP – The Session Initiation Protocol
- Securing the Session Management
- Securing the Media Streams
- Conclusions

Session Initiation Protocol (RFC 3261)



Basic SIP Trapezoid



udp/sip or tcp/sip Session Management

udp/rtp Media Streams

Securing the Session Management

Zürcher Hochschule Winterthur

Authentication methods: PSK Pre-Shared Keys PKI Public Key Infrastructure	Authentication	Data Integrity	Confidentiality	
HTTP 1.0 Basic Authentication	PSK	-	-	Deprecated by SIPv2 Insecure transmission of password
HTTP 1.1 Digest Authentication	PSK	-	-	Challenge/response exchange based on MD5 hash of [strong] password
Pretty Good Privacy (PGP)	PKI	✓	✓	Deprecated by SIPv2
Secure MIME (S/MIME)	PKI	✓	✓	For encryption the public key of the recipient user agent must be known
SIPS URI (TLS)	PKI	✓	✓	SIP application and proxies must tightly integrate TLS
IP Security (IPsec)	PKI	✓	✓	Integration with SIP application not required but proxies must be trusted

Securing the Media Streams

Zürcher Hochschule Winterthur

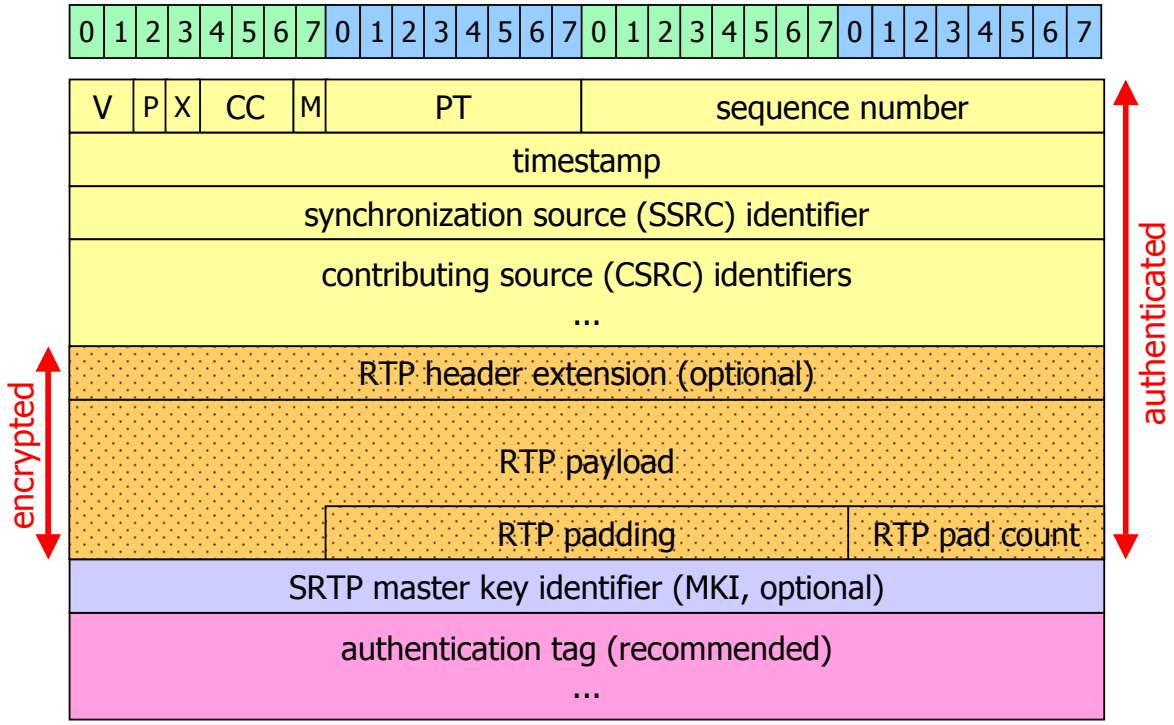
Authentication methods: PSK Pre-Shared Keys PKI Public Key Infrastructure	Authentication	Data Integrity	Confidentiality	
Secure RTP (SRTP)	PSK	✓	✓	Uses master key which must be distributed by other means
IP Security (IPsec)	PKI	✓	✓	Integration with SIP application not required but peer must be trusted

Zürcher Hochschule Winterthur

Securing the Media Streams

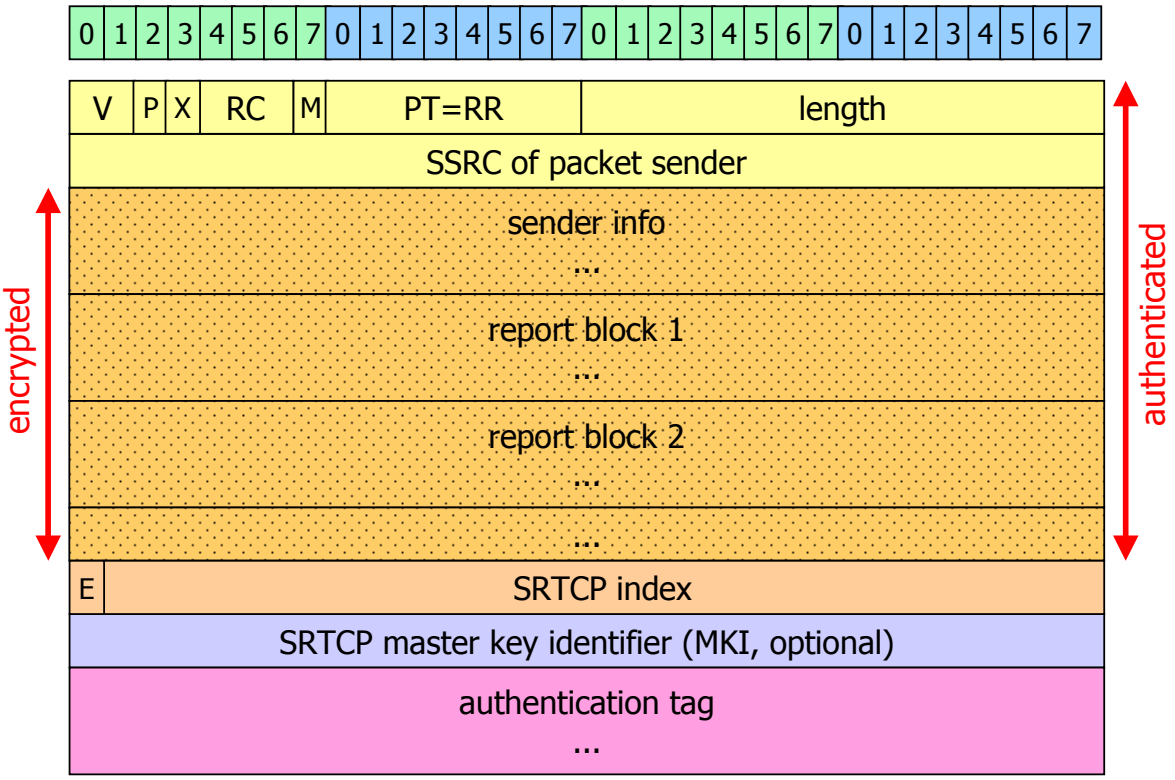
Secure RTP Packet Format (RFC 3711)

Zürcher Hochschule Winterthur



Secure RTCP Packet Format (RFC 3711)

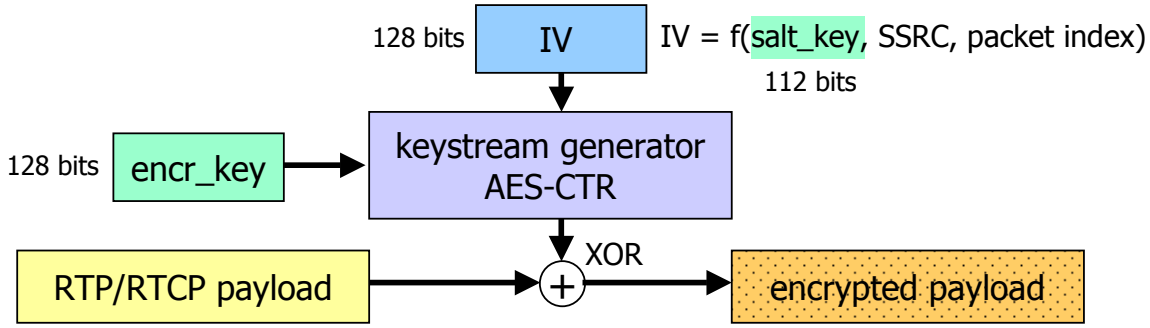
Zürcher Hochschule Winterthur



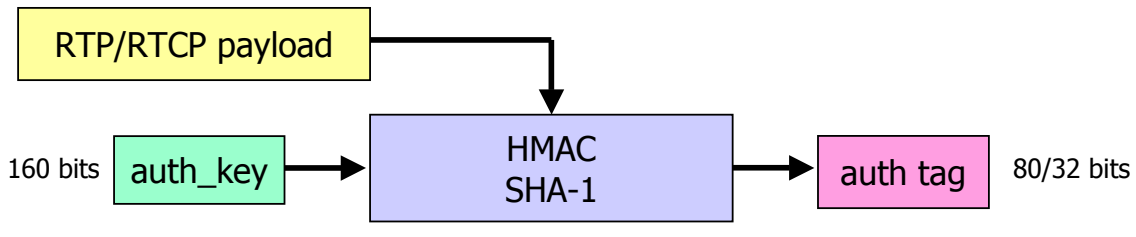
Default Encryption and Authentication Algorithms

Zürcher Hochschule Winterthur

- Encryption uses AES in Counter Mode (AES-CTR) with 128 bit key

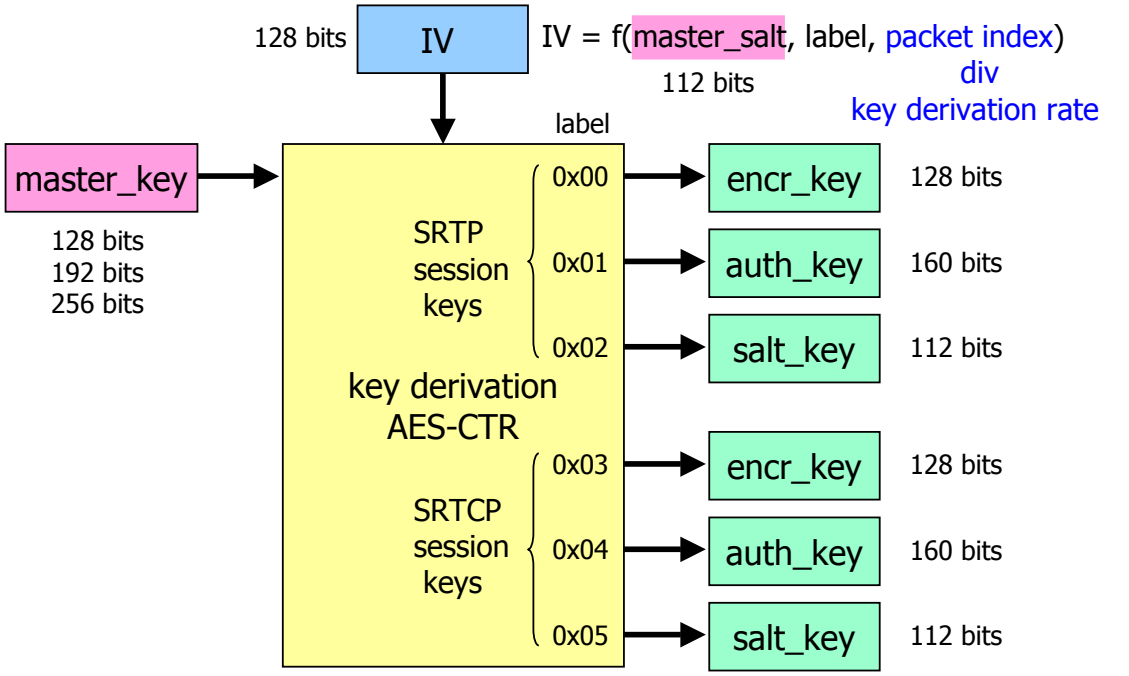


- Authentication uses HMAC-SHA-1 with truncated 80 bit MAC



Session Key Derivation

- Key Derivation uses AES in Counter Mode (AES-CTR)



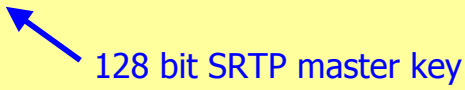
Securing the Session Management

SIP INVITE Request

Zürcher Hochschule Winterthur

```
INVITE sip:bob@zhwin.ch SIP/2.0
Via: SIP/2.0/UDP 160.85.170.139:5060;branch=z9hG4bK4129d28b8904
To: Bob <sip:bob@zhwin.ch>
From: Alice <sip:alice@zhwin.ch>;tag=daa21162
Call-ID: 392c3f2b568e92a8eb37d448886edd1a@160.85.170.139
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@dskt6816.zhwin.ch:5060>
Content-Type: application/sdp
Content-Length: 239

v=0
o=alice 3157331353 3157331353 IN IP4 160.85.170.139
s=DA SIP Security 2003
c=IN IP4 160.85.170.139
t=0 0
k=clear:910bc4defa71eb6190008762fca6ae2f1d959e87cdf3c0c5c5076ad38ee8
m=audio 10000 RTP/AVP 0
a=ptime:20
a=rtpmap:0 PCMU/8000
```



S/MIME based Authentication and Encryption

Zürcher Hochschule Winterthur

```
INVITE sip:bob@zhwin.ch SIP/2.0
Via: SIP/2.0/UDP 160.85.170.139:5060;branch=z9hG4bK4129d28b8904
To: Bob <sip:bob@zhwin.ch>
From: Alice <sip:alice@zhwin.ch>;tag=daa21162
Call-ID: 392c3f2b568e92a8eb37d448886edd1a@160.85.170.139
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@dskt6816.zhwin.ch:5060>
Content-Type: multipart/signed;boundary=992d915fef419824;
micalg=sha1;protocol=application/pkcs7-signature
Content-Length: 3088
--992d915fef419824
Content-Type: application/pkcs7-mime;
smime-type=envelopeddata; name=smime.p7m
Content-Disposition: attachment;handling=required;filename=smime.p7m
Content-Transfer-Encoding: binary
<envelopedData object encapsulating encrypted SDP attachment not shown>
--992d915fef419824
Content-Type: application/pkcs7-signature;name=smime.p7s
Content-Disposition: attachment;handling=required;filename=smime.p7s
Content-Transfer-Encoding: binary
<signedData object containing signature not shown>
--992d915fef419824--
```

Practical Results and Conclusions

Zürcher Hochschule Winterthur

- Practical Results
  - ZHW diploma thesis in 2003 demonstrated feasability of S/MIME protected session management and SRTP secured media streams.
  - reSIPprocate available from www.resiprocate.org implements a SIPv2 stack and offers basic S/MIME support using OpenSSL.
  - TinyCA available from tinyca.sm-zone.net was used as a graphical interface on top of OpenSSL for X.509 certificate generation.
  - libsrtp library available from srtp.sourceforge.net implements SRTP.
- Conclusions
  - S/MIME encrypted and/or signed attachments in SIP messages are an attractive alternative to the hop-by-hop security offered by TLS and allow the secure transfer of secret SRTP master keys via end-to-end encryption.
  - Similar to S/MIME protected email, the verification of peer certificates on a global scale remains one of the open problems yet to be solved.