Non-Repudiation in Internet Telephony

Andreas U. Schmidt, Nicolai Kuntze
Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany

Christian Hett
ARTEC IT, Karben Germany
VoIP – a shift of paradigms in business communication

- VoIP is becoming the prevalent form of voice communication in commercial environments
  - Will carry more than 50% of business voice traffic in few years
  - 2007, over 60% of contact centres worldwide have switched to VoIP (up from 50% 06)
- Major reasons for switching to VoIP
  (Dimension Data’s Global Contact Centre Benchmarking Report)
  - Flexibility of architecture
  - Cost savings
  - Improved business functionality
  - Replacement of end-of-life technology
- „Since contact centres depend on a range of I&C technologies, converged technology can significantly increase efficiencies.“
- VoIP is gaining shares in mobile communication
- Industry quickly adopted the relevant standards SIP/RTP
  (Even Skype recently announced adopting them)
SIP – Session Initiation Protocol

Two RTP channels, one for each direction; Independent (different port and possibly IP numbers) from signalling
Incoming call example

INVITE sip:49601234567@es.178.139.124:5060 SIP/2.0
Record-Route: <sip:213.227.15.225;lr=on>
Record-Route: <sip:+49601234567@es.178.139.124:5060;lr=on>
Via: SIP/2.0/UDP 212.227.15.197;branch=z9hG4bK57df8239ft650eef1b391f8b5eaf30f
Via: SIP/2.0/UDP 212.227.15.225;branch=z9hG4bK6861.3b05c5c5.0
Via: SIP/2.0/UDP 212.227.15.197;branch=z9hG4bK6861.3b05c5c5.0
Via: SIP/2.0/UDP 217.188.44.231;branch=z9hG4bK6861.3b05c5c5.0
Via: SIP/2.0/UDP 1und1-1.sip.mgc.voip.telefonica.de:5060 ;received=195.71.3.100;branch=z9hG4bK7ae1-18556-+zf9171234567649601234567
From: <sip:+491713306700@sip.3lund.de;tag=1168841412>
To: sip:+4906123456700@sip.3lund.de;tag=1168841412
Call-ID: 78d1be21c-a32b0f7-73ae04b2-b9828b2b@subscriber1.interconnect.mgc.voip.telefonica.de
CSeq: 1 INVITE
Supported: timer
SemVer-Expires: 1800
Min-SE: 1000
Contact: <sip:491712345678@1und1-1.sip.mgc.voip.telefonica.de:5060>
Allow: INVITE, ACK, PROOF, SUBSCRIBE, BYE, CANCEL, NOTIFY, INFO, REFER, UPDATE
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 518
Divergence: <sip:456012345678@sip.3lund.de;user=phone>;reason=additional

v=0
o=1710955 0 IN IP4 62.53.226.3
s=Connect SIP 0
c=IN IP4 62.53.226.3
t=0 0
m=audio 22354 RTP/AVP 0 99 101 2 103 3 104 105 106 107 108 0 125 101 100
m=rtcpmap:99 G729-16/64000
m=rtcpmap:102 G729-24/64000
m=rtcpmap:103 G723-1-W/20000
m=rtcpmap:104 G723-1-L/64000
m=rtcpmap:105 G729b/8000
m=rtcpmap:106 G723-2-W/64000
m=rtcpmap:107 G723e-L/24000
m=rtcpmap:125 GN264/64000
m=rtcpmap:101 telephone-event/8000
a=rtcpmap:101 0-15
m=rtcpmap:101 X-MEEX/64000
a=rtcpmap:101 192-134,200-202
a=K=x
a=a2=m:1 audio RTP/AVP 100
a=a2=m:rtcpmap:100 X-MEEX/64000
a=a2=m:rtcpmap:100 192-134,200-202
a=a2=m:2 audio udppl 150

d=audio 22353 RTP/AVP 0 99 101 2 103 3 104 105 106 107 108 0 125 101 100
m=rtcpmap:99 G729-16/64000
m=rtcpmap:102 G729-24/64000
m=rtcpmap:103 G723-1-W/20000
m=rtcpmap:104 G723-1-L/64000
m=rtcpmap:105 G729b/8000
m=rtcpmap:106 G723-2-W/64000
m=rtcpmap:107 G723e-L/24000
m=rtcpmap:125 GN264/64000
m=rtcpmap:101 telephone-event/8000
a=rtcpmap:101 0-15
m=rtcpmap:101 X-MEEX/64000
a=rtcpmap:101 192-134,200-202
a=K=x
a=a2=m:1 audio RTP/AVP 100
a=a2=m:rtcpmap:100 X-MEEX/64000
a=a2=m:rtcpmap:100 192-134,200-202
a=a2=m:2 audio udppl 150
Salient characteristics of VoIP

- As a communication channel, VoIP has rather specific features
- Telephony is **bidirectional** and **interactive**.
  - The medium consists in **linearly time-based full duplex channels**
  - Interactivity allows to make further enquiries in case of insufficient understanding
- VoIP chops communication into small pieces - packets, and transmits them independently
  - Packet loss is tolerated, methods to conceal it are standard and rather effective
  - Jitter (loss of temporal order) is common
  - Latencies >150ms are intolerable
- Typical: G.711 codec produces 64kbit/s, RTP packets come with 160 bytes of payload ~ 20ms
Packet loss vs. quality

The tests were performed by Dynstat, Inc., an independent test laboratory.
Score system range: 1 = bad, 2 = poor, 3 = fair, 4 = good, 5 = excellent
VoIP Security

- Basic issues are tackled
  - Protocols like SRTP can provide end-to-end security to phone calls, making them independent from the security of the transport medium. SPIT and DoS are future threats.
  - Spam over Internet Telephony (SPIT) considered a major threat – approaches are Gatekeepers, CAPTCHAs, IDS, ...
  - ITU Recommendations for Secure Telecommunications

- „Application-level security?“
  - Verbal communication is traditionally bestowed with a high level of trustworthiness
  - Is the integrity of VoIP communication as high as the interpersonal character of conversations suggests?
  - Recent court cases (contact centre v customer, digital recording accepted as evidence) suggest there might be a problem
SRTP – confidentiality and authenticity on packet level

Authentication by HMACs (symmetric) and only on packet level
Non-repudiation for VoIP

- Goal: **Non-repudiation** of conversations by caller and callee, for speech over packet-oriented, digital channels, and in particular for VoIP conversations

- Providing tenable evidence of
  - Contents of a call
  - Identity of caller and callee
  - Ancillary information (forensic), time & date, ...

- For electronic documents, this is usually done by **electronic signatures**
Trivia: What does this machine do?
To all whom it may concern:

Be it known that I, THOMAS ALVA EDISON, a citizen of the United States, residing at Llewellyn Park, Orange, in the county of Essex and State of New Jersey, have invented certain new and useful Improvements in Recording-Telephones, of which the following is a description.

My invention relates to telephones and has for its object the provision of means whereby the electrical vibrations or undulations which are received over the line may be recorded phonographically, whereby a record is formed which may be used in any ordinary phonograph, and the message repeated at any future-time.

telephonic receiver and a portion of the mechanism for driving the friction wheel; Fig. 4 is a section on line 4—4 of Fig. 3; and shows also the electrical connections.

In all the above views corresponding parts are designated by the same reference numerals.

The recording surface may be a cylinder 1 of suitable material for receiving a phonographic record and the mechanism for supporting and rotating said cylinder may be similar to the parts of an ordinary phonograph comprising a tapered mandrel 2 on which the cylinder 1 is held by frictional engagement and carried by a shaft 3 supported at its end by pivot pins 3' and 4.
Requirements for Non-repudiation 1/2

- **Protection Target** **Congruence**
  - Meaning can vary between sender and receiver
  - Electronic documents: “What You See is What You Sign“ tacitly assumes all parties „see“ the same
  - The receiver’s understanding is essential
  - **What is Heard is What is Signed**
  - Communication partners need to agree on what was heard

- **Requirements**
  - 1.1 **Integrity**: The complete conversation and its atomic parts must be secured
  - 1.2 **Treatment of losses**: a secure detection of losses enabling a proper handling on the application level as well as a later inspection.
  - 1.3 **User interaction policies**: e.g. notify users of quality under-runs, enforce breaks or repeats
Requirements for Non-repudiation 2/2

- **Protection Target Cohesion**
  - protection and preservation of the sequence the information flows in all directions of the channel
  - temporal reference frame of a conversation can be meaningful – fix conversation in absolute time

- **Requirements**
  - **2.1 Start times** of conversations must be determined and recorded. This is analogous to the signing time of documents (the assignment of which is a requirement for qualified signatures according to the EU Signature Directive).
  - **2.2 Temporal sequencing** within conversations must be protected and related to the reference time frame
  - **2.3 Continual authentication** of communication devices and if possible even communication partners is necessary, e.g., to prevent hijacking
  - **2.4 Determined break points** must allow for non-repudiation of conversations until they are terminated intentionally or inadvertently.
The interval chaining method

A signs a conversation with B, assuming no packet loss

\[
\text{Sec}_I : M_I \stackrel{\text{def}}{=} (D, \text{SIP\_Data}, \text{Auth\_Data}, \text{nonce}, \ldots) \rightarrow B;
\]
\[
S_0 \stackrel{\text{def}}{=} ((M_I)_A)_T \rightarrow B;
\]
\[
\text{Sec}_l : S_l \stackrel{\text{def}}{=} (I_l, S_{l-1})_A \rightarrow B; \quad l = 1, \ldots, 2N
\]
\[
\text{Sec}_F : M_F \stackrel{\text{def}}{=} (\text{termination\_condition}, \ldots) \rightarrow B;
\]
\[
S_F \stackrel{\text{def}}{=} ((M_F, S_{2N})_A)_T \rightarrow B;
\]
\[
(\cdot)_X \stackrel{\text{def}}{=} \text{Priv}_X(h(\cdot))
\]

Denotes the signing of data by entity X
Catering for packet loss by reporting of actually received packets

- List of packets actually received by B in interval l \( \delta_l \subset \{1, \ldots, K_l\} \)
- Reduced packet set in interval l \( I'_l \overset{\text{def}}{=} (p_{l,j})_{j \in \delta_l} \)
- For direction A to B, security procedure is modified as follows
  \[
  \text{Sec}'_{2k-1} : \text{repeat}
  \]
  \[
  \text{repeat}
  \]
  \[
  \text{interval \_ termination} \rightarrow B;
  \]
  \[
  \text{until} \ \delta_{2k-1} \rightarrow A;
  \]
  \[
  \text{until} \ S_{2k-1} \overset{\text{def}}{=} (I'_{2k-1}, S_{2k-2})_A \rightarrow B;
  \]

- For direction B to A
  \[
  \text{Sec}'_{2k} : \text{repeat}
  \]
  \[
  S_{2k} \overset{\text{def}}{=} (I'_{2k}, S_{2k-1})_A \rightarrow B;
  \]
  \[
  \delta_{2k} \rightarrow B;
  \]
  \[
  \text{until success};
  \]
Unidirectional signing procedure and architecture

The original RTP-stream is forwarded to the recipient in real time without noticeable delay. The sequencer extends the truncated 16Bit-sequence number of RTP-packets to 64 Bit, absolute sequence numbers starting with zero. A replay window as defined in annex A of the SRTP-RFC is used to detect duplicate packets.

The packet-collector collects all sent or received packets and sorts them by their absolute sequence number. It buffers all packets belonging to the current interval. This has much less and only static memory requirements than storing the complete call for later signature.

For the channel A to B: A gets from B the list with packet numbers that B actually received. A as the sender of these packets was able to collect them all. A then discards the packets that B did not receive. After that QoS-policies can be applied: If B lost to many packets, the call becomes ambiguous and A may terminate the call or take other measures. A builds the interval signature package with metadata and the hashes of the contained RTP-packets and sends this to B. The full RTP-packets need not be send again over the wire thus resulting in an efficient implementation.
Multi-lateral signatures

- Combine interval chaining with **round-robin** scheme
- A participant not carrying the token waits and buffers packets **sent by himself**
- When participant A_m carries the token he waits D, and buffers packets **sent by himself**
- A_m terminates an interval, secures it, and foregoing intervals not yet secured and broadcasts the **security package**
- Packet loss: include hashes of packets received by **at least one** participant in the security package
- Signatures are **verifiable for all receivers**
- The security package is used by A_m+1 to continue the chaining
### Auditable information from the interval chaining method

<table>
<thead>
<tr>
<th>Auditable item</th>
<th>Req.</th>
<th>Protection target</th>
<th>Verifies/indicates</th>
<th>When applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial time stamp</td>
<td>2.1</td>
<td>Cohesion</td>
<td>Start time</td>
<td>Always</td>
</tr>
<tr>
<td>Initial signature &amp; certificate</td>
<td>2.3</td>
<td>Cohesion</td>
<td>Identity of signer</td>
<td>Always</td>
</tr>
<tr>
<td>Interval Chaining</td>
<td>2.2, 1.1</td>
<td>Cohesion</td>
<td>Interval integr. &amp; order</td>
<td>Always</td>
</tr>
<tr>
<td>Packet loss in intervals</td>
<td>1.2, 2.4</td>
<td>Congruence</td>
<td>QoS, understandability</td>
<td>Always</td>
</tr>
<tr>
<td>Monotonic increase of RTP-sequence numbers</td>
<td>1.1, 2.2</td>
<td>Integrity &amp; cohesion</td>
<td>RTP-stream plausibility</td>
<td>Always</td>
</tr>
<tr>
<td>Relative drift of RTP-time marks against system time</td>
<td>2.2</td>
<td>Cohesion</td>
<td>RTP-stream plausibility</td>
<td>During convers.</td>
</tr>
<tr>
<td>Relative drift of RTP-time marks against ([l/2] \cdot D)</td>
<td>2.2</td>
<td>Cohesion</td>
<td>Packet &amp; stream plausibility</td>
<td>Ex post</td>
</tr>
<tr>
<td>No overlaps of RTP-time marks at interval boundaries</td>
<td>2.2</td>
<td>Cohesion</td>
<td>Packet &amp; stream plausibility</td>
<td>Always</td>
</tr>
<tr>
<td>Replay-window</td>
<td></td>
<td>Integrity</td>
<td>Uniqueness of recorded audio stream</td>
<td>Always</td>
</tr>
<tr>
<td>Final time stamp</td>
<td>2.2</td>
<td>Cohesion</td>
<td>Conversation duration</td>
<td>Ex post</td>
</tr>
<tr>
<td>Forensic analysis of recorded conversation</td>
<td></td>
<td>(Semantic)</td>
<td>Speaker identity, mood, lying, stress, etc.</td>
<td>Ex post, forensic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authenticity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Application: Self-signed VoIP Archive

Separation of duties between long-term archive and security module that secures and signs archived calls

Trusted time source or time-stamping authority to securely pinpoint exact start of call

VSec can be a passive listener or have an active role and enforce policies

Only one point in channel A→B needs to be digital and packet-based

Main Benefit: high accountability by separation of duties and resulting administrator security
Interval chaining – **VoIPS** – achieves non-repudiation for VoIP conversations with the salient features

- Saves investment and operational cost
  - Modular architectures
  - Scalability
  - Pluggable into existing telecommunication infrastructures with minimal effort
  - Operates **without interference** (causes no latency)
- Highest security for reasonable investment
  - Complete **audit trail** for digital voice communication
  - **Administrator-proof** security essential for accountability
  - Cost-efficient **backup and failover** solutions
- Enabling new forms of non-repudiation in co-operation
  - Continual **caller authentication**
  - **Verbal contracts** between unacquainted persons
  - Non-repudiation in (multi-media) **conferences**
- Potential users:
  - Call centres, small businesses, administrations, financial institutions, mobile users, …

**Patent pending**