

PROCESSING SENSITIVE INFORMATION OVER VOIP

BACKGROUND

5 a. Field of the Invention

Contact centres are extensively used by service providers for delivering services to, and communicating with, customers. Contact centres typically comprise a large group of agents taking or making telephone calls with customers. Contact centres
10 often use call recording technologies, where an audio recording of the customer conversation is stored, and/or screen recording technologies, where a video or static snapshot of the agent's computer terminal is stored in order to aid in staff training, customer complaint management, compliance monitoring or record-keeping.

15 In many contact centre transactions, the customer is either required to confirm his identity by providing the answer to security-based questions, or to provide his payment card details to pay for a transaction. The nature of much of this information is highly sensitive. In particular, the information can include passwords, personally-identifiable information such as a date of birth, a PIN, a memorable phrase, bank
20 account numbers, credit card security codes and the like.

Data and identity theft, as well as fraudulent financial transactions, are widespread, and so it is of particular interest to the caller to keep secret as much of the information as possible. Disclosing personally-sensitive financial or other security
25 information to a contact centre agent has the potential to increase personal data loss in a number of ways. For example, the contact centre agent can write down or memorise the customer's information for later use. It has even been known for agents to make their own personal recordings of the information using their personal mobile phones or devices.

30

Furthermore, where audio or video recordings or screen shots are recorded, such data is vulnerable to fraudulent access.

The Payment Card Industry (“PCI”) has developed a Data Security Standard (DSS) for businesses that store, process and/or transmit credit card data. Compliance with the PCI security standards is not optional for such businesses. The DSS dictates the methods and ways in which companies processing credit card data (including telephone-based credit card transactions) can store card and personal data. Regulations and guidelines such as these have a direct impact on contact centre which take customers' sensitive data in telephone conversations.

- Secure telephony payment systems have been developed which can be used in order to allow potentially sensitive information such as payment card information to be transmitted directly to a payment processing system whilst preventing such information being transmitted in any form to the contact centres agent or contact centre agent terminal. In general, a call is routed via the secure system and the system uses one of a number of various techniques such as suppression of Dual Tone Multi Frequency (DTMF) tones or muting the caller's voice stream in order to prevent potentially sensitive data from reaching the contact centre.

Contact centres have complex telephony systems optimised to provide bulk routing of calls at minimum cost. The majority of calls into the contact centre may not typically contain sensitive information, but it is important for the contact centre to be able to handle sensitive information securely should the need arise during any call handled by the contact centre staff. It is therefore desirable, but more expensive, to route all calls through the secure telephony system prior to entry into the contact centre. As the proportion of an individual call actually containing the sensitive information is small compared to the total length of the call it is not desirable or cost effective to use the secure telephony payment system for the entire duration of the call.

- Ideally the secure telephony payment system would only be utilised for the relatively short period of time whilst secure information is being relayed to the payment processing system, but would be available for use by other transactions once the

part of the call requiring transmission of secure information is complete.

However, it is problematic to switch a secure telephony payment system in and out of the call path once the call has been received by an agent in the contact centre.

- 5 The process typically involves terminating the call and the contact centre agent calling back the original caller on a secure line. Alternative methods, such as creating a conference call with the secure payment system are ineffective as the sensitive data will still be detectable within the contact centre telephony system and therefore the advantage of removing the sensitive data from the contact centre is
- 10 lost. Processes to place the caller 'on hold' within the public telephony system (i.e. external to the contact centre) whilst the contact centre agent is disconnected and reconnected via the secure payment system are also typically problematic as, for efficiency, in most contact centre systems when a call is terminated the agent handling the call generally becomes free again and available for subsequent calls.
- 15 Hence the agent handling the initial call might not be available once the call returns to the contact centre via the secure payment system.

Historically calls have been routed using circuit switched connections in the public switched telephone network (PSTN). A caller would call the contact centre via the

20 PSTN and the call centre private branch exchange (PBX) and the Automatic Call Distribution (ACD) system would connect the caller to an agent. All signalling was transmitted over the voice channel and the signalling and voice were very much bound together.

- 25 However, with the advent of Voice over Internet Protocol (VoIP) technologies signalling and voice are generally transmitted using different protocols from one another. VoIP is not a protocol itself. Rather, VoIP is an umbrella term for a set of protocols involved in transporting voice information using IP. VoIP protocols include Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP) and
- 30 H.323, for example. Whilst VoIP protocols are not yet standardised, SIP appears to be emerging as a popular choice. For secure transmissions of SIP messages over insecure network links, the protocol may be encrypted with Transport Layer Security

(TLS).

SIP does not encode audio information in a phone call, nor does it transport audio information. SIP simply initiates and terminates communications sessions, for
5 example the session may be a voice call between two people or a video conference between a whole team.

The job of SIP is to set up a call, conference or other interactive communication session and terminate it when it is over. This is achieved by sending messages
10 between endpoints known as “SIP addresses.” SIP does not do much during the session itself as its primary purpose is to establish the session and then end it. Therefore, the bandwidth of a SIP signalling stream is relatively small, for example, approximately 5Kbps.

15 The session media (for example speech/voice or image data/video) is transmitted via a separate media stream. SIP can be used in conjunction with various protocols that specify and carry the session media. Media type and parameter negotiation and media setup is performed using Session Description Protocol (SDP), which is carried as payload in SIP messages.

20 Before voice can be sent over IP, it is encoded using a voice codec to convert audio signals into data.

The encoded packets of audio data are usually sent using Real-time Transport
25 Protocol (RTP) or Secure Real-time Transport Protocol (SRTP), specialised application-layer protocols for transporting audio and video data when real-time streaming is necessary.

30 Signalling or media stream packets are themselves transmitted using transport layer protocols such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). TCP is a protocol designed to transmit packets in an ordered sequence and to retransmit any packets that are lost along the way. Packet headers specify the

order of each packet in the sequence. If packets are received out of order, they can be reordered at the receiving end. UDP is a protocol designed to transmit data without retransmission of lost packets or detection of out-of-sequence packets.

- 5 UDP is better than TCP for voice streams. Lost and out-of-sequence packets can cause audio quality issues, but usually these are not detectable by the human ear. The amount of delay caused by the re-ordering and retransmission of TCP packets can ultimately result in much worse audio quality problems. SIP signalling streams on the other hand are usually transmitted using TCP.

10

Two of the most common codec standards are G.711 for uncompressed digital voice and G.729 codec for compressed voice. The bandwidth of the media stream is relatively large compared to that of the signalling stream, for example the bandwidth of an uncompressed voice stream is likely to be 100Kbps. Compression degrades
15 audio quality in order to reduce the amount of data transmitted in order to reduce the amount of bandwidth consumed by the call. However, compression usually corrupts. Dual Tone Multi-Frequency (DTMF) tones which have been sent over the voice stream.

- 20 Historically this problem has been overcome by using 'out of band' DTMF whereby DTMF tones are detected and sent using an uncompressed voice stream. Alternatively, the DTMF data may be sent as separate packets in the RTP stream. More recently the data represented by the detected DTMF tone is sent over a SIP signalling stream associated with the voice stream.

25

b. Related Art

- Patent document GB 2548413 A describes a secure data collection system which uses an on demand appliance (ODA) in the contact centre to place a call out to a
30 secure data collection system whilst sensitive data is transmitted. The secure data collection system prevents the sensitive data from reaching the agent. However, the sensitive data is routed through the ODA, which is located in the contact centre, to

the secure data collection system. Whilst any security risk may be mitigated by physical security measures to prevent access to the ODA it is undesirable for the sensitive data to ever pass through the contact centre.

- 5 The separation of the signalling stream from the voice stream allows for a novel and inventive solution to the problem of processing sensitive information over VoIP.

SUMMARY OF THE INVENTION

- 10 According to the invention there is provided a method of processing, by a call processor, a Voice over Internet Protocol (VoIP) media call comprising sensitive information, the method comprising the steps of:

receiving at the call processor a first signalling stream from a first entity;

creating a second signalling stream from the call processor to a second entity;

- 15 forwarding signals received from the first signalling stream to the second signalling stream;

receiving a third signalling stream at the call processor from the second entity;

creating a fourth signalling stream from the call processor to the first entity;

and

- 20 forwarding signals received on the third signalling stream to the fourth signalling stream;

the first signalling stream containing instructions to set up a VoIP media call between the first entity and the second entity such that:

- 25 (a) media comprising audio information is transmitted over a first media stream from the first entity to the second entity without intervention by the call processor; and

(b) media comprising audio information is transmitted over a second media stream from the second entity to the first entity without intervention by the call processor;

- 30 in which the method comprises, when said sensitive information is to be included in said audio information, receiving at the call processor of a message from the second entity to reroute said media streams so that these are redirected via the

call processor, said media streams being rerouted by:

(i) the call processor sending a message to the first entity to cause media comprising audio information to be transmitted over a third media stream to the call processor, the call processor creating a fourth media stream from the call processor to the second entity and forwarding media comprising audio information received from the first entity via the third media stream to the second entity over the fourth media stream; and

(ii) the call processor sending a message to the second entity to cause media comprising audio information to be transmitted over a fifth media stream to the call processor, the call processor creating a sixth media stream from the call processor to the first entity and forwarding media comprising audio information received from the second entity via the fifth media stream to the first entity over the sixth media stream; and

using the call processor to modify media comprising audio information received from the first entity by removing sensitive audio information from said received audio information before forwarding said media comprising audio information over the fourth media stream to the second entity; and

using the call processor to modify media comprising audio information received from the second entity by removing sensitive audio information from said received audio information before forwarding said media comprising audio information over the sixth media stream to the first entity.

In one embodiment the call processor modifies the media received from the first entity by removing sensitive information before forwarding the media stream to the second entity.

In another embodiment the call processor modifies the media received from the first entity by removing DTMF tones before forwarding the media stream to the second entity.

In a third embodiment the call processor modifies the media received from the first entity by removing spoken sensitive information before forwarding the media stream

to the second entity.

Preferably, when the second entity is a contact centre, the method further comprises the steps of: the contact centre sending a message to a secure data collection server to indicate secure data collection is to be initiated on a particular media call; the secure data collection server returning to the contact centre a personal identification number; and in which the message received by the call processor from the contact centre contains said personal identification number.

Advantageously the media streams are reconnected to bypass the call processor, the method further comprising the steps of the call processor sending a message to the first entity to cause the media to be sent over the first media stream to the second entity; and the call processor sending a message to the second entity to cause media to be sent over the second media stream to the first entity.

The first entity may be a user and the second entity may be a contact centre.

The signalling streams may be SIP streams. The media stream may be an RTP stream.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a call processing environment for use in a system for collection of sensitive information;

Figure 2 is a simplified illustration of call paths when a call is in unsecured mode;

Figure 3 is a simplified illustration of call paths showing a call conferenced with the call processor;

Figure 4 is a simplified illustration of call paths showing removal of sensitive information from a media stream sent to a contact centre; and

Figure 5 is a simplified illustration of call paths showing removal of sensitive information from a media stream sent to a user.

5 DETAILED DESCRIPTION

Referring to Figure 1, a call processor 14 is accessed via a firewall 11 (e.g. AWS), and a Session Border Controller 12 (SBC) (e.g. AudioCodes or Sonus). The call processor 14 interfaces with a secure data collection environment 16.

10

A first entity, which in the embodiment described here, is a user 17, initiates a VoIP call to a second entity, in the embodiment described here, a contact centre 18. The VoIP call may originate from the PSTN via a trunk provider. When the contact centre's address is detected in the signalling stream (for example, when during call set up using a SIP INVITE message) the trunk provider redirects the signalling stream to the call processor 14.

15

When call processor 14 receives a first signalling stream 20 from a user 17 the call processor 14 creates a second signalling stream 21 to the contact centre 18 and forwards any messages received via the first signalling stream 20 from the user to the contact centre 18 via the second signalling stream 21. Reciprocally the call processor 14 forwards any messages received via a third signalling stream 22 from the contact centre to the user 17 via a fourth signalling stream 23. The user is unaware that the signalling messages are intercepted and passed on by the call processor 14. Hence once signalling messages are exchanged to set up a VoIP call between the user 17 and the contact centre 18 the VoIP call is created between the user 17 and the contact centre 18 without intervention by the call processor 14. Hence, the bandwidth of the data that the call processor 14 needs to process is approximately 5Kbps x 2. Because the call processor 14 retains signalling paths to both the user and to the contact centre, the call processor 14 has the ability to control the interaction between the user 17 and the contact centre 18.

20

25

30

In more detail, using SIP protocol the call set up process may be as follows:

- 1) SIP INVITE (first call ID) is sent by the user 17 to the call processor 14.
- 2) SIP INVITE (second call ID) is sent by the call processor 14 to the contact centre
5 18.
- 3) SIP OK (second call ID) is sent by the contact centre 18 to the call processor 14.
- 4) SIP OK (first call ID) is sent by the call processor 14 to the user 17.
- 5) A first voice media stream 24 (usually using RTP) is created from the user 17 to
the contact centre 18.
- 10 6) A second voice media stream 25 (usually using RTP) is created from the contact
centre 18 to the user 17.

Figure 2 is a simplified illustration showing the signalling and media streams when
the call is in an 'unsecured' mode i.e. when it is not required to transmit sensitive
15 information between the user 17 and the contact centre 18.

When it becomes necessary to transmit sensitive information between the user 17
and the contact centre 18 a request 26, which may be initiated by an agent in the
call centre, is sent to the secure data collection server 16. The request 26 may be
20 sent via the internet, via a private network or any other suitable means. The request
from the contact centre 18 contains a unique identifier (sometimes called a
SessionID) that identifies the contact centre agent within the contact centre. The
unique identifier may be created (for example) when the contact centre agent logs
onto the web interface of the secure data collection system 16.

25

The secure data collection system 16 generates a Personal Identification Number
(PIN) that is sent back to the contact centre agent over the Internet (typically
displaying in a web browser).

- 30 The secure data collection server 16 returns a response 27 containing a unique
identifier identifying the signalling streams and the media call in question.

The contact centre agent enters the PIN and generates a message requesting that a media call goes into 'secure mode' which is sent via the third signalling stream 22 to the call processor 14. This message contains the PIN. The call processor 14 liaises with the secure data collection server 16 to confirm that the request is
5 legitimate, for example by comparing the PIN received to those which have been previously sent out.

Assuming the request is legitimate, the call processor 14 reroutes the media stream so that it is redirected via the call processor.
10

In more detail, using SIP protocol the call rerouting process may be as follows:

- 1) re-INVITE (first call ID) is sent by the call processor 14 to the user 17
- 2) SIP OK (first call ID) is sent by the user to the call processor 14
- 15 3) re-INVITE (second call ID) is sent by the call processor 14 to the contact centre 18
- 4) SIP OK (second call ID) is sent by the contact centre 18 to the call processor 14.

The call processor 14 then initiates a conference call with the user 17 and the
20 contact centre 18. Figure 3 is a simplified illustration of the resultant signalling and media streams.

A third VoIP media stream 30 is created between the user 17 and the call processor 14. VoIP data is transmitted over the third VoIP media stream 30 to the call
25 processor 14. The call processor 14 creates a fourth VoIP media stream 31 and forwards VoIP data received from the user 17 via the VoIP third media stream 30 to the contact centre 18 over the VoIP fourth media stream 31.

This will enable the call processor to modify VoIP data received from the user, for
30 example by removing DTMF tones or spoken sensitive information before forwarding the media to the contact centre 18.

Figure 4 shows schematically sensitive data being removed from the fourth media stream 31 before being forwarded to the contact centre 18.

5 A fifth VoIP media stream 32 is created between the contact centre 18 and the call processor 14. VoIP data is transmitted over the fifth VoIP media stream 32 to the call processor 14. The call processor 14 creates a sixth VoIP media stream 33 and forwards VoIP data received from the contact centre 18 via the VoIP fifth media stream 32 to the user 17 over the VoIP sixth media stream 33.

10 This will enable the call processor to modify VoIP data received from the contact centre 18, for example by removing DTMF tones or spoken sensitive information before forwarding the media to the user 17.

15 Figure 5 shows schematically sensitive data being removed from the sixth media stream 33 before being forwarded to the user 17.

The call processor 14 liaises with the secure data collection system 16 to obtain the required sensitive data from the user 17 and removes the sensitive data from the media that is forwarded to the contact centre 18, thus preventing the sensitive
20 information from ever entering the contact centre 18.

The call processor 14 only needs to process the bandwidth required for the media call during the time that the call is in 'secure' mode. Once the sensitive data has been collected the media stream can be reconnected directly between the user 17
25 and the call centre 18 and the call processor 14 will drop out of the media stream.

The call is rerouted in a similar manner to previously:

- 1) re-INVITE (first call ID) is sent by the call processor 14 to the user 17
- 30 2) SIP OK (first call ID) is sent by the user to the call processor 14
- 3) re-INVITE (second call ID) is sent by the call processor 14 to the contact centre 18

4) SIP OK (second call ID) is sent by the contact centre 18 to the call processor 14.

The call paths revert to those shown in Figure 2.

- 5 It will be appreciated that features of the invention which are, for brevity, described in the context of a single embodiment, may also be provided separately, or in another suitable combination.

- 10 It will be recognised that various alterations, modifications, and/or additions may be introduced into the constructions and arrangements of parts described above whilst remaining within the scope of the invention as claimed.

CLAIMS

1. A method of processing, by a call processor, a Voice over Internet Protocol (VoIP) media call comprising sensitive information, the method comprising the steps
5 of:

receiving at the call processor a first signalling stream from a first entity;
creating a second signalling stream from the call processor to a second entity;
forwarding signals received from the first signalling stream to the second
signalling stream;

10 receiving a third signalling stream at the call processor from the second entity;
creating a fourth signalling stream from the call processor to the first entity;
and

forwarding signals received on the third signalling stream to the fourth
signalling stream;

15 the first signalling stream containing instructions to set up a VoIP media call
between the first entity and the second entity such that:

(a) media comprising audio information is transmitted over a first media
stream from the first entity to the second entity without intervention by the call
processor; and

20 (b) media comprising audio information is transmitted over a second
media stream from the second entity to the first entity without intervention by the call
processor;

in which the method comprises, when said sensitive information is to be
included in said audio information, receiving at the call processor of a message from
25 the second entity to reroute said media streams so that these are redirected via the
call processor, said media streams being rerouted by:

(i) the call processor sending a message to the first entity to cause media
comprising audio information to be transmitted over a third media stream to
the call processor, the call processor creating a fourth media stream from the
30 call processor to the second entity and forwarding media comprising audio
information received from the first entity via the third media stream to the
second entity over the fourth media stream; and

(ii) the call processor sending a message to the second entity to cause media comprising audio information to be transmitted over a fifth media stream to the call processor, the call processor creating a sixth media stream from the call processor to the first entity and forwarding media comprising audio information received from the second entity via the fifth media stream to the first entity over the sixth media stream; and

using the call processor to modify media comprising audio information received from the first entity by removing sensitive audio information from said received audio information before forwarding said media comprising audio information over the fourth media stream to the second entity; and

using the call processor to modify media comprising audio information received from the second entity by removing sensitive audio information from said received audio information before forwarding said media comprising audio information over the sixth media stream to the first entity.

2. The method according to claim 1, in which the call processor modifies said received media by removing DTMF tones from the audio information before said forwarding of said media stream.

3. The method according to claim 1, in which the call processor modifies said received media by removing spoken sensitive information from the audio information before said forwarding of said media stream.

4. The method according to claim 1, in which the second entity is a contact centre, further comprising the steps of:

the contact centre sending a message to a secure data collection server to indicate secure data collection is to be initiated on a particular VoIP media call;

the secure data collection server returning to the contact centre a personal identification number; and

wherein the message received by the call processor from the contact centre to reroute said media streams contains said personal identification number.

5. The method according to claim 1, in which the method further comprises after said sensitive audio information has been transmitted in said media streams, the steps of:

the call processor sending a message to the first entity to cause said media to

5 be sent over the first media stream to the second entity; and

the call processor sending a message to the second entity to cause said media to be sent over the second media stream to the first entity;

whereby the media streams are reconnected to bypass the call processor.

10 6. The method according to claim 1, in which the first entity is a user.

7. The method according to claim 1, in which the signalling streams are SIP streams.

15 8. The method according to claim 1, in which the first media stream is an RTP stream and the second media stream is an RTP stream.

9. The method according to claim 1, in which the second entity is a contact centre.

20