

Information Leakage in Ubiquitous Voice-over-IP Communications

Thorsten Neumann, Heiko Tillwick and Martin S Olivier

Information and Computer Security Architectures (ICSA) Research Group,
Department of Computer Science, University of Pretoria, South Africa,
tozzi@intdev.co.za, htillwick@cs.up.ac.za, molivier@cs.up.ac.za,

Abstract. In VoIP, proxies are used by end-devices to perform a number of tasks including call setup and routing. Setup and routing is achieved through the exchange of call control messages which are forwarded among all involved proxies as well as the communicating end-devices. This paper will explore the information exchanged in Voice-over-IP (VoIP) call control messages and any possible implications this has on personal privacy. We assess the explicit and implicit deductions that can be made from handling messages in transit and evaluate these with a conceptual anonymity model. We aim to show that profiling is a threat in current VoIP implementations and that this threat becomes increasingly relevant with the growing adoption of VoIP. We consider these facts in light of possible future scenarios whereby VoIP has the potential to become a truly ubiquitous technology.

1 Introduction

Many organisations are in pursuit to converge their communication networks, allowing for the provisioning of services over a single shared infrastructure. These services, such as voice, video and data, are being transported by packet-switched networks, extending the reach of our global communications infrastructure.

The motivating factors for convergence are the reductions in cost, the continuous innovations allowing for greater service integration and the potential for ubiquitous access and service delivery. However, with these advantages certain privacy concerns surrounding the unification of services into a single *global* network emerge [1].

The growing dependence on technology by society brings with it various privacy issues. More and more people make use of intelligent communication services when performing their day-to-day activities [2]. They knowingly (and unknowingly) transmit large amounts of personal information, thus putting themselves at risk of being monitored.

One technology that has the potential to considerably raise privacy concerns is VoIP, an emergent voice communications technology over the Internet. VoIP will eventually replace our current private-switched telephone network (PSTN).

VoIP is still in its infancy. The implementation of services has not yet matured sufficiently to address the multitude of privacy issues. Details about a call,

such as the participating individuals, are visible to various end-devices, proxies and unauthorised observers. Besides exposing potentially incriminating personal information, individuals also risk having their information being exploited by targeted marketing or insurance companies.

In business, the collection of information for customer relationship management (CRM) and business intelligence (BI) has developed into recognised disciplines. These activities support marketing initiatives in directing and focusing their efforts on particular user segments or individuals. Often, however, available information is averaged to summarise the activities of the collective for specific business purposes.

In VoIP, the analysis of captured private information could similarly be processed. Records can be aggregated to describe the behaviour of a group. Individuals can be monitored allowing users to be profiled. Such profiling makes it possible to determine an individual's activities and habits. Any exploitation of such sensitive information is an obvious infringement of privacy.

Various mechanisms exist that attempt to protect an individual's privacy. Some approaches include using pseudo-identities [3], encrypting sensitive data [4] and information hiding [5]. These privacy-enhancing technologies (PETs) attempt to provide individuals with an acceptable level of privacy.

However, adoption of PETs in VoIP services has received limited attention, largely due to more pressing technical challenges such as voice quality [6], seamless mobility [6] and call management protocols such as SIP [7]. A session management protocol is central to VoIP communication, and many of the privacy concerns relating to VoIP fall back on SIP. Because of SIP's popularity, this paper places specific focus on this protocol.

This paper highlights privacy implications when communicating using VoIP. More specifically, we discuss how private data is leaked when by SIP.

In Section 2 we present background on SIP. Section 3 takes an in-depth look at information leakage by applying the Freiburg Privacy Diamond [8] to show that the exchanged details reduce an individual's anonymity. We show that a communicating individual is not action, device, location and identity independent. This leads onto section 5 which discusses profiling as an invasion of privacy. Finally, we will conclude with section 6.

2 Background

Voice over IP (VoIP) is a general term for any voice communication that is transmitted over the Internet Protocol. This effectively means that voice communication is available to anyone who has access to the Internet and who is using appropriate software.

VoIP commonly distinguishes between two types of a communication: a control channel and a data channel. The data channel is used to transfer the encoded audio stream between two remote parties. The channel is datagram-oriented by design and hence often uses UDP and not TCP. The data channel is set up

according to instructions received from the control channel during session initiation. The control channel, however, ensures that the data channel is established, maintained for the duration of the session and terminated at the end. It is used to exchange messages with the destined remote party, containing details about the source and destination, capabilities of the communicating devices and session information [7]. The control channel is used for, what in traditional telephony, is described as signalling. A protocol commonly used for the control channel is SIP [7]. SIP is the successor to H.323 [1] and has been adopted by the IEEE as the new signalling standard. A more detailed discussion of SIP is therefore appropriate.

An individual, wishing to communicate using a SIP-enabled device would instruct the device to *call* a remote party, identified by either a number or an alias. Gartner predicts (with a probability of 0.9) that users will continue to use traditional numbering in VoIP [9]. This numbering scheme allows for the use of the ITU-T's international public telecommunications numbering plan (E.164) [10] in VoIP. Since devices are no longer bound to physical locations, it allows for the smooth transition from traditional PSTN to VoIP, while ensuring that every device is reachable. Since SIP is designed to work as a distributed architecture, it requires the assistance of intermediaries. It would be impossible to *locate* the remote device without these intermediaries.

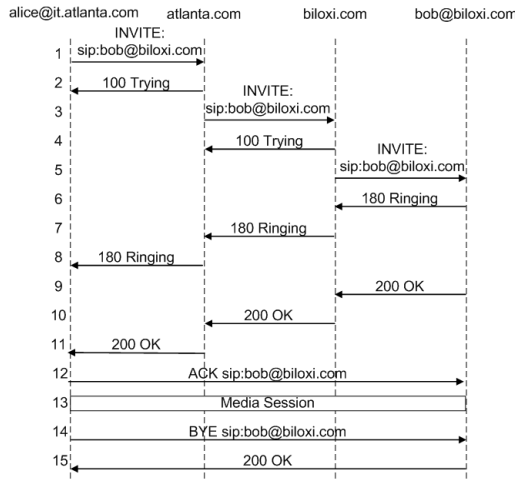


Fig. 1. SIP message exchange

We refer to Fig. 1 to illustrate the steps involved in setting up a SIP session between caller Alice and remote party Bob. SIP initiates a session by sending an INVITE request (step 3). This invite is forwarded by a number of proxies (steps 3,5) until the final proxy is reached. Every proxy is only responsible for its authoritative domain (e.g. biloxi.com), and messages not destined for it are

passed on. This effectively allows for a hierarchical structure – for example: calls destined for Bob working in the human resources (HR) department at a company called Biloxi can be directed to proxy biloxy.com which subsequently forwards the call to proxy hr.biloxi.com. Therefore, proxies dynamically map out a route, from one proxy to another, before the INVITE finally reaches the destination.

This “loose routing” establishes a path which is used for the exchange of subsequent messages. Responses are sent along this path but in the reverse direction. Every proxy, only knows the previous and next proxy. Optimal routes are created, which allow for efficient passing of messages and fail-over mechanisms to ensure sessions are maintained. Call status messages, such as ringing (steps 6–8) and answered (steps 9–11), are back to the calling proxy.

Once the call has been acknowledged (step 11), a data channel is established between the calling and final proxy (step 12). Each proxy will interface with the end-devices; which in our example are operated by Alice and Bob.

Various attributes are exchanged during a session. These attributes are useful to proxies, devices and users, and stored in SIP headers. Required headers are *To*, *From*, *Contact*, *Call-ID* and *Timestamp* values. The *To* and *From* headers are URIs identifying a device or user reachable a domain (e.g. bob@hr.biloxi.com). Additional headers can be used to convey location, alternate contact numbers or device capabilities such as codecs or firmware versions.

Whilst many individuals assume that voice conversations are private, few understand the implications that a signalling protocol has on their privacy. This is understandable as the VoIP environment bear little relation to existing PSTN networks. Telephony operators control the PSTN network, its interconnects to other networks and call routing; unlike the Internet environment.

We pay specific attention to the SIP headers, analyse what information can be acquired and subsequently retrieved from the headers. Furthermore, the inadequacies of the SIP protocol allow intermediate proxies to monitor as well as alter a SIP session. The method in which SIP operates raises concerns over the amount of personal information that is *leaked*.

We investigate the SIP message exchange, in particular SIP headers, in light of the mentioned privacy concerns. We explore what sensitive data is exchanged and how callers can be linked to a device or location. A proxy might have no knowledge about the source or destination, but consider the impact of aggregating messages from multiple proxies and different sources, which could lead to identifying and profiling users.

3 Information Leakage

In this section we discuss possible sources of information leakage and particulars visible to intermediaries.

For example, details about a user and his actions can be inferred. This argument is supported by the RFC 3261 [4] which states that “SIP messages frequently contain sensitive information about their senders”. It elaborates on the privacy of users and that it is possible to know with whom, when, how long

and from where a user communicates. While known security threats exist, this section highlights the privacy issues in SIP.

We first discuss the explicit and implicit attributes which are exchanged during a SIP session. We then examine how this can be used to compromise a users privacy in section 5.

3.1 Explicit Attributes

SIP exchanges many messages during a session, thus ensuring that engaging parties can continue to communicate. The messages contain explicit attributes which are defined in the protocol. These are connection properties which are exchanged among various entities and across networks. They are stipulated in SIP headers as shown in Fig. 2.

```
INVITE sip:01127117931486@atlas-east.vonage.net SIP/2.0
Via: SIP/2.0/UDP pc33.intdev.co.za;branch=z9hG4bK776asdhd8;received=192.0.2.1
Record-Route: <sip:pl.vonage.net;lr>
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>;tag=28491840-EE2
Call-ID: a84b4c76e66710e192.168.0.120
CSeq: 314159 INVITE
Contact: <sip:tozzi@intdev.co.za:5060>
User-Agent: <Motorola VT1000 mac: 000F9F466CD0 sw:VT20_1.1.16e ln:0 cfg:1097174/100282>
Content-Type: application/sdp
Content-Length: 142

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP logging.vonage.net
;branch=z9hG4bK776asdhd8;received=192.0.2.3
Via: SIP/2.0/UDP pc33.intdev.co.za
;branch=z9hG4bK776asdhd8;received=192.0.2.1
From: "Thorsten Neumann" <sip:14169079479@atlas-east.vonage.net>;tag=122965585
To: <sip:01127117931486@atlas-east.vonage.net>;tag=28491840-EE2
Call-ID: a84b4c76e66710e192.0.2.1
CSeq: 2 INVITE
Content-Type: application/sdp
Content-Length: 160
```

Fig. 2. SIP Message with Headers

Each device requires an IP address to communicate giving some indication as to its location on the Internet. IP address information revealed in the SIP header does not tie to a particular location, but does bear on a user's locality. It can be established if a user is at work, communicating from corporate domain, on a mobile network or at home using a broadband connection. It can be argued that this information has carries little weight, yet tied to a users pseudo-identity has greater implications.

A user will assume a pseudo-identity, and use it to engage in a VoIP communication. This pseudo-identity is an address in the form of a SIP URI, and comparable an email address, denoted by an *alias@domain*. Devices and intermediaries assisting in the session resolve this address and communicate with the proxy responsible for the *domain*.

The SIP message can contain auxiliary headers that enhance the communication through informative attributes. A user might be reachable at more than one location and provide multiple contact points. This includes *sip*, *mailto* and

tel addresses. While the latter is not compulsory, a device must convey how it can be contacted directly [4].

Individuals might want to conceal their name, pseudo-identity or contact points. This becomes increasingly important when SIP messages are sent through numerous intermediaries. The communication for a realm is often controlled by an authoritative proxy, which a user has little control over what is communicated. In order to receive calls the user authenticates to this proxy, thereby confirming his identity and his presents.

Depending on vendor implementations, some devices might inform the proxies of additional device specific functionality. Since SIP is a generic implementation for session management, it allows remote parties to determine a devices capabilities. A device might want to provide additional functionality such as video support, presents information or mobility options. In our research we found that Vonage devices disclose the device model, its MAC address, software version and latest configuration.

Other more subtle deduction can be made by watching the transaction within a session. Next we identify how particulars about a user can be interred from these attributes.

3.2 Implicit Attributes

The above listed attributes are communicated in SIP headers. They are explicit and fact, while further implicit properties can be deduced from observing a complete session. Numerous messages are exchanged during a session, as illustrated in Fig. 1, and reveal subtle behavioral attributes. We agree with RFC 3261 which notes there are also less direct ways in which private information can be divulged.

Two important factors are those of time and the duration of a session. Observing SIP messages exchanged at a particular time has a bearing on the users location. A user could have left the office, yet still be communicating thus implying that he or she is possibly at home. Secondly, the progression of a session and its cumulative duration indicate the nature of the call. Many longer calls after work can be assumed to be personal, while those with a duration of less than a minute are most likely work related. This is comparable to the usage patterns found in fixed and mobile phone usage [11, 12] and instant messaging [13].

The final state about a call can be seen in the responses exchanged by devices. SIP response codes are consistent with, and extend, HTTP/1.1 response codes [4] and allow for both machine and human interpretation. These give insight as to how a session was directed or terminated. States such as *Redirected*, *Moved*, *Busy Here*, *Do Not Disturb* or *Rejected* are communicated in these system generated response. These indicate the state of a device or a conscious action of a user.

In the deprecated RFC 2543 (13.3) it is noted that “location and SIP-initiated calls can violate a callee’s privacy”. This includes revealing alternatives can infringe on privacy concerns of the user or the organization.

The SIP protocol does not provide sufficient security to protect these attributes transmitted during a session. Messages can be intercepted, inspected, stored or routed without the users consent.

In the following section we assess the implications of how the discussed attributes can be used to infer personal information. The Freiburg Privacy Diamond will be used as a model to show that an attacker can launch an inference attack on a user.

4 Freiburg Privacy Diamond

We apply the the Freiburg Privacy Diamond [14] which is a model that can be used to analyze anonymity. This model captures the essence of anonymity with regard to device and user mobility. It considers four entities which impact on the users level of privacy. They are: the action itself, the device, the location of the device, and the user, visually (see Fig. 3(a)). These different entities are related. The user performs an action, using a device at a particular location. In order to achieve anonymity, an attacker should not be able to link these entities when observing a single message, or complete session.

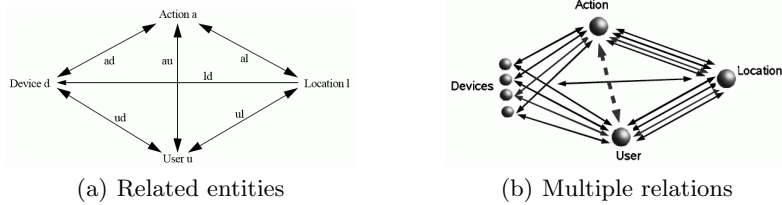


Fig. 3. The Freiburg Privacy Diamond

The model has been extended to describe the additional challenges faced in achieving anonymity in pervasive computing [8]. It shows how communicating devices must protect a users privacy through working together in achieving anonymity. Assessing these entities, an attacker would have to reveal the relations between a user and his action to deduce the identity of a user. Depending on the information captured, the attacker could correlate a user to a device or location. Any such relationship would breach the users privacy by revealing the action performed on a device and at a specific location.

A user would be reachable at, or perform actions using a set of possible devices. The user could make use of more than one device. A devices could be mobile (cellphone or softphone) or bound to a location (as is the case with traditional telephones). It is assumed that the user is in close proximity to the device. While this creates an immediate relation between the user and his location, it does not imply that the user can be identified. The semantics of the Freiburg Privacy Diamond require an attacker to determine which user or which device performed the action.

We apply the Freiburg Privacy Diamond to VoIP communication. It is well suited to our research of information leakage during SIP communication. The

flexibility of SIP allows for users to utilise any device and from any location. The SIP headers disclose private information and have notable implications on a users anonymity.

In order for a user to be *contacted*, it must be possible to locate the device being called. Considering that the utilised device will authenticate on the user's behalf, an implicit relation between the user and a device is created, contravening the Privacy Diamond entities. The exchanged information could also reveal the users location.

Two situations arise when a user is *contacted*. In the first scenario the user is contacted, and accepts the incoming call. The SIP session is initiated in which particulars about the session, therefore the user, are exchanged. This includes the users name, direct contact details and device used. Further, particulars about the users current location, presents and availability could be deduced. Redirection instructions such (181 Call Is Being Forwarded, 300 Multiple Choices, 301 Moved Permanently, 302 Moved Temporarily or 380 Alternative Service) communicate this information as part of the response.

An alternate scenario is when the user can not be located or does not accept the incoming call, thereby communicating back a state of a device or a conscious action of a user. If the user is not present at the time (480 Temporarily Unavailable), the resulting SIP headers would reveal alternate contact numbers or locations at which the user could be reached. In contrast, a conscious action would indicate that the user was contacted but unreachable (486 Busy here, 600 Busy everywhere) or declined the call (603 Decline).

Reverting to the Freiburg Privacy Diamond, the user can therefore be tied to the action, and can be associated with a device and possibly a location. Further assumptions can be made through observing the session, and the extracting the implicit attributes.

5 Profiling

We consider profiling of a VoIP user and the possible privacy implications thereof. The Freiburg Privacy Diamond provides a model through we we have shown that a users privacy is at risk. The Voice over IP Security Alliance [15] remarks that VoIP "faces different threats than other Internet applications, triggering unique security and privacy concerns." Profiling in VoIP is the process of analysing personal information found in call data. We have introduced explicit and implicit attributes as two sources of personal information found in call data.

During the establishment of session, a proxy could unknowingly to the caller insert a *Record-Route* header. This instructs the participating devices to relay subsequent SIP messages through the proxy for the duration of the SIP session. The host specified in the *Record-Route* header need not be the proxy handling the SIP message. An simple example to illustrate the risk of information leakage is where *eve.com* would forward the SIP INVITE with this additional *Record-Route* header. While *eve.com* should no longer play an role in the session, the proxy will receive all messages and event updates exchanged between the communi-

cating parties. As indicated in Fig. 1, neither Alice nor Bob are aware of this intermediary.

SIP devices and proxies additionally rely on the *Route* directive to pass messages to specific hosts for processing and routing. A misconfigured or compromised proxy can manipulate messages without consent from the user, such as injecting additional headers. The SIP header will force the message to be forwarded to a specific intermediary before reaching the intended destination.

The possibility exists where *eve.com* inserts a *Route* instruction to have the current SIP message forwarded to *profiling.com*. This allows the next en route proxy to collect the Explicit Attributes described in Section 3.1. Further, one could consider this in combination with the aforementioned *Record-Route* header. This gives *profiling.com* the ability to monitor and profile the user, correlating the actions and ability to deduce the implicit attributes described in Section 3.2.

The users of a SIP session are not in control over the communication environment, often restricted to the interface of the device (or softphone). The communicating parties might not be aware of intermediaries logging and recording call control messages. While the mentioned records are specific to call control events, they expose a great amount of detail about a user.

With the growing adoption of VoIP profiling becomes an increasingly dangerous threat. Analysing a collection of calls performed or received by an individual could expose a substantial amount of information about a user's behaviour, habits or preferences. Whilst these threats are currently minor, one should consider a case where VoIP becomes a truly ubiquitous communications technology.

One could consider the case whereby many household, workplace and public devices are networked and support IP communications. Not every device needs to be a communications device. It could be used to inform an individual if his phone is ringing or if messages are available. If this were the case, more personal information would be available.

Further research is required to study the implication that a widespread acceptance of VoIP has on personal privacy. An interesting case is a probable future scenario whereby communication is possible from anywhere and by anybody using his own unique pseudo-identity or telephone number. We have only briefly touched on the implications hoping to stimulate ongoing discussions.

6 Conclusion

The aim is to show that information leakage in VoIP, and specifically for SIP, affects a user's privacy. Personal details about the user are exposed, thus compromising a user's anonymity. Information about a user's action, the device used, location and identity can be correlated. A user is therefore not assured a sufficient level of privacy when communicating over the Internet.

We identified what the information is revealed when communicating with a remote device and discussed implicit attributes that can be deduced from this. The Freiburg Privacy Diamond [14] was used to support our argument.

Future research will assess viable methods of ensuring privacy and anonymity. Research surrounding security mechanisms to prevent the misdirection messages and manipulation of SIP Headers have been suggested [16]. This does, however, require the collaboration of multiple devices which must strive to protect the user's identity.

The trends indicate that the VoIP will increasingly dominate cable telephony, and start replacing traditional telephone lines [1]. This raises concerns about a users privacy as this pervasive technology starts replacing our existing communications infrastructure.

References

- [1] Phil Sherburne and Cary Fitzgerald: You Don't Know Jack About VoIP. *Queue* **2**(6) (2004) 30–38
- [2] Weiser, M.: The Computer for the 21st Century. *Scientific American UbiComp* **3** (1991) 94–104
- [3] Peterson, J., Jennings, C.: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), RFC 3323 (2003)
- [4] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol, RFC 3261 (2002)
- [5] Peterson, J.: A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323 (2002)
- [6] Varshney, U., Snow, A., McGivern, M., Howard, C.: Voice over IP. *Commun. ACM* **45**(1) (2002) 89–96
- [7] Schulzrinne, H., Rosenberg, J. In: The Session Initiation Protocol: Internet-centric signaling. Volume 38., IEEE (2000) 134–141
- [8] Zugenmaier, A., Kreuzer, M., Müller, G.: The freiburg privacy diamond: An attacker model for a mobile computing environment. In: *KiVS Kurzbeiträge*. (2003) 131–141
- [9] Fraley, D.L.: Voice Over IP Communications Must Be Secured. Gartner, Inc. (G00124016) (2004) 5 of 6
- [10] Faltstrom, P.: E.164 number and DNS. RFC 2916 (1998)
- [11] Palen, L., Salzman, M., Youngs, E.: Going wireless: behavior & practice of new mobile phone users. In: *CSCW '00: Proceedings of the 2000 ACM conference on Computer supported cooperative work, USA*, ACM Press (2000) 201–210
- [12] Hindus, D., Schmandt, C.: Ubiquitous audio: capturing spontaneous collaboration. In: *CSCW '92: Proceedings of the 1992 ACM conference on Computer-supported cooperative work, New York, NY, USA*, ACM Press (1992) 210–217
- [13] Isaacs, E., Walendowski, A., Whittaker, S., Schiano, D.J., Kamm, C.: The character, functions, and styles of instant messaging in the workplace. In: *CSCW '02: Proceedings of the 2002 ACM conference on Computer supported cooperative work, NY, USA*, ACM Press (2002) 11–20
- [14] Zugenmaier, A.: The Freiburg Privacy Diamond - A Conceptual Model for Mobility in Anonymity Systems. In: *Proceedings of Globecom*. (2003)
- [15] Alfonsi, B.: Alliance addresses VoIP security. *IEEE Security & Privacy* **3**(4) (2005) 8
- [16] T. Neumann and Martin S Olivier: Enhancements to SIP to prevent abuse of Voice-over-IP services. In: *Southern African Telecommunication Networks and Applications Conference (SATNAC) Proceedings*. (2005)

T Neumann, H Tillwick and MS Olivier, "Information Leakage in Ubiquitous Voice-over-IP," in S Fischer-Hübner, S Furnell and C Lambrinoudakis (eds), *Trust, Privacy and Security in Digital Business*, LNCS 4083, 233-242, Springer, 2006

Copyright ©Springer-Verlag

Source: <http://mo.co.za>