International Working Group
on Data Protection
in Telecommunications

675.52.10

**Working Paper: Update on Privacy and Security Issues
in Internet Telephony (VoIP) and Related Communication Technologies**

*59th meeting, 24-25 April 2016, Oslo (Norway)*

## Introduction

In September 2006, this Group published a Working Paper on Voice over IP (VoIP) applications[1] in an attempt to anticipate possible privacy and security challenges. That paper depicted the situation as seen by the Working Group at the time: it described emerging services, possible future privacy and security risks, and contained a set of privacy- and security-related recommendations to manufacturers of hardware, software developers and VoIP service providers.

In the subsequent 10 years, VoIP has found widespread application by organisations as well as by end users. Furthermore, voice communication has been integrated with a number of other communication technologies, such as instant messaging, text and video. In some regions discussions have already started about phasing out the “Plain Old Telephony System” (POTS), which is now labelled as “legacy infrastructure” by some.

The recommendations in this working paper apply to all types of multi-media services, including instant messaging, real-time text, and video services[2]. This document furthermore makes no distinction between a VoIP service offered by a telecommunication provider and an over-the-top provider. Even if the technology being used by various companies differs, similar privacy and data protection risks remain and therefore the recommendations apply to all.

In addition to standardised solutions, there are many proprietary products and services available which provide different degrees of security, data protection and privacy. Unfortunately, non-technical users are often uninformed about the protection provided or are not presented with privacy friendly default settings.

[1] International Working Group on Data Protection in Telecommunications: “Working Paper on Privacy and Security in Internet Telephony (VoIP)”, adopted at the 40th meeting on 5-6 September 2006 in Berlin (Germany); http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_en.pdf

[2] We use the terms ‘voice and video’ and ‘multi-media’ interchangeably since the content of this recommendation refers to the more generic concept of multi-media communication but for historical reasons and improved readability the term voice is more frequently used.

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

With this additional Working Paper, the Working Group updates the recommendations provided in the initial publication based on a re-evaluation of the state of the art as of today (2016). The following considerations motivate the re-evaluation of this topic:

- The revelations by Edward Snowden indicate that law enforcement agencies and secret services across the globe have – with or without the co-operation of companies offering services on the Internet (including VoIP service providers) – unprecedented access to VoIP conversations as well as to associated traffic data. This global monitoring calls into question user trust in both developers and service providers. Similarly, leakage of traffic data, such as IP addresses, DNS queries, and application layer signalling headers, is a challenge to the confidentiality of the communication[3]. While this traffic data does not leak the content of the communication, it often provides enough information about the communicating parties to compromise their privacy.

- Standardisation in the area of VoIP has progressed and the market today is more mature than in 2006 when the initial paper was published. The standardisation of the Session Initiation Protocol (SIP) and of various extensions has been finalised and many products are now available on the market. Additionally, a new standardisation effort that aims to offer better alignment with Web technologies (and browsers in particular), namely Web Real-Time Communication (WebRTC)[4], has been started and early deployments are available. The aim of WebRTC is to offer easier integration of real-time communication into the browser. This gives rise to new security and privacy challenges[5].

- The deployment of high bandwidth cellular radio technology as well as Wi-Fi networks has substantially increased. Users are able to use these networks to establish reliable and high-quality VoIP and video calls. Additionally, easy to use VoIP software is either available on consumer devices pre-installed or downloadable via application stores. In early 2000 VoIP was mostly in use by businesses and technically savvy users while today it is in widespread use by ordinary end users.

- Privacy and security practices vary considerably throughout the different service offerings. Unfortunately, these practices are not well communicated to end users.

- POTS were traditionally installed and managed by a single operator, commonly owned and managed by the State. This contrasts with the current VoIP environment which is evolving into a composition of many parts (e.g., network services, operating systems, application software). These “parts” are often developed and managed by separate entities (e.g., the network operator, the hardware or software developer and the device manufacturer), each of them acting independently and, in most cases, without any coordination. Whilst this proliferation of roles could provide the user with greater choice, the incentives and objectives

[3] R. Barnes, et al., " Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement" (RFC 7624), August 2015, available at https://tools.ietf.org/html/rfc7624

[4] W3C, WebRTC 1.0: Real-time Communication Between Browsers, available at http://www.w3.org/TR/webrtc/

[5] E. Rescorla, "WebRTC Security Architecture", IETF draft (work in progress), March 2015, available at https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-11

of each entity does not necessarily lead to an improvement in the protection of privacy as each stakeholder is focussing only on their part in the chain.

## Technical Background

Conceptually, VoIP solutions are fairly simple: a user enters the phone number or another identifier (many of which look similar to an email address) in order to “dial” another user. With the help of a support infrastructure, sometimes called proxies, the VoIP client then initiates signalling communication to find a device of the called party. The messages exchanged in the course of this procedure are referred as signalling messages.

For VoIP solutions that do not support interworking with other providers, all users need to have their devices registered with the same VoIP provider. In more open systems, this discovery step may be complicated since users may be registered with different VoIP providers and the discovery procedure may be expanded to third party providers. It should be noted that interworking with other VoIP systems (or even with the Public Switched Telephone Network – PSTN) may lead to a loss of functionality and inferior security and privacy properties.

Once the device of the other communication partner has been found, voice packets can be exchanged between the two parties. While signalling messages are often routed indirectly via the support infrastructure between the two parties, multi-media traffic (such as voice and video) is ideally transmitted directly. This direct communication ensures lower latency. Voice packets, may be encapsulated in a Secure Real-Time Transport Protocol (SRTP)[6] payload. Different protocols exist which deal with the risk of pervasive monitoring.[7]

In practical scenarios, signalling messages offer more functionality than pure discovery of communication devices, including negotiation of protocol parameters and features. For more sophisticated usage scenarios, such as conference calls or call transfers, the call setup procedure may be more complex. Furthermore, offering channel security via SRTP requires the establishment of cryptographic keys and algorithms. Hence, various different key management protocols for the establishment of keys required for securing media traffic have been developed, which all provide slightly different properties[8].

---

[6] M. Baugher, et al., "The Secure Real-time Transport Protocol (SRTP)", March 2004, RFC 3711, available at https://tools.ietf.org/html/rfc3711

[7] IAB Statement on Internet Confidentiality, November 2014, available at https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

[8] For an analysis of key exchange technologies and their properties see RFC 5479 (https://tools.ietf.org/html/rfc5479) and RFC 7201 (https://tools.ietf.org/html/rfc7201)

## Recommendations[9]

In light of the above, the Working Group makes the following recommendations to the different stakeholders:

### Legislators and Regulators

Legislators and regulators at the national, regional and even global levels are reminded that gaps exist in the legal protection of the confidentiality of communications at the different regulatory levels with respect to VoIP services. They are called upon to thoroughly investigate the legal situation and make changes as necessary with a view to ensuring that the provisions for telecommunications secrecy as foreseen in many national constitutions, regional and global regulatory instruments also fully cover VoIP and other multi-media communication services.

### VoIP Providers, Software Developers and Hardware Manufacturers

*Transparency*

VoIP service providers should inform customers about the privacy and security characteristics of the VoIP service(s) they offer.

*Privacy Impact and Third Party Assessments*

Hardware and software manufactures should perform Privacy Impact Assessments. The Working Group also encourages analysis and assessment by independent, trustworthy third parties. An example of such an assessment is the “Secure Messaging Scorecard“ provided by the Electronic Frontier Foundation (EFF)[10]. Examples of automated tools are those provided by the XMPP Foundation[11] and the GSM Map[12] .

*Design Considerations*

Software developers and hardware manufacturers should take appropriate technical measures to protect signalling traffic as well as voice and video traffic against unauthorised pervasive monitoring. As a default design consideration, it is imperative that software developers strive for implementations based on end-to-end encryption for both signal and content.

VoIP signalling traffic must be authenticated, and integrity and confidentiality must be protected between participating VoIP signalling nodes. Providing end-to-end integrity for the entire VoIP

---

[9] The recommendations for VoIP are to be read in conjunction with those from the first Working Paper of the Group from 2006; cf. http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_en.pdf

[10] Electronic Frontier Foundation (EFF), “Secure Messaging Scorecard”, October 2015, available at https://www.eff.org/secure-messaging-scorecard

[11] XMPP (Extensible Messaging and Presence Protocol) Foundation, “XMPP Security Tests”, October 2015, available at http://xmpp.net

[12] GSM – *Global System for Mobile* Communications (previously „Groupe Spécial Mobile“). Cf. Karsten Nohl, “GSM Map”, October 2015, available at https://gsmmap.org

signalling traffic is unfortunately not possible in most VoIP architectures since the signalling payload is modified in transit[13]. The transmission of signalling messages over non-cryptographically protected links must be avoided. It should be noted that relying on physical security alone is not an appropriate state-of-the-art security technique in today's Internet with the level of pervasive monitoring in use[14].

Traffic data about the communication, such as identifiers of the communicating parties, communication preferences (such as codecs and language), length of the (encrypted) data packets and online status, often reveal a surprising amount of information. The Working Group therefore recommends to limit the amount of data being exposed to intermediaries, such as signalling gateways, and to avoid the use of persistent identifiers as much as possible.

The Working Group strongly encourages VoIP providers to use key management mechanisms that do not allow intermediaries to obtain keying material (because it is transmitted in plaintext embedded in the signalling messages) and to make use of a key management protocol offering perfect forward secrecy (PFS)[15]. PFS is a security property that prevents an adversary from decrypting past conversations when the long term secret keys are compromised. While recognising the limitations of some VoIP architectures, priority should still be given to implementing end-to-end security for voice and video communication.

Measures should be developed to allow users to verify whether a "man-in-the-middle" attack has occurred by verifying the keys if certificates are needed to establish end-to-end communication. Certificates[16] could be issued by (trusted) third parties, and – as an option – could be linked to pseudonyms (telephone numbers, user names, or names of organisations), and these certificates should be displayed to the communicating parties.

VoIP service providers must, by default, restrict the amount of personal data stored and processed to what is necessary for the provision and billing (as applicable) of the service, unless additional storing or processing of data is explicitly mandated by law. Protection against unauthorised access to stored data must be ensured.

VoIP service providers must offer basic privacy-relevant features, such as withholding caller ID, at least in the same manner as is common place in fixed and mobile telephone networks. Since the suppression of caller id information and caller id spoofing facilitate certain types of attacks, recently

---

[13] Since the modification of signalling message payloads breaks signature algorithms, as described on page 16 of RFC 7340 (https://tools.ietf.org/html/rfc7340) and most VOIP architectures modify signalling payload in transit, the number of participating nodes must be kept as small as possible to ensure the integrity of the entire VOIP signal traffic. RFC 7044 offers a solution to incrementally apply message protection as messages are routed through the SIP communication network. This offers history information to the communication party (https://tools.ietf.org/html/rfc7044).

[14] While the wired network infrastructure used for "classic" telecommunications services used to be seen as „safe by definition", this assumption does not hold true anymore: today wires are tapped by secret services on a large scale.

[15] The PFS property is further explained in https://en.wikipedia.org/wiki/Forward_secrecy . Cf also A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, USA, 1996 (see page 496).

[16] J. Peterson, et al., "Secure Telephone Identity Credentials: Certificates", IETF draft (work in progress), March 2016, available at https://tools.ietf.org/html/draft-ietf-stir-certificates-03

developed protection mechanisms[17] should be taken into account. Caller identity hiding makes access control lists, sometimes called buddy lists, less effective. Due to the direct connection between the parties to the communication, their IP addresses will be disclosed to each other. To prevent this, the optional use of proxies or anonymisation services (e.g., Tor[18], TURN[19]) should not be prohibited.

Existing open standards that have enjoyed widespread review and verification by a large number of independent experts should be re-used. Several standardised solutions for the protection of voice communication are available[20,21]. It should be noted that the standardisation process in different organisations allows technical specifications to be published without significant expert review taking place or, in the worst case, without any review at all. Hence, a decision about what technical specification to utilise has to take the level of review into account and standardisation organisations are encouraged to provide more transparency about the process by which that specification was developed.

*User Participation*

VoIP providers should allow their users to choose their own identity provider where such a separation between identity provider and VoIP service provider is technically possible.

VoIP providers should offer data portability (where appropriate) to provide their customers convenient access to relevant data, such as buddy lists, and configuration data.

*Operational Considerations*

All stakeholders in the supply chain must react quickly to security or privacy flaws in the protocols and the hardware or software in use. For vulnerabilities in distributed software, such as smart phone apps or other downloadable software, this requires incorporating a software update mechanism.

VoIP service providers must make sure that security and privacy features of their products are activated by default. Security and privacy mechanisms should be offered without prohibitive costs for the customer.

VoIP service providers should offer federated access to their VoIP services. This allows users to interface with users from other VoIP providers without the need to download and install different VoIP clients. At a minimum, users must be informed about changes of security and privacy features of

---

[17] IETF, “Secure Telephone Identity Revisited (STIR) Working Group”, October 2015, available at http://datatracker.ietf.org/wg/stir/charter/

[18] More information about the onion routing technology Tor can be found at https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[19] R. Mahy, et al., "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, Apr. 2010, available at https://tools.ietf.org/html/rfc5766

[20] M. Westerlund and C. Perkins, "Options for Securing RTP Sessions", RFC 7201, April 2014, available at https://tools.ietf.org/html/rfc7201

[21] D. Wing, et al., "Requirements and Analysis of Media Security Management Protocols", RFC 5479, April 2009, available at https://tools.ietf.org/html/rfc5479

their communication when interworking with other VoIP systems (or even the PSTN) and any loss of functionality, security or privacy protection that may result from such changes.

*Purpose limitation*

Providers, software developers and hardware manufacturers that process traffic data shall respect the principle of purpose limitation.

**Users**

Users of VoIP services should be aware of the possible risks for the security and privacy of their communications. They should educate themselves about the security and privacy properties of the different services, and choose the services and service providers they use accordingly. Finally, they should make sure that existing security and privacy features of a service are activated before using the service.

## About the International Working Group on Data Protection in Telecommunications ("Berlin Group")

The International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group") includes representatives from Data Protection Authorities and international organisations dealing with privacy matters from all over the world. It was founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners at the initiative of the Berlin Commissioner for Data Protection, who has since then been chairing the Group. The Group has since 1983 adopted numerous recommendations ("Common Positions" and "Working Papers") aimed at improving the protection of privacy in telecommunications. Since the beginning of the 90s the Group has in particular focused on the protection of privacy on the Internet. More information about the Work of the Group and the documents adopted by the Group are available for download on the website of the Group at http://www.berlin-privacy-group.org .