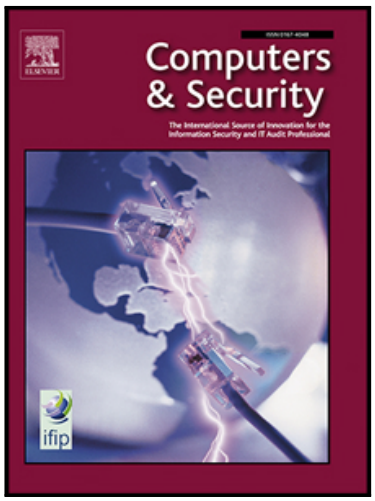

Exploiting IP Telephony with Silence Suppression for Hidden Data Transfers

Sabine Schmidt, Wojciech Mazurczyk, Radoslaw Kulesza,
Jörg Keller, Luca Caviglione

PII: S0167-4048(18)30577-7
DOI: https://doi.org/10.1016/j.cose.2018.08.006
Reference: COSE 1385

To appear in: *Computers & Security*

Received date: 21 May 2018
Revised date: 5 August 2018
Accepted date: 20 August 2018

Please cite this article as: Sabine Schmidt, Wojciech Mazurczyk, Radoslaw Kulesza, Jörg Keller, Luca Caviglione, Exploiting IP Telephony with Silence Suppression for Hidden Data Transfers, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.08.006

Exploiting IP Telephony with Silence Suppression for Hidden Data Transfers

Sabine Schmidt[1], Wojciech Mazurczyk[2], Radoslaw Kulesza[2], Jörg Keller[1], Luca Caviglione[3]

Abstract

Information hiding is increasingly used by malware for creating covert channels to exfiltrate data, orchestrate attacks, as well as to download additional code for extending its functionalities at runtime. Since the popularity of the carrier used for embedding secrets is fundamental to guarantee a suitable degree of stealthiness, this paper investigates how to create a covert channel within ubiquitous Voice over IP (VoIP) conversations. Specifically, we propose to hide information in fake RTP packets generated during silence intervals obtained by transforming a VoIP stream with Voice Activity Detection (VAD) into a non-VAD one. Experimental results collected in different scenarios indicate that embedding a covert channel in the VAD-activated VoIP stream offers a good trade-off between stealthiness and steganographic bandwidth. Guidelines to detect and mitigate information-hiding-capable threats targeting IP telephony applications are also provided.

Keywords: information hiding; network covert channel; VoIP; IP telephony; network steganography; network security.

1. Introduction

Nowadays, information hiding is primarily used by malware to conduct large-scale attacks or exfiltrate stolen data in a stealthy manner (Mazurczyk and Caviglione, 2015a; Wendzel et al., 2014). Other possible use cases include the development of anti-forensics mechanisms, privacy-preserving hidden file systems, or communication services to prevent censorship and protect the identity of sources in investigative journalism (Caviglione et al., 2017b).

In general, *information hiding* is used as an umbrella term for a wide variety of data hiding and steganography mechanisms. Put briefly, it allows to hide secret information within innocent looking carriers, such as image, video or audio files. Network steganography is the most recent and young form of information hiding. In this case, the secret data is injected in network traffic, for instance by using fields of the protocol headers, the inter-packet time, the jitter, the throughput, and the number of data units generated by a specific protocol (Zander et al., 2007). The main use of steganographic mechanisms applied to network traffic is to set up a covert channel allowing a secret sender and a secret receiver to exchange data in a stealthy manner. Even if exploiting a network flow to create a covert channel for malicious purposes is nowadays a well-studied topic, the process mutated during the years, e.g., from secrets injected into unused fields of the IP header, to sophisticated cloud-based mechanisms (Ahsan and Kundur, 2002; Carrara and Adams, 2016; Caviglione et al., 2017a). Today, many covert channels exploit the hardware of modern smartphones, for instance, short-range connectivity or metadata generated by the GPS and accelerometers (Mazurczyk and Caviglione, 2015b).

Obviously, the carrier should not represent an anomaly and its alteration should not reveal the secrets. For the case of network steganography, the presence of a covert channel could be revealed by signatures such as incoherent protocol behaviors, inflated data volumes or uncommon timing statistics (Zander et al., 2007; Mazurczyk and Caviglione, 2015b). In this perspective, Voice over IP (VoIP) is an excellent candidate for the creation of network covert channels. In fact, it is ubiquitously available, produces a huge amount of traffic and offers a rich set of features suitable for steganographic purposes (Mazurczyk and Caviglione, 2015b; Bonfiglio et al., 2009). In the following, we will use the terms IP telephony and VoIP interchangeably, except when doubts arise.

Unfortunately, there is no "miracle solution" for taming malware equipped with information-hiding-capable features. Thus, a relevant part of research aims at finding possible workarounds and methods to prevent exploitable ambiguities of new services (Zielińska et al., 2014). Therefore, investigating covert channels is mandatory to evaluate the cybersecurity of the Internet in a complete manner. Along the lines of the preliminary work of Schmidt et al. (2017), this paper introduces a technique to establish a covert channel within the traffic produced by VoIP applications. Differently from similar methods, we take advantage of the Voice Activity Detection (VAD) feature, which allows to save bandwidth by suspending the transmission of packets during speech pauses. In essence, we propose to transform a VAD-activated VoIP stream into a non-VAD one, and inject the hidden information into fake Real-time Transport Protocol (RTP) packets generated during silence intervals. Accordingly, we named this method *stegVAD*. Results demonstrate that the proposed approach guarantees a good network covert channel capacity with a negligible impact on the quality of the conversation. However, the alteration of the stream reflects into "sig-

[1]FernUniversität in Hagen.
[2]Warsaw University of Technology.
[3]Institute for Applied Mathematics and Information Technologies.
Corresponding Author: wojciech.mazurczyk@fernuni-hagen.de