available at www.sciencedirect.com

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

A survey on fraud and service misuse in voice over IP (VoIP) networks

Yacine Rebahi [a,*], Mohamed Nassar [c], Thomas Magedanz [b], Olivier Festor [c]

[a] Fraunhofer Fokus, Kaiserin Augusta Allee 31, 10589 Berlin, Germany
[b] Technische Universität Berlin, FR 5-14, Franklinstr. 28/29, D-10587 Berlin, Germany
[c] INRIA Research Center, Nancy - Grand Est 54602 Villers-Lès-Nancy, France

Keywords:
Security
Fraud
Service misuse
VoIP
Fraud detection
Rule-based detection
User profiling
Neural networks
Fraud data collection

ABSTRACT

The migration from circuit-switched networks to packet-switched networks necessitates the investigation of related issues such as service delivery, QoS, security, and service fraud and misuse. The latter can be seen as a combination of accounting and security aspects. In traditional telecommunication networks, fraud accounts for annual losses at an average of 3%–5% of the operators' revenue and still increasing at a rate of more than 10% yearly. It is also expected that in VoIP networks, the situation will be worse due to the lack of strong built-in security mechanisms, and the use of open standards. This paper discusses the fraud problem in VoIP networks and evaluates the related available solutions.

1. Introduction

There are different definitions of fraud in the literature. However, fraud can simply be defined as any activity that leads to the obtaining of financial advantage or causing of loss by implicit or explicit deception. It is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss. Fraud losses keep impacting every business enterprise. The costs of fraud are passed on to the society in the form of increased customer inconvenience, opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by the fraudulent gains. Despite significant advances in fraud detection technologies, fraud losses continue to pose a significant problem to many industries, including telecommunications, banking and finance, insurance, e-commerce and many others.

VoIP is the set of technologies that enable voice calls to be carried over the Internet. Contrary to the traditional telephone system - the Public Switched Telephone Network (PSTN)-, the potential driving the use of the VoIP technology is not only the very low cost or free voice calls, but also its ability to converge with other technologies, in particular presence and Instant Messaging, which in turn will result in new services and applications.

VoIP networks are based on complex technologies, which in turn, involve different components, protocols, and interfaces. As a consequence, fraud detection in VoIP is harder than the one in the current telecommunication networks. Through this paper, we would like to discuss briefly the VoIP fraud problem and survey the anti-fraud solutions proposed in various areas, and their usability in the VoIP context.

The rest of this paper is organized as follows: Section 2 gives an overview of the dominant underlying VoIP protocol. Section 3 provides some concrete VoIP fraud scenarios, and Section 4 discusses existing anti-fraud solutions. Section 5 presents our approach in the context of the Scamstop project. Finally we conclude in Section 6.

* *Corresponding author*. Tel.: +49 30 34637141; fax: +49 30 34638000.
E-mail addresses: yacine.rebahi@fokus.fraunhofer.de (Y. Rebahi), Mohamed.Nassar@inria.fr (M. Nassar), thomas.magedanz@tu-berlin.de (T. Magedanz), Olivier.Festor@inria.fr (O. Festor).
1363-4127/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.10.012

2. Voice over IP (VoIP) networks

There are many protocols that may be employed in order to provide VoIP communication services, However, the Session Initiation Protocol (SIP) (RFC 3261) is rapidly gaining widespread acceptance as the signaling protocol of choice for fixed and mobile Internet multimedia and telephony services.

SIP is an application-layer control protocol that allows users to create, modify, and terminate sessions with one or more participants. It can be used to create two-party, multi-party, or multicast sessions that include Internet telephone calls, multimedia distribution, and multimedia conferences.

In SIP, a user is identified through a SIP Uniform Resource Identifier (URI) in the form of user@domain. This address can be resolved to a SIP proxy that is responsible for the user's domain. To identify the actual location of the user in terms of an IP address, the user needs to register his IP address at the SIP registrar responsible for his domain. Thereby when inviting a user, the caller sends his invitation to the SIP proxy responsible for the user's domain, which checks in the registrar's database the location of the user and forwards the invitation to the callee. The callee can either accept or reject the invitation. The session initiation is then finalized by having the caller acknowledging the reception of the callee's answer. During this message exchange, the caller and callee exchange the addresses at which they would like to receive the media and what kind of media they can accept. After finishing the session establishment, the end systems can exchange data directly without the involvement of the SIP proxy.

3. Fraud scenarios in VoIP

The traditional telecommunication fraud could take different shapes such as subscription fraud, roaming fraud, technical fraud, premium rate fraud, and others. While all of these fraud use cases can be seen as direct threats to VoIP networks, the VoIP technologies add some other risks as well:

(1) Service plan misuse: In general VoIP services are offered as flat-rate services. Operators calculate these plans based on average usage scenarios. While such services are intended for personal use only, some subscribers offer this service to other people -family and friends- as well resulting in high usage and high losses to the operator.
(2) Credit Card fraud: In this case, fraudsters use the toll free service of a VoIP provider to find out the PIN numbers of a stolen credit card. That is, while sitting in Nigeria for example, the fraudster would call a premium service in the USA and that would require the credit card and PIN number and keep trying this till the right number was found.
(3) Identity theft: While the access control scheme of the VoIP protocols (based of MD5 hash technology) is fairly robust it can be attacked. This would result in reviling a user's password to the attacker which would then misuse the user's service.
(4) Viruses and malicious code: As some of the VoIP components will be connected to the public Internet, it might be possible that a virus or a malicious code that was downloaded, by mistake, by a customer can call premium numbers or deliver unwanted content. Unfortunately, the customer will be charged for these services that he did not intend to use.

Many vulnerabilities in VoIP systems and products may lead to technical forms of fraud. Keromytis (Keromytis, 2010) proposes to classify VoIP vulnerabilities based on three landmarks:

(1) The VoIPSA taxonomy: The key elements of this taxonomy are: (1) Social threats, (2) Eavesdropping, interception and modification, (3) Denial of service threats, (4) Service abuse threats, (5) Physical access threats and (6) Interruption of service threats. For a complete description refer to (VoIP Security alliance, 2005).
(2) The corrupted security property: confidentiality, integrity or availability.
(3) The cause of the vulnerability: Protocol, Implementation or configuration.

The study covers more than 220 VoIP vulnerabilities. Moreover, fraudsters employ Internet hacking techniques in order to reach their goals:

(1) Eavesdropping on public transactions to obtain personal data. This can be done by looking behind the shoulder of a person performing a transaction or by sniffing on VoIP transactions packets especially if encryption is not used
(2) Using viruses and Trojan horses to get private data stored in computers
(3) Phishing, impersonate a trusted organization or a VoIP provider and ask customers for some private data in order to fix a pretended problem.
(4) Spam: most of Spam activities require you to take advantage of the good deals they are offering. If some personal data are given to them, this information will be used for carrying out their attacks.
(5) Browsing into social networks, for instance web sites of public domains where personal data are posted
(6) Equipment stealing or hacking

Keromytis has surveyed the VoIP security research state of the art (Keromytis, 2009). It turns out that little work has been addressing the service abuse threats (only 8 over around 200 research items visited in the study).

Real fraud scenarios show that VoIP suffers from the inherited security issues of the Internet. In one of the most famous stories (Pena's case) that had been covered by the VoIP Security Alliance (VoIPSA)[1], VoIP gateways and other routers are remotely compromised due to weak or unchanged default passwords, and exposed management ports. We estimate that the main difficulty with VoIP fraud detection is the correlation of events across different layers and from different sources.

[1] http://www.voipsa.org