Computer Communications 32 (2009) 203–212

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

OntoSPIT: SPIT management through ontologies

S. Dritsas, V. Dritsou, B. Tsoumas, P. Constantopoulos, D. Gritzalis *

Information Security and Critical Infrastructure Protection Research Group, Dept. of Informatics, Athens University of Economics and Business (AUEB), 76 Patission Ave., 10434 Athens, Greece

ARTICLE INFO

Article history:
Received 23 March 2008
Received in revised form 6 October 2008
Accepted 6 October 2008
Available online 18 October 2008

Keywords:
SPIT (SPAM over Internet telephony)
Ontology
VoIP
SPAM

ABSTRACT

VoIP enables new ways for communication. At the same time, it provides new means, in terms of transmitting bulk unsolicited messages and calls, namely SPam over Internet telephony (SPIT). In this paper, we propose a conceptual model, based on an underlying ontology, which describes the SPIT domain. The ontology provides capabilities, such as modeling the SPIT phenomenon in a SIP-based VoIP environment, a common understanding of SPIT domain, as well as reusable SPIT-related knowledge interoperability, aggregation and reasoning. We demonstrate that the proposed ontology, combined with a set of SPIT identification criteria, as its underlying axioms and rules, could enhance the correlation and management of SPIT incidents. It could also support SPIT detection, thus facilitating the better protection of VoIP environments in a holistic, cooperative, and effective way.

1. Introduction

Voice-over-IP (VoIP) increasingly penetrates the telephony market, as it appears to be an attractive alternative compared to traditional telephony. VoIP seamless integration with the existing IP networks (and especially the Internet), its lower costs compared to PSTN telephony, the use of computer-based soft-phones, as well as the existence and the implementation of sophisticated end-user services, in terms of portability, accessibility and convergence of telephone networks, are some of the reasons that make VoIP an increasingly attractive and advantageous network application.

However, the use of VoIP also facilitates the exploitation of new threats and vulnerabilities that Internet protocols pose [22,18]. For example, low-cost calls and zero-cost instance messages, combined with the pervasiveness of Internet, could be used by malicious users to make bulk unsolicited calls and/or send bulk unsolicited instant messages. This is a new form of SPAM, in the context of VoIP environments, which is called SPAM over Internet telephony (SPIT). SPIT is expected to cause stronger impact on users, than email SPAM, as it appears to be more intrusive [12,20].

SPIT has received low attention until now, mainly due to its rather embryonic stage of employment. However, several anti-SPIT frameworks have been already proposed, focusing on countering the SPIT phenomenon by adopting concepts, approaches, and techniques mainly used for fighting email SPAM [13]. The effectiveness of these tools is usually considered inadequate, mainly due to their ad hoc nature, as well as due to the real-time nature of VoIP communications.

In this paper, we show that the effectiveness of an anti-SPIT technique depends on several factors, and relates to different elements that are incorporated within a VoIP infrastructure. Next, we propose an ontology that describes the SIP (session initiation protocol)-based SPIT (or anti-SPIT) domain, and we show that this ontology (called ontoSPIT) can provide a common understanding of the SPIT domain, facilitate the reuse of domain knowledge, and, finally, help solve several domain interoperability issues, mainly through making domains' SPIT assumptions explicit.

The paper is organized as follows. First, we briefly present the necessary background, regarding the VoIP environment and the SPIT phenomenon and we refer to a number of issues regarding the ontology paradigm. In the sequel, we introduce the SPIT-related conceptual model together with the essential terms that define the SPIT domain. Next, we present a set of SPIT identification criteria, which can facilitate the detection of SPIT traffic in a VoIP environment. Based on the above criteria, we build an event-condition-action (ECA) model, which acts as the basis for a detailed SIP-oriented SPIT ontology (ontoSPIT). Then, the ontoSPIT model is presented in detail and comment upon. After presenting the model, we demonstrate the applicability of it, through the use of the semantic web rule language (SWRL). Finally, we conclude by providing the reader with an overview of our findings.

2. Background

In this section, we provide the reader with a brief description of the SPIT phenomenon, together with some comments on ontologies and their applicability.

* Corresponding author. Tel.: +302105810116.
E-mail addresses: sdritsas@aueb.gr (S. Dritsas), vdritsou@aueb.gr (V. Dritsou), bts@aueb.gr (B. Tsoumas), panosc@aueb.gr (P. Constantopoulos), dgrit@aueb.gr (D. Gritzalis).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.10.004

2.1. SPIT phenomenon overview

VoIP is a technology that takes advantage of existing data networks and provides the establishment of voice sessions and sending voice as data packets over IP networks. Currently, VoIP implementations are usually based on the SIP, which tends to be the dominant underlying technology for providing services, such as IP telephony, instant messaging and presence [16]. SIP is an application layer protocol used to create, maintain, and terminate multimedia sessions. The basic SIP entities that support its functionality are: (a) user agents (UA), which act as communication end-points, and (b) SIP servers, which help and support the SIP sessions. Fig. 1 presents the basic operation model of SIP protocol including its main components.

The rapid adoption of VoIP technologies is expected to introduce new types of threats. Such a new threat is the SPIT phenomenon, which is defined as a set of bulk unsolicited voice calls or instant messages. Currently, three different types of VoIP SPAM types have been recognized, namely [17]: (a) *call SPIT*, which is bulk, unsolicited session initiation attempts to establish a multimedia session, (b) *instant message SPIT*, which is bulk, unsolicited instant messages, known as SPIM, and (c) *presence SPIT*, which is bulk, unsolicited presence requests, enabling a malicious user become a member of the address book of one or more users.

Nowadays, SPIT is not yet a major issue. However, it is expected to become soon attractive to malicious users ("spitters"), thus making the further growth of VoIP technology practically challenging. On the other hand, the anti-SPIT frameworks, which have been introduced so far, are often considered inadequate [13]. Also, the existing methods of defeating SPAM filtering, combined with the enhanced capabilities of spammers, may result in more complex and effective SPAM attack strategies, which could be really difficult to detect and fight. Moreover, the real-time nature of VoIP services, in contrast with the store-and-forward communication pattern of email technology, led us to consider that it is more efficient to handle SPIT in the signaling phase, where SIP protocol is applied, than to filter the payload of a session (i.e. the content of a call).[1]

Having the above in mind, we suggest that an efficient SPIT handling process involves three distinct steps (see Fig. 2), namely: (a) *prevention*, where specific actions are required, so as to impede a SPIT call or message to be transmitted and leave the callers' domain, (b) *detection*, where appropriate actions should be applied, in order to detect a SPIT call or message in the callee's domain, and (c) *reaction*, where appropriate actions for handling a SPIT attack (e.g. place the specific caller/sender to the domain's black list) should be used.

2.2. Ontologies and their applicability to the SPIT problem

An ontology is an explicit specification of a conceptualization, which can be used to describe structurally heterogeneous information sources, helping both people and machines to communicate in a concise manner [7]. Ontologies are discussed in the literature as a means to support knowledge sharing and reuse [4]. The reusability approach is based on the assumption that if a modeling scheme – i.e. ontology – is explicitly specified and mutually agreed upon by the parties involved, then it is possible to share, reuse, and extend knowledge.

An ontology is comprised by three major building blocks: concepts, relationships, and axioms. Concepts are abstract terms, which are typically organized in taxonomies. Hierarchical concepts are linked with an *"is-a"* relationship. Furthermore, concepts can have properties, which help in establishing relationships between either hierarchically classified or completely unrelated concepts. Axioms, which are expressed by integrity constraints, are rules that are valid in the modeled domain, finally constraining the possible (i.e. meaningful) interpretations for the defined concepts.

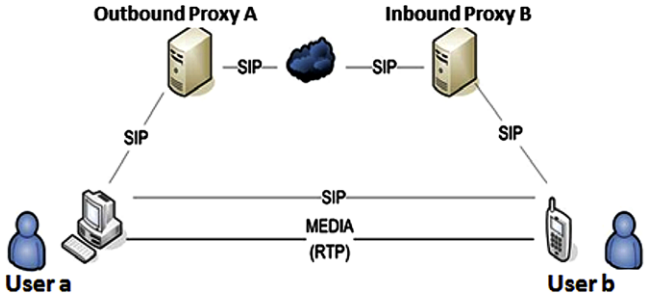

Fig. 1. SIP basic operation ("Trapezoid").

Due to their beneficial characteristics, ontologies have been used in several different domains, so as to provide information normalization and in cases where the scope is to represent the necessary knowledge of a specific domain [15]. For example, ontologies express the knowledge of experts on a specific domain explicitly, by supplying and analyzing all the necessary information. As this information is expressed by an explicit way, it can be well understood by both humans and machines, thus making the knowledge mutually comprehensible. This latter fact enables the reuse of the domain knowledge from different parties, thus avoiding the development of new ontologies from scratch. Ontologies can be used in any system, regardless of its architecture and technology given the semantics of the ontology are clearly defined. Moreover, decision-making logic can be embedded in a natural way via the use of ECA rules which can lead to implicit knowledge acquisition, thus enriching the ontology knowledge. Finally, the ontology paradigm follows the open world assumption (OWA), which makes it a perfect choice for simulating uncertain real-world scenarios where incomplete knowledge is present.

3. Related work

In this section, we will refer to some related work. Most of this work focuses on detecting email SPAM, and this is done for two main reasons. First, because email SPAM and SPIT have certain similarities (and differences, as well), therefore such a brief review makes sense for better understanding the situation in SPIT, and second because SPIT detection is dealt with in really few publications.

A system that uses an ontology to determine whether an email should be deleted or not is used in [19]. The approach takes as input a set of email messages and, based on predefined requirements, decides whether a message should be retained or not. The system is implemented using Protégé-2000 [14]. It identifies the special features of each message (expressed by a set of rules), which are then categorized by an underlying Bayesian classifier. Probabilities regarding the categorization of the messages are assigned to them, as well as for further training the system. A similar approach analyzes each incoming mail in order to identify its purpose [3]. This is accomplished by developing an ontology that classifies the messages in terms of the intended scope of the email sender (e.g. make a request, propose a meeting, etc.). The delivered messages are then compared to the existing classes of the ontology, so as to identify and categorize them.

[1] It is theoretically possible to filter the payload of a session (i.e. the RTP traffic), but this requires devices with high computational resources, so as to realize the real-time nature of VoIP communications. In this paper, we deal with the signaling phase of a SIP-based VoIP session.