available at www.sciencedirect.com

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Clustering NGN user behavior for anomaly detection

Claudio Mazzariello [a,*], Paolo De Lutiis [b], Dario Lombardo [b]

[a] Computers and Systems Engineering Department, Federico II University of Napoli, via Claudio 21, 80125 Napoli, Italy
[b] Security Innovation, Telecom Italia S.p.A., via Reiss Romoli 274, Torino 10148, Italy

Keywords:
User behavior modeling
User behavior monitoring
NGN security

ABSTRACT

In the vision of both researchers and standardization committees, networks and services will evolve in the direction of increasing pervasiveness, convergence, and quality of service management capability. Consequently, users will gain an increasing dependency on the presence and availability of network connectivity and the huge plethora of provided services. Yet fostering the development of our society, such dependency on a relatively young technology poses serious threats, especially from the trustworthiness, security and privacy point of view. In this paper, we will describe and critically evaluate user behavior clustering aimed at monitoring and assuring the security of NGN-based applications. Different models of user behavior, developed within both ISP and academic research projects will be described, and several techniques for manipulating and exploiting such model for the anomaly detection purpose will be described and evaluated.

1. Introduction

Computer Networks were originally thought of as a technology aimed at solving the interconnection problems of a small amount of very specialized groups of people, for very specific purposes. Through the years, networks have become widely used, for a high number of heavily differentiated purposes, by a very large number of people. The evolution of both network technology and hardware is the root cause of an increasing availability of cheap, heterogeneous, yet computationally powerful terminals, able to exploit the everincreasing connection speed provided by ISPs. These technological factors, alongside with a developing familiarity of people in using networked services, have fostered the pervasiveness of connectivity and allowed the increase in number and type of such services, thus encouraging the development of novel communication paradigms, sometimes mimicking, sometimes influencing human communication and interaction patterns. Modern services exploiting networking are developing in the direction of an increasing *social* connotation of their nature (Katz and Rice, 2002). As a consequence, human interactions have become more and more dependent on the existence of a networking *infrastructure*, instantly and constantly interconnecting people. Thereby, network connectivity is nowadays considered an asset as crucial and critical, as water and electricity provisioning.

The diffusion of networks as a fundamental technology, and the cheaper and cheaper availability of connectivity, have been the enablers for the convergence of services which were traditionally based on different technological platforms. IP based infrastructures are often chosen as the transport media for services like telephony or television and radio broadcasting, traditionally characterized by the presence of ad-hoc infrastructures. Furthermore, such infrastructures are typically different in different geographical areas, and need considerable standardization efforts and bi-lateral agreements in order to be able to cooperate. Hence, the transition to a single infrastructure, based on well established yet flexible design, results in several benefits both for service providers and end users. From the operators' point of view, in fact, a heavy reduction of costs

* *Corresponding author.*
E-mail addresses: Claudio.Mazzariello@UniNA.it (C. Mazzariello), Paolo.DeLutiis@TelecomItalia.it (P. De Lutiis), DarioLombardo@TelecomItalia.it (D. Lombardo).
1363-4127/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.10.011

is motivating investments, coupled with the undoubtable simplification in managing and operating the communication infrastructure; from the end-users' point of view, instead, service quality and usability improve, together with an increase in the number of available services.

The next step envisioned in the evolution of networks and services is the development of the so called Next Generation Network, as defined by ITU-T (NGN working definition by ITU-T), promoting the usage of packet switched networks as a transport media for both services born and developed in such environment, and services typically hosted on circuit switched media. The inherent resilience and flexibility of packet switched networks, indeed, needs to be complemented by the guaranteed quality of service and availability typical of circuit switched networks, in order to overcome the issues arresting the development of the encouraged convergence, due to dissimilarity in offered service primitives. Therefore, study and research in this area are focused on the definition of technologies and protocols aimed at transporting many of the desirable properties of circuit switched networks within packet switched networks, still retaining the latter's interesting properties (Moyer and Umar, 2001). Even though clever strategical planning and technological development can make the transition seamless for end users, which are not, and don't need to be, bothered by technical issues, the social implications of moving well established services to packet switched networks can generate a plethora of issues which have not been critical so far, but may become such in the near future. End users, and consequently service providers, will be forced to cope with problems which are common in packet switched networks, and could become crucial for the successful deployment of convergent services.

This paper will discuss the social implications tightly related to current networks' and networked services' evolution patterns. Starting from this analysis, in Section 2 we will point out the main security threats related to the increasing reliance on network technologies, and the subsequent increasing usage of network resources and provided services by end users. The analysis will be carried out from both the telecommunication operator's and the end-users' point of view. As an outcome of the more in-depth analysis, we will focus on some classes of misuse, and anomalous or unwanted behavior. This will lead to the definition, in Section 3 of a model of user behavior and user interaction and interconnection patterns. Such a model will be defined in terms of features describing the current status of the network and the provided service. The obtained data will be analyzed by means of detection algorithms, discussed in Section 4. Based on past trend information and measures of conformism, users and issued calls will be grouped into clusters of instances, each containing those users sharing a common behavior, as described in Section 5. Those users which will exhibit an utterly non conventional behavior, or abrupt changes with respect to their past behavior, will raise an alert triggering further action or demanding action by the network security administrator. Conclusions will be drawn in Section 6.

2. Threats for NGN

Security has always been an issue in networks, since many of its communication mechanisms were designed without security in mind. This is not actually a design flaw, since at its origins, the idea of networking was mainly applied to small communities of scientists or military, deliberately willing to make their computational facilities remotely available, and to quickly distribute information about their scientific results, or willing to implement a communication infrastructure resilient to external threats. Many of the security-related issues only emerged when the internet became popular in large communities of users, thus totally removing the implicit reciprocal trust the previously small community of users used to share.

Conversely, traditional telecommunication services evolved dramatically, and became an important part of peoples' lives. In fact, while telephone and TV/radio broadcasting systems have been around for decades, the real breakout of the Internet as a planetary social media can be dated back to the 90's. Those we are referring to as traditional telecommunication services are accepted as a reality, have overcome in most cases the digital divide, and are widely and seamlessly used by people of all ages, as well as cultural and economic extraction. Hence, such systems still retain, and have undergone an increase in, the trust level among groups of users, and between users and service providers.

The diffusion of network connectivity and networked services in user communities which are untrusted and neither homogeneous nor uniform, together with the little attention paid to security issues until they became seriously incumbent, has paved the way to the emergence of numerous security-related threats. Such threats are nowadays an increasingly dangerous plague which is often hard to fight, since it exploits the peculiarities which contributed to make network-provided services popular, such as network flexibility and capillarity, its loose distributed control and management structure, and its inherently public nature.

The transition from dedicated and well tested architectures will expose users of traditional services to threats which are quite common in the networking world (Zar, 2005), such as interception, eavesdropping and Denial of Service, whereas the lack of trustworthy infrastructure and basic connectivity services will enable the development of novel attack strategies, specifically targeting the weak links in the chain of components and functionality allowing to operate converged services. Furthermore, attackers' motivation has evolved as well, changing curious script kiddies in cyber criminals. Nowadays, in fact, many attack strategies involve the deployment and exploitation of world-wide distributed networks of infected computers, named botnets (Nassar et al., 2009), which can be coordinated in order to perform complex cooperative attacks.

As to this paper, we will mainly focus on one specific operational environment, carrying out a detailed analysis of our studies and practice on Telecom Italia's VoIP infrastructure and service. Within this framework, we will cite some of the most popular threats, and describe their impact, trying to generalize high level conclusion to the whole NGN scenario.

Voice over IP systems which are currently being deployed on a large scale by telecommunication operators can be used as a good representative example of what a typical future internet application looks like, how it will have deep social implications, and how such implications will result in the genesis of specifically suited attacks. The social characteristic of the telephone system allows for the definition of novel