A Framework for Secure and Verifiable Logging in Public Communication Networks

Vassilios Stathopoulos[1,*], Panayiotis Kotzanikolaou[1,⋆], and Emmanouil Magkos[2]

[1] Authority for the Assurance of Communications Security and Privacy (ADAE)
3 Ierou Lochou str., 15124 Maroussi, Greece
{v.stathopoulos,p.kotzanikolaou}@adae.gr
[2] Ionian University, Department of Informatics,
Palaia Anaktora, 49100, Corfu, Greece
emagos@ionio.gr

Abstract. In this paper we are focusing on secure logging for public network providers. We review existing security threat models against system logging and we extend these to a new threat model especially suited in the environment of telecommunication network providers. We also propose a framework for secure logging in public communication networks as well as realistic implementations designs, which are more resilient to the identified security threats. A key role to the proposed framework is given to an independent Regulatory Authority, which is responsible to verify the integrity of the log files.

1 Introduction

Public network providers, (fixed, mobile telephony and Internet Providers) consider privacy in communication as a valuable asset. Indeed, attacks against the confidentiality of communications and the privacy of their customers may lead to severe consequences of commercial and legal nature. In many countries Regulatory Authorities (*RA*s) are responsible to regulate and audit the security level of public network providers, in order to preserve communications security and privacy for the citizens.

Although a lot of security measures are in place in telecommunication networks and well defined standards exist there are still security holes. Threats such as external intrusion, communication interception, unauthorized access to private data (*e.g.* CDR files) and abuse of privileges by insiders must be considered. Existing vulnerabilities such as overestimation of security measures, non conformance with security measures and lack of dependable and secure logging and auditing mechanisms increase the security risks. Since it is not always possible to prevent security breaches, it is required to have in place adequate detective security measures.

* Research supported by the Hellenic Authority for the Assurance of Communications Security and Privacy (ADAE) – http://www.adae.gr

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 273–284, 2006.

System logging is the most important detective security measure. Log files are maintained in almost every system and they are usually examined during security audits, either external or internal. Indeed, during regular security audits, log files may be examined and correlated, in order to assure that the intended technical measures are in place and that the security policies and procedures are implemented. During non-scheduled security audits, *e.g.* as a response to a security incident, log files are analyzed in order to discover the cause of the incident, such as lack of security measures, non conformance with security procedures, system miss-configuration etc.

In this paper we are focusing on secure logging for public network providers. We review existing security threat models against system logging and we extend these to a new threat model especially suited in the environment of telecommunication network providers. We also propose a framework for secure logging in public communication networks as well as realistic implementations designs, which are more resilient to the identified security threats. A key role to the proposed framework is given to an independent Regulatory Authority. Each provider is responsible to send integrity proofs of its log files to the Regulatory Authority, which in turn is responsible to to remotely store the integrity proofs and verify the integrity of the log files.

Our paper is motivated from the recently announced interception case in a mobile telecommunications provider in Greece (see for example [1]). As the Greek authorities and the provider itself revealed, part of the core network of the provider was compromised by some unknown trojan-like program. According to published information, the malicious software infected the core network. Then, it activated the Lawful Interception (LI) component in the infected elements, which is by default installed in inactive mode, and made possible the call interception of several subscribers.[1] The malicious program turned off several logging procedures in order not to alarm about its presence or the fact that the LI component had been activated. The underestimation of several security threats and vulnerabilities regarding logging procedures and mechanisms, did not allow the immediate detection of the incident.

The rest of this paper is organized as follows. In Section 2 we review the related work in secure logging. In Section 3 we describe our threat model for secure logging in telecommunication networks in comparison with existing threat models. In Section 4 we describe the proposed framework for secure logging which deals with the identified threats. Finally, Section 5 concludes this paper.

2 Related Work

In *real logging systems*, the security of logging and auditing procedures is usually relied on the assumption that the host's Operating System is not corrupted. Secure systems aim at improving the robustness of the logging system itself without relying on the security features of the underlying system. The *Syslog-sign*

[1] The announced list of the victims included among others the Prime Minister, Ministers and Ex-Ministers.