Chapter 12

A Pervasive Polling Secret–Sharing Based Access Control Protocol for Sensitive Information

Juan Álvaro Muñoz Naranjo
Universidad de Almería, Spain

Justo Peralta López
Universidad de Almería, Spain

Juan Antonio López Ramos
Universidad de Almería, Spain

ABSTRACT

This chapter presents a novel access control mechanism for sensitive information which requires permission from different entities or persons to be accessed. The mechanism consists of a file structure and a protocol which extend the features of the OpenPGP Message Format standard by using secret sharing techniques. Several authors are allowed to work in the same file, while access is blocked for not authorized users. Access control rules can be set indicating the minimum number of authors that need to be gathered together in order to open the file. Furthermore, these rules can be different for each section of the document, allowing collaborative work. Non-repudiation and authentication are achieved by means of a shared signature. The scheme's features are best appreciated when using it in a mobile scenario. Deployment in such an environment is easy and straight.

DOI: 10.4018/978-1-60960-042-6.ch012

INTRODUCTION

Protection of sensitive information is an ever-present concern which is gaining more and more attention as digitalization of information and use of Internet increase. Numerous privacy protocols, standards and applications exist in order to keep information away from unauthorized persons, as well as to authenticate its author. Most of them regard privacy while information is being transmitted through the web and provide authentication (OpenSSH) (Dierks&Rescorla, 2008) (Atkinson, 1995) (Kohl, 1989) (Paterson &Yau, 2006). GnuPG (GnuPG) and PGP (PGP) applications also protect information while stored in a device. Both implement the OpenPGP Message Format standard (Callas, Donnerhacke, Finney, Shaw, & Thayer, 2007).

Those protocols and applications usually work on an individual basis, that is, a single user manages the privacy of its own information. Some examples are: communicating in a private and/or authenticated way with a Web server, protecting personal information and keeping a private and/or authenticated email conversation.

Some scenarios may require, in addition to protection and authentication of information, some kind of access control measures. That is the case of governmental classified documents (defense, foreign affairs, historical, etc.) or high-value information in private companies. Controlling the access to this kind of documents is critical, and may require the approval of third-party entities or individuals, or even a set of them. Security restrictions will be even higher when modifying the classified information.

On a different matter, advances in smart devices and connectivity have given us the chance to access Internet from almost anywhere and at any time. Internet access is no longer confined to static devices that cannot be taken with us. Now that the technology already exists, it is time to develop new mechanisms and applications that take advantage of it.

Having all this in mind we have designed a polling-based file access control mechanism that is presented in this chapter. This mechanism includes an extension of the OpenPGP Message Format and a protocol: access to the file is granted only under the approval of a minimum number of authorized users, and modifications are signed for authenticity and integrity verification. The first feature is achieved by using secret sharing techniques; the later by using a shared signature.

Section Background explains and discusses some technologies that keep some similarity, along with the OpenPGP Message Format, the secret sharing techniques and the shared signature. Section Our Proposal introduces our scheme with some mobility and security considerations, and finally the last section shows the conclusions of the chapter.

BACKGROUND

Alike Technologies: Publish/Subscribe Systems and Version Control Systems

There are two technologies that keep some relation to the one proposed here. They are (1) publish/subscribe systems and (2) version control systems.

State-of-the-art publish/subscribe systems consist of an infrastructure that provides communication capabilities for large-scale, wide-area distributed systems. They nicely fit multi-domain, heterogeneous environments. The communication pattern is based on a per-event, asynchronous basis, either one-to-many or many-to-many, depending on the scenario. Such a system is presented in (Pietzuch & Bacon, 2002), along with a wider bibliographic review. A typical case-of-use appears in (Pesonen, Eyers, & Bacon, 2007): a multi-domain network that handles car plate recognition for fee-charging purposes in the London metropolitan area. Additionally, several works and proposals have been presented in order to cover