Research Article

International Journal of Advanced Computer Research, Vol 6(23)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.623028

How to secure web servers by the intrusion prevention system (IPS)?

Yousef Farhaoui*
Faculty of sciences and Techniques, Moulay Ismail University, Errachidia, Morocco

Received: 17-February-2016; Revised: 26-March-2016; Accepted: 28-March-2016

Abstract
Information technology and especially the Internet are playing an increasing role in our society. Approaches by signature show limits on intrusion detection/attacks by the fact that most web vulnerabilities are specifically for specific applications may be developed in-house by companies. Behavioral methods are therefore an interesting approach in this area. An IPS (Intrusion Prevention System) is a tool that is used to enhance the security level. We present here the secure IPS architecture web server. We will also discuss measures that define the effectiveness of our IPS and very recent work of standardization and homogenization of our IPS platform. The approach relies on preventive mechanisms: it is then to develop devices capable of preventing any action that would result in a violation of the security policy. However, experience and results show that it is impossible to build a fully secure system for technical or practical reasons.

Keywords
Intrusion prevention, Web server, Architectures, Security.

1.Introduction
Information technology and especially the Internet are playing an increasing role in our society. Many critical applications from the point of view of their safety are deployed in various fields such as military, e-commerce, etc. The security of computer systems becomes a key issue both for individuals and for businesses or states.

Each computer system, a security policy must be defined to ensure the security properties that have to be made by the latter. This policy is expressed in rules governing six distinct objectives:

- Integrity: It aims to ensure that the data cannot be affected.
- Confidentiality: It is supposed to assure that the people alone are authorized can have access to resources exchanged.
- Availability: It allows keeping the good work of the information system.
- Non-repudiation: It allows ensuring that the transaction cannot be denied.
- Authentication: It consists in ensuring that only authorized people can have access to resources.
- Access Control: It means that the user access to information in a computer is restricted and controlled.

In this article we mean by the intrusion, a violation of one of the six goals. Several approaches have been developed to ensure that the defined security policy for a computer system is well respected. It can indeed be circumvented by a malicious user or simply a design fault may be the cause of a violation thereof. The first approach relies on preventive mechanisms: it is then to develop devices capable of preventing any action that would result in a violation of the security policy. However, experience shows that it is impossible to build a fully secure system for technical or practical reasons. It is also very difficult to develop complex software free of design errors, some of which can be exploited to produce a breach of the security policy [1] [2].

Accepting this, a second approach for dealing with intrusions is to detect violations of security policy and report to administrators so they can take the necessary steps to remedy any problems that could generate such violations. Intrusion detection is based on analysis on the fly or delayed from what is happening on the system. A third approach, tolerance to intrusion, is to ensure that the service remains assured and Security Policy of the overall system remains inviolate even in the presence of intrusions in certain system components. The intrusion can affect certain components of the system, but privacy properties, integrity and availability of the overall system must be checked.

*Author for correspondence