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

The work we present in this paper are part of essential way in the field of intrusion detection and enable more some tolerance to intrusion [3].

In intrusion detection, two approaches are used primarily: the signature approach (misuse detection) and the behavioral approach (anomaly detection) [27] [28].

2.Methods intrusion detection

The approach is to define signing of attack scenarios and look for traces of these scenarios, for example in the system audit files. This approach poses problems, including that of detecting new attacks (which requires the update of the base of extremely common way signatures) or that of detecting unknown attacks.

The basic principle of the behavioral approach is to build a reference model the behavior of the supervised entity (user, machine, service and application) to which we can compare the observed behavior. If it is too far from the reference, a warning is issued to indicate the anomaly. Conventional techniques based on the behavioral approach propose a reference model constructed explicitly. However, it is not easy to define what is representative of the behavior modeling and intrusion prevention systems (IPS) based on this method generates a large number of false alarms. The major advantage of the behavioral approach in relation to the signature approach is not to try to characterize intrusions, but the expected behavior of the system and therefore is able to detect unknown intrusions.

In general, IPS based on this approach are reliable as an intrusion often generates an anomaly in the observed behavior. It remains an open question, as noted by Myers [1] and Anderson [2] and as shown by the recent developments in the field of mimicry attacks [3] [4]. For cons, the IPS is generally irrelevant. There are relatively few behavioral IPS performance studies in terms of false positives: Helman and Liepins [5] studying both theoretical performance of statistical models and practices of a simple statistical detector and W & S. [6] This study shows that the results of the IPS are far from the objectives set by DARPA: detection rate of 99% for a false positive rate below 0.1% [7].

In addition, the learning curve has some problems: make sure that the learning base is free from intrusions. Otherwise, the IDS could learn intrusive behavior and would therefore not be able to detect them later. The behavior of the supervised entity may also change over time, it is possible to change the profile continuously during the detection phase in the latter still represents as closely as possible the behavior of the entity. In this case, the system can gradually learn intrusive behavior introduced by an attacker.

In this article, we chose a different approach to those proposed in the work by detecting behavioral intrusion by deciding not to build the express normal behavior pattern but using several software components in parallel. The behavior of each software is considered normal behavior model for other programs: one speaks of implicit model.
This model is, obviously, because incorrect software components contain vulnerabilities. To limit the number of false positive, you have this model to be as complete as possible.

To test intrusion detection methods we have proposed, we decided to develop an IPS for web servers. In the next section, we present the specific previous work in intrusion detection for web servers regardless of their approach.

3.Intrusion detection web

Web servers are an interesting test environment for intrusion detection, firstly, by their importance and universality of HTTP [8] (Hypertext Transfer Protocol) and, secondly, by the number the striking vulnerabilities. Web servers are the showcase of businesses, associations, states or individuals via blogs on the Internet. They are, in some cases, a source of significant revenue. More and more web applications are deployed on the Internet: medical applications, e-commerce, virtual offices, mapping services, social networks, payment services, administrative services (including payment of taxes), etc.

These servers and the applications running on them are accessible from the outside and can have vulnerabilities. The servers have far less vulnerability than a few years; developers have recognized the importance of security. This is, by cons, not yet the case for web applications: from Robertson et al. [9] 25% of the entries CVE (Common Vulnerabilities and Exposures) from 1999 to 2005 are related to web vulnerabilities; moreover, this figure does not take into account all the applications developed in-house, in different companies, to meet special needs. Hackers try to take advantage of these vulnerabilities to install fake sites in order to phishing (phishing) or to install malware that will infect visitors to the site [10]. The

security of web servers and applications running on these servers is a priority for both the entity represented by the server for visitors to these servers.

Intrusion detection tools "generic" can be used to detect intrusions against web servers: NIPS as Bro [11] NSM [12], [13] (Network Security Monitor) or Snort [14] or Host-based IPS that monitor the behavior of programs such as those developed by Forrest et al. [15] [16] and Ghosh [17] for example.
Although this IPS have not been specifically evaluated in the field of intrusion detection web, the web remains a chosen field of intrusion detection, including the IPS network level: In version 2.3.3 Snort signatures in 1064 in 3111 are devoted to the detection of web attacks. The intrusion detection tools to detect attacks against web servers primarily use a scenario approach that behavioral approaches have emerged recently.

A. Discussion

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. The first behavioral IPS [18], [19] offered only took into account that the first line of the HTTP request, the only one present in the audit and file servers are not able to detect the attacks that will influence this part of the query. More recent approaches take into account the semantic queries by performing a lexical analysis of the protocol [20], [21]. These tools seem to get better results. [22] Our approach is distinguished by taking into account the behavior of web servers and not only the characteristics of the application and seek to detect anomalies in the behavior of servers to identify intrusions, with the aim to differentiate the intrusion of possible attacks or abnormal requests.

4.Error detection

Our intrusion detection approach is based on a technique from the field of dependability: the functional diversification. In this section, we define the basic concepts of dependability and the various ways of ensuring the IT security properties.

The end of this section is devoted to the analysis of concepts in the field of security in the area of operational safety.

A. The model error-error–failure

The definitions are from the guide dependability. [23] The dependability of a computer system is the property that allows users to place a justified confidence in the service it delivers to them. A user is not necessarily a human being but may well be another system that interacts with the service in question. The service provided by the system is the behavior perceived by users. The security of a system can be analyzed according to different properties called attributes:

- Being ready for use leads to availability;
- Continuity of service leads to reliability;
- The non-occurrence of catastrophic consequences for the environment led to the security-safety;
- The non-occurrence of unauthorized disclosures of information leads to confidentiality;
- The non-occurrence of inappropriate alterations of information leads to integrity;
- The ability to repair and changes leads to maintainability.

The association, confidentiality, integrity and vis-à-vis availability of authorized shares, led to the security-privacy. Safety as we understand it, that is to say, the security-privacy part of the security operation is an integral part of the field of operational safety.
In a given system, it is considered that these properties can be defaulted by barriers within the system. These barriers are of three types:

- Failures that occur when the service delivered deviates from fulfilling the function of the system;
- Errors are the parts of the system status could cause failures;
- Faults cause awarded or supposed mistakes.

These barriers form a logical causal chain: one mistake can result in an error, which can itself cause a failure. Also, this string is recursive, and an external failure of a component, can cause an internal fault in the component, which can itself cause an error, etc.

The faults can be classified according to five criteria: phenomenological their cause, their nature, their creation phase or occurrence, location relative to system boundaries, and persistence. We distinguish because of their phenomenological: physical faults and mistakes caused by humans. Depending on the nature of the faults, there are: accidental mistakes and intentional misconduct. Their creation phase or occurrence, faults development and operational faults. Depending on the situation of misconduct in relation

to the system borders: internal faults and external faults. Next persistence: permanent faults and temporary faults.
Although we can detect physical faults through functional diversification, as part of our work, we focus on the mistakes caused by humans. These can be divided into four classes of combined faults:

- The faults of design, which are accidental or intentional misconduct development without malicious intent;
- The faults of interaction, which are external, accidental or intentional misconduct without malicious intent;
- Malignant logic (worm, virus, logic bomb, backdoor, horse Troy) that are intentionally harmful internal faults;
- Intrusions which are intentionally harmful external operational faults.

A fault is active when an error. An active fault is an internal fault that was previously dormant and has been activated by the treatment process, an external fault. An internal fault can cycle through its states dormant and active. An error may be latent or detected; an error is latent until it has been recognized as such; an error is detected by an algorithm or a detection mechanism. An error may disappear without being detected. For propagation, an error creates new errors. A failure occurs when, for propagation, an error affecting the service provided by the system. This failure can appear to be a mistake from the point of view of another component. This yields the following fundamental channel:

…. → failure → fault → error → ….

The arrows on this string expressing the causal relationship between faults, mistakes and failures. They should not be interpreted narrowly: by spreading more errors can be created before a failure occurs. The means to ensure that the attributes of dependability are present and maintained within the system are classified into four areas:

- Fault prevention: how to prevent the occurrence or introduction of faults;
- Fault tolerance: how to provide a service capable of fulfilling the function of the system in the presence of faults;
- Elimination of mistakes: how to reduce the presence of faults;
- Forecasting mistakes: how to estimate the presence, creation and the consequences of mistakes.

These means are complementary and dependent and must be used in combination. We will focus on the remainder of this section to the various fault tolerance techniques and especially to a particular technique: functional diversification.

B. Fault tolerance

Fault tolerance is implemented by processing errors and processing errors. The error handling is designed to eliminate errors, preferably before a failure occurs. The lack of treatment is to prevent or mistakes that are activated again.

The error processing uses three types of primitives:

– Error detection to identify an erroneous state;
– The error diagnosis to estimate the damage caused by the error that was detected and the error eventually propagated before detection;
– The error recovery allows to substitute an error-free state in the wrong state, this substitution may take three forms:
  - The recovery that replaces current state a previously saved state at a checkpoint;
  - Pursuit, which is a state from which the system can operate;
  - The error compensation that builds an error-free state for just a sufficient level of redundancy was introduced in the application.

The treatment of errors, in turn, can be divided into three stages: diagnosis of faults of determining causes of errors, passivation mistakes that can prevent a new activation of faults, and reconfiguration, which aims to change the state of the system for it to continue to deliver a service, even degraded. The error compensation can be applied systematically, even in the absence of error, while providing a fault masking (e.g. by majority vote). The error detection is not so strictly speaking necessary to effect recovery; However, to avoid a reduction in uncollected redundancy available when a component fails, implementations masking practices generally include error detection, which in this case can be performed after recovery. Our works are part of the error detection and error compensation. We seek to detect system status where a violation of the security policy has taken place and we are trying to hide this condition from the outside through component redundancy.

5.Architecture of a network with IPS

The control strategy is to determine how to manage multiple probes of the same IPS, or how to manage

multiple IDS in a network. Depending on the layout of the various components of IPS, several architectures can be adopted:

A.Centralized architecture

Some provision will control all events from a central console, analyze, and decide what action to take. Different models of IPS can be used in the same network at different strategic points in order to gather information from different IDS and treat it at a central point.

B.Partially distributed architecture

This arrangement allows the server to discharge all tasks. A hierarchy is established. Each sub network is managed by local point. Measures are taken from the console of the level above.

C.Fully distributed architecture

In this case, the network is divided into several sub-networks, each one is managed by its own IPS. The tasks of audit and analyzes are made at the local level.

6.Evaluation of an IPS

Many measures are used to compare and measure the effectiveness of IPS. IPS are very important components in security policy; Then, the choice of the IPS is very crucial and must be based on the IPS characteristics. In [27] [28] [29], we can evaluate the IPS based on several criteria such as:

- The rate of false positive and false negative.
- Response of the IPS in an overloaded environment.
- The possibility to update the signature database or modify certain signatures.

7.Standardization

Several IPS consist of a single block that handles the entire analysis. This imposed monolithic approach has considerable constraints such as [24]:

- The consumption of system resources.
- Difficulty of updating.
- The central point is a weakness if an attack is launched against the IPS.
- Need of many audit data.

To overcome these weaknesses, new trends in the design of IPS exist. Current trends are towards distributed intrusion detection. The first project, which used this approach of gathering of audit information was the NADIR project, it analyses by an expert system [25]. A standard model for IPS established by the DARPA committee. This model is adopted in the development of the Majority of new current IPS. This model is composed of four blocks: the source of information, the sensor, the analyzer and manager. For effective intrusion detection, it is important to show the characteristics required of any IPS, [27] [28]: the distributive property, autonomy, communication and cooperation, responsiveness and adaptability.

8.Discussion of results

The study of intrusion detection systems has allowed us to realize the importance of the role played by IPS (HIPS (Host Intrusion Prevention System), NIPS (Network Intrusion Prevention System)) in security policy. The characteristics of the IPS must meet certain requirements; the choice should be based primarily on the needs and security hardware and software constraints. According to [29] type of IPS can be determined:

- The location of the IPS.
- The frequency of use.
- The detection method.
- The response of the IPS.

Figure 1 shows the global solution diagram.

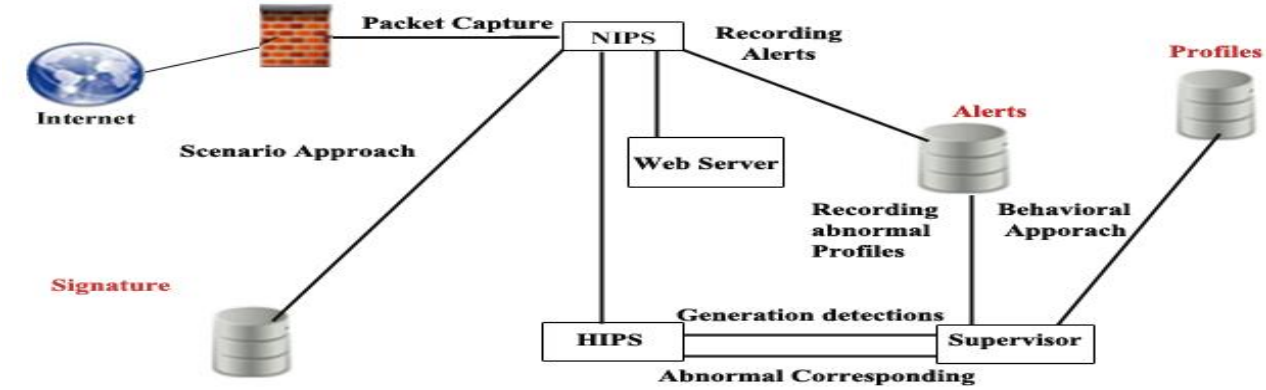

Figure 1 Global solution diagram

According to our model, the use of databases is very important, we will use three databases:

a. Profiles database: contains all information relating to user profiles. The data are generated by the HIPS during the learning phase.
b. Signatures database: It includes all known attacks using a certain format. There is no standard model for coding signatures. The attributes which will be used to represent an attack, must be based on information contained in the packets [26].
c. Alerts database: can list all the alerts generated by the sensors of the two components of the IPS. This database will be accessed by the administrator to identify traces of attacks or abnormal behavior [28].

9.Results

The experimental results of our solution are the following:

Table 1 Experimental results

	Number of False Positive	**Number of False Negative**
Our solution IPS	short	short
Snort (IPS)	long	long

Table 1 shows a count of the number of false positive and Number of false negative. 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 [27]. So our IPS platform is able to detect and prevention of attacks and also reduced the number of false positive and false negative by many at the other IPS. 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 shows that it is impossible to build a fully secure system for technical or practical reasons [28].

10.Conclusion

The choice of the implementation of an IPS is very important, especially when the IPS will be deployed on a network with multiple machines with different hardware and software configurations. Then, the IPS is designed in a hierarchical manner and is distributed on several machines requiring the analysis of data from different sources. So we designed a hybrid IPS (NIPS + HIPS), analyzing the two sources of information and using both immune theories. Tests on our solution aimed to define the contribution of immune systems for intrusion detection. The use of clonal theory can generate from an attack signature more detectors can recognize not only the attack in question, but also variants of this attack, or further similar attacks. However, the use of the theory of negative selection in the case of analysis with a behavioral approach to detect any abnormal behavior and which is different from the typical behavior of the user. Our future work will focus on the development of a new and safe method for strengthening authentication at IPS.

Acknowledgment

None.

Conflicts of interest

The author has no conflicts of interest to declare.

References

[1] Myers PA. Subversion: the neglected aspect of computer security. Naval Postgraduate School, Monterey CA; 1980.
[2] Anderson JP. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania; 1980.
[3] Tan KM, Killourhy KS, Maxion RA. Undermining an anomaly-based intrusion detection system using common exploits. In recent advances in intrusion detection 2002 (pp. 54-73). Springer Berlin Heidelberg.
[4] Wagner D, Soto P. Mimicry attacks on host-based intrusion detection systems. In proceedings of the 9th ACM conference on computer and communications security 2002 (pp. 255-64). ACM.
[5] Helman P, Liepins G. Statistical foundations of audit trail analysis for the detection of computer misuse. IEEE Transactions on Software Engineering. 1993;19(9):886-901.
[6] Vaccaro HS, Liepins GE. Detection of anomalous computer session activity. In IEEE symposium on security and privacy 1989 (pp. 280-9). IEEE.
[7] McHugh J. Intrusion and intrusion detection. International Journal of Information Security. 2001;1(1):14-35.
[8] Fielding R, Gettys J, Mogul J, Frystyk H, Masinter L, Leach P, et al. Hypertext transfer protocol--HTTP/1.1. 1999.
[9] Robertson W, Vigna G, Kruegel C, Kemmerer RA. Using generalization and characterization techniques in the anomaly-based detection of web attacks. NDSS 2006.
[10] Mavrommatis NP, Monrose MA. All your iframes point to us. In USENIX security symposium 2008 (pp. 1-16).
[11] Paxson V. Bro: a system for detecting network intruders in real-time. Computer Networks. 1999 ;31(23):2435-63.

[12] Heberlein LT, Dias GV, Levitt KN, Mukherjee B, Wood J, Wolber D. A network security monitor. In IEEE computer society symposium on research in security and privacy 1990 (pp. 296-304). IEEE.
[13] Mukherjee B, Heberlein LT, Levitt KN. Network intrusion detection. Network, IEEE. 1994; 8(3):26-41.
[14] Roesch M. Snort: lightweight intrusion detection for networks. In LISA 1999; 99 (1): 229-38.
[15] Forrest S, Hofmeyr SA, Somayaji A, Longstaff TA. A sense of self for unix processes. In IEEE symposium on security and privacy 1996 (pp. 120-8). IEEE.
[16] Warrender C, Forrest S, Pearlmutter B. Detecting intrusions using system calls: alternative data models. In IEEE symposium on security and privacy 1999 (pp. 133-45).
[17] Ghosh AK, Michael C, Schatz M. A real-time intrusion detection system based on learning program behavior. In recent advances in intrusion detection 2000 (pp. 93-109). Springer Berlin Heidelberg.
[18] Kruegel C, Vigna G. Anomaly detection of web-based attacks. In proceedings of the 10th ACM conference on computer and communications security 2003 (pp. 251-61). ACM.
[19] Tombini E, Debar H, Mé L, Ducassé M. A serial combination of anomaly and misuse IDSes applied to HTTP traffic. In 20th annual computer security applications conference 2004 (pp. 428-37). IEEE.
[20] Estévez-Tapiador JM, García-Teodoro P, Díaz-Verdejo JE. Measuring normality in http traffic for anomaly-based intrusion detection. Computer Networks.2004; 45 (2): 175-93.
[21] Ingham KL, Somayaji A, Burge J, Forrest S. Learning DFA representations of HTTP for protecting web applications. Computer Networks. 2007;51(5):1239-55.
[22] Ingham KL, Inoue H. Comparing anomaly detection techniques for HTTP. In recent advances in intrusion detection 2007 (pp. 42-62). Springer Berlin Heidelberg.
[23] http://webhost.laas.fr/TSF/LIS/Guide.html. Accessed 20 Novmber 2015.
[24] Zissman M. DARPA Intrusion Detection Evaluation Datasets.1999.
[25] Boudaoud K. Un système multi-agents pour la détection d'intrusions. Proceedings of the Journées Doctorales Informatique et Réseaux (JDIR). 2000.
[26] Hochberg J, Jackson K, Stallings C, McClary JF, DuBois D, Ford J. NADIR: an automated system for detecting network intrusion and misuse. Computers & Security. 1993 ;12(3):235-48.
[27] Farhaoui Y, Asimi A. Performance method of assessment of the intrusion detection and prevention systems. International Journal of Engineering Science and Technology. 2011;3(7);5916-28.
[28] Farhaoui Y, Asimi A. Performance Assessment of Tools of the Intrusion Detection/Prevention Systems. International Journal of Computer Science and Information Security. 2012;10(1):7-13.
[29] Farhaoui Y, Asimi A. Performance assessment of the intrusion detection and prevention systems: according to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance. In 6th IEEE international conference sciences of electronics technologies information and telecommunication (SETIT), Sousse, Tunisia 2011.

Dr. Yousef Farhaoui is an professor, Department of Computer Science in Faculty of Sciences and Techniques, Moulay Ismail University, Morocco.He received his PhD degree in computer security from the University IBN Zohr. His research interest includes computer security, Data Mining, Data Warehousing, Data Fusion etc.
Email: Youseffarhaoui@gmail.com