PROPOSING A REAL TIME INTERNAL INTRUSION DETECTION SYSTEM TOWARDS A SECURED DEVELOPMENT OF E-GOVERNMENT WEB SITE

Al-Khanjari, Z.
Alanee, A.
Kraiem, N.
Jamoussi, Y.
Department of Computer Science, College of Science,
Sultan Qaboos University, Muscat, Oman

Abstract

As society becomes more and more reliant on software systems for its smooth functioning, software security is emerging as an important concern to many researchers in the field of Computer Science. We describe a prototype implementation based on the internal sensors to perform internal intrusion detection in e-Government website. The internal sensors consist of code source added to the e-Government website inside ISP where monitoring will take place. It shows check for specific conditions that indicate an attack is taking place, or an intrusion has occurred in a real time to building internal intrusion detection systems. These systems are based on internal sensors and classification of data collection mechanisms for intrusion detection systems. It shows that it is possible to build e-Government website which is able to detect different types of intrusions and places of implementation that are most effective in detecting different types of attacks. In this paper, we introduce the work that will attempt to show that it is possible to perform real time internal intrusion detection using small sensors embedded in e-Government website source. These sensors will look for signs of specific intrusions and will perform target monitoring by observing the behavior of the website directly in real time. In this work we speak about the image file and how to protect it.

Keywords: E-government, IDS, software engineering, sensors and detectors

1. Introduction

An intrusion detection system is an important component to enhance security in e-Government website. The security environment in e-Government website differs from other websites that are used for browsing the internet. Therefore, more exposed to threats and the Attacks on computer infrastructures are becoming an increasingly serious problem nowadays in e-Government. Hence, several information security techniques are available today to protect the e-Government infrastructures. In order to achieve the security goal, a set of security services in e-Government should be implemented. These services include deterrence, prevention, detection, and protection in real time. Historically, the detection technology dated back to 1980. Anderson [1] introduced the concept of intrusion detection. Anderson proposed a "security surveillance system" involving formal examination of a system's audit logs. In examining the system threats, Anderson also introduced the notion of categorizing intruders based upon their access to a system, and he defined the internal intruders with permissions to access the system and external intruders without any permission.

A wireless sensor networks for intrusion detection application is capable of detecting any physical existence of external intruder [2]. Katneni and colleagues considered scenarios where traditional methods of sensor deployment do not perform well with regard to intrusion

detection at the boundary of an area under protection. Katneni proposed a Hybrid Gaussian-Ring Deployment that provides a higher intrusion detection probability with fewer nodes for attacks at the edge of the network [3]. Wilkerson and colleagues applied Random sensor deployments following Poisson or Gaussian distribution are the most widely adopted deployment strategies for hostile and unpredictable application scenarios such as environment surveillance and malicious mobile target detection [4].

E-Government refers to the use of information technologies like wide area network by government agencies. The internet and mobile computing that have the ability to transform relations with citizens, businesses. Haque [5] focused on exploring the Grid Framework for the e-Government communication and collaboration system. Zissis and colleagues [6] explore increasing participation and sophistication of electronic government services, through implementing a cloud computing architecture. Zhou and colleagues [7] stated that security risk management analyzes the procedures of e-Government security risk management from three aspects: risk identification, risk analysis and risk control. The corresponding countermeasures were proposed. Unfortunately, most of the work in e-Government security is kept as secrets of countries and is not published. In this paper, we advocate improving the embedded sensors for real time internal intrusion detection system. This involves adding code to the e-Government website where monitoring will take place. The sensors check for specific conditions that indicate an attack is taking place, or an intrusion has occurred. Embedded sensors have advantages over other intruder detection techniques (usually implemented as separate processes) in terms of reduced host impact, resistance to attack, efficiency and effectiveness of detection.

We describe the use of embedded sensors in general, and their application to the detection of website attacks to protect Image file in e-Government website. The Design and development of the sensors have been done in the real website hosting. Our tests show a high success rate in the detection of the attacks.

The work we propose is divided in four stages:

1. Designing infrastructure for the development of the sensors,
2. Implementing sensors for detecting intrusions,
3. Performing analysis on the data obtained in step (2) and validating if the existing sensors can be used to detect new attacks,
4. Connecting to other ISP to open same e-Government website.

This paper proposes a method to detect internal intrusion for protecting e-Government website using Java language. This is done by dealing with the classes of the HTML file. This file contains all programmable steps to detect internal intrusion and protect all files, which deal with that site from unauthorized changing by an intruder inside ISP. Automatic audit for all files provides high security to the site protection without using any other protection programs. These programs might be used to detect intruder inside e-Government website in ISP. With this method we can protect all files, which are dealing with the e-Government website, and automatically check for all files inside class file. This method differs from other methods by not providing the program code inside the HIML file. Therefore, it is difficult to discover and analyze the proposed method because it is inside the class file.

By using real time technique, we can use our method to detect internal intruder and protect all kinds of files inside e-Government website and all those which deal with them without returning to or getting the help of the ISP and without stopping the site for service in case of intrusion through operating an alternative site from another ISP.

The rest of the paper is organized as follows. Section 2 explains the Intrusion Detection System (IDS) and the difference between Intruder and Intrusion. Section 3 discusses some of the Sectors and Stages of e-Government and the Barriers and Challenges of e-Government. Section 4 describes the purpose of the development of the sensors and provides the meaning of Sensors and Detectors. It also describes Embedded Sensors for Intrusion Detection. This is

followed by providing the main Functions of the Proposed System and the infrastructure of the internal embedded sensor. Section 5 provides concluding remarks of the work. Section 6 presents our suggestions for future work.

2. Intrusion Detection

Intrusion detection has been defined as "the problem of identifying individuals who are using a computer system without authorization (i.e., 'crackers') and those who have legitimate access to the system but are abusing their privileges (i.e., the 'insider threat') [8]. Intrusion detection and assessment systems are an integral part of any physical protection system. Detection and assessment provide a basis for the initiation of an effective security response. Intrusion Detection Systems (IDSs) should be designed to facilitate the detection of attempted and actual unauthorized entry into designated areas and should complement the security response by providing the security force with prompt notification of the detected activity from which an assessment can be made and a response initiated [9].

2.1 Intruder: A person who is the perpetrator of a computer security incident often referred to as hackers or crackers. An intruder is a vandal who may be operating from within the boundaries of an organization or attacking it from the outside [10]. There are two types of intruders [11]:

- External Intruders who have no authorized access to network resources.
- Internal Intruders who have authorized access to network resources.

2.2 Intrusion: Intrusion is the set of actions that attempts to compromise integrity, confidentiality or availability of network resources; while an intruder is any user or group of users who initiates such intrusive action [11]. Intrusion generally refers to unauthorized access by outside parties, whereas misuse is typically used to refer to unauthorized access by internal parties [12].

2.3 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station [13]. IDS perform a variety of functions as shown in Figure 1.

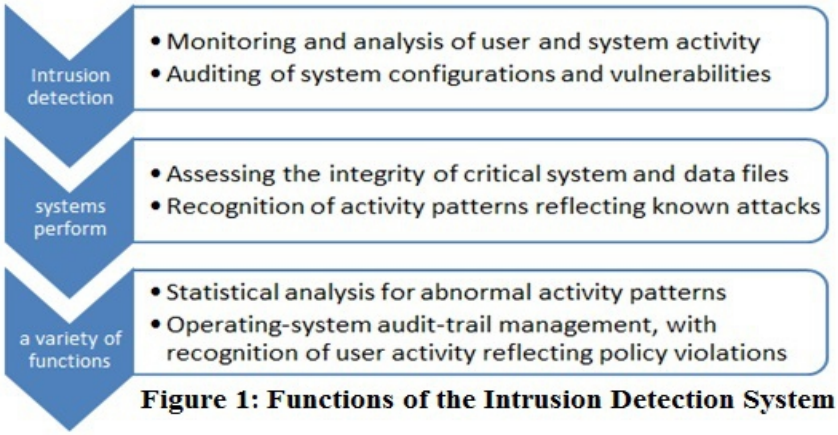

Figure 1: Functions of the Intrusion Detection System

3. E-Government

E-Government is also known as a digital government, online government or in a certain context transformational government refers to government's use of information and communication technology (ICT) to exchange information and services with citizens and businesses. E-Government may be applied by legislature, judiciary or administration in order to improve internal efficiency, the delivery of public services, or processes of democratic

governance. The primary delivery models are Government-to-Citizen (G2C), Government-to-Business (G2B) and Government-to-Government (G2G) [14].

3.1 Sectors of E-Government

Although e-Government encompasses a wide range of activities and actors, three distinct sectors can be identified. These include government-to-government (G2G), government-to-business (G2B), and government-to-citizen (G2C). Some observers also identify a fourth sector, government-to-employee (G2E).

3.1.1 Government-to-Government (G2G)

In many respects, the G2G sector represents the backbone of e-Government. Some observers suggest that governments (federal, state, local) must enhance and update their own internal systems and procedures before electronic transactions with citizens and businesses can be successful [15].

3.1.2 Government-to-Business (G2B)

Government-to-Business (G2B) initiatives receive a significant amount of attention, in part because of the high enthusiasm of the business sector and the potential for reducing costs through improved procurement practices and increased competition [16] .The G2B sector includes both the sale of surplus government goods to the public, as well as the procurement of goods and services. Although not all are directly dependent on the use of information technology, several different procurement methods are used in relation to the G2B sector [17].

3.1.3 Government-to-Citizen (G2C)

The third e-Government sector is Government-to-Citizen (G2C). G2C initiatives are designed to facilitate citizen interaction with government, which is what some observers perceive to be the primary goal of e-Government. These initiatives attempt to make transactions, such as renewing licenses and certifications, paying taxes, and applying for benefits, less time consuming and easier to carry out [18].

3.2 Stages of E-Governance

In order to accomplish e-Government initiatives, there must be a phased approach applied to the infrastructure Development which transforms an initial e-Government initiative into final desired service. There are four stages of e-Government, which in most cases follow each other [19]: Figure 2 demonstrates Stages of e-Governance.

Figure 2: Stages of e-Governance

Integration of Services: This is the highest level of any e-Government where technology is utilized to its full potential [20].
Complete Transaction over Web: The stage involves transaction between a citizen and government being completed over the internet.
Interaction between Citizen and Governments: The second stage is marked by the presence of an interactive web interface where some kinds of communication occur between government and its citizens through the web.
Presence on the Web: The first stage on any e-Government is marked by its presence on the web which acts as a common place for distributing information to the public. It is the most basic part of any e-Governance system and has limited capabilities.

3.3 Barriers and Challenges of E-Government

According to case studies from different countries, there are many challenges and issues that need to be addressed for successful implementation of e-Government. Security and privacy of information are other serious technical challenges. Challenges are identified as follows: [21]
IT Infrastructural weakness plus Lack of qualified personnel and training courses
Lack of knowledge about the e-Government program
Lack of security and privacy of information plus Lack of strategic plans
Lack of policy and regulation for e-usage and Lack of partnership and collaboration
Resistance to change to E-Systems as well as the shortage of financial resources

4. Purpose of the Development of the Sensors

We discuss the development of the sensors and the results obtained to protect Class and Image file in e-Government website. The two hypotheses that underlined in this paper are practical in nature. **First,** they intend to show that it is feasible to build an intrusion detection system in e-Government website using both internal sensors and embedded detectors. **Second**, it can be used to detect both known and new attacks.

The internal embedded sensor was also used to confirm the possibility to building e-Government website security. Therefore, Designing infrastructure for the development of the sensors e-Government website was a center point for the development of this paper.

4.1 What are Sensors and Detectors?

Internal sensors and embedded detectors. An internal sensor is a piece of code built into e-Government website that monitors a specific variable or condition of that site. By being built into the program that it is monitoring, an internal sensor can perform direct monitoring on the system, which allows it to obtain information that is reliable (very difficult to modify) and real-time (obtained almost at the moment it is generated). An embedded detector is a piece of code built into e-Government website that looks for specific signs of specific attacks or intrusions. An embedded detector bases its decisions on an internal sensor, explicitly (when the sensor is clearly differentiable from the detector). Embedded sensors operate in a different manner in comparison to other intrusion detection systems. The sensors are themselves resistant to attack. They are also effective in detecting attacks in real-time with minimal impact on website performance.

4.2 Embedded Sensors for Intrusion Detection

An embedded sensor is defined as a piece of code in e-Government website that monitors a specific variable, activity or condition of a host. Because the sensor monitors the system directly (real-time) and not through an audit trail or through packets on a network, we say that it performs direct monitoring, and because the sensor is part of the e-Government website program or system it monitors, it is said that it is an internal sensor.

Embedded sensors are built by modifying the source code of the program that will be monitored. Sensors should be added to the code at the point where a security problem can be detected in the most efficient way by using the data available at that moment.

4.3 The Main Function of the Proposed System

The proposed system operation started by initializes the request signal of website through internet browser for controlling the e-Government website inside ISP. After initialization stage; the proposed system starts the check collection information about the site. The first stage checks the watermark inside the e-Government website. The information about copyright protection will be detected and analyzed for accepting to check other files in e-Government website before opening it. The internal embedded sensor receives the request and tries to detect any threats inside ISP. If there is an attack, then the internal embedded sensor

will try to stop this attack by sending signal to other ISP to open the same e-Government website and sending Email to the administrator or the supervisor site, which contains a changed file. The main stages of the internal embedded sensor are:

1. Initialization Stage:
Initializing the request signal of e-Government website through internet browser
Checking the watermark or copyright protection
Initializing the analysis phase

2. Analyzing Stage:
Analyzing Image file
Analyzing HTML file

Figure 3 shown the basic flowchart of the proposed system

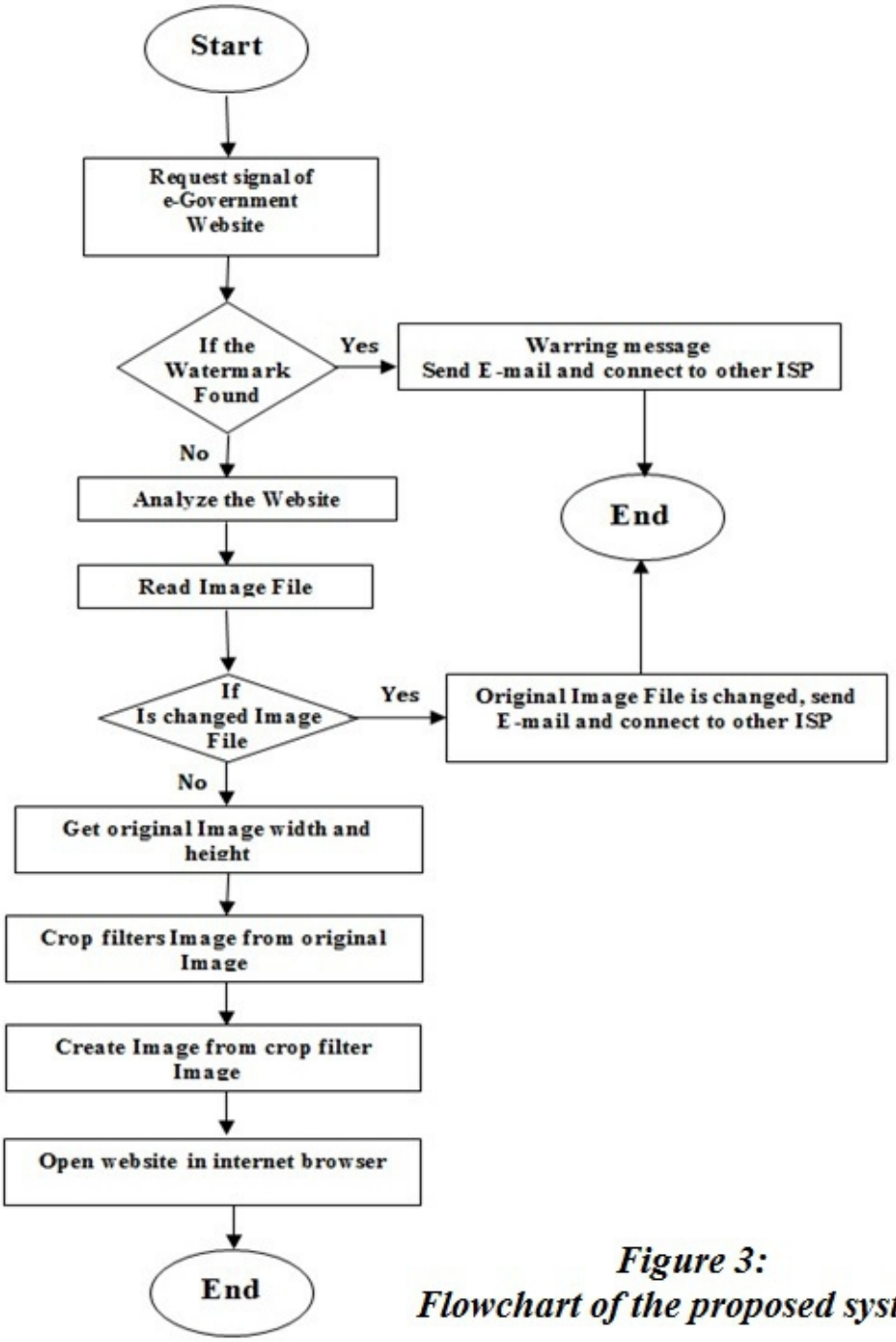

Figure 3:
Flowchart of the proposed system

4.3.1 Check Image File

After determining the initialization stage and checking watermark (copyright protection) of the proposed system put the second stage to check each file. Generally the basic flowchart of the proposed system, that checks Image file, is as shown in Figure 4.

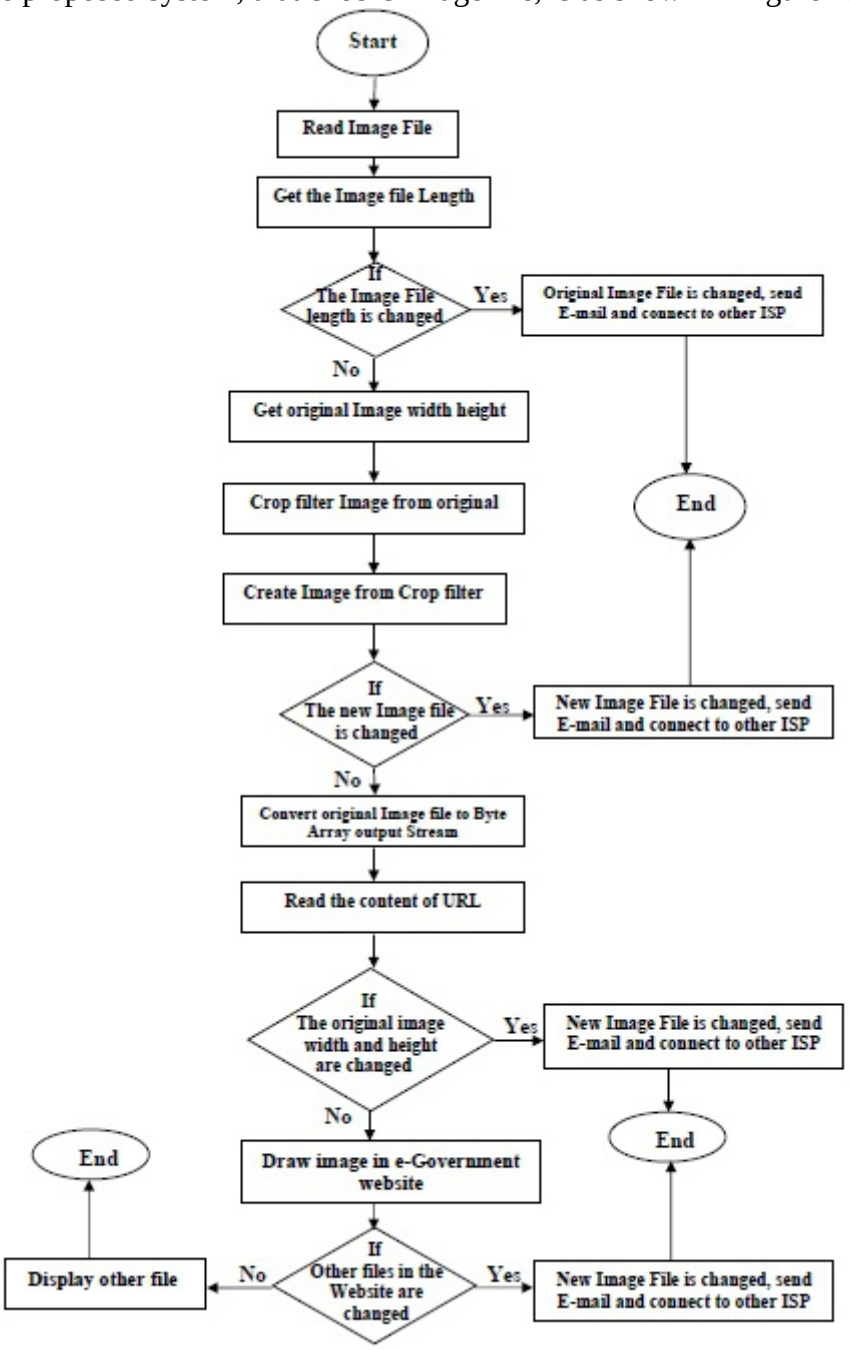

Figure 4: Flowchart of the Proposed System that checks Image File

4.4 Infrastructure Internal Embedded Sensor

The main aim of the proposed system is to design real time internal intrusion detection in website to detect the intruder that tries to attack the website. The first step of the working proposed system is start up checking the watermark (copyright protection) as sending parameter from HTML file to Class file like <PARAM name="copyright"

Value=" **Sultan Qaboos University - Computer Science Department20 13** ">

Figure 5 shows the HTML file code. The method code of copyright protection is:

public void init(){ public String copyright = " **Sultan Qaboos University - Computer Science Department 2013**";String copyrightParam = getParameter("copyright")if

((copyrightParam == null) || !copyrightParam.equals(copyright)) { throw new SecurityException("**Thank you to maintain the original copy of the change (Sultan Qaboos University - Computer Science Department 2013)**");}}

File Edit Format

```
<HTML>
<HEAD>

<TITLE>" Sultan Qaboos Uinversity  </TITLE>
</HEAD>
<BODY>

<applet code="Squ.class" width=250 height=250>
<PARAM name="copyright" value="Sultan Qaboos Uinversity - Computer Science Department 2013 ">
</applet>

</BODY>
</HTML>

```

Figure 5: HTML File Code

The proposed system will check other files step by step. After checking the watermark copyright protection the system will check Image file. Figure 6 shows the original image file and crop filter Image from original image.

Figure 6: The Original Image File and Crop Filter Image from Original Image

If Image has been changed, then the proposed system will send Email to supervisor site and Security Officer and send signal to other ISP to open same e-Government website.
The method of connect to other ISP is
squ = new Site (" Same site ", "http://www.test.com/squ.html");public Site(String siteTitle, String siteLocation) { title = siteTitle; try {location = new URL(siteLocation);} catch (MalformedURLException e) { System.err.println("Invalid URL: " + siteLocation); }

4.5 Advantages of Embedded Sensors in E-Government Website

Using embedded sensors for e-Government website in an internal intrusion detection system has the following advantages over using external sensors (implemented as separate programs):

Data in the website is never stored on an external medium before the sensor obtains them. Therefore, the possibility of an intruder modifying the data to hide its tracks.

Embedded sensors are part of the code in e-Government website they monitor.

Therefore, they cannot be disabled (as it is possible with an external sensor, which can be killed or disabled). Also they are coming very difficult to modify to produce incorrect results.

Embedded sensors can analyze the data (at real time). Therefore, reducing impact on the host.

They can obtain data at its source, or at the place where it is more convenient to obtain. Data does not have to traverse through an external program interface for the sensor to get it, because the internal sensor in the website can read it directly off the program's data structures. This reduces the delay between the generation of the data and when the intrusion detection system can make use of it.

Embedded sensors in e-Government website are only executed when the task they perform is required (this is, when the section of code they are a part of is executed). They are not executed as separate processes or threads, but as part of the monitored program of e-Government website.

Embedded sensors in e-Government website can look for very specific conditions that signal attacks, instead of reporting generic data for analysis.

This means that the amount of data that needs to be reported, collected and analyzed by higher level analysis engines is much smaller.

Disadvantages of Embedded Sensors in E-Government Website

Embedded sensors in the website have the following disadvantages with respect to external sensors:

They are more difficult to implement, because they require modifications to the source code of the e-Government website.

Their implementation requires having access to the source code of the website.

They have to be implemented in the same language as the e-Government website program in which they are being incorporated.

Improperly implemented sensors can have detrimental effects on the performance of the website.

5. Conclusion

This paper proposed an architecture based on using internal sensors built into the source code of the programs that are monitored by real time and able to extract information from e-Government website inside the ISP in which it is generated or used, Furthermore, by expanding those internal sensors with decision-making logic. Also, this paper provides an architectural and practical framework in which future study of internal sensors and embedded detectors in intrusion detection can be based in e-Government website. It also provides a classification of data source types for internal intrusion detection and a description of the characteristics and types of internal sensors and embedded detectors which are used inside e-Government website like image, sound, text, class and HTML file.

The internal sensor is an approach for the development of real time internal intrusion detection in e-Government website and Transition Analysis Technique is used to detect internal intruder in e-Government website.

This Section describes the result of applying the internal sensor in e-Government website to develop an intrusion detection family.

The work supports efficient development of new internal intrusion detection sensors because the main mechanism is used to detect any internal intruder on e-Government website in real time. However, in practice, the design of an internal intrusion detection system may not follow the functional model. In most cases, the designers of the intrusion detection system face constraints imposed by the environment in which the intrusion detection system is going to operate.

We have shown how internal sensors for intrusion detection attacks are used in e-Government website. The following points are concluded from the proposed system.

The excellent detection rate is very encouraging.

The internal sensors have been the simplest in the cases where they embedded themselves in all files on website and checked all attacks.

This internal intrusion detection system can operate without any external components.

The prototype implemented is able to detect previously unknown attacks.

The proposed method detects internal intrusion for protecting an e-Government website using Java language for dealing with the classes.

Using automatic audit for all files provides high security to the site protection without using any other protection programs.

By using the real time technique, we can use our method to detect internal intruder and protect all kinds of files inside e-Government website and all those which deal with them without returning to or getting the help of the ISP and without making the site stops providing service in case of intrusion through operating an alternative site from another ISP.

It cannot attack the e-Government website because the Java applet makes garbage collection to the memory.

The proposed method to detect the internal intrusion and protect files using Java language is very flexible in dealing with any kind of operating systems.

6. Suggestions for Future Work

The work presented in this paper has explored the basic concepts of using internal sensors for intrusion detection by showing their feasibility. However, there is a considerable amount of work that needs to be done to further study and characterize their properties. Future work could also explore improving the detection new attacks in data base by implementing internal detectors for a larger number of records inside Database. Another possibility would be the automatic generation of components that could be used by programmers to insert sensors and detectors in their source code.

This paper has explored the feasibility of extracting information about the behavior of a computer system that is more complete and reliable than any data that had been available before to intrusion detection systems. This availability opens multiple possibilities for future exploration and research, and may lead to the design and development of more efficient, reliable and effective intrusion detection systems.

References:

Anderson.: Computer Security Threat Monitoring and Surveillance. February 1980.

Hailong, Pandit, Katneni and Agrawal: A Reverse Gaussian deployment strategy for intrusion detection in wireless sensor, IEEE International Conference, 2012.

Katneni, Pandit, Hailong and Li,Agrawal:Hybrid Gaussian-Ring Deployment for intrusion detection in wireless sensor networks, IEEE International Conference, 2012.

Wilkerson, Yun Wang and Xudong Yu :Hybrid sensor deployment for surveillance and target detection in wireless sensor networks, Wireless Communications and Mobile Computing Conference (IWCMC), 7th International, 2011.

Sirajul Haque and Riaz Memon E-Government using Grid Technology: Developing a Grid framework for G2G E-Communication and Collaboration System, International Journal of Independent Research and Studies IJIRS Vol. 2, No.1, January, 2013.

Zissis and Dimitrios Lekkas: Securing e-Government and e-Voting with an open cloud computing architecture Government Information Quarterly, Volume 28, Issue 2, April 2011.

Zhitian Zhou and Congyang : Study on the E-government Security Risk Management, International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008.

Linda McCarthy ,IT Security: Risking the Corporation", February 24, 2003.

Intrusion Detection Systems and Subsystems, U.S. Nuclear Regulatory Commission, March 2011.

Schweitzer: Incident Response: Computer Forensics Toolkit, Wiley Publishing, 2003.

Ojugo, Eboka, Okonta and Yoro:Genetic Algorithm Rule-Based Intrusion Detection System Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 8 Aug, 2012.

Kirk Hausman, Diane Barrett and Martin Weiss : Security+ Exam Cram™ 2 April 10, 2003.

Scarfone, Karen and Mell, Peter :Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource, Retrieved 1 January 2010.

Sirajul Haque and Riaz Memon : Developing a Grid framework for G2G E-Communication and Collaboration System , International Journal of Independent Research and Studies – IJIRS , Vol. 2, No.1 ,January, 2013.
Robert Atkinson and Jacob Ulevich, Digital Government: The Next Step to Reengineering the Federal Government, Progressive Policy Institute, March 2000.
Alorie Gilbert: President Bush Backs E-Government, Digital Signatures, 6 April 2001.
Greg Langlois: An Equal Slice of Success,14 May 2001.
William Matthews: Setting a Course for E-Government, 11 December 2000.
SOFIEN BEJI, YASSINE JAMOUSSI NABIL EL KADHI :Towards context-awareness security for mobile applications, The International Conference on Service, Security and its Data management technologies in Ubi-com, IEEE, China, October 2010.
Sami M. Alhomod and Mohd Mudasir Shafi: Best Practices in E government: A review of Some Innovative Models Proposed in Different CountriesInternational Journal of Electrical & Computer Sciences Vol: 12 No: 01, 2012.
Nugi Nkwe ,E-Government: Challenges and Opportunities in Botswana Department of Accounting and Finance University of Botswana Gaborone, Botswana International Journal of Humanities and Social Science Vol. 2 No. 17; September 2012.