A STANDARD-COMPLIANT INTEGRATED SECURITY FRAMEWORK

Hassen Sallay, Khaled Al-Shalfan

{sallay, kshalfan}@ccis.imamu.edu.sa
Research Center & Scientific Consultations
College of Computer Science & Information Systems
Al-Imam Mohammad Bin Saud Islamic University
PO Box 84880, Riyadh 11681 (Saudi Arabia)

ABSTRACT

Security intrusion incidents have dramatically risen over the last decade. The organizations are becoming more and more aware of the importance of safeguarding their critical information. They need also to measure the degree of compliance of their security measures with the standards to enhance their degree of security, avoid the lack of accountability problem, and satisfy the regulatory obligations. While there are many tools and practices that can reduce security risks, there is a real need for security framework that specifies a security model and architecture in order to satisfy these security requirements. In this paper, we propose a preliminary specification of such a framework. A security model as well as an architecture able to perform automated and procedural security safeguards are proposed. In addition, an implementation guideline of the proposed architecture (AMANSystem) based on active network approach is presented.

key words— Security, Policies, Compliance, Architecture, Active technology

1. INTRODUCTION

Information security has evolved significantly over the last decade and even more quickly over the last few years. In earlier days, critical data was in paper format; thus physical security was the major concern. The large amount of electronic data coupled with how organizations are networked together (e.g. via the Internet) has made security of electronic data a challenging problem today. The objective of information security is to protect information from a wide range of accidental or malicious threats or attacks. Organizations should not look at security only as technology, but instead as people, processes, and technology. Fortunately, several information security standards, such as ISO17799, have been developed and information security best practices have been defined. Depending on their reliance on information technology, all organizations need to fully understand their overall security posture, and whether they are compliant with industrial standards or not. Reviews of their security posture need to cover all areas from Business Continuity, Planning to Intrusion Detection and Anti-Virus programs.

On the other hand, organizations need to know how the information security is beneficial to them and thus how the security measures that addresses their risk with cost-effective manner have to be implemented. Having a comprehensive information security framework that is based on standards and addresses the specific risks that an organization is facing is a current goal for many organizations. There is no perfect solution that will secure all organization information assets and systems in compliance with all contractual and legal requirements. We believe that multiple and integrated protection strategies must be used to reduce and to manage the risks that may affect organization systems. We particularly believe that an efficient security framework is based on the three following principles:

- Security is a process not a product: Technology in the world can be ineffective if it is not used adequately by the people;
- Defense in depth: By combining multiple security measures to create a layered protection, we can protect systems even when one layer of security fails;
- Scalable and real-time security management architecture: by distributing as much as possible the security processing and data over the organization infrastructure, we can make the security system more efficient and able to perform real-time detection of critical security events to minimize the impact of security risks.

The rest of the paper is organized as follows. Section 2 provides a description of work related to information security management. The proposed security model is presented in Section 3. Section 4 is dedicated to the description of the security architecture. An active-based technology implementation of this architecture is described in Section 5. Some conclusions together with an outlook for future works are given in Section 6.
2. RELATED WORK

So far, several approaches have been proposed for the management of security information. There are some best practices standards helping the organizations to develop and to monitor their information security program. Two of these standards are GASSP (Generally Accepted System Security Principles) and the ISO17799, which was based on British standard BS7799 [1, 2]. These standards are vendor neutral and do not focus on specific technologies, but mainly focusing on the process of information security. ISO17799 pertains to what should be an information security program, but does not provide how security requirements can be achieved. GASSP was developed to promulgate comprehensive generally accepted system security principles using input from information security practitioners in the private and public sectors from USA and abroad [3]. The other regulations and standards such as Sarbanes-Oxley, HIPAA, GLBA, BSI, COBIT, GMITS and ISF Standard of good practices provide also information security guidelines and regulations and give comprehensive guidance on information security with regards to its planning [4]. All these standards can be used as a basis for evaluating an organization security posture. Several security tools and architectures were developed in the research field. Reference [6] provides a survey of the existing security architectures, it also introduces a general approach to security architecture. Some security measures and an architectural approach for ensuring systems integrity using multi-agent systems has been proposed in [9, 10, 15]. A specification for building diagrams that describes the security features of systems and serves as support to organizations with large and distributed applications is proposed in Reference [12]. In addition, a collaborative approach for access control, intrusion detection and security testing has been developed in Reference [11]. Other tools dedicated for a specific security application target such as data filtering, intrusion detection, and antivirus programs are available in Reference [17, 18, 16]. Finally, other technical security specific-purpose such as a framework for security architecture risk assessment in e-commerce security services and a policy-driven security architecture for wireless organization applications have been developed [8, 13, 14].

Even though these approaches, architecture and tools provide some important security tasks, they remain insufficient and incomplete because the technology can be ineffective without the proper people and processes integrated with it. Some of these proposals contain approaches and architectures dedicated to assess the security policies applied in the organization and verify their compliance with the standards, but do not provide the technical solution to implement them. Some others provide some architectures to implement and monitor specific policies, but do not provide a standard compliance service. We believe that making security management applications (policy design, technical policy enforcement implementation and global security monitoring) working together is very important to get the best of the organization security infrastructure investment. It is possible to achieve this objective by:

1. Specifying a security model that considers the Security as a process not as a product. This model should integrate security policies, security products and security management related tasks;

2. Designing an underlying architecture that implements this model in one uniform integrated security architecture that contains some components providing mainly the following functionalities:

   - Verifying the compliance of the security policies with the best practices standards and measuring the gap between the security policies and their technical implementation;
   - Balancing the level of risk, the value of the information, the amount of investment in security safeguard and the capabilities of security technology to provide a solution overcoming either the gap between a given policy and its implementation and/or improve the security policy and its implementation to be compliant with the security standards;
   - Maintaining a real-time picture of the security services operations and ensuring that they correctly operate;

3. Providing an open source security software to enhance the credibility degree of the used security techniques and its large acceptance. We expect that our open source implementation will be an other alternative to high cost commercial products available in the market.

3. SECURITY MODEL

To prevent dangerous security threats and to comply with to a variety of industry mandated standards, the organizations need to deploy a proactive information security strategy. The first step to execute this strategy is to define a solid and enforceable security policy. This policy should be implemented correctly and monitored continuously in a real-time fashion. Thus, we can deal with the organization’s security by three facets: (a) logical view (b) technical view and (c) real-time view. Each view represents a part of the global integrated security framework, executes a specific security process and produces a specific report.
3.1. Logical View

The logical view exposes and defines the most appropriate security policies that should be adopted by the organization. It iterates in a cyclic process containing three phases specific for the security policies (see Fig 2). They perform three security tasks (1) assessing, (2) validating and (3) generating.

3.1.1. Assessing Policies

This phase aims at the collecting of a detailed information about the policies used by the organization. It includes the assessment of the people, processes, procedures and security risks. The risk assessment should be calculated to minimize expenses without exposing an organization to unnecessary risk. This assessment will help in determining the proper allocation of resources once the security policy is effectively in place. Generally, this task is performed by answering a survey containing some parts that evaluates current security status and identifies potential threats. The survey will focus on what is being protected in the organization with strong security awareness in order to mitigate the risks. Some assets within an organization will be more valuable than others, but monetary value should not be the only factor. Determining both the monetary value and the intrinsic value of an asset is essential to accurately gauge its worth. To calculate an asset monetary value, an organization should consider the impact of compromising this assets which can be data, networks etc.

3.1.2. Validating Policies

The main objective of the validation phase is to determine the security gap between the organization policies and the standard regulations. The validation of the policy compliance reveals whether a security control procedure is correctly deployed. In this phase, we decide whether information is under-protected, overprotected or adequately protected referring to the standards and the best practices guidelines. The policy compliance validation and the policy assessment are both critical first-line tactics to proactively defend against escalating security threats.

3.1.3. Generating Policies

Based on the result of the validation phase, we generate the appropriate policy that an organization should adopt to mitigate the detected compliance gap. The generated report either defines complete new policies or improves the existing policy by proposing the adequate enhancements. A security policy should be generated based on the nature of business and the size of the organization. It should be generated also in a way such that it does not need to be updated or changed regularly. Because long security policies are not only hard to remember for employees, but also become cumbersome to maintain, it is better to generate many short security policies rather than a long security policy. These small generated policies remains valid until there is a security problem or a formal/informal audit. The updating process may concern the totality of these policies or a part of them.

3.2. Technical View

The technical view specify the security infrastructure that an organization should provide to adequately implement its policies. It iterates in a cyclic process that contains three phases performing three security tasks: (1) monitoring, (2) designing and (3) implementing (see Fig 3). These
tasks are specific for the organization security platform and infrastructure.

3.2.1. monitoring

In this phase, we identify the strengths and the vulnerabilities in the organization security infrastructure. The vulnerability assessment process determines potential weaknesses that may represent target for possible attacks. This evaluation task is made by performing some vulnerability tests, such as network penetration tests, services penetration tests by using security incident and other vulnerability databases for tracking.

![Technical View Diagram]

Fig 3: Technical View

This phase results in a detailed report that describes technical details of the current security status of the components, the current technical security configurations implementing the security policy, and the possible security vulnerabilities.

3.2.2. Designing

The monitoring report will enable to design the most appropriate security configuration that helps the organization to implement improved security procedures, controls and processes to enable optimum security. Sometimes, rather than grafting security onto existing systems, it is more effective to redesign systems to make security an integral part of them. In all cases, the main goal of this phase is to create an optimal security configuration that implements the already generated security policy. We take into account the global security policy, the organization security investment amount and the organization current policy configuration and infrastructure.

3.2.3. Implementing

In this phase, we implement the security configuration specified in the designing phase. We automatically translates the new global policy for the organization infrastructure and allocates all the resources needed. The operability and the compatibility of the used security products are also considered in this phase. This can be met by supporting all major vendors device configurations and properties such as vendor, version etc.

3.3. Real-Time View

The real-time view performs on-line tracking of the aforementioned the two above logical and technical views in order to detect potential security threats and to perform the appropriate defense reaction and measures. It iterates in a cyclic process that contains three phases performing three security tasks: (1) tracking, (2) analyzing and (3) reacting. These tasks are specific for the organization security platform and infrastructure as well as the organization security policies (see Fig 4).

3.3.1. Tracking

The process of tracking in real-time continuously scan the global security system. It assesses potential threats that affect the security policies as well as the security platform. External and internal threats must be considered in tracking. External threats include viruses, worms, trojan horses, hacking attempts and anything that tries to break an organization's security infrastructure from the outside. On the other hand, internal threats include abuse of critical systems and data, surfing Internet content, and inappropriate Internet use.

![Real Time View Diagram]

Fig 4: Real Time View

The real costly danger with internal threats comes from inside users having very extensive access to the organization infrastructure. The tracking task produce a real-time picture of a potential or real security threat attacking the security policy or its implementation.

3.3.2. Analyzing

Following the identification of the assets and the threats by the tracking phase, an analyzing phase is necessary. The goal here is to determine the nature of the attack, its degree of danger and its potential damage. According to the output of the analysis, the proper defense strategy should be defined and the security solution (policies and infrastructure) and measurements should be taken.

3.3.3. Reacting

In the reacting phase, the adopted defense strategy and the security solution is implemented. All the required resources are allocated and the new security configuration is
mapped directly on the infrastructure and the proper security procedures are executed.

3.4. Global View

The global view consists in three phases (1) analyzing, (2) revising and (3) regulating, the security infrastructure should be reviewed regularly to ensure that it is not outdated for any reason (see fig 5).

![Global View Diagram](image)

Fig 5: Global View

The security policies are supported by standards and guidelines, can be updated on a more frequent basis. After each update we should ensure the policy compliance. Careful, repetitive reviews of an organization’s security system is necessary to ensure security implementations are appropriate, secure, and cost effective to operate.

4. SECURITY ARCHITECTURE

In this section, we present a new security management architecture that implements the above security processes. Although a centralized security management approach can be efficient in a short term period for small organizations, the resources required to install, to maintain and to repair large numbers of free security managed computers that are infected or compromised will be very costly in the long term. A distributed security management will be more suitable. We adopt a distributed three-tiered architecture: (1) data tier, (2) processing tier and (3) presentation tier. The global architecture basically contains four components: the logical security manager, the technical security manager, the real-time defender and the report generator. Each of these components has its own internal architecture.

4.1. Logical Security Manager

The logical security manager is composed of three architectural components that collaborate to perform the security tasks defined in the logical view (section3.1). The internal architecture of the LSM is illustrated in fig 6.

- **Automatic Survey Builder (ASB):** The main goal of this component is to perform the assessment phase described in Section 3.1. It is a web-based tool for full automatic building, distribution of the security surveys as well as the collection of its responses. The user can include some well designed policy survey from the ASB database. The questionnaire builder offers a large set of survey question types. Finally, this component produces a detailed report that assess the current security status and that will be used as an input for the validation process.

- **Automatic standard-compliance Validator (ASV):** The ASV performs the validation process. It automatically measures the compliance of the current security policies evaluated in the previous phase with the regulatory standards. ASV is an expert system composed by an inference engine and a database of facts. The database contains the different security rules. Based on the ASB report and the database of facts, the ASV helps in discovering and fixing vulnerabilities, measuring the security gap with the standard and finally producing a detailed report of the organization policy vulnerabilities and its degree of compliance.

- **Automatic Policies Designer (APD):** Based on the ASB report, the organization security investment amount and the current policy installed, the APD performs a constraint-based calculation to generate the optimal security policies that satisfies the organizations priorities and mitigate compliance gap of the current security policy status with the standards.

4.2. Technical Security Manager

The technical security manager is composed of two architectural components which collaborate to perform the security tasks defined in Section 3.2. The internal architecture is illustrated in fig 7.

- **Policy visualizer and Network scanner (PVNS):** Through a periodic scanning of the organization infrastructure, PVNS represents via its graphical interface the state of the security policy design systems running in the organization as well as its current technical
configurations. PVNS depicts the security vulnerabilities and offers an easy and fast way to verify the correctness of policy requirements and rules.

- **Automatic Configuration Generator and Mapper (ACGM):**
  Based on the global security policy defined by APD and the current policy configuration, ACGM determines the optimal rule order satisfying the priority of the security policies and create a new optimal configuration. The ACGM engine will transform the global policy into consistent device configurations. In other words, it ensures that all the desired policies will be configured consistently across the entire network. When enabling a new policy on the network, ACGM (a) analyzes which flows must be implemented within the organization (b) identifies all the target security devices that must be changed (c) updates each target configuration and (d) deploys all the modifications without error. It provides also an easy and fast way for adding/updating/deleting the policies based on a visual representation of the policy on the network map.

ACGM offers mainly two advantages to the human manager (a) he/she has not to manually manage the interactions between the network specific devices that saves a lot of time and (b) he/she has not to be an expert in all the device technologies we are managing in order to achieve desired policy outcomes.

4.3. Realtime Security Defender (RSD)

The main function of the real-time security defender is to maintain a real-time picture of the operation of all the security services (see Fig 8). To speed up the organization reaction times against an internal or external security threat, RSD tracks allowed users actions during the runtime of the network in order to know who made a particular configuration change, or what was modified and when. It checks the status of the organization network devices against the intended active policy, at any time, and discover whether any device configuration has not been up to date or has been modified since the last configuration. In addition, it compares the running configurations with the expected ones, evaluates the differences, analyzes the unwanted changes and detects potential security threats. To perform these tasks RSD integrates several tools such that Intrusion Detection Systems, Event correlation Systems, our policy visualizer and network scanner tool.

![Real-Time Security Defender architecture](Fig 8)

4.4. Report Generator

This component is responsible for the generation of the different reports of all the security process. Basically, it will generate the different reports produced in the different security phases. It is based on the XML technology for portability reasons (for example, the human security manager should be notified by any critical security incident in real time. He should be able to display the report in his PDA for example.(see Fig 9)).

![Report Generator architecture](Fig 9)

5. GUIDELINES FOR AN ACTIVE-BASED IMPLEMENTATION OF THE ARCHITECTURE

The previously presented architecture can be implemented in several ways. This can be done with feature and protocol extensions of specific security approaches or through a standard management framework like SNMP with dedicated Management Information Models and associated MIBs together with usage scenarios. We chose an alternative to the above solutions, namely to exploit the benefit of active network technology in terms of flexibility and extensibility, to host the various components of the architecture ([19], [20], [21]). We use this technology to dynamically download and operate security agents, enabling a seamless evolution that follows the policy changes of the managed organization system. The availability of a dynamic code distribution facility and the presence of execution environments on all organization infrastructure nodes enables rapid and online security strategies change, update of security components, activation of tests for security management purpose or more generally to push the security man-
management functions where they are needed. The resulting implementation called AMANSystem (Active-based Management Architecture for iNtegrated Security System) is illustrated in Fig 10. Within AMANSystem, security functions are designed as a set of dedicated active applications called plug-ins (RSD plug-in, PVNS plug-in, SP plug-in...). Plug-ins are stored in a repository within a centralized server repository. Once installed on the centralized server repository, these components can be downloaded by security agents where they are executed. Plug-ins uninstall themselves when they are no longer in use. The FLAME active network framework is the execution environment that we can use to build AMANSystem. This execution environment enables both dynamic installation and removal of active applications but also APIs and associated libraries enabling the execution environment to dynamically extend the interface it offers to active applications (e.g. providing a new packet capture service). All AMANSystem plug-gins are defined as FLAME applications. For the logical manager, the tasks are basically static and thus executed in one centralized system. In contrast, each component of the technical and real-time managers is represented by one or more of plug-in which will be dynamically plugged where and when they are needed to perform and execute the different required security processes.

6. CONCLUSION AND FUTURE WORK

In this paper, the need for developing of a standard compliant integrated security architecture was addressed. A security model was proposed and an architecture implementing this model was described. The FLAME execution environment has been selected to host the architecture. The resulting environment is called AMANSystem. Within AMANSystem, security functions are defined in terms of active applications which can be downloaded on demand. These plug-ins perform the different security functions implementing the different security phases defined in the security model. Pushing forward the implementation of the architecture within the FLAME active network constitutes our first goal in the near future. This mainly requires some refinement in the specification of the the different security management plug-ins. Finally, the architecture need to be extended to be deployed in a multi-domain (multi-party) environment.

7. REFERENCES


[18] Ludovic M’e and C’edric Michel, Intrusion Detection: A Bibliography, Sup’elec, Rennes, France, SSIR-2001-01, September 2001,

