Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2001 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2001

A Framework for Managing Information Systems Security

Irene Woon
National University of Singapore

A Framework for Managing Information Systems Security

I.M.Y Woon
School of Computing, National University of Singapore
Kent Ridge, Singapore 119260.

Abstract

A review of current systems in the market place reveals that popular approaches such as checklists and security tools address specific problems or particular aspects of the security issue. This is inadequate and ineffective for today's complex information and computer systems. The framework we propose is able to provide an overall solution to manage security in an effective manner. In the paper, we describe the components of this framework and show how they interact with each other to address the concerns of all levels of the organization hierarchy, the various and different parts of the security labyrinth. Feedback from initial evaluations shows promising results.

Keywords: Information Systems Security, Information Systems Security Framework, Information Systems Security Assessment

1. Introduction

Computer site managers have an arsenal of security tools for protecting their information systems. They also have access to an assortment of security policies, security risk assessment tools and methodologies, enforcement check procedures and software. However, they do not have a structured approach in organizing the tools and procedures. Indeed, security in most heterogeneous environments is too often a patchwork of ad hoc security mechanisms. This is the result of the "quick and dirty" approach that most security administrators adopt to cope with new security risks, given that the time to respond each new threat is critical. In addition, security mechanisms utilized in organization over time, tend to deviate and change beyond their original purposes and become "loose" and disorganised, thereby introducing security threats and reducing the effectiveness of security mechanisms applied to counter the threats in the first place. Furthermore, the security architecture in most organization is not built on any formal security standards but either adopted and modified from other organizations or built by inexperienced and unqualified programmers doubling up as IT security manager. Thus, these organizations need a framework that will seamlessly integrate new security mechanisms with the existing security structure, at the same time adhering to strict and formal security concepts.

The proposed solution, **I**nformation **S**ecurity **S**elf **A**ssessment **S**ystem (ISSAS), provides a security framework that assists computer site managers in organizing information security mechanisms. The basic building block of the system is derived from the set of standards spelled out in ITSEC (ITSEC, 1991) and TCSEC (DoD, 1985) There are several divisions within each of these standards and these divisions are ordered hierarchically with the highest division reserved for systems providing the most comprehensive security. These sets of standards encompass a wide range of areas such as password security standards, network security standards, etc. ISSAS uses the profile of a user's site i.e. the hardware and software configurations and its business activity to determine the areas of security to assess and the

division to assess these at. Another essential component of ISSAS is the knowledge base of heuristic rules used to derive an aggregated security rating for site and to identify serious security breaches and violations. Access to tools and procedures are provided to help the user during the assessment phase to verify the state of a specific item e.g. password cracker program and the post-assessment phase where the user might desire to rectify the security loopholes identified by the system. Thus, ISSAS is founded on reputable standards which is able to:

- incorporate all facets of computer security from the platform independent issues such as personnel security to platform dependent issues such as operating system vulnerabilities.
- address concerns of all levels of the organization hierarchy.
- be extended and updated easily.

In this paper, we will describe in the main components of the framework. Subsequently, we will analyse the results of the tests we have performed using ISSAS and conclude with a discussion of the possible extensions to this work.

2. Design of ISSAS

There are 4 basic components in ISSAS:

1. Security Standards
2. Profile of User site
3. Assessment Heuristics
4. Automated Tools and Procedures

The relationship and interaction between these components is shown in Figure 1.

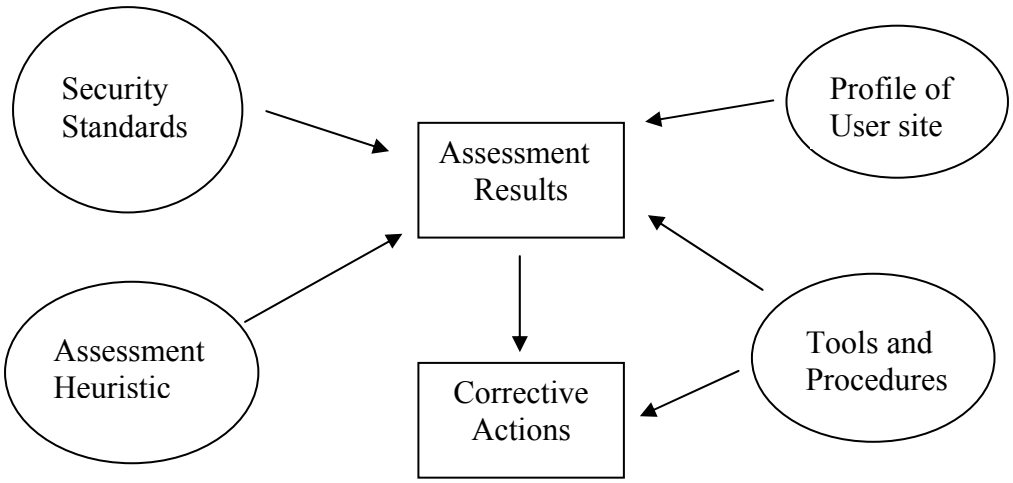

Figure 1: Components of ISSAS

2.1 Security Standards

ISSAS derives its set of standards from the set of standards spelled out in TCSEC and ITSEC **T**rusted **C**omputer **S**ystem **E**valuation **C**riteria (TCSEC), commonly known as the Orange Book was developed by the National Computer Security Center for the United States'

Department of Defense. It defines four divisions: A, B, C, and D with A denoting the system with the most comprehensive security rating. Each division represents a level of confidence one can place in the system for the protection of sensitive information. The subclasses (given as numbers) for the B and C divisions indicate further levels of confidence within the division. **I**nformation **T**echnology **S**ystem **E**valuation **C**riteria (ITSEC) is the set of standards established by vendors and sponsors in Netherlands, France, Germany and United Kingdom. It defines six classes with class E6 being the class that provides the best assurance of security.

TCSEC concentrates on confidentiality requirements while ITSEC covers this as well as integrity and availability requirements. In reality, not many systems have been evaluated beyond class B1 as the implementation of the stringent requirements laid down for satisfying these classes are resource intensive. As such, we decided that a fine-grained stratification was not necessary. The simple and effective classification system also ensures that users will not be confused by a myriad of choices. Table 1 shows the correspondence between the various classes and divisions.

Standards	Corresponding Class/Division			
ISSAS	1	2	3	Standalone
TCSEC	A1 – B3	B2 – C2	C1 – D	Un-rated
ITSEC	E6 – E5	E4 – E2	E1 – E0	Un-rated

Table 1: Security class correspondence between ITSEC, TCSEC and ISSAS

The classes of policies that is available in ISSAS for corporate sites are:

- Class 1(Very Strict) - Security is of the utmost importance and the corporation's competitive advantage and health depends on it.
- Class 2 (Strict) - Security is important and is needed to meet most corporate needs
- Class 3 (Normal) - Security is viewed only as a supporting role
- Standalone - Security for standalone PCs that are not connected to any network

The TCSEC and ITSEC documentation specifies requirements that are useful and necessary for the development of a secure site. These requirements are given in terms of control objectives to be attained such as the existence of a well-defined policy, the provision of an accountability system. For example, the control objective for accountability is given as:

> *"Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty"*

However, in an assessment system, the user needs to have a more specific set of questions to help him in deciding if these control objectives have been met. ISSAS identifies the areas of information system that are related to the control objectives. For example, accountability is dealt with in areas such as account security, intrusion detection, password and login. By analysing the entire set of control objectives, the security areas given in Table 2 were derived.

Security Areas	
Password Security	Application Security
Login Security	Waste Security
Intrusion Detection	Label Security
Account Security	Device File Security
Personnel Security	Batch Jobs Security
Security Audit	Physical Security
Anti-Malicious Software Security	PC Security
Network Security	Operating System Security
Backup Security	Hardware Component Security
E-mail Security	Penetration Testing
Network Printer Security	

Table 2: Areas of security covered by ISSAS

Table 3 is an expanded sub-section view of the area of password security. It shows some of the questions the user needs to answer.

Password Security	
Are password features enabled?	○ Y ○ N
Are tokens used for authentication?	○ Y ○ N
Is the number of passwords that the SA (Security Administrator) has to remember more than 7?	○ Y ○ N
Is the length of passwords used >= 7 characters?	○ Y ○ N
Are passwords alphanumeric (i.e. mixture of numbers and letters)?	○ Y ○ N
Are passwords unique (i.e. not used before)?	○ Y ○ N

Table 3: Part of the question set for Password Security

2.2 Profile of the User site

ISSAS defines a user profile in terms of its hardware and software configurations its business activity, and the value it places on its IT assets. The questions to elicit this information can be divided into 3 sets:

- The Basic Policy Set
  The main purpose of this question set is to determine the degree to which the site is networked. Networked sites will have more security issues to address and a greater degree of networking will increase the number of security issues will be encountered. A question in this set is: "Is your site linked/connected to the Internet (i.e. WWW/FTP)?"
- The General Security Template Set
  The main purpose of the questions in this set is to establish the nature and use of information stored within the site and how IT resources are used. A question in this set is: "Are Executive Information System (EIS) available on this site?"
- The Specific Security Template Set
  The main purpose of the questions in this set is to confirm the level of security classification the site should be assessed at. A question in this set is: "Are employees

allowed to work from home or outside the company (e. g. through dialup/wireless communication)? ".

This user profile is then used to determine the level of security classification that is required for that site. Different sets of questions will be posed to the user, depending on his site's user profile. Table 4 shows that the user will have to answer 3 additional questions (Question 1,3 and 4) if his site is to be assessed at the Very Strict Class rating. These questions will not be posed to him, if his site is to be assessed at a lower rating than this i.e. Strict or Normal Class. In addition, the question on password length (Question 2) differs for different class ratings. Under the Normal Class evaluation, the length is 6 or more characters while under the Very Strict Class evaluation, the length is 8 or more characters.

Password Security		
1	Are tokens used for authentication?	○Y ○N
2	Is the length of passwords used >= 8 characters?	○Y ○N
3	Are passwords unique (i.e. not used before)?	○Y ○N
4	Are passwords changed periodically (forced)?	○Y ○N

Table 4 - "Different" questions on Password Security for Class 1 evaluation

Not all areas of security will be assessed for all evaluation classes. For the Normal class evaluation, questions on areas like Label, Device File and Batch Job security will not be asked.

2.3 Assessment Heuristics

Assessment heuristics are employed during the assessment phase of the system. This assessment phase is preceded by the identification of the user's profile. Heuristics for security analysis were derived by studying well known security literature (DoD 1985; ITSEC, 1991; National IT Standards Committee) and observing current trends. The heuristics use a 5-point rating scale as well as a description for each point in the scale. This rating scale reflects the fact that some security breaches have more severe consequences than others do. In Table 5, "Immediate failure" denotes security measures or items that are of the utmost importance to the organization and the failure to implement them offers an immediate opportunity of security breach. It is important to note that the ratings given reflect the needs of the industry in the authors' country. Hence, the weight given is based on *current* trends and can be, and should be, changed over time to reflect the ever-changing needs of the IT industry and the needs of different countries and domains.

Descriptive Rating per item	Points
Immediate failure	5
Very important/Very serious	5
Important/Serious	4
Average	3
Must implement if have the chance	2
Implement for a complete security solution	1

Table 5: Rating scale for Security Items

The rating system for the Table 3 is given in Table 6. A multi-dimensioned matrix establishes the relationship between all security items, via area of security or individually. The points allocated to the site and the weight of points is tagged to this relationship. For example, if password feature is NOT enabled, then any intrusion detection measure may not work. Thus, the user will not be queried on any intrusion detection measure and will be given the maximum points (indicating immediate failure) for that area of security.

Password Security	
Are password features enabled?	5, immediate failure
Are tokens used for authentication?	5, Very important
Is the number of passwords that the SA (Security Administrator) has to remember more than 7?	4
Is the length of passwords used >= 7 characters?	3
Are passwords alphanumeric (i.e. mixture of numbers and letters)?	2
Are passwords unique (i.e. not used before)?	2

Table 6: Ratings for part of the Password Security Measures

Currently, the point allocation system is static. A dynamic point allocation system that considers the user site profile would be more realistic and would be part of our enhancement efforts. With each security item weighted and described, a scoring system for the site can thus be derived. The overall site assessment status is thus arrived by considered the total number of points allocated to the site, the number of immediate failures and very serious breaches detected. Table 7 shows all the possible site security ratings

Site Security Labels	What it means
Excellent	Site passes security check with flying colours
Very Good	Site has good security
Adequate	Site has adequate security
Poor	Site failed security check
Very Bad	Site failed security check badly

Table 7: Site Security Labels

2.4 Automated Tools and Procedures

Tools and procedures can be in-house developed or by third-party vendors (Fyodor, Singcert). They are provided to users to:

- check and verify a particular area of security, for example if the user's password is alphanumeric.
- implement particular security features.
- promote the user's awareness of the availability of hacking tools

Hence, they are organized according to the areas of security given in Table 2. Basically, there are 2 types of tools:

- standalone, operating system specific tools for e.g. password crackers

- generic tools, which are accessible and executed online e.g. SATAN-like utilities for checking ports etc.

Procedures, on the other hand, are provided with on-line checklists that can be used to confirm the implementation of procedures. Thus, with the use of procedures and tools, users can further verify the activation of a particular security feature. This makes the security check process easier and more transparent.

2.5 Reports

Two types of reports will be generated after site check has been conducted:

1. Quantitative analysis report
   This set of reports gives a graphical picture of security breaches of the site using:
   - Status Bar to display the security rating or state of site. The status bar shows a continuum from "unhealthy" to "healthy".
   - Pie Chart to portray the top 5 areas with the worst security breaches. The size of each slice of the pie indicates the severity of breach of each area.
   - Bar Chart to show the security breaches that occurred in the most vulnerable area that was obtained in the pie chart in order of importance.
2. Qualitative analysis report
   This gives a detailed result of security compliancy and coverage for the site. This includes a point-by-point breakdown of the detected security loopholes, statistics such as number of immediate failures and number of very serious breaches as well as total points allocated .

3. Evaluating ISSAS

An initial evaluation of the ISSAS prototype was conducted on the following units:

- Profiling of site. Tested for correctness of result from response (i.e. path that achieve *Very Strict, Strict, Normal* and *Standalone* classifications for site.
- Security checks. The check reports are checked for correctness with reference to the ratings (i.e. *Excellent, Very Good, Adequate, Poor* and *Very bad)* given to the site after the check by verifying the statistics such as total points manually.
- Procedures and Tools. The procedures and tools are tested in implementation (during acceptance testing).

A brief description of the result obtained is as followed:

- Profile: *Normal*
- Result of check:
  - Security status: ***ADEQUATE***
  - Total critical breaches: ***5***
  - Total very serious breaches: *2*
  - Total serious breaches: *8*
- The critical breaches detected are:
  - D(1) Did not assign proper rights for important accounts.
  - E(1) SA/SSA are not cleared for the job.

- F(1) Auditing not done.
- H(1) Firewall/proxy not set-up.
- R(1) Passwords are embedded into system/batch files.

The feedback we received from the technical manager and the system administrator was very encouraging. We also received invaluable feedback from them and will be incorporating these as part of our enhancement efforts. We are unable to divulge further details of the site or the testing results for obvious confidentiality reasons.

4. Future Enhancements

This section describes security mechanisms that can be included or "plugged" into ISSAS:

- From general checks, evolve subsequent level checks. This would involve the following tasks:
  - Defining System-specific checks based on the security areas. These check should caters for all servers with different Operating Systems installed on the site.
  - Providing tools to carry on the check by connecting to the site via a point or PC using privileged and non-privileged accounts (automated or semi-automated that does not implement correction). Correction features should not be enabled to prevent unauthorized or unannounced changes to the systems.
- Exhaustive penetration tests. Explore the possibility of using ISSAS as a tool to identify weak points of the site. The penetration test should be:
  - a semi-automated process that does not implement correction.
  - be activated within site, which at time of check is isolated externally and internally (i.e. no user).
  - explore potential breaches (e.g. areas such as login, intrusion, network, account etc) on all servers (inclusion of mail, news and web) within the site.
  - explore potential breaches by conducting tests from outside the site.
  - explore potential breaches during normal operations e.g. probe station attack etc.
- Explore a generic interface mechanism to integrate and incorporate results from other security tools such as SATAN
- Usage of ISSAS for TCSEC/ITSEC equivalence site certification. As a result of compliance with the above ISSAS provided checks and implementation, the site can be given an ISSAS security classification which is recognised e.g. a site is certified to *Class 2 (Strict)* will be on par with another site given the TCSEC level of *Excellent.*

5. CONCLUSION

The biggest problem any security administrator can face is to build a coordinated and extendable architecture that is based on proven security standards that will make security a breeze, and which is compatible with existing policies and structures. Work in the area of ISSAS serves to address this problem. ISSAS provides a coordinated, platform independent easy-to-understand and implementable framework based on proven security standards and current trends that can be modifiable and easily extendable over time. It can become the backbone of any organization's security solution whereby tools and procedures acts as "plug-ins" that will evolve over time.

ACKNOWLEDGEMENT

Implementation of the system was carried out by Aloysius Cheang as his honours year student project in the School of Computing, National University of Singapore.

REFERENCES

Department of Defense (U.S), Trusted Computer Security Evaluation Criteria, 1985, retrieved February 1999, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

Fyodor, retrieved February 1999, http://www.insecure.org/tools.html.

ITSEC, Information Technology Security Evaluation Criteria, v1.2, 1991, retrieved February 1999, http://www.itsec.gov.uk.

National Information Technology Standards Committee, National Computer Board (Singapore), retrieved February 1999, http://www.itsc.org.sg.

SingCert, Singapore Computer Emergency Response Team, retrieved February 1999, http://www.singcert.org.sg/resource.shtml.