SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

VOLUME 5 NO 4, 2017
ISSN 2054-7390

Role of Management and Policy Issues in Computer Security: Rand Report R-609 within Organization

N. Tagmouti, Jamal Boujmil, N. Raissouni
RS&GIS Lab. Dept. Telecommunications
The National School for Applied Sciences of Tetuan
Tetuan, Morocco
jamal.boujmil@gmail.com, nohatg@gmail.com, nraissouni@uae.ma

ABSTRACT

The need to provide strengthened Security for Information Systems within organization increases day after day seeing the large development of interconnection of the World Wide Web and the clear effect that results by the frequent and multiple productions of attacks and threats. This feebleness and gap in current information technologies urge researcher to face by developing more secure systems of Sharing Resources. The history of securing Information Systems began with the concept of Computer Security in its Global meaning Physical and Non-Physical. Thus, by 1967 the Department of Defense of USA published the R-609 which is considered as the first step in the wide world of Information security including Securing the data, Limiting random and unauthorized access to that data and Involving personnel from multiple levels of the organization in information security. The purpose of this paper is to analyze and evaluate the role of management and policy issues in computer security that proposes Rand Report R-609 within organization.

Keywords: Information Systems, Information Security, R-609

1 Introduction

Information security begins with computer security. The Advanced Research Projects Agency (ARPA), during June 1967, designed a special commission to carry out a study and research of the process of securing classified information systems. This commission assembled in October 1967 with regular meetings has formulated recommendations ultimately becoming the contents of the Rand Report R-609 [1].The need for computer security (i.e., the need to secure physical locations, hardware, and software from threats) ascended during World War II when the first mainframes, developed to aid computations for communication code breaking, were put to use.

The Rand Report R-609isconsidered the pioneer and formerextensively recognized issuedmanuscript to recognize the role of management and policy issues in computer security. It is noted in the report, that the wide exploitationin information systems of networking components is introducing security risks. These last not mitigated by the routine practices used then to secure these systems. The reportindicated a crucial moment in computer security historywhen the choice of computer security lengthenedmeaningfully from the safety of physical locations and hardware to take account of the following points:

DOI: 10.14738/tmlai.54.3209
Publication Date: 15th August, 2017
URL: http://dx.doi.org/10.14738/tmlai.54.3209

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matters pertaining to information security

Our objective in the present research is to carry out an analysis and a comparative study based on the documents dealing with role of management and policy issues in computer security. The study will focus mainly on the multiple levels of security been implemented to protect the mainframes and maintain the integrity of the data (e.g., access to sensitive military locations was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards). Furthermore, the growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

2 Arpanet Program Plan Development

ARPANET come to bestandard and more widely used during the 1970s and 80s, and the potential for its misuse developed. In December of 1973, Robert M. "Bob" Metcalfe, creditedwith the development of Ethernet (one of the furthermostwidely held networking protocols) identified major problems with ARPANET security. Individual remote sites are not having sufficient controls and safeguards to protect data from unauthorized remote users. In addition, other difficultiesoverflowed [1]:

Password structure and formats vulnerability.

Lack of safety procedures for dial-up connections.

User identification and authorization to the system absence.

Phone numbers were commonly distributed and openly exposed on the walls of phone booths,providing hackers easy access to ARPANET. Due to these drawbacks, and because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity [2].Subsequently, in 1978, theeminentresearch entitled "Protection Analysis: Final Report" was appreciatively published. This study focused on the project started by ARPA to discern the weaknesses of operating system security. Chronologically, including this and other seminal studies in early computer security shown below:

1968- Maurice Wilkes discusses password security in Time-Sharing Computer Systems.

1973- Schell, Downey, and Popek examine the need for additional security in military systems in "Preliminary Notes on the Design of Secure Military Computer Systems"[3].

1975- The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the Federal Register.

1978- Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software[4].

1979- Morris and Thompson author “Password Security: A Case History,” published in the Communications of the Association for Computing Machinery (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.

1979- Dennis Ritchie publishes “On the Security of UNIX” and “Protection of Data File Contents,” discussing secure user IDs and secure group IDs, and the problems inherent in the systems.

1984- Grampp and Morris write “UNIX Operating System Security.” In this report, the authors examine four “important handles to computer security”: physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security[5].

1984- Reeds and Weinberger publish “File Security and the UNIX System Crypt Command.” Their premise was: “No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users … the naïve user has no chance” [6].

The programconcerning security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand Report R-609. Whichattempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The paper was confidential for almost a decade, and is nowadays, considered thedocument that impulses the study and analysis of computer security.

Therefore, the role of management and policy issues of security of the entire systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring-summer of 1967. Meanwhile, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.

3 Security Control Definitions

A wide terminologyis being used in relationtosecurity control for which practice is not completely standardized. In this paragraph, we present the terms used throughout the Rand Report R-609 respecting the way they were defined as a group [1-6].

• **CLEARANCE:** The privilege granted to an individual onthe basis of prescribed investigative procedures to have formal access to classified information when such access is necessary to his work. The three formal national clearances are Top Secret, Secret, and Confidential. However, it is also expedient from the computer point of view to recognize Uncleared as a fourth level of clearance. A clearance is a necessary but not sufficient condition to have access to classified information. By extension, the concept of clearance can be applied also to equipment. For example, when a computer terminal is spoken of as having a given level of clearance, it is implied that certain investigative procedures and tests have established that the corresponding level of classified information can be safely transmitted through that terminal. When referring to an aggregation of equipment, together with its management controls and procedures, facility clearance is some- times used.

• **NEED-TO-KNOW**: An administrative action certifying that a given individual requires access to specified classified information in order to perform his assigned duties. The combination of a clearance and a need-to-know constitutes the necessary and sufficient conditions for granting access to classified information.

- **CLASSIFICATION**:The act of identifying the sensitivity of' defense information by ascertaining the potential level of damage to the interests of the United States were the information to be divulged to an unfriendly foreign agent. The classification of in formation is formally defined in Executive Order 10501. There are only three formal levels of national classification: Top Secret, Secret, and Confidential, but it is expedient from the computer point of view also to consider Unclassified as a fourth level of classification. The identifiers associated with an item of classified information, indicating the level of classification or any special status, are generically called labels.

- **SPECIAL CATEGORY = SPECIAL-ACCESSCATEGORY =COMPARTMENT**:Classified defense information that is segregated and entrusted to a particular agency or organizational group for safeguarding. For example, that portion of defense classified information that concerns nuclear matters is entrusted to the Atomic Energy Commission, which is responsible for establishing and promulgating rules and regulations for safeguarding it and for controlling its dissemination. Classified information in a special category is normally identified by some special marking, label, or letter; e.g., AEC information, whether classified Confidential, Secret, or Top Secret, is collectively identified as Q-information. It is often called Q-classified, but note that this use of classification is an extended sense of the formal usage of the word.Sometimes, special investigative procedures are stipulated for granting access to information in special categories. Thus, while formally there are only three broadly defined national clearance levels, in practice there is a further structure within each level. In part, this reflects the separation of information into special categories, and, in part, the fact that many different agencies are authorized to grant clearances. For example, an individual functioning within the AEC domain and cleared to Top Secret will often be said to have a Q-clearance because he is authorized access to Top Secret information entrusted to the AEC for safeguarding and identified by the special category Q. These special types of clearances at given levels are not always specifically identified with a unique additional marking or label.

- **CAVEAT**: A special letter, word, phrase, sentence, marking, or combination thereof, which labels classified material as being in a special category and hence subject to additional access controls. Thus, a caveat is an indicator of a special subset of information within one or more levels of classification. The caveat may be juxtaposed with the classification label may appear by itself; or sometimes does not appear explicitly but is only inferred. Particular kinds of caveats are:

  - CODEWORDS: An individual word or a group of words labelling a particular collection of classified information.
  - DISSEMINATION LABELS = ACCESS CONTROL LABELS: A group of words that imposes an additional restriction on how classified information can be used, disseminated, or divulged; such labels are an additional means for controlling access. Examples: "No Foreign Dissemination," "U.S. Eyes Only," "Not Releasable Outside the Department of Defense".
  - INFORMATION LABELS: A group of words that conveys to the recipient of information some additional guidance as to how the information may be further disseminated, controlled, transmitted, protected, or utilized. Examples: "Limited Distribution," "Special Handling Required," "Group 1 Excluded from Automatic Downgrading and Declassification".

• **FULLY CLEARED**: An individual who has the clearance and all need-to-know authorizations granting him access to all classified information contained in a computer system. By extension, the term can be applied to equipment, in which case it implies that all necessary safeguards are present to enable the equipment to store and process information with many levels of' classification and caveated in many different ways.

• **SECURITY FLAG**: For the purposes of this Report. It is convenient to introduce this new term. It is a composite term, reflecting the level of classification. All caveats (including codewords and labels), and need-to-know requirements, which together are the indicators establishing the access restrictions on information or the access privileges of an individual. By extension, the concept can be applied to equipment and indicates the class of information that can be stored and processed.Thus, the security flag contains all the information necessary to control access. One security flag is considered to be equal to or higher than a second if a requestor with the first flag is authorized access to information which has the second flag.

• **SECURITY PARAMETERS**: The totality of information about users, files, terminals, communications, etc., which a computer system requires in order to exercise security control over the information that it contains. Included are such things as user names, clearances, need-to-know authorizations, physical location; terminal locations and clearances; file classifications and dissemination restrictions. Thus, a set of security parameters particularizes a generalized security control system to the specific equipment configuration, class of information, class of users, etc., in a given installation.

4 Management and Administrative Control

An effective andagreed set of management and administrative controls and procedures governing the information'sstreamto and from the computer systemmust be added to overall policy guidance and to technical methods. In addition to the movement and actions within the system environment of people and transportable components. The Standardization of activities and the requirement for standards all through the system is the essential aspect of effective and agreed control.Standards are effective in severalapproaches. Thus, with strictlyagreed procedures, the different operators will be reticent from taking shortcuts that can result in leakage. Therefore, typical procedures that are required with some details of each are presented in the following[1-6].

4.1 Operational Start-Up

Procedures must be established for putting a resource-sharing system into operation, and must include provisions for loading a fresh, certified copy of the Supervisor software, for verification of its correct loading, for validation of system security checks, for inserting relevant security parameters, and for certification of system security status by the System Security Officer.

4.1.1 Scheduled shutdown

The procedures for a scheduled shutdown of operations must take account of proper notification of the System Security Officer, physical protection of demountable storage (tapes, discs) as required, orderly closing of internal files, validation of the suspension of operation of all terminals, demounting of all copies (or required parts) of the Supervisor software, erasure of any parts of the Supervisor software remaining in working storage, verification of erasure of the Supervisor, disconnection of remote communication circuits, and physical securing of the power controls.

4.2 Unscheduled shutdown

An unscheduled shutdown must initiate procedures for immediate surveillance and recording of all indicators .to help ascertain what happened; any needed emergency actions in case of fire, water hazard, etc.; special surveillance or physical protection measures to guarantee that no demountable items are removed; immediate notification of the System Security Officer; and special security controls (for example, protecting all printouts, including those at terminals, in accordance with protection rules for the highest classification handled in the system until the situation can be resolved).

4.3 Restart after unscheduled shutdown

If a trouble condition has caused the system to shut down, it is necessary that there be procedures to handle restart, including the loading of a new, certified copy of the Supervisor software, clearing the internal state of the equipment in order to clean up memory untidiness resulting from the shutdown, verifying correct loading of the Supervisor, validating security controls and security parameters, and certifying the system security status by the System Security Officer.

4.4 File control

File control procedures include those for identifying the cognizant agency of each file, scheduling changes for files, modifying access restrictions of files, giving operators access to demountable files, moving files into and out of the computing area, pre-operator handling of files (including mounting and demounting of tapes and discs), and sanitization of files.

4.5 Control of magnetic tapes and discs

These procedures must account for and control the circulation and storage of tapes and discs; their use, reuse, and sanitization; and their classification markings and entrance to and release from the area.

4.6 Control of paper-based media

Procedures for punchcards, forms, paper-tape, and printouts must cover their accountability, classification marking, storage, and entrance to and release from the area. Additionally, manuals, guides, and various system documents must be covered.

4.7 Personnel control

Personnel control procedures include measures for verifying clearances and special-access authorization for personnel entry to each area of the system, visual surveillance of operating and maintenance areas, and logging and escorting of uncleared visitors. The reporting of suspicious behavior and security infractions is included among the personnel control procedures.

4.8 Terminal control

Various procedures are required with respect to the operation of remote terminals. These include provisions for logging user entry to the terminal area, removal of hardcopy, proper marking of hardcopy not marked by the system, clearing of displays, and securing as required during orderly shutdown.

4.9 Security parameter control

Procedures must be provided for authorizing security parameters to be entered into the system; for verifying correct entry; for changing them on the basis of shift, day of the week, etc.; for receiving and processing requests to modify them; and for actions to be taken in case of a system emergency or an external crisis.

4.10 Software control

These include procedures for rigid control and protection of certified copies of the Supervisor and other software bearing on system security or threat to the system, for loading the Supervisor, for making changes to it, and for verifying the changes.

4.11 Maintenance

All maintenance to be performed on hardware or software must be covered by appropriate procedures, including measures for surveillance of maintenance personnel by properly cleared personnel, for verifying with the System Administrator any adjustments made to the system's configuration, and for manually logging all changes and adjustments made or errors discovered

4.12 Certification

Certification procedures should embrace various personnel responsibilities, tests and inspections to be performed and their conduct, the responsibilities of the System Security Officer, etc.

4.13 User aids

The production, distribution, and document control of manuals, guides, job procedure write-ups, etc., must be covered by appropriate procedures; there must be approved ways of conducting personnel training.

4.14 Change of mode

These procedures include the provision of checklists for actions required in changing mode, removal and storage of paper media and demountable files, physical and electronic surveillance of the machine area, purging of printers by running out the paper, purging of punchcard equipment by running out cards, removal or erasure of Supervisor software from the previous mode and proper verification thereof, loading of the Supervisor for the new mode and proper verification thereof, clearing of all storage devices so that residual information from the previous mode does not carry forward, removal of print ribbons from printers and terminal typewriters for storage or destruction, mounting of files for the new mode, and certification of the security status of the new mode.

4.15 Assurance of security control

Security control assurance includes procedures for reporting anomalous behavior of the system or security infractions; for monitoring security controls, including those on communications; for assuring continuity of security control; for devolution of responsibility in case of personnel nonavailability; and for auditing user and system behavior.

5 Conclusion

In the present paper, we present an evaluation through definitions respecting the way they were defined as a groupof the role of management and policy issues in computer security that proposes Rand Report

R-609 within organization. Important to note that an effective and agreed set of management and administrative controls and procedures governing the information's stream to and from the computer system must be added to overall policy guidance and to technical methods.

REFERENCES

[1] Willis Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." Published for the Office of the Secretary of Defense Edited by Willis H. Ware. R-609-1. Reissued October 1979.

[2] Roberts, Larry. "Program Plan for the ARPANET." 8 February 2007 www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.

[3] Schell, Roger R., Downey, Peter J., and Popek, Gerald J. Preliminary Notes on theDesign of Secure Military Computer System. January 1973. File, MCI-73-1, ESD/AFSC, Hanscom AFB, Bedford, MA 01731.

[4] Bisbey, Richard, Jr., and Hollingsworth, Dennis. Protection Analysis: Final Report.May 1978. Final report, ISI/SR-78-13, USC/Information Sciences Institute, Marina DelRey, CA 90291.

[5] Grampp, F. T., and Morris, R. H. "UNIX Operating System Security." AT&T BellLaboratories Technical Journal 63, no. 8 (1984): 1649–1672.

[6] Peter Salus. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. 19November 1998. Accessed 26 March 2007 from www.nluug.nl/events/sane98/after-math/salus.html.