A Study on the Network Isolation Security Requirements for e-Taiwan

Kwo-Jean Farn[a, b, *], Shu-Kuo Lin[a], Chi-Chun Lo[a]
a Institute of Information Management, National Chiao-Tung University,
No. 1001, Ta Hsueh Road, Hsinchu 300, Taiwan, R.O.C.
b Taipei EC/EDI Committee Member
* Corresponding Author: Tel: 886-3-5712301; Fax: 886-3-5723792

Abstract: Network isolation has become the last line of defense in the cyberspace information security. Cyberspace strives hard to strike the balance between information interchange and the implementation of network isolation techniques. This paper investigates the summary of network physical isolation techniques for e-Taiwan and comes up with the framework of Net GAP physically separated equipments. Besides, we further explore the extended family of the physically separated equipments security assurance requirements.

Key words: Evaluation Assurance Level (EAL), Network Isolation, Security Assurance Requirement (SAR), Target of Evaluation (TOE), TOE Security Functionality (TSF)

1. Introduction

On October 21, 2004, the Executive Yuan of Taiwan proclaimed "the concrete solutions that the governmental institutions deal with the emergency of information security incidents," requiring the governmental institutions should store their top-secret or secret confidential documents, data, and files in the way of data encryption. Apart from the essential interconnection, they should take the protective measures like physical isolation in order to prevent from being invaded, destroyed, interpolated, deleted, or unauthorized accessed. These control measures lay emphasis both on the management and on the operation so as to anticipate the gradual reduction of the information security risk in e-Taiwan [1].

Owing to the rapid development of the Internet along with the problems of network attack, from 1990 to 2000, some countries such as the U.S., Russia, Israel, China, South Korea and Australia begin to study the techniques of network isolation. They hope to solve the safety problems of information interchange and resource sharing from network connection. The existing products can be roughly divided into two types - Simple physical isolation technique and Net GAP physical isolation technique. In the following chapter, they are called two types of Net GAP and they are stated as follows.

1.1 Simple physical isolation technique

Simple physical isolation technique can be usually divided into two parts -terminal equipment and network equipment. The isolation technique of terminal equipment can be done with the help of storage devices and isolation card that divide secure area, insecure area and interchange area in the hard disks. Then the control logic of the isolation card makes secure area and insecure area exclusive in order to attain the effect of information isolation. The principle of the isolation technique of network equipment is similar to that of terminal isolation equipment. We should divide network into secure network and insecure network, and apply isolation card, secure hub, and terminal store equipment so as to achieve the effect of information isolation.

1.2 Net GAP physical isolation technique

The main principle of Net GAP isolation technique is through two independent information systems that respectively are linked with secure and insecure network. Net GAP equipment is used between these two systems and guarantees to stop the connection with insecure network when the storage devices are connected with secure network. Then simple physical isolation technique and protocol translation method can be used to get rid of Malicious Code and its conducting capability, and vice versa in order to achieve the target of network isolation and information interchange.

Based on this, this paper is going to discuss the digital data interchange principle of Net GAP isolation technique in Section 2 and Section 3 [2~4]. Besides, we discuss the rough framework and the security requirements of Net GAP products [5~9]. In Section 4, we explore the extension of Security

Target (ST) that follows Common Criteria (CC), and concluded this paper in Section 5.

2. Brief introduction of digital data interchange in Net GAP isolation technique

The network interconnection is on the basis of communications protocol. The direct way of its isolation technique is to separate all protocols in the Physical Layer (Layer 1), Data Link Layer (Layer 2), Network Layer (Layer 3), etc, and Application Layer (Layer 7) in the communications protocol. The recent framework of digit interchange techniques that carries out Net GAP isolation is shown in Fig.1. The internet sends the data through control workstation to store media and after separation the data are sent from store media via control workstation to intranet. After separation, it is reversed into the state of Fig.1 [2], and vice versa.

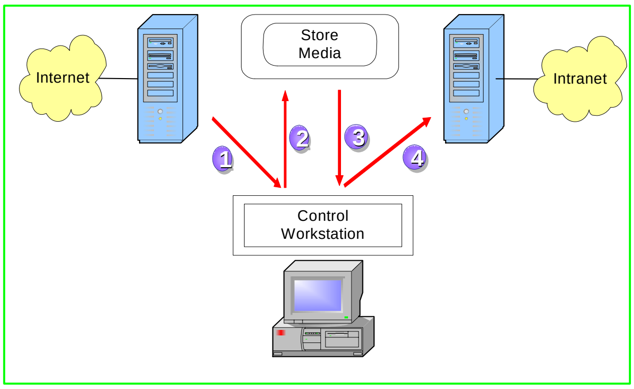


Fig.1: Methodology of network physical isolation technique

Its principle is illustrated as follows:

a) To interchange information content via store media.

b) Dual-protocols translated between control workstation and store media.

c) Physical Layer: It had better guarantee 100% disconnections between internet server and intranet host at any time and their storage devices can interconnect sometimes but can not be simultaneously interconnected. Usually network switched circuit is used to reach this target.

d) Data Link Layer: It had better guarantee to interchange data or deliver information without applying any communications protocol, such as applying Small Computer System Interface (SCSI).

e) Application Layer: It had better guarantee to reestablish the proxy application protocol after the stripping of application protocol.

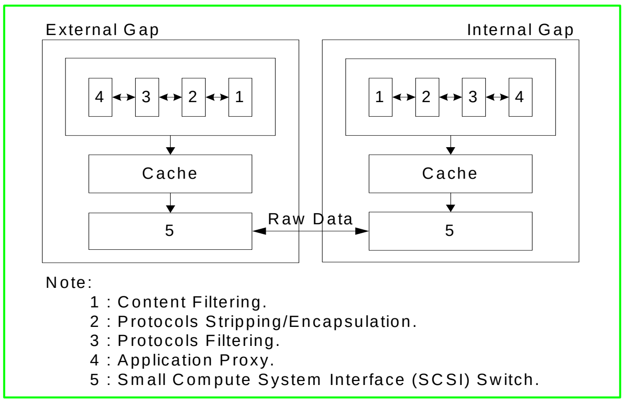
f) One-way connection: The service policy of Net GAP that conducts one-way information flow in the intranet. In other words, intranet can access the information of internet but internet cannot access the information in intranet.

g) Security mechanisms: Generally speaking, Net GAP adopts both content filtering and intrusion detection technique simultaneously in order to get rid of the potential attack from internet. In addition, there are multiple measures to prevent from revealing secrets and the common approaches include:

- Identification and Authentication,
- Format control,
- Network Address Translation (NAT),
- Key words filter (e.g., the information access from internet to intranet is not allowed to use the commands such as GET and POST, etc.),
- Prevention of revealing secrets of interfaces and ports,
- Prevention of revealing secrets of the storage equipment such as printers, etc.,
- Security management of document (e.g., Microsoft Word, etc.), and
- Alert and audit management of operation status.

3. Brief introduction of the Net GAP equipment framework

Network isolation technique means two or more than two networks of information systems are separated but can securely interchange information if necessary. As a Net GAP product, its framework is indicated in Fig.2. In order to promote the security, the sharing data storage devices that conduct digital data interchange between internet server and intranet host should be divided and then connected through Small Compute System Interface (SCSI) [2~6].



Note:
1 : Content Filtering.
2 : Protocols Stripping/Encapsulation.
3 : Protocols Filtering.
4 : Application Proxy.
5 : Small Compute System Interface (SCSI) Switch.

Fig.2: Network physical isolation framework

On the basis of the existing multiple functions of network security defense systems and file protection security management systems of a Net GAP [5~7], the different services (e.g., e-mail, www) can be categorized, and the design of Net GAP protocol translation and reverse translation can be conducted in the external and internal gap respectively as shown in Fig.2. The implementation, for the purpose of Table 1, fits the miniature form of Net GAP [5~9].

Table 1: The basic security requirements of cyberspace physical isolation equipment

1 Information interchange:

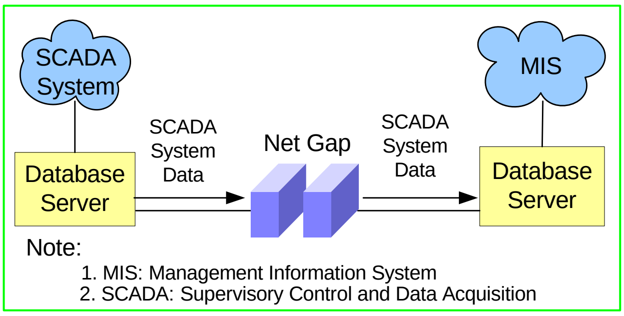
- Intranet is not connected with internet.
- Only intranet has the right to ask to interchange information with internet.
- Intranet can interchange information with internet through physical isolation equipment.

2 Malicious Code:

- As intranet interchange information with internet, physical isolation equipment implements verification, and sends information content to intranet after the validation of no Malicious Code.
- The verification and validation of physical isolation equipment needs to pass the formal analysis.

Owing to protocol stripping/encapsulation module of inbound gap and outbound gap in Net GAP, the protocol that internet delivers information will be first transferred into reserved protocol of Net GAP. Then the information content after protocol stripping can be seen as Raw Data, which is delivered to inner Net Gap through SCSI. Inner gap returns information content of Raw Data to original status according to the deterioration of protocol translation and encapsulates it with the application protocol of intranet. Theoretically, it can satisfy the purpose of information equipment of intranet avoiding the threat of Malicious Code attack.

Net GAP not only often deploys between the Internet and the Intranet to prevent the threat of hacker intrusion, but also deploys Net GAP in the secure Supervisory Control and Data Acquisition (SCADA) System and the Management Information System (MIS) as shown in Fig.3, so as to reduce the risk that SCADA System takes place by man-made.



Note:
1. MIS: Management Information System
2. SCADA: Supervisory Control and Data Acquisition

Fig.3: Network isolation deployment of SCADA and MIS system

The deployment of Net GAP is for the sake of security. Take Fig.4 for example, gateway consists of Net GAP, Intrusion Detection System (IDS), Router, and Firewall. The traffic of one gateway is outbound, while the traffic of the other gateway is inbound. In other words, Malware can attack at most the outer Net GAP. However, with the proper segregation of responsibility, the inbound/outbound traffic go through different gateway to reduce the risk of "Trojan Code" to the acceptable level.

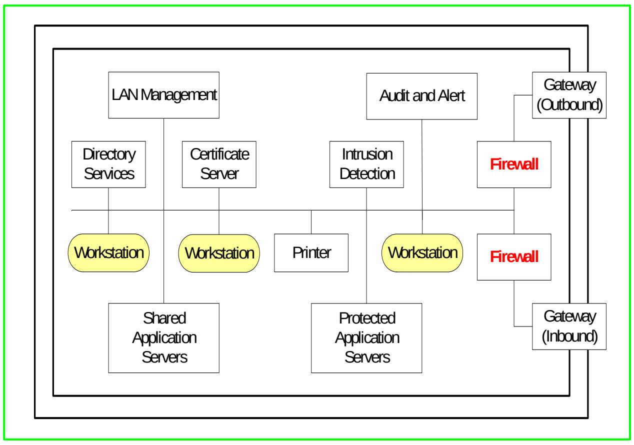


Fig.4: Illustration of Intranet Net GAP deployment

4. Extended Security Assurance Requirements (SARs) in Net GAP products

The object of CC is to provide the paradigm of information technique security evaluation, and reliable protection [9]. CC requires to broaden the width, depth, and strength of information technique security evaluation so as to test the security effectiveness of information security product or system. Generally speaking, Protection Profile (PP) / ST offer customer/evaluator with one way of collating a specific security set. Therefore, customer/evaluator can much more easily go on verification and validation to these requests. Based on the existing basis of Net GAP product [4~8], this Section discusses the essential extension of threat, security objectives and requirements of sensitive file access control in Net GAP as follows [8]:

4.1 Denial of the threat from external attack by Malicious Code and the Security Objectives:

a) T.Denial_Malware (Extended Threat): Known and potential Malicious Code.

b) O.Denial_Malware (Extended Security Objectives): The Security Function of Target of Evaluation (TOE) must be designed and implemented to ensure the capability of denying the known and potential Malicious Code.

4.2 Rationale:

a) Security Objectives for IT Environment Rationale:
Denial_Malware: It has designed and implements the capability to deny the known and potential Malicious Code to anti-attack T.Denial_Malware.

b) Security Functional Requirements Rationale:
Denial_Malware: FDP_ACC.2, FDP_IFC.2 and FDP_IFF.5 make sure that TSF is thoroughly protected to execute the function of Denial of Malicious Code.

4.3 Extension of security assurance requirements:

Net GAP should follow the required implementation of Evaluation Assurance Level (EAL) 4. However, the security assurance class of vulnerability Assessment needs to extend so-called Denial of Malicious Code as shown in Fig.5. The AVA_DOM Family and its two components are stated as follows:

AVA_DOM
AVA_DOM.1
AVA_DOM.2

Fig.5: AVA_DOM and its component

a) Denial of Malicious Code (AVA_DOM)

- Objectives:
  The concern of this family is the execution of Malicious Code analysis to deny the existence of usable code and potential capability.
  The assurance requirements illustrate the access of usable code. The potential threat has been taken into consideration in security policy function.
- Component leveling:
  The components in this family are leveled on the basis increasing extent in scope of the analysis of Denial of Malicious Code.
- Application notes:
  If the security objectives of ST contain no requirement of Denial of Malicious Code; then the family of Assurance Requirements is no longer applicable, because this family can only be used for the security objectives of Denial of Malicious Code.

b) AVA_DOM.1 Analysis of systematic Malicious Code

- Objectives:
  By means of the analysis of systematic Malicious Code, to deny the execution capability of Malware and its potential capability
- Application notes:
  Developers need to deny Malicious Code in an organized and repeatable way, with a systematic way to implement the analysis of Malicious Code.
- Dependencies:
  - ✧ ADV_FSP.2: Fully defined external interfaces.
  - ✧ ADV_HLD.2: Security enforcing high-level design.
  - ✧ ADV_IMP.3: Structured implementation of the TSF.
  - ✧ ADV_LLD.1: Descriptive low-level design.
  - ✧ AGD_ADM.1: Administrator guidance.
  - ✧ AGD_USR.1: User guidance.
- Developer action elements:
  - ✧ AVA_DOM.1.1D: With regard to every control policy of information system, developers should execute the analysis of Malicious Code.
  - ✧ AVA_DOM.1.2D: Developers should have analysis document of convert channels.
- Content and presentation of evidence elements:
  - ✧ AVA_DOM.1.1C: This analysis document should describe the procedure of Denial of Malicious Code and the essential information of the execution of Malicious Code.
  - ✧ AVA_DOM.1.2C: This analysis document should explain the method and its principle of Denial of Malware.
  - ✧ AVA_DOM.1.3C: This analysis document should provide evidence to prove the Denial of Malware is a systematic way.
- Evaluator action elements:
  - ✧ AVA_DOM.1.1E: Evaluator should validate all the provided information can correspond to all the requirements of the content and performance of the evidence.
  - ✧ AVA_DOM.1.2E: Evaluator should validate the analysis results of Malicious Code can represent the TOE and correspond its functional requirements.

  - ✧ AVA_DOM.1.3E: Evaluator can optionally validate the Denial of Malicious Code by means of tests.

c) AVA_DOM.2 Analysis of Brute-Force Malicious Code

- ■ Objectives:
  By means of the analysis of Brute-Force Malicious Code, to denial the execution of Denial_of_Malware and its potential capability.
- ■ Application notes:
  The execution of Malicious Code analysis in a Brute-Force manner needs to provide extra evidence to verify the plan which Denial of Malware follows is sufficient in order to ensure all the possible means to deny Malware and its potential capability.
- ■ Dependencies:
  - ✧ ADV_FSP.3: Semiformal functional specification.
  - ✧ ADV_HLD.2: Security enforcing high-level design.
  - ✧ ADV_IMP.3: Structured implementation of the TSF.
  - ✧ ADV_LLD.2: Semiformal low-level design.
  - ✧ AGD_ADM.1: Administrator guidance.
  - ✧ AGD_USR.1: User guidance.
- ■ Developer action elements
  - ✧ AVA_DOM.1.1D: With regard to every control policy of traffic, developers should execute the analysis of Malicious Code.
  - ✧ AVA_DOM.1.2D: Developers should provide analysis document of convert channels.
- ■ Content and presentation of evidence elements:
  - ✧ AVA_DOM.1.1C: This analysis document should describe the procedure of Denial of Malicious Code and the essential information of the execution of Malicious Code.
  - ✧ AVA_DOM.1.2C: This analysis document should explain the method and its principle of Denial of Malware.
  - ✧ AVA_DOM.1.3C: This analysis document should provide evidence to prove the Denial of Malware is a systematic way.
- ■ Evaluator action elements:
  - ✧ AVA_DOM.1.1E: Evaluator should validate all the provided information can correspond to all the requirements of the content and performance of the evidence.
  - ✧ AVA_DOM.1.2E: Evaluator should validate the analysis results of Malicious Code can represent the TOE and correspond its functional requirements.
  - ✧ AVA_DOM.1.3E: Evaluator can optionally validate the Denial of Malicious Code by means of tests.

5. Conclusion

This paper investigates the framework of Net Gap and proposes the extendable security assurance requirements. How to improve it to fit the purpose of firmness and convenience is still the issue being developed.

Acknowledgements

The authors would like to express our appreciation to Mr. Tung-Sheng Cheng for his invaluable help.

References:

[1] The Executive Yuan of Republic of China, MOE document No.0930090197, Taipei, Taiwan, October 21, 2004.

[2] Kwo-Jean Farn, *Brief Introduction of Network Isolation Technique*, Internet Security Solutions Taiwan Co., Taipei, Taiwan, 2004.

[3] Whale Communications, *e-Gap® Application Firewall Appliance: A Technical Overview*, 2003.

[4] Kwo-Jean Farn, et al., A Study on Network Physical Isolation Technique, *Proc. of 2005 Workshop of Internet Security Engineering*, Taipei, Taiwan, 2005, pp.133-154.

[5] Internet Security Solutions Taiwan Co., *GuardAngel™ Users' Manual, Version 1.88*, Taipei, Taiwan, 2004.

[6] Internet Security Solutions Taiwan Co., *GuardAngel™ File Protection Security Management System Guideline*, Taipei, Taiwan, 2004.

[7] Internet Security Solutions Taiwan Co., *Development of the Best Effects of Network Service Firewall (December, 2003-November, 2004)*, Final report, Taipei, Taiwan, 2004.

[8] Kwo-Jean Farn, Shu-Kuo Lin, & Kung-Yu Lu, et al., A Study on Evaluating Access Control Secure Technology for Open Source Code Agility Files, *Proc. of 2005 Workshop of Internet Network Security Engineering*, Taipei, Taiwan, 2005, pp.195-235.

[9] ISO, *Information technology - Security techniques - Evaluation criteria for IT security* (all part), ISO/IEC 15408:1999(E), 1999.

[10] Kwo-Jean Farn, et al., A Study on Information Security Standards and Guidelines for Involving Nation Security - Illustration of Mainland e-Government Network Security, *Communications of the Chinese Cryptology and Information Security Association*, Vol.11, No.1, 2005, pp.1-14.