Network Security Improvement with Isolation Implementation Based on ISO-17799 Standard

Yeu-Pong Lai and Jui-Heng Tai

Department of Computer Science and Information Engineering,
Chung Cheng Institute of Technology,
National Defense University, Taoyuan, Taiwan, 33509, R.O.C.
Tel.: 886-3-3805249-212
Fax: 886-3-3894770
{lai,g961201}@ccit.edu.tw

Abstract. In these years, many researchers proposed the way — to isolate the computers with sensitive information from outside attackers or unauthorized users. The Taiwan government has ruled the importance of network isolation in several policies, such as "The Handling Implementation Program of Information Security Emergency Incidents for government departments" and "The Responding Protocol of Notifying Information Security Events in Executive Yuan and its Departments." However, there are few materials available for implementing network isolation. In ISO-17799, there is no implementation guidance for practicing network isolation but auditing network physical isolation. This paper provides the implementation guidance of network isolation with some logical isolation techniques and management polices.

Keywords: Network isolation, Physical and environmental security, Security network control, Segregation in networks, Sensitive system isolation, ISO-17799.

1 Introduction

That becomes more important to prevent secrets from being stolen, since attackers have gradually organized into a union and developed more complex and more devastating attacks in multi-combination styles. Network attacks aim at specific targets.[1] The spend in information security has grown 17% to US$25.7 billion from 2004 to 2005. Expectedly, it may be US$40.7 billion in 2008.[2] Unfortunately, the increasing budgets and labors might not reduce network security events.

In Taiwan, the regulation, "The Practical Plan to Eliminate Crisis Events in Information Security for Departments," announced by Executive Yuan in October 2004, demands departments have to encrypt "the most important" and "important sensitive" documents, data, and files.[3] Intranets should be physically isolated for preventing information from being revealed, modified, or accessed by unauthorized people. The "handling procedure", in the responding procedures, mentions that "Each department should establish an environment for protecting the security of information in communication systems and networks. … Physical isolation may be applied and

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 69–78, 2007.

practiced."[4] The network isolation is one selection to protect these important information and systems in networks.

Network isolation techniques are different from other network security devices, such as firewall, virus wall, and Intrusion Detection System. They consist of two aspects, management procedures and technique equipment, to carry out physical isolation or logical isolation. Physical isolation means that network devices are exactly disconnected to other networks. It should be audited frequently with proper policies and procedures from information security management. Logical isolation allows a connected node in each network system to exchange data. The connections between networks, however, are via these interfaces, "network separate equipment". The equipment switches the connection to one network at a time.

In 1997, Mark Joseph Edward proposed the ways for "Physical Isolation" and "Protocol Isolation".[5] E. NYONI defined and illustrated isolation schemes in many different ways.[6] Faithfully, both schemes, "Physical Isolation" and "Protocol Isolation" expatiated by Mark Joseph Edwards and E. NYON, are not "real" isolation in our views with referring to our national policies. Besides, the company, CISCO, proposed the Network Admission Control (NAC) architecture that is a combination of CTA (Cisco Trust Agent), ACS (Cisco Secure Access Control Server), and network access devices. These devices verify the statuses of hosts in intranet for quarantining those disqualified hosts from others.[7] Microsoft in 2004 presented Network Access Protection (NAP) architecture. That consists of IPSec internal network isolation, VPN remote connection, IEEE802.1X authentication, enforced DHCP, and CM (Connection Manager) to check whether hosts have installed security measures, such as personal firewall, anti-virus system, system vulnerability repairing program, and virus code update program. These, not fitting the requirement of security, would be isolated. In fact, both NAC and NAP are mechanisms for the network access management. They do not achieve the intra-network disconnected.

Section 2 describes the definitions "logical isolation" that satisfies the isolation requirement in our national policies with the property of network disconnection. Section 3 depicts the logical isolation techniques, products, and architecture. The implementation of network isolation in ISO-17799 is then discussed in Section 4. These implementation outlines of logical isolation can be devoted to establishing network security standards for our nation.

2 The Concept of Network Isolation

Differing from the network quarantine by CISCO NAC and Microsoft NAP, in practicing network isolation, the network disconnection mechanisms are required, which can prevent intra-systems from outside attacks. In this section, the definitions of network isolation are provided. Section 2.1 is for the physical isolation. Logical isolation is defined in Section 2.2.

2.1 The Concept of Network Physical Isolation

The physical isolation network implies an independent network without any connection or data transforming with outside services. For implementing two physical isolated