NETWORK SECURITY DEVELOPMENT PROCESS

- A Framework for Teaching Network Security Courses*

T. Andrew Yang, Tuan Anh Nguyen
Univ. of Houston – Clear Lake, Houston, Texas
Contact: (281) 283-3835, yang@UHCL.EDU

ABSTRACT

Teaching *Network Security* course is a challenging task. One of the challenges is that networks have become more complicated and prone to attacks. In response to the challenge, the set of networking and security protocols and mechanisms continue to evolve, increasing the number of security technologies a network engineer needs to master in order to secure a network. This paper describes our experience of applying a network security development model to developing a network security lab. Developing network security is an iterative process, encompassing the analysis of vulnerabilities and threats, construction of policies, design of network architecture, integration plan of control measures, implementation of the design, and the operation and maintenance of a secure network. While *Network Security* has become an increasingly complicated topic to teach, we have learned from experiences the significance of a well-defined network security development process for teaching the development of secure networks.

1. INTRODUCTION

Efforts have been made to design network labs for testing computer and network security principles and practices. Padman, etc. [2], for example, present their design of the ISIS *Lab* as a model of highly reconfigurable laboratory for information security education.

In order to develop a secure networking lab for teaching and research (henceforth, the *Lab*), we decided to adopt a formal network security development process [1]. As illustrated in Figure 1, the model consists of seven steps:

(a) Asset Identification: To identify what should be protected.

(b) Threat Assessment: To determine what you are trying to protect the network from.

(c) Risk Assessment: To determine how likely the threats are. A risk rating between 1 (lowest) and 5 (highest) is assigned to each of the assets with respect to each of the security goals (confidentiality, data integrity, origin integrity, non-repudiability, and availability) [3].

(d) Policy Construction: To construct network security policies, based on the risks.

(e) Network Security Design: To design the network security architecture and the control measures, in order to enforce the defined policies.

(f) Network Security Implementation: To implement the design and integrate the mechanisms.

(g) Audit and Improvement: To review the process continually and make improvement each time a weakness or a threat is found, or when an asset is added or changed.

As shown in Figure 1, the development process is iterative, meaning it is often necessary to revisit an earlier stage in order to rectify the existing requirements, design, or deployment of the network. Our experience has shown that, although the development model is useful in guiding the development process, there still exists in the model room for improvements. In the rest of this paper, we first describe the refined model (Figure 2), and then our experience of using the model in developing the *Lab*. The paper concludes with a summary and possible future work.

2. A REFINED NETWORK SECURITY DEVELOPMENT MODEL

While designing the *Lab* following the 7-step model [1], we came to realize that it was difficult to assess the risks of the identified assets (step C in Figure 1). For most of the assets, the assessments are mainly based on the assessor's subjective evaluation and experiences, hence resulting in somewhat arbitrary assignment of risk ratings. To mitigate this difficulty, we refined the model by assessing the risks based on the *services* provided by the underlying network (step 5 in Figure 2), rather than directly on the assets. There are two reasons why we evaluate services instead of assets:

- First, each service is built upon one or more network assets. Services of a network are the "business" functions of the network. Ultimately, to protect a network is to maintain secure operation of the network services.
- Secondly, evaluating the risks associated with services is more logical than evaluating the risks associated with assets. The "business" goals to be achieved by the services provide guidelines for evaluating the confidentiality, data integrity, origin integrity, non-repudiability, and availability of those services. On the other hand, it is comparatively difficult to evaluate the risks associated with an asset, because a particular network device or server is typically used to support multiple, higher-level services, each of which has its own security requirements and risks.

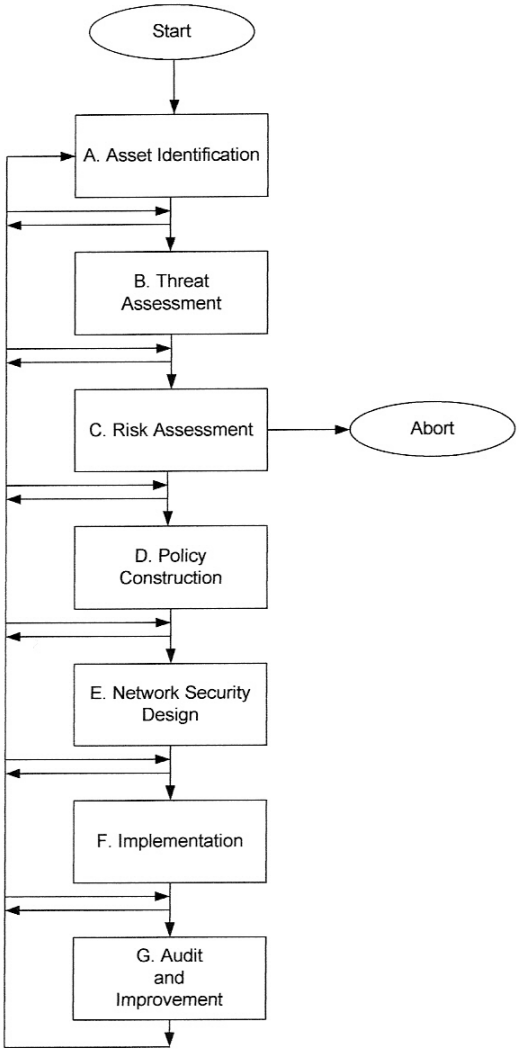

Figure 1: The 7-step model of Network Security Development Process [1]

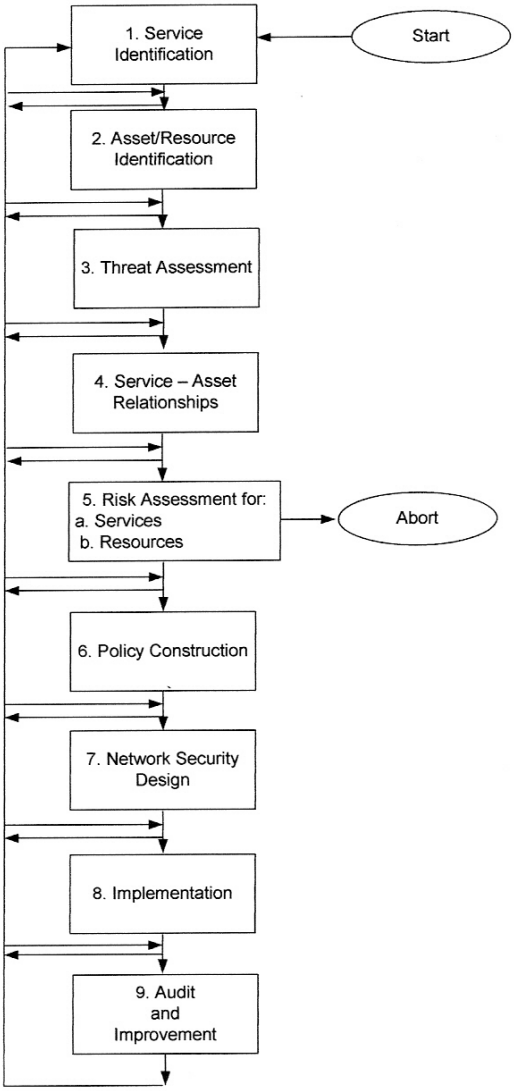

Figure 2: The refined 9-step model of Network Security Development Process

The modifications we made to the original model are illustrated in Figure 2, and the new or modified steps are highlighted below:

Step 1) Service Identification: To identify the services the underlying network should provide and protect.

Step 4) Service-Asset Relationship: To clarify the relationship between network services and network assets. While a service may require the support of multiple assets, an asset, in contrast, may be used to support multiple services. Therefore, there exists a many-to-many relationship between *services* and *assets*.

Table 1 shows the relationships between two sample services (S1 and S2) and some sample assets (A1, A2, A3).

Table 1: Relationship between Services and Assets

Service / Asset	S1	S2
A1	✓	
A2	✓	✓
A3		✓

Note: The check sign (✓) means that the service is supported by the asset.

Step 5) Risk Assessment of Services and Assets: To determine how likely the threats are against the services and the assets.

5.a In step 5a, risks associated with the services are first assessed, based on the "business" goals. Table 2 shows risk ratings of the two sample services, S1 and S2, with respect to the security goals.

Table 2: Rating of Sample Services

Service / Security goal	Confiden-tiality	Data Integrity	Origin Integrity	Availa-bility	Non-repu-diability
S1	5	4	3	2	1
S2	1	2	3	4	5

5.b In this step, given the rated services (from 5a) and the relationships between services and assets (from step 4), risks associated with the assets are inferred. Table 3 is the combined result of Tables 1 and 2. Attention should be given to asset A2, which supports both S1 and S2. In Table 3, the risk rating of A2 take the higher rating between the ratings of S1 and S2, with respect to each of the goals.

Table 3: Rating of Sample Assets

Asset / Security goal	Confiden-tiality	Data Integrity	Origin Integrity	Availa-bility	Non-repu-diability
A1	5	4	3	2	1
A2	5	4	3	4	5
A3	1	2	3	4	5

3. THE REFINED MODEL IN ACTION

In this section, we describe our experience of adopting the refined network security development model.

3.1 Service Identification

For the *Lab*, the following services were identified:

- For ordinary users: Internet and DMZ Web access, FTP access, File storage, Wireless network access, DNS service, WINS service, DHCP service, VPN service (site-to-site and remote), and three-tier client/server framework
- For administrators: In addition to the normal user services, an administrator is granted *telnet* service to remotely access network equipments.

3.2 Asset Identification

The assets range from physical network devices such as routers to intangible network resources like bandwidth, authentication information, privacy of users, etc. In the *Lab*, the assets are classified as follow:

- Network equipments: Cayman ADSL router, Cisco Pix firewall 515a, Cisco Access Control Server, Cisco VPN concentrator 3005, Cisco catalyst switch 3550
- Network servers: DMZ Windows 2003 ftp/web server, Windows 2003 file server, Windows 2003 domain controller server, and Linux servers
- Student workstations: There are 26 workstations in the teaching network, all of which are connected to the resources in the *Lab*.
- Data files: Configuration files and account information of network equipments and servers, and data and account information of student workstations
- Other network resources: Network bandwidth, network connection including Internet connection, wireless coverage, and IP addresses

3.3 Threat Assessment

Every network is faced with ubiquitous internal and external threats. We divide threats into two main groups, *internal* and *external* threats, each containing three categories [1]:

- Unauthorized access to network equipments, servers or information,
- Unauthorized manipulation and alteration of information on the network, and
- Denial of service

3.4 Service–Asset Relationships

Based on the identified services and assets, we then create a table to represent the relationships between assets and services. In Table 4, the *file storage* and the *DMZ FTP access* services are used as examples to illustrate such relationships. A check mark (✓) indicates the given asset is needed to support the service.

Table 4: Sample service-asset relationships

Services / Assets	File storage	DMZ FTP access
Access Point	✓	✓
Cisco Catalyst Switch	✓	✓
Access Control Server	✓	
Domain Control server	✓	
User Account Information	✓	✓
IP address	✓	✓
DNS server	✓	✓

PIX firewall		✓
DMZ web server		✓

3.5 Risk Assessment for Services and Resources

A network service is rated against each of the security goals. In Table 5, we take *file storage* and *DMZ FTP access* as example services. File storage service provides file storage capability, so integrity of these files is important. However, user files are not necessarily available all the time. Short downtime is acceptable during holidays or weekends, for scheduled maintenance. Through a similar procedure, risk ratings of the DMZ FTP access service are also assigned.

Table 5: Risk Rating of sample services

	Confidentiality	Data Integrity	Origin Integrity	Avai*la*-*b*ility	Non-repudiability
File storage	5	4	4	3	2
DMZ FTP	5	5	4	3	3

Ratings for network assets are listed in Table 6. Based on the procedure described in section 2, by combining Tables 4 and 5, the risk rating of each of the assets is assigned.

Table 6: Risk rating of sample assets

	Confiden-tiality	Data Integrity	Origin Integrity	Availa-bility	Non-repudiability
Access Point	5	5	4	3	3
Cisco Catalyst Switch	5	5	4	3	3
Access Control Server	5	4	4	3	2
Domain Control server	5	4	4	3	2
User Account Info	5	5	4	3	3
IP address	5	5	4	3	3
DNS server	5	5	4	3	3
PIX firewall	5	5	4	3	3
DMZ web server	5	5	4	3	3

3.6 Construction of Network Security Policy

Network policy forms a framework to protect services and assets identified in step 1 and 2, against risks discovered in step 3 of the model. According to *RFC2196* [4], a good security policy includes nine elements: Accountability Policy, Acceptable Usage Policy, General Access Policy, Internet Access Policy, DMZ Web server and FTP Server Access Policy, Authentication Policy, Availability Statement, Computer Technology Purchasing Guidelines, Privacy Policy, and Information Technology Systems and Network Maintenance Policy. Due to the limited space, details of the policy documents are not included here. They can be viewed at our web site (http://www.dcsl-uhcl.net/public/experiments.html), which includes up-to-date information about network security implementation, latest network diagrams, the lab components, and the series of experiments we have conducted for designing the *Lab*.

3.7 The Remaining Steps

Once the network security policy is created, the next step is to implement the policy in the form of network security design, which results in the overall network architecture and the detailed integration of control measures. Once the design is available, the next step is its implementation, involving tasks such as laying wires, integrating, configuring, and testing the devices, etc. While implementing the network design, we have encountered several difficulties, mainly due to unforeseen incompletes in the design, resulting in a series of revisions. The current design of the *Lab* can be viewed from our web site.

SUMMARY AND FUTURE WORK

In the paper, we present our experience in applying network security process to the development of the Network Security Lab. The difficulty we encountered in applying this template process and our solution to overcome it are discussed in this paper. We revise the template network security process [1] by adding two new steps into the process and refining an existing step. The revised process was applied to developing the *Lab*.

Developing security for a network is a time-consuming and tedious process. The refined security development process helps to ease the difficulty in developing a secure network, by providing a well-defined framework for the developers to analyze the security requirements, construct the network security policy, design security into the network architecture, implement the design, and be ready for new requirements.

ACKNOWLEDGEMENT

The authors are partially supported by the Institute for Space Systems Operations (ISSO), and the National Science Foundation (DUE 0311592).

REFERENCES

[1] Malik, Saadat. *Network Security: Principles and Practices*. Cisco Press. 2003.

[2] Padman, V., N. Memon, P. Frankl, and G. Naumovich. Design of a Laboratory for Information Security Education. *Proceedings of World Conference on Information Security Education*. 2003.

[3] Bishop, Matt. *Computer Security - Art and Science*. Addison Wesley. 2003.

[4] Fraser, B. *RFC 2196. Site Security Handbook*. 1997. http://www.faqs.org/rfcs/rfc2196.html