Network Security Development Process

T. Andrew Yang
University of Houston – Clear Lake
2700 Bay Area Blvd.
Houston, Texas 77058
(281) 283-3835
yang@uhcl.edu

Tuan Anh Nguyen
University of Houston – Clear Lake
2700 Bay Area Blvd.
Houston, Texas 77058
tuandecember@yahoo.com

Shamima Rahman
University of Houston – Clear Lake
2700 Bay Area Blvd.
Houston, Texas 77058
rahmanshamima@yahoo.com

ABSTRACT

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 stage of a secure network. In the process, it is often necessary to revisit an earlier stage to rectify the requirements, the design, or the deployment. This paper describes our experience of designing and implementing a network as a secure platform for researching, learning, and testing computer security principles and practices, by adopting a network security development model [1]. Starting with a prototype network, we went through the iterative process of the model, and built a production version of the network. Our experiences also enabled us to refine the development model by introducing the notion of *risk assessment of services* into the model.

Categories and Subject Descriptors

C.2.0 [**General**]: *Security and protection*

General Terms

Security, Design

Keywords

Network Security Development

1. INTRODUCTION

Efforts have been made to design network labs for testing computer and network security principles and practices. Padman, etc., for example, present their design of the ISIS lab as a model of highly reconfigurable laboratory for information security education [2]. They emphasize that it is important to build an insulated environment in which students can test the theoretical principles of network security and their analysis in a network testbed.

In one of our previously published papers [3], we emphasize the importance of setting up "real-world" computer security labs without negatively affecting the rest of the campus network. To achieve this overall goal, we have identified five *design goals*: (i) an insulated but connected lab, (ii) an easily configurable lab, (iii) support for Virtual Private Network (VPN), (iv) a sharable and secure lab, and (v) incorporating emerging technology.

We adopted a 'rapid prototyping' approach in designing the initial *edition* of our network. The outcome is a "prototype network" as shown in Figure 1, which represents a simplified corporate network, consisting of a stacked two-layer firewalls, a De-Militarized Zone (DMZ), and a back-end server network. The prototype network connects to the Internet through a DSL subscription, making its Internet connection separate from the campus network.

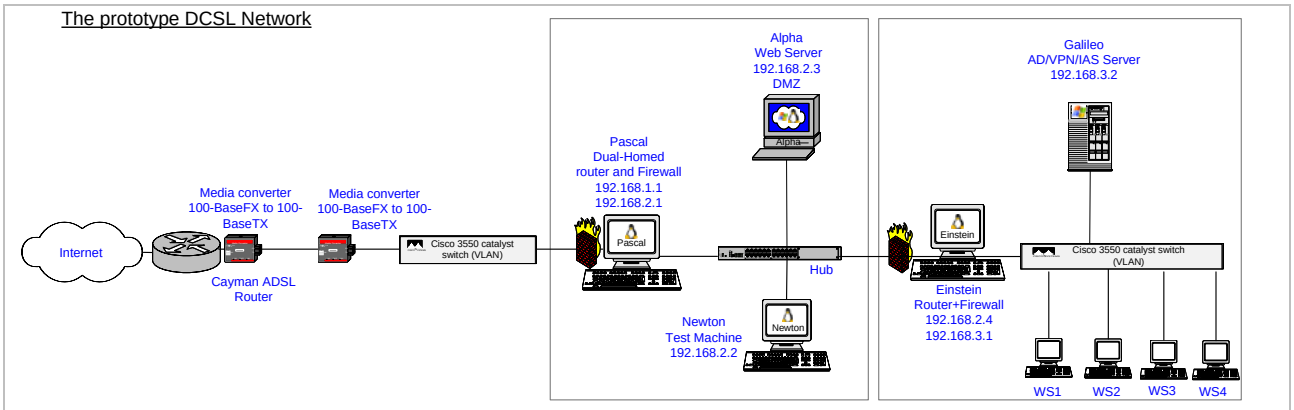

Figure 1: The prototype computer security network

In order to develop the production version of the network (henceforth, the *Lab network*), we decided to adopt a formal network security development process [1]. Illustrated in Figure 2, 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 number between 1 (lowest risk) 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) [4].

(d) Policy Construction: To construct a set of network

security policies, based on the assessed 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 control measures

(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 2, 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, on one hand, the development model is useful in guiding the development process; on the other hand, we have identified room for improvements in the model.

In the rest of this paper, we describe first the refined model (Figure 3), and then our experience of using the model in developing the production edition of the Lab network. The paper concludes with a summary and possible future work.

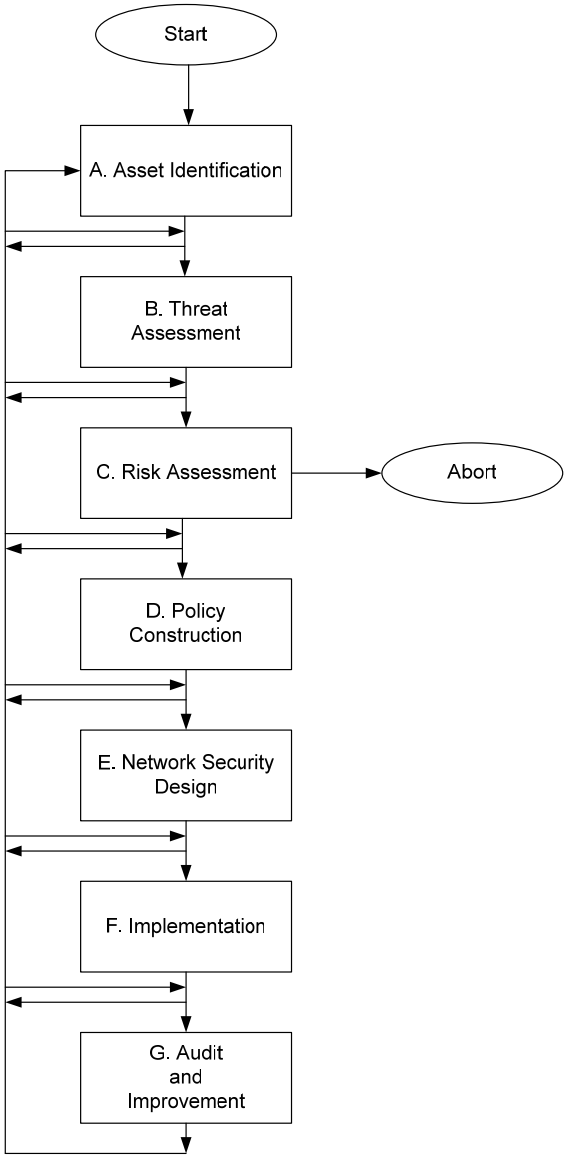

Figure 2: The 7-step model of Network Security Development Process [1]

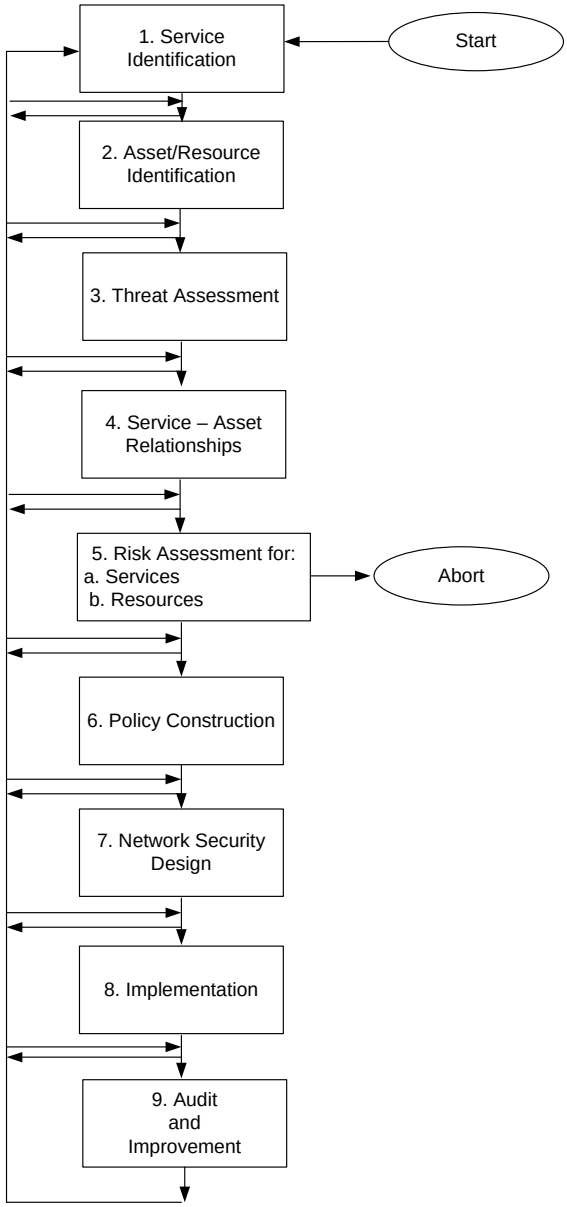

Figure 3: The refined 9-step model of Network Security Development Process

2. A REFINED NETWORK SECURITY DEVELOPMENT MODEL

While designing the Lab network 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 2). 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 3), rather than directly on the assets. There are two reasons why we evaluate services instead of assets:

- First of all, 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.

The modifications we made to the original model are illustrated in Figure 3, and summarized below, with the new or modified steps highlighted.

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

Step 2) Asset Identification: the same

Step 3) Threat Assessment: the same

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 relationship between two sample services (S1 and S2) and some sample assets (A1, A2, A3).

Table 1: Relationship between Services and Assets

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

✓ 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

5a. 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.

5b. 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 security goals.

Table 2: Rating of Sample Services

Service \ Security goal	Confidentiality	Data Integrity	Origin Integrity	Availability	Non-repudiability
S1	5	4	3	2	1
S2	1	2	3	4	5

Table 3: Rating of Sample Assets

Asset \ Security goal	Confidentiality	Data Integrity	Origin Integrity	Availability	Non-repudiability
A1	5	4	3	2	1
A2	*5*	*4*	*3*	*4*	*5*
A3	1	2	3	4	5

Step 6) Policy Construction: the same

Step 7) Network Security Design: the same

Step 8) Network Security Implementation: the same

Step 9) Audit and Improvement: the same

In the next section, we discuss how we have applied the refined model to developing our computer security network.

3. THE REFINED MODEL IN ACTION

In the real world, new system vulnerabilities are constantly discovered, and new attacks are continually invented. Therefore, to keep a network secure is an ongoing process. Adopting the refined network security development model will help to make the challenge of developing a secure network be more manageable.

1) Service Identification

Services provided to users as well as those to the network administrator(s) are identified in this step. For the Lab network, 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.

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 network, 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 include DMZ Windows 2003 ftp/web server, Windows 2003 file server, Windows 2003 domain controller server, and Linux servers.
- Student workstations: There are 30 workstations in the teaching network, all of which are connected to the resources in the Lab network.
- Data files include 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) Threat Assessment

This step is generally straightforward. Every network is faced with ubiquitous internal and external threats. We divide threats into two main groups, *internal* and *external* threats. Each group contains three categories [1]:

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

4) Service–Asset Relationships

Based on the identified services and assets, we then create a table to represent the relationship between assets and services. In Table 4, the *file storage* and the *DMZ FTP access* services are used as examples to illustrate such relationships. As stated in section 2, a check mark (✓) indicates the given asset is needed to support the service.

Table 4: Sample service-asset relationships

Assets \ Services	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		✓

5) Risk Assessment for Services and Resources

A network service is then rated against each of the security goals. As shown in Table 5, we again 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 is also assigned.

Ratings for network assets are listed in Table 6. By combining Tables 4 and 5, each of the assets is assessed and its rating assigned.

Table 5: Risk Rating of sample services

	Confidentiality	Data Integrity	Origin Integrity	Availability	Non-repudiability
File storage	5	4	4	3	2
DMZ FTP access	5	5	4	3	3

Table 6: Risk rating of sample assets

	Confidentiality	Data Integrity	Origin Integrity	Availability	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 Information	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

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 should include nine elements, as listed below:

- 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
- Information Technology Systems and Network Maintenance Policy

Two of these elements, Computer Technology Purchasing Guidelines and Privacy Policy, are not yet defined for the Lab network, and we have added a new policy, the Encryption Policy, to handle the encryption requirements.

- **Accountability Policy**

All users are accountable for their behaviors that result in network security concern. It is the responsibility of all users to be familiar with the guidelines of using the services offered through the network. It is also the user's responsibility to report to the system administrator any inappropriate or malicious activity on the network.

- **Acceptable Usage Policy**

The network is available for use by users anytime of the day and night for the sole purpose of studying and research. Using network resources for any function over and above that is prohibited. The network may be temporarily unavailable for scheduled maintenance or troubleshooting.

- **General Access Policy**

Access is strictly restricted. Access is controlled by assuming that all access is denied unless specifically granted. Access to network resources is given on demand. Information assets are protected by giving access to specific groups and denying access to all others. The changes in access, including increasing or decreasing privileges, need approval from the lab manager.

Wireless user or VPN client must have approval before accessing the resources of the Lab. Once connected, the wireless user or VPN client has equal rights as local users of the network.

It is the responsibility of the remote or VPN users to ensure their equipments are not used by unauthorized person to access the network resources.

- **Internet Access Policy**

There are two types of 'Internet access': (i) type 1 - users using the Internet to access the assets in the Lab network; (ii) type 2 - users using the computers in the network to access the global Internet. Type 1 access should be available all the time for administrative and studying purposes.

Internet connection is used by VPN clients to connect to the Lab network. Internet connection is used by external users to access the DMZ web server in the Lab network. Type 2 access should be available for HTTP traffic of student workstations.

- **DMZ Web server and FTP Server Access Policy**

DMZ web server is open to the public. It has two areas: public area and private area. Normal external users are encouraged to access the web server's public area for advertised information of educational and security services. Access to the private area is restricted to authorized users only. FTP is only for authorized users to upload/download files or to update web pages.

- **Authentication Policy**

All access to the network require authentication and are logged for auditing and accounting purpose. Wireless and VPN users must go through 2 layers of authentication: The user will first be authenticated by the access server, and then by the access controller of the individual resource on the network. Authentication is carried out using Access Control Server, which must be protected against attacks both inside and outside the Lab network.

- **Encryption Policy**

All connections initiated from outside trying to access a network resource must be encrypted. Symmetric encryptions, asymmetric encryptions, or both can be used for this purpose. The encryption algorithms must be strong.

- **Availability Statement**

The network should be ready to use all the time, except due to unexpected system problems or pre-advertised activities, such as update, upgrade, installing new equipments, troubleshooting, implementing new security rules, etc. Availability is one of the critical security goals.

Table 7: Roles and responsibilities in the Lab network

Title	Role	Responsibility
Lab manager	Defining and maintaining overall Lab security policy	- Main contact for changes to security policy - Responsible for final approval of new network implementation that will affect network security - Responsible for cross-faculty communications on security issues - Administrative control over staff directly responsible for network security - Main architect of network design and network security
Network administrator	Managing the daily operation of the Lab network	- Ensure that security is properly enforced in all network implementations - Involved in the design of network and network security - Main contact for all network incidents - Resolve network troubles and attacks
Secondary administrator	Assisting the network administrator	- Take the role of network administrator when main administrator is not available - Involved in all network implementations

- **Information Technology Systems and Network Maintenance Policy**

The Lab network is supervised by the Lab manager. Administrators of the Lab are appointed by the Lab manager,

and manage all the network equipments and services. Remote administration is allowed but the connection must first be authenticated by the access server and then all subsequent communications must be encrypted. All administrative sessions, both inside and outside, must be encrypted.

- **Violations and Security Incident Reporting and Handling Policy**

Documented processes must be established to identify actions to be taken when intrusions or network attacks occur. The following steps need to be set up for incident reporting and handling:

- A process must be in place so the administrator(s) will be informed when attacks happen.
- A process needs to be set up to identify and record all information relevant to the attack, for the purpose of later investigation and prosecution.
- A process must be in place to trace the attack in order to identify the exploited vulnerabilities of the system, so that future attacks may be avoided.

- **Supporting Information**

The Lab manager has ultimate responsibility for the formulation and enforcement of the security policy. Table 7 defines the roles and responsibilities of people involved in managing the Lab network.

7) Network Security Design

Once the network security policy is created, the next step is to implement it in the form of network security design. Figure 4 is the network diagram resulted from the design phase.

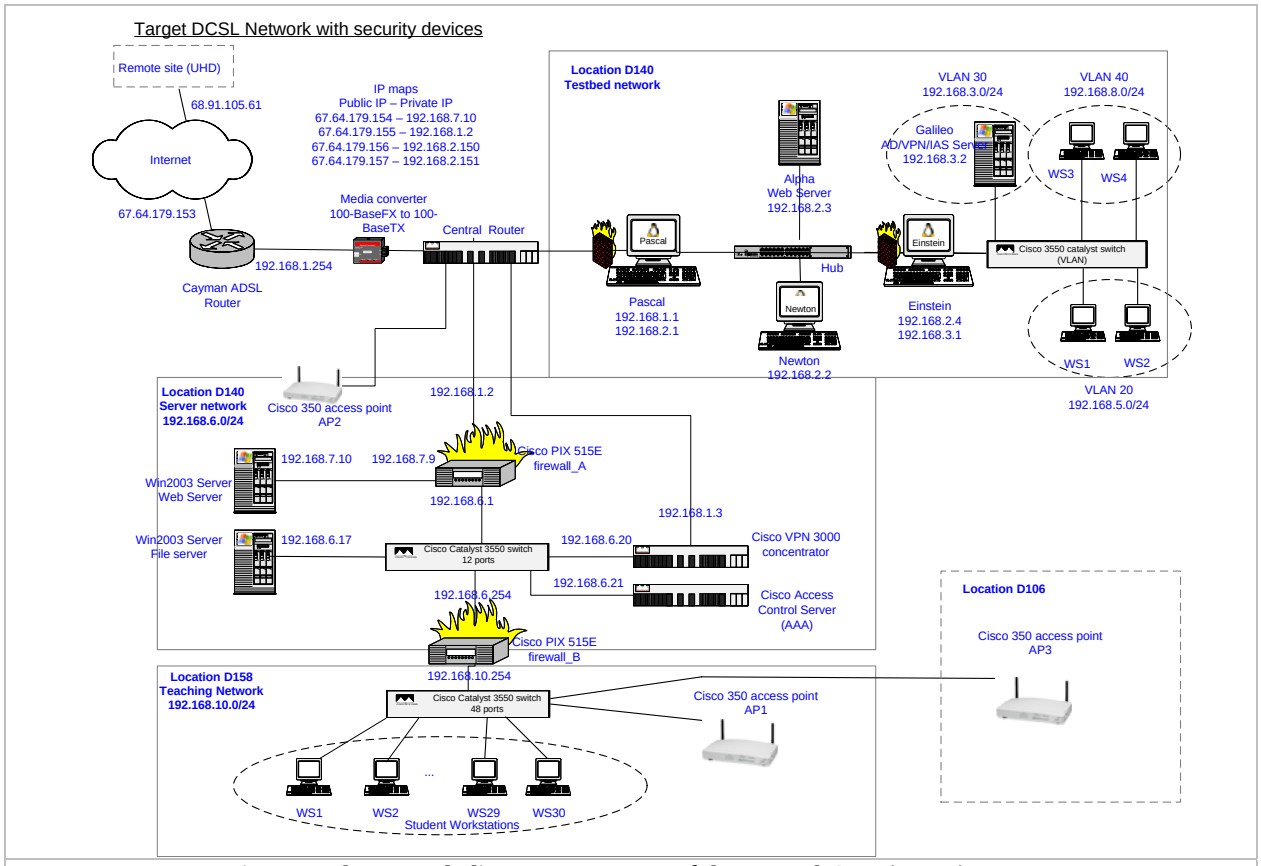

Figure 4: The network diagram as outcome of the *Network Security Design* step

The design phase involves the following elements:

A. Translate the policy into procedures. These procedures are often presented as a set of tasks.

B. Choose appropriate network devices or security appliances to accomplish the tasks.

C. Integrate the chosen devices into the network and make sure they are compatible with the existing network devices.

D. To protect the Lab network from outside attacks, a firewall needs to be placed in between the network and the Internet. This is the first-layer firewall. Another firewall layer is installed between the DMZ and the sub-networks, including the server network, the teaching network, and the testbed network. The firewalls are configured so only specific types of traffic are allowed to move through.

To accomplish this task, Cisco Pix firewalls were used. This model of firewall is suitable for small and medium size network. With three fast Ethernet interfaces, throughput of 188 Mbps, the firewall has enough capability to meet our requirements.

E. Two network servers are needed to manage the whole network. One is the main Domain Controller (DC) and

the other is a Backup Domain Controller (BCD). The user database is duplicated and synchronized between these two servers. These servers run Microsoft Windows 2003 Enterprise Edition operating system.

F. An access control server is needed to provide central authentication for the whole network. The chosen access server is Cisco 1111 Access Control Server. It supports many Extensible Authentication Protocol types, such as EAP-FAST, EAP-TLS and Protected EAP. The access server can work together with Microsoft Windows User Database to support authentication service.

A comprehensive user database is needed to store information of all network users. This database also needs to be backed up for high availability.

G. Any remote access to the network require a VPN connection. The remote user must authenticate with the access control server. A Cisco VPN concentrator is used to support both remote access and site-to-site connection. It supports almost all of the current tunneling protocols and encryption algorithms, such as PPTP, LSTP, IPSec, L2TP over IPSec, AES, DES, 3DES, etc.

H. Wireless users must be authenticated before connecting to the network. For wireless connections, we chose Linksys wireless access points, which support IEEE 802.11g standard and various security modes, such as WEP, WPA, and WPA radius.

8) Network Security Implementation

Once the overall network architecture (Figure 4) and the detailed design are available, the next step is to implement the design. Implementing network security involves tasks such as laying wires, integrating, configuring, and testing the devices, etc.

In implementing the network design, we have encountered several difficulties, mainly due to unforeseen incompletes in the design. Figure 5 represents the current design of the Lab network after the initial design was revised due to the newly incorporated solutions.

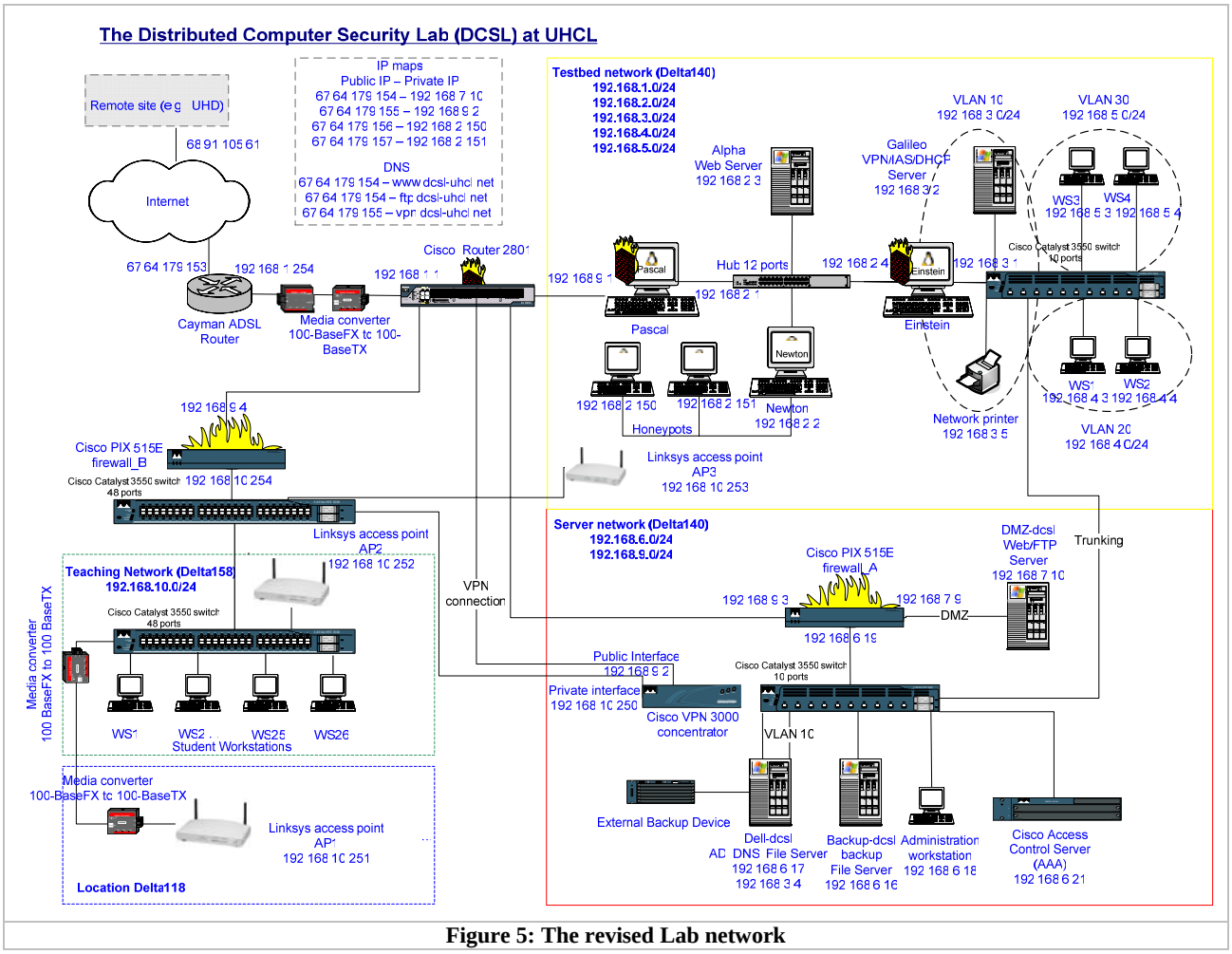

Figure 5: The revised Lab network

The difficulties we encountered and their respective solutions are described below:

A. We realized that a new firewall layer should be installed between the boundaries of sub-networks. Since the Cayman router does not provide this capability, our solution was to add a central router (see Figure 4) with switching and routing features as well as security firewall feature. We chose Cisco router 2801 with Advanced Security K9 Internet Operating System to achieve that goal.

B. The teaching network is behind two layers of firewalls, so

it has higher security level than that of the server network. That caused configuration problem when we tried to add Internet connection to the teaching network. The traffic coming in from the Internet (destined to the teaching network) cannot go through the server network. Our solution was to disconnect the teaching network from the central switch of the sever network and re-connect it to the central router (Figure 5).

A side effect of this solution is that it turns the server network into a one-layer firewall model. To maintain the consistency between the network design, which requires a two-layer firewall model, and the current implementation, we need to either add one more firewall layer into the server network or to revise the network design.

C. Another difficulty is that several connection ports such as DNS, Net-BIOS, RPC have to be open in order to allow the synchronization traffic. This will cause a big hole in the firewall of the server network, hence not a desirable solution. We decided to create trunking connection between the old DC server in the testbed network and the new DC server in the server network. In this way, the server in the server network has become the new DC of the Lab network, and the old DC server (in the testbed network) has become a BDC server.

9) Audit and Improvement

Security of the Lab network must be regularly revised or improved, especially when a security breach is discovered or a new security requirement is needed.

While web applications were deployed on the Lab network, new security requirements emerged. We need an internal certificate service system to support public key encryption/decryption. Certificates need to be created for the following purposes:

i. Certificate for the Access Control Server, in order to use PEAP authentication method

ii. Certificate for the Internet Information Service, to provide web Secure Socket Layer (SSL) service for password change function

iii. Certificate for secure connection between web server and database server

To provide public key encryption service, an internal Certificate Service Authorization system is necessary. Thus, we revisited the *network security design* step and added the new item into the design. This system will handle all certificate requests and certificate authentication. We chose to use Microsoft Windows Certification Authority (CA). It is a free service integrated in Windows 2003 server. That is Microsoft's security solution for Public Key Infrastructure (PKI) deployment in enterprise network.

For implementation, we installed the Enterprise Root CA in the BDC server, and an Enterprise subordinate CA in the DC server. Every certificate request to a CA will be carried out through web interface. The certificates will be automatically deployed to users or computers.

4. SUMMARY AND FUTURE WORK

In the paper, we present our experience in applying network security process to the development of the Lab network. 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 modifying an existing step. The revised process is then applied to the development of the Lab network. The details of the Lab network security development can be viewed at http://www.dcsl-uhcl.net/public/experiments.html.

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.

5. ACKNOWLEDGMENTS

This work is partially supported by the National Science Foundation (Grant DUE-0311592), and UHCL Faculty Research and Support Fund (No. 859), and a grant awarded by the Institute for Space Systems Operations (ISSO 2004 Yang).

6. 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] Yang, T. Andrew, Kwok-Bun Yue, Morris Liaw, etc. Design of a Distributed Computer Security Lab. *Journal of Computing Sciences in Colleges. 20(1).* 2004.

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

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