

PRACTICAL SECURITY

Implementing Security Education at a Small Community College

Corrinne Sande

Whatcom Community College

Abstract: This paper discusses modifying an existing two-year degree to include an information security track. In addition, it discusses various efforts made to bring information security awareness to the local community and to underserved populations.

Key words: IT Security, Security Education, Community College

1. INTRODUCTION

Small community colleges are typically lacking in resources, and introducing an information security specialty into an existing degree can be challenging.

At Whatcom Community College, several changes have been made to the Computer Information Systems (CIS) program. Information security topics have been incorporated into existing courses and new courses are being developed for an Information Security specialty. Information assurance topics have also been incorporated into presentations made to potential new students and to members of the community. We are raising community awareness of security issues by integrating the topic into speaking engagements with various underserved groups. The goal is to reinforce the need for information security at all levels in the community.

2. EXISTING INFORMATION ASSURANCE CURRICULUM

At the beginning of the 2003-2004 academic year, Whatcom had one security course: Network Security I. This course addressed the CompTia Security + objectives (CompTIA, 2004) and a student had to be near the end of their degree in order to meet all the prerequisites. Only students in certain tracks in the CIS degree were required to take the security course. As a result, some students were graduating with CIS degrees with very little exposure to security topics.

After attending the WECS 5 conference, one of my objectives was to gain practical experience in the field, with the idea that this experience would be used to write a case study for the students in Network Security I. In fall of 2003, I spent several weeks working at a small non-profit organization. The purpose of the project was to do a security audit and suggest changes that might be made to their network. The project included setting up their server for them, implementing

active directory, developing a security policy, and doing a presentation to employees on password complexity requirements. Out of this project I developed a case study for students to use in the Network Security I class.

2.1 The Case Study

I spent approximately 40 hours at this agency, and the result is a case study that can be done on paper. The students are given a handout listing the initial conditions of the organization, including a network map. The case study is intended to be done over the course of the quarter, so as the students learn new aspects of information assurance, they can apply this to the case study. Initially the students are told of the current situation:

There are 17 computers at the site, 14 PCs and 3 Macintoshes. Machines are networked together in a peer-to-peer configuration. All hard drives are fully shared (except for the accounting machine). Three PCs are on wireless connections. Security consists of a logon to the local machine. From there a user can access any other hard drive on the network. Passwords have been found on sticky notes and it is a common practice for users to logon under other user's accounts. The data on these machines has never been backed up, and one machine has over 2500 documents that all users in the organization access. In addition, the organization has a large database of names, addresses and other information, which has also never been backed up. The organization recently purchased a server with Windows 2003 on it, but it is set up as a workgroup server and functions as an additional host machine on the network.

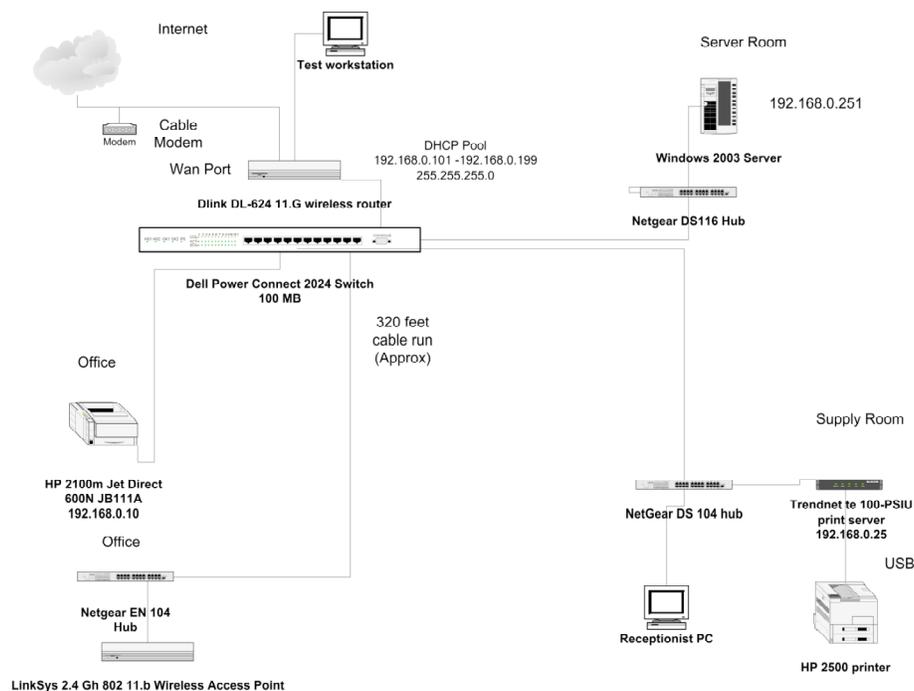


Figure 1. Workgroup Server with Fat file system. Mix of 98, XP home, and XP professional machines. Peer to Peer file sharing. Bottlenecks at printer. Duplicate ip addresses on devices, network performance poor. Wide open wireless access, no security policy, disaster recovery plan, or backup of critical files.

The list of problems with the network is about 2 pages long. For their first assignment, the students are asked to identify the network security threats and list them under their appropriate category (technology weakness, configuration weakness, policy weakness). They are then asked to explain why this is a weakness and how it can be corrected.

The students are then asked to design a plan for securing the network, addressing the following in the plan:

1. Physical security
2. Configurations
3. Policies
4. Documentation
5. Monitoring

The students are expected to develop a security policy for the organization and are directed to sites such as the SANS Institute (SANS, 2004) to look at sample policies. They also are expected to produce a network map in Microsoft Visio showing the changes made to the network. The students are to present their plan to the class at the end of the quarter.

Part of the project includes developing a disaster recovery plan for the organization and thoroughly documenting every step needed to recover from a major catastrophe, including restoring from backup tapes when the server has been completely destroyed.

Throughout the case study emphasis is placed on the human factor in security, which is commonly overlooked. For this particular organization, politics played a large role in the lack of security. The technical support for the organization was handled by a contractor who would come in and fix problems as they arose, but there was no overall management of the information technology resources. Individuals were used to bringing in their own devices from home and connecting to the network. The problem was compounded by the fact that this agency had a large public area. It had wide-open wireless access, which I was able to demonstrate to management by accessing their network from the middle of their public area, using my laptop and wireless network card.

The case study gives the instructor the opportunity to address several aspects of information security in a real world situation, and it was a useful addition to the information security curriculum at Whatcom. I have used it to illustrate concepts in my networking classes and will use the completed project in next years Network Security I course.

3. THE BELLINGHAM COMMUNITY

I addressed several Turning Point Classes at Whatcom Community College during the year. These are classes for displaced homemakers who are returning to work. The purpose of my presentation is to encourage these women to consider a career in computer information systems. Since most of the women are also parents, I integrated basic security topics into the presentation, such as what a virus is, what dangers lurk on the Internet, and keeping their kids safe.

I also spoke at three sessions at the Road Less Traveled in Bellingham Washington. This is a conference that introduces women to nontraditional careers. At these speaking engagements I emphasized that information security is a growing field and that women looking for a career might want to consider this. I illustrated this by bringing up the CISR site (The Center For Information Security Studies and Research, 2004), The Internet Storm Center (Internet Storm Center, 2004) and some other sites to demonstrate that cyber security has become increasingly important as the Internet grows.

Whatcom Community College recently received a small grant to recruit people into nontraditional careers. Part of this grant included recruiting high school girls into the computer field. As part of this grant I developed a presentation to be given at the high schools. I included information assurance as one of the career possibilities for young women to consider.

Whatcom Community College also received a grant from the United States Department of Education to establish a center for border security. Part of this grant will include introducing a forensics class into the CIS program next year. We also have discussed including a cyber security component in training provided to first responders in the community.

4. CHANGES TO THE CURRICULUM

The Department of Education grant also will be used to develop an Information Security specialty within the Computer Information Systems two-year degree. The CIS department is very small and is comprised of two full time faculty and one part time faculty person. We developed three new courses to add to our existing CIS degree.

The core courses (all students in the CIS program have to take these) will include a new course:

Introduction to Computer Security. This course is intended for students just beginning the program, in their first year of the two year degree. The goal is to have the students start thinking about security as it relates to computing at an early stage, so that by the time they graduate it will become second nature. This course also fills a gap in the program, because all students in the CIS program will be required to take this course.

We also created a new specialty in the degree that includes three security courses. They are:

Computer Forensics. We added this course at the request of local law enforcement, because there are very few people in the area that have any knowledge of this particular topic.

Network Security I. This is our original security course, which was based on the COMP TIA Security + objectives. We have expanded this course to include ethics and legal issues for the security professional.

Network Security II. This course is intended to build on the concepts learned in Network Security I, with more emphasis on defense in depth, and a quarter long case study that is still to be developed. This course will also include live exercises based on examples provided by speakers at the WECS 5 conference. The two Network Security courses will be held in our Cisco CCNP lab, and this equipment will be utilized in the design of the live exercises.

5. LESSONS LEARNED

Practical experience in the field greatly enhanced my ability to understand the issues surrounding information assurance and to develop a practical case study that reflects a real world situation.

The CIS department at Whatcom Community College has traditionally focused on typical computer topics such as computer support and networking. As events have occurred in the world, it has become obvious there is a need for more emphasis on security and introducing this to the curriculum is possible regardless of the resources available.

In addition, ethics and legal issues regarding the role of the technician should be included in any information security education. These topics can also be introduced into existing curriculum.

6. SUMMARY

Security education can be implemented at a small community college, provided there is a motivated faculty and backing by the administration. Whatcom Community College has been fortunate to receive several grants that have enabled us to develop an information security specialty within our current CIS degree.

In addition, recruiting underserved populations into the CIS program has always been a priority and we are now emphasizing a career in information security as one possibility for these populations to consider.

The WECS 5 conference was very informative as to the types of programs offered at other institutions, and I was able to incorporate many of these ideas into the development of the new information security specialty in the CIS degree.

REFERENCES

- Cisco. (n.d.). Retrieved May 25, 04, from <http://cisco.netacad.net/public>
CompTIA. (2004). *Security +* Retrieved June 4, 2004, from <http://www.comptia.org/certification/security/default.asp>
Internet Storm Center. (n.d.). Retrieved June 1, 2004, from <http://isc.incidents.org>
SANS. (n.d.). Retrieved June 5, 2004, from <http://www.sans.org>
The Center For Information Security Studies and Research. (n.d.). Retrieved June 1, 2004, from <http://cistr.nps.navy.mil>