Network Security: A Case Study

Susan J. Lincke
Computer Science Department
University of Wisconsin-Parkside
Kenosha, WI
lincke@uwp.edu

Abstract

This paper reviews 3 case studies related to network security. The first two exercises deal with security planning, including classifying data and allocating controls. The third exercise requires more extensive TCP knowledge, since the exercise includes evaluating a computer power-up sequence… but with interesting results!

1 Introduction

The Internet has changed crime in a huge way. No longer does a bank robber even need to be in the same country to rob a bank or financial institution – they can crack an unprotected web site from the comfort of their own home. No gun or physical presence is needed to rob a store – simply monitoring a poorly equipped store's WLAN can provide many credit card numbers. It is hard to safeguard your computer or prosecute criminals, when the criminal is in another country, possibly attacking through botnets. The Health First Case Study provides students a foundation on how to protect networks securely.

Three case study exercises are useful in providing students a foundation in network security. All three each include a PowerPoint lecture and active-learning exercise, which serves as the case study. Three case studies related to networking include:

- Designing Information Security: Classifies information by confidentiality and criticality.
- Planning for Network Security: Determines services, connection establishment directions, security classifications, and access control and builds a colorful network diagram for security
- Using a Protocol Analyzer: Analyzes a protocol sequence generated upon laptop power-up, to determine which services, connections, and ports are used then.

Case studies have been used in business since the 1930s [1,2], and in engineering [3]. Lu and Wang [1] point out that case studies enable student-centered learning, by promoting interactivity between students and faculty, reinforcing educational concepts taught in lecture, and deepening student understanding by building knowledge into students. Students not only learn to apply theoretical knowledge to practical problems, but also to be creative in discovering solutions. Wei et al. [2] agree that case studies "constitute the basis for class discussion." They add that cases help students transition to the workplace, by exposing students to diverse situations, thereby enhancing adaptation skills to new environments, and increasing students' self confidence in dealing with the world. Chinowsky and Robinson [3] stress that case studies enable interdisciplinary experience, which students are likely to encounter in the real world.

Case studies relating to security include business- and legal-related case studies. Dhillon [4] has written a security text which includes a focused case study problem for each chapter. ISACA provides graduate-level teaching cases [5,6], which emphasize corporate governance problems related to security management and COBIT. Schembari has students debate legal case studies, to help them learn about security-related law [7].

Our case study exercises also help to prepare students for security planning and security evaluation. Two security planning exercises help students to learn the perspective of business (in this case, a doctor's office), in addition to the technical perspective. A protocol analysis helps students to exercise deep technical skills, when they evaluate a protocol analyzer dump, for a security scenario. The Health First Case Study provides the conversations (or information) for students to complete the exercises. A Small Business Security Workbook guides students through the security planning process, by using introductory text, guiding directions, and tables for students to complete. We next review the case study exercises in detail.

2 Case Study Exercises

There are two related case study exercises related to planning security, and one related to reading protocol dumps.

Designing Information Security: This is a prerequisite exercise for the next case study. Understanding an organization's data is the first step to securing their network. Data will have different confidentiality and reliability requirements. An organization must define different classes of data, and how each class is to be handled. They must also define access permissions for the various roles in the organization.

In this Health First case study, students consider Criticality and Sensitivity Classification systems for a doctor's office. What different classes of information should exist for Sensitivity (or confidentiality) and Criticality (or reliability), for a Doctor's office? How should each Sensitivity classification be handled in labeling, paper and disk storage, access, archive, transmission, and disposal? By reading a conversation from a small doctor's office, students make these decisions and enter them into tables in the Small Business Security Workbook. Students then review a Requirements Document to determine which roles should have access to which forms, or data records.

Once the organization's applications and permitted access is understood, then network security can be addressed.

Planning for Network Security: Network security requires: 1) identifying the services used within the network, and 2) allocating services to virtual or physical computers, based on their Criticality/Sensitivity classification and role-based access control.

In this continuation of the doctors' office case study, students complete various tables to determine required services and appropriate controls. The first step determines which services are allowed to enter and leave the network, and in which directions connections normally originate. This information is important in configuring the firewall(s). The second step considers which applications can be stored together on physical or virtual machines, based on access control (who can access what) and the Criticality classification. Based on the Criticality classification, students then define the required controls for each service (e.g., encryption, hashing, anti-virus). Firewalls need to protect the organization's data from both the internet and wireless access!

Finally, students draw a network map with Microsoft Visio, and color code the different systems according to their Sensitivity Classification. Figure 1 shows a network map, where red indicates Confidential information, yellow Private information, and green Public information. Red lines indicate VPN protection.

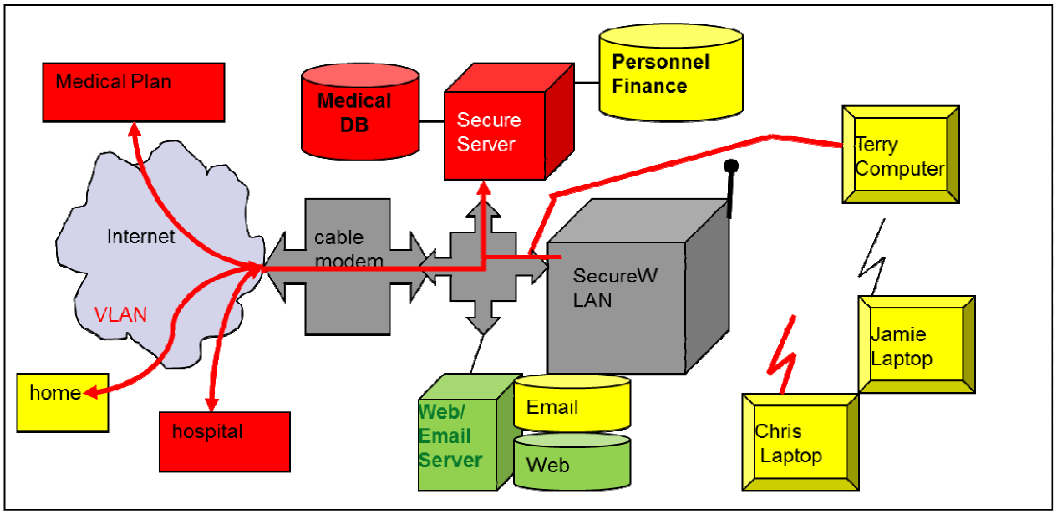

Figure 1: Network Diagram for Security.

Using a Protocol Analyzer: If students are to protect a network, they must be able to understand a protocol analyzer dump. Understanding protocols is essential to recognizing attack traffic, and programming a firewall or Intrusion Detection/Prevention System (IDS/IPS). For example, which ports should remain open in a firewall, and in which direction do connections normally occur? Sometimes this is not easily known, but must be determined by monitoring the normal traffic.

In this case study lab, students evaluate a protocol analyzer dump (from Windump) that includes a computer power-up sequence. The computer is not new and could have a worm. So the purpose of the lab is to determine required ports for the firewall, but also to see if there are unusual transmissions during the power-up sequence. Windump is used instead of Wireshark, because Windump generates a smaller dump that can easily be printed for case study purposes.

In this exercise, students sift through TCP packets, to determine if any connections look suspicious. Students practice recognizing TCP SYN (Synchronize) packets, and the Domain Name Server (DNS) packets that precede them, to determine where the connections are being made. Students evaluate how much data is being sent and received, which requires understanding TCP sequence numbers. The interesting thing about this sniffing session is that for a couple of connections, the computer is uploading more information to the network than it is downloading… and the destination is hackerwatch.org!

While this destination was a surprise to the author, McAfee Antivirus software uploads networking information to track port usage. For example, if port 2042 becomes suddenly popular over millions of computers, it is likely a new worm has been introduced that uses this port. The web site www.hackerwatch.org shows in real-time the most active ports in use.

This very technical exercise is definitely better done in class as an active-learning exercise, than as homework. It is difficult for students without detailed TCP protocol competence. The instructor must walk through the first two protocol sequences with the students, then students can complete the remaining themselves (with your help as needed). While the exercise is a useful exercise in network security, the exercise may be more appropriate for a Computer Networks class, where the TCP protocol has been fully covered.

3 Planning the Case Study

The case studies are best taught as an active learning exercise in class, where students can ask questions and the instructor can monitor progress. These case study materials are available since they were funded by NSF, including PowerPoint lectures, Health First Case Study, Small Business Security Workbook, and Small Business Requirements Document. There is also a Small Business Security Workbook Solution, which includes case study solutions.

PowerPoint lectures are given in the first half of a 3-hour class, and the second half is the active learning exercise. The lectures have been enhanced to include appropriate example tables from the Small Business Security Workbook, for a University application. (The students complete the Doctor's office application.) These examples help students to observe how tables are properly used, and may provide ideas for their solution (or not!) The lecture notes are made available to students from my web page during the active-learning exercise, and they are often referred to.

During the security planning exercises, students move to a computer room where they can edit the Small Business Security Workbook directly on a computer. Students are grouped into 3-4 person teams, and each team is provided a computer. All students should be able to see the display, so computers are selected and manipulated for the best display. The best computers tend to be the ones at the end of a row of tables, providing 3 sides for students to sit, discuss, and observe Workbook use. Each student is also given a paper copy of the case study.

It is possible to do the protocol analysis exercise in a lab environment, too. However, I usually print the protocol dump and case study exercise and provide them to 2-person teams.

I review the exercise at the end of the class. If people finish early, it is possible for them to review their solution with yours before they go.

4 Lessons Learned

The full Health First Case Study includes a number of security planning exercises, including risk, business continuity, physical security, metrics, etc. Thus, we have much experience working with case studies. Our first four security planning labs had an average 78% agreement rate to the statement: "I understood what was expected as part of the case study exercise, and it helped me to learn the material." During the next six labs this rate increased to 87.5%. (In both cases, all remaining students selected “Neither agree nor disagree”.) To fix this, we currently start the case study as a class (and not groups). Volunteers read the case study out loud and discussion begins class-wide. Our initial approval rating then started out higher, with 93% ‘agreeing’ with the statement: “I understood what was expected as part of the case study exercise, and it helped me to learn the material.”

5 Acknowledgments

The development of the Small Business Security Workbook, lecture materials, and Health First Case Study was funded by the National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning. These materials are available at: www.cs.uwp.edu/staff/lincke/infosec. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

6 Conclusion

These case studies help students to practice their trade for their real world careers, by planning for security and by analyzing a protocol dump for a realistic application. In the security planning exercises students actually get to experience working as an interdisciplinary group, including a doctor, registered dietician, and medical administrator. This enables students to understand a non-technical, business perspective. The protocol dump gives students confidence that they could analyze a security protocol dump on their own, if they needed to – or use the protocol analyzer for debugging a non-security-related communications problem.

References

[1] S. Lu and Y. Wang, “The Research and Practice of Case Teaching Method in Computer Curricula for Undergraduates”, *Proc. 2009 4th International Conf. on Computer Science and Education*, IEEE, 2009, pp. 1460-1463.

[2] H. Wei, C. Xin, and H. Ying, “Non-computer Professional IT Education in the MBA Model”, *The 5th International Conf. on Computer Science & Education*, IEEE, pp. 612-614, 2010.

[3] P. S. Chinowsky and J. Robinson, “Facilitating Interdisciplinary Design Education Through Case Histories”, *1995 IEEE Frontiers in Education Conf.*, IEEE, pp. 4a3.6-4a3-9, 1995

[4] G. Dhillon, *Principles of Information Systems Security*, John Wiley & Sons, Inc., 2007.

[5] ITGI, *IT Governance Using COBIT® and Val IT: Student Book, 2nd Ed.*, IT Governance Institute, www.isaca.org, Rolling Meadows, IL, 2007.

[6] ISACA, *Information Security Using the CISM® Review Manual and BMIS™: Caselets*, www.isaca.org, Rolling Meadows, IL, 2010.

[7] N. P. Schembari, “An Active Learning Approach for Coursework in Information Assurance Ethics and Law”, *Proc. 14th Colloquium for Information Systems Security Education (CISSE)*, www.cisse.info, pp. 1-8, 2010.