An Information Assurance Curriculum for Commanding Officers using Hands-on Experiments

Joel Brynielsson
Swedish National Defence College, P.O. Box 27805, SE-115 93 Stockholm, Sweden
joel@kth.se

ABSTRACT

To authorize and initiate necessary investments and enforce appropriate policies and procedures, decision-makers need to have at least a fair understanding of computer security fundamentals. This paper presents the course design and the laboratory settings that have been developed for, and used within, the high rank officer curriculum at the Swedish National Defence College. The developed course looks at computer security from an attack versus defend viewpoint, meaning that computer attacks are studied to learn about prevention and self-defense. The paper discusses the pedagogical challenges related to education of high rank officers and similar personnel in light of recently-held courses and contrasts the course relative to similar undertakings. A standpoint taken is that computer security is best taught using hands-on laboratory experiments focusing on problem solving assignments. This is not undisputed since, e.g., high rank officers are busy people who are not fond of getting stuck learning about the peripherals.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection; E.3 [**Data**]: Data Encryption; K.3.2 [**Computers and Education**]: Computer and Information Science Education

General Terms

Security

Keywords

Computer security, hands-on experiments, high rank officer training, information operations, isolated computer lab

1. INTRODUCTION

From an officer's perspective, computer security is interesting not only because of computer vulnerabilities in itself but also from the perspective of information operations, i.e., the use and management of information to shape perceptions, manage opinions, and control behavior [1]. Hence, there are (at least) two important aspects of computer security that must be considered: the technical aspect and the operational aspect. Considered one at a time, these two aspects tend to cause a perceptual misunderstanding where the required computer skills are confused with the intentions of information operations and vice versa. That is, operations utilizing computers need to be based on knowledge and reasonable assumptions about what can actually be accomplished with computers. Most certainly, the opposite also holds true, i.e., that computer security should not be considered on its own but rather in conjunction with a reasonable understanding of the surrounding threat situation. This paper targets the former problem, i.e., to give high rank officers a reasonable understanding of computer security so that they will be able to, e.g., make informed decisions regarding acquirement of new computer systems and obtain a reasonable understanding of the threat posed by so-called computer network operations.

The paper starts by describing the set-up of a computer laboratory that provides the necessary means to make it possible to develop courses accounting for the great variety of computer crime that can be anticipated. Then, the outline of a two-week computer security course is presented, followed by a description of the actual lab assignments that the students perform during the course. The following section describes the research methodology that has been used and the assessment that has been made. A discussion about the didactical challenges follows and a section on related work places and contrasts the course relative to other courses, before the conclusions wrap up the paper.

2. PHYSICAL LABORATORY SET-UP

A requirement posed on the physical structure of the lab was that it should both be easy to reconfigure and that it should resemble the computer infrastructure that can be found within ordinary organizations. To do this, efforts have been made to build a computer network that incorporates two large organizations that communicate with each other using a simulated Internet connection and have the possibility of using all kinds of ordinary services that can be expected within an ordinary firm or governmental organization. This set-up makes it possible to initiate attacks from within one of the networks to attack assets residing on the other network using the simulated Internet connection which, henceforth, account for realism. Also, an administrative network according to Figure 1 has been built to make it

SIGCSE'09, March 3–7, 2009, Chattanooga, Tennessee, USA.

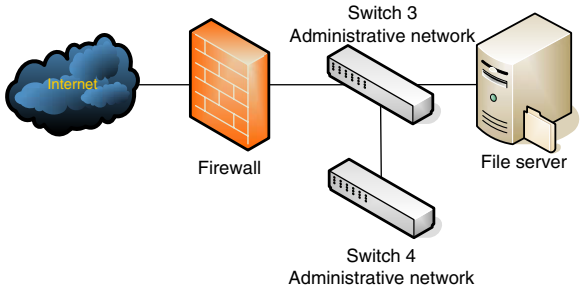

Figure 1: The administrative network spans the two companies by the use of interconnected switches.

possible to easily maintain and administrate the lab and provide the necessary parts that constitute the outside world.

The company networks are connected via two routers that conceptually indicate the Internet connection seen from the perspective of the company network. Seen from the perspective of the administrative network, depicted in Figure 1, this is where the network starts. The routers route traffic between the two networks using a wide area network (WAN) connection cable and route the rest of the traffic to the administrative network that is, in turn, connected to the Internet through a firewall. The administrative network also holds a large file server along with software for creating hard disk drive images which, hence, makes it possible to easily manage various lab set-ups that can be alternated between rapidly. Each of the two company networks is autonomous and can be configured independently. Depending on future requirements, the set-up makes it possible to connect additional networks as desired.

In the current lab configuration, each of the two company networks, depicted in Figure 2, consist of a demilitarized zone (DMZ) network and an internal network. The DMZ sits between the router and the internal network and contains a web server and a firewall that protects the internal network. The internal network holds four additional internal servers, a number of workstations, and a network printer. For network monitoring purposes two hubs, denoted "Hub 1" and "Hub 2" in Figure 2, have been connected so that network traffic can be analyzed immediately at the inside of the router and immediately at the inside of the firewall, i.e., to be able to intercept network streams that travel back and forth from the Internet and the internal network respectively. Here a computer using a packet sniffer can be plugged in to, e.g., monitor network usage, spy on other network users, gather clear text passwords, detect network intrusion attempts, and everything else that can be performed by someone that has gained access to a computer network at some point.

The main body of the server environment is physically mounted in two racks corresponding to the respective company networks, i.e., one set-up according to Figure 2 resides in each of the two racks. The administrative network, on the other hand, is best understood in terms of that it resides in both of the two racks. Although most of the administrative network's hardware resides in one of the racks, the two switches are placed so that they reside in each of the two racks and, hence, serve the purpose of interconnecting the two racks. These two switches, denoted "Switch 3" and "Switch 4," are depicted on both Figure 1 and Figure 2, which makes it easier to see how they interconnect

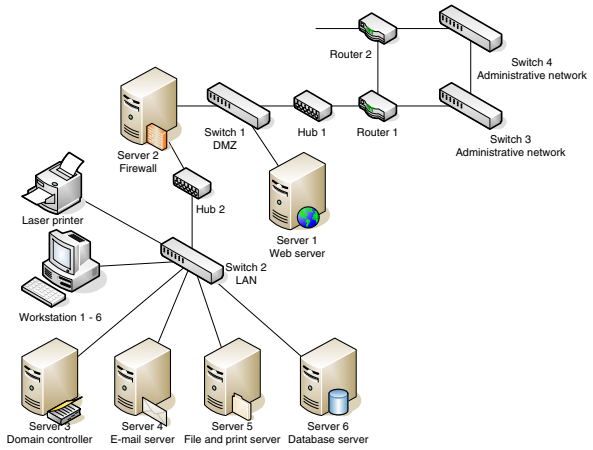

Figure 2: The company network structure is located on the inside of "Router 1" which separates the company network from the administrative network.

the two racks seen from the different network perspectives that the two figures represent. Hence, the only two connections between the racks consist of the WAN cable that simulates Internet and the network cables that interconnect the administrative network switches. From the perspective of the company network administrator, i.e., the role taken by the student, it is thus fairly easy to envision that the constituents in a sole rack belong to him and that the rest should be considered belonging to, e.g., Internet.

The client workstations and the two printers reside in a classroom that is separated from the server room by the use of a well-insulated door that keeps the noise down. The two rooms are connected through a patch panel which makes it easy for students to make connections by attaching patch cables in the desired way.

3. COURSE OUTLINE

Information systems security spans an extensive area and typically requires several semesters when taught for ordinary university students within, e.g., computer science [12]. Consequently, the ordinary university curricula could not be used when designing a shorter course as described herein. The purpose was not to design an in-depth course but rather to design a course giving the student sufficient awareness to make the right organizational decisions using in-depth experiments. The security course was structured during two full weeks but was preceded by two intense days containing introductory computer training. Typically, Swedish officers tend to have very different computer knowledge background which made it vital to gain some additional experience to get everyone "beyond the Windows Start Menu" before the security classes started.

The two weeks were structured so that the morning session contained the necessary theory which was taught using a mixture of lecturing and short well-guided hands-on exercises. The afternoon sessions were devoted to the students' laboratory assignments with guidance given in the laboratory. Although the assignments could be fulfilled at any time, the students mostly chose to do them during the scheduled lab slots—which is normal practice at the defense college where the "students" are at the same time officers

working full time. The targeted audience was the high rank commanding officer course consisting of students elected for the last two years of Swedish military training. These students differ from ordinary university students in that they are older and have about 15 years of professional experience to build upon.

For the extent of the course, the students were assigned two desktop computers—one in each of the two simulated organization networks so that the needed communication resembled ordinary Internet connectivity between, e.g., two companies. The workstations were pre-installed in two ways so that the student got hold of one Linux computer and one Windows computer. The Linux computer was an up-to-date Debian installation while the Windows computer ran Windows XP patched up to service pack 2 (SP2) but did not include any of the security patches that have come out since the release of SP2. In our opinion the chosen operating system installations represent extremes and are examples of a strict and secure installation on the one hand and a vulnerable installation on the other hand—of course, this is a subjective judgment that we will not delve further into within the scope of this paper.

During the course the students typically learn by attacking their own system to see what happens, and using the gained experience to set up the appropriate countermeasures. Typical areas that were covered include encryption schemes, typical system vulnerabilities within operating systems and network protocols, means to protect an insecure system, analysis of network traffic, etc.

4. THE LAB ASSIGNMENTS

Three of the labs focused on networking issues and two of the labs were more directly concentrated on security issues. The approach chosen was to delve into some areas more thoroughly by providing hands-on experience whilst other topics, e.g., buffer overruns, cryptographic protocols, man-in-the-middle-attacks, etc., were demonstrated or covered theoretically during the lectures. The software used for the duration of the course could be obtained freely, which was used in the assignments where the students were supposed to obtain and install the software as part of the assignment.

Lab assignment N1, "ping, traceroute, and sniffing," had the purpose of making students confident in using a number of ordinary network tools and to see how easy it is to intercept and obtain non-protected network information. The `ping` command was used to answer a number of questions regarding various IP addresses and domain addresses which, at the same time, provided knowledge about the naming conventions used on the Internet and the nature of specific IP addresses such as the 127.0.0.0/8 addresses that have been reserved for the local computer. Next, the student was instructed to install a packet sniffer, i.e., a tool that listens and captures the network stream passing by the network interface card of the computer, and capture some network traffic that needed to be analyzed to answer a series of questions relating to the protocols and connections discussed during the lecture. The packet sniffer soon turned into the student's best friend and was used extensively throughout the course whenever something strange happened. Using the packet sniffer, the operation of `traceroute`, i.e., to determine the servers that the packet passes on its way between two computers, could be pedagogically explained. Lastly, the lab ended by having the students intercept their own web based login system by using the packet sniffer to eavesdrop the password.

Lab assignment N2, "hubs, switches, routers, and DNS," aimed at teaching the foundations of the various forms of network hardware that can be encountered. The set-up for the lab meant that one computer on the same company network was set to automatically download various web pages at short intervals, partly from computers located on the other company network and partly from the real Internet. The assignment given to the students was to investigate what was happening by using the network sniffer to listen at various places in the network, e.g., the wiretapping hubs shown in Figure 1 and possibly the switch in the other network. The exercise has proven most successful by leading to an increased understanding of the functionality that the devices provide, i.e., the hub broadcasts everything, the switch uses MAC addresses and the router performs routing according to the designated IP address. Lab N2 also conveyed information about the workings of DNS which was performed by having the students answer a number of questions using `nslookup`, `dig`, and so forth.

Lab assignment N3, "ports, port scanning, SMTP, construction of own packets, and BitTorrent," aimed primarily at teaching the way ports work and to use network tools to create artificial network traffic. After finding and installing a port scanner the students performed various port scans on the lab computers to see what could be found. As usual, they were encouraged to use the network sniffer to learn more about the actions performed. After learning about the standard ports that can be used the students learnt how to fake e-mails by manually connecting to the SMTP server—many were amazed about how easy this was in practice. Next, the use of a packet injection program was taught by having the students capture a (clear text) telnet session. As usual the attack was performed on oneself which makes the process easier. By investigating the telnet traffic found by using the packet sniffer, the students were supposed to inject a command by creating an artificial command using the packet injection program which required some trial-and-error before one succeeded. Lastly, by using most of the knowledge obtained during the network part of the labs, the students were supposed to investigate which computer was set to do what. Three computers were set up to simulate three users that were 1) using a popular file sharing program, 2) using a port scanner, and 3) surfing the web.

In lab assignment S1, "encryption and signing of e-mails, hard disk drives, and files," the students were assigned to use publicly available software to learn about how one can ensure confidentiality and integrity by using encryption and digital signatures. In the e-mail part of the lab the students used the PGP format for creating various types of signed and encrypted e-mails. A lesson learnt is that hands-on experience is indeed needed to make the idea of public key cryptography become entirely clear. After that the TrueCrypt program was used to encrypt files and whole disk volumes.

Lab assignment S2, "passwords and the quest for security vulnerabilities," had the students reset the administrator password on their Windows computers—which is a fairly straightforward task using a certain Linux distribution that has been designed for this very purpose. Next, a number of available tools were investigated. First, the program Nessus was used to find a number of security vulnerabilities—which

was not difficult given the non-patched environment. After that, the command line tool `dsniff` was used to find passwords efficiently given a large amount of network traffic. Lastly, Cain & Abel was used to exemplify how easy it is to crack a poor password.

5. METHODOLOGY AND ASSESSMENT

The course has been brought about and further refined using action research methodology with diaries, oral reflection, and questionnaires being the primary data sources [3]. That is, the course was developed through continuous reflection on, and adjustment of, the actions taking place in the classroom. By careful collaborative planning, observation, and reflection, we altered, e.g., the lab content, the available time for various course elements, the presentation style, theory versus practice, time spent on hands-on experience versus lecturing, level of guidance, etc. Everyone in the classroom, both teachers and students, contributed to this development in a collaborative manner, i.e., in line with the ideas behind the action research paradigm. As an example of the adopted research methodology, lab assignment S1, see Section 4, was altered so that public key cryptography was taught using built-in e-mail program functionality instead of command line tools. Although the comparatively low level command line tools provided in-depth understanding, the less time-consuming e-mail program functionality along with suitable lab exercises was considered more appropriate for the student category in question.

The course evaluations were answered by all students and included both quantitative and qualitative questions. The quantitative questions mostly concerned generic course characteristics regarding, e.g., the relevance of the course relative to the student's prior knowledge and ability, the level of increased knowledge that the student thinks he/she has obtained, the level of own commitment that the student has felt during the course, whether the task load during the course has been reasonable, whether the teachers have adhered to the administrative documents and procedures, relevance for the overall educational program goals, etc. These quantitative questions received overwhelmingly positive feedback along with positive comments about the teachers' commitment and administration. However, although it is important to secure the quality of one's work, the quantitative questions have not really been useful when it comes to being innovative and formulating the action research questions leading to change. Instead, the qualitative part of the questionnaires, as well as qualitative information obtained using other means, was what really gave us the necessary inspiration to change. A common student comment stated that "the labs could have been more instructive to keep up the pace." When making the labs more straightforward, however, we saw that the students started to adhere to a non-desired behavior meaning that they tried to cut corners instead of being open-minded and actively searching for information.

Another comment regarding the labs had to do with content rather than the extent of being straightforward, namely: "Labs are great. But the content should make a clear distinction between the number-one concern and the side issues. Time is limited and it is of utmost importance that the lab time is devoted to the primary concern rather than the side issues." This is something that we have been working hard to accomplish by trying to make the labs more straightforward in the subsidiary parts and more inspiring when it comes to the actual content that we feel it is important for the student to grasp in full and reflect upon. This is not an easy task, however, and much can still be done.

6. DISCUSSION

The increasing use of information technology makes it important for officers to learn about computer security to be able to fulfill their missions both on a daily basis and while serving operationally. To educate high rank officers and similar decision-makers is however challenging due to the available time and the variations in previous computer knowledge. Our course focuses on problem-solving in realistic environments where the students obtain knowledge by studying attacks and ways to avoid future attacks by making informed decisions using the obtained knowledge. The idea has been to obtain deep knowledge within a few important areas that, in turn, represent the broad spectrum of topics covered within the theoretical part of the course. We do not make an attempt to educate skilled computer security people, but rather decision-makers that need to acquire an insightful understanding of the field as a whole.

Exposing the students to "attacks" that they initiate themselves and analyze has been a fruitful way to work in the laboratory. We have found that a good learning process is obtained by mixing theory with hands-on training according to an attack/defend approach. Criticism can be raised against the attack/defend approach in that it can be used to educate computer criminals—a problem that has been observed among students taking similar courses taught at regular universities [8]. Technically, we feel convinced that this is unavoidable—knowledge leads to power and can be used for both good and bad purposes. To avoid malicious use of the obtained skills, attacks and exploits should be taught along with a discussion about the legal aspects.

7. RELATED WORK

When placing and contrasting security education undertakings relative to existing classification schemes and other courses two commonly used factors ought to be considered: depth and content. Starting with education depth, this is conveniently measured by distinguishing between awareness, training, and education as governed by the National Institute of Standards and Technology (NIST) [14]. First, awareness activities consist of all the activities where the learner is a, more or less passive, recipient of information. Typically, awareness activities are too short to allow for hands-on, aim at reaching large audiences using traditional lectures or denote other passive means for transferring knowledge. Second, training activities strive to teach particular skills and competency to be used by a practitioner in a particular role other than information technology (IT) security, e.g., management, procurement of IT systems, etc. Third, education targets IT security specialists and professionals who need to be knowledgeable in all of the security skills and competencies that are learnt in the aforementioned awareness and training activities. Hence, it follows that the education depth of our work ought to be classified as training using this scheme. Now turning to education content, we distinguish between training and scholarship as suggested in [2]. Training differs from scholarship in that training emphasizes particular systems, situations and environments to prepare students for specific tasks or roles whilst scholarship empha-

sizes the underlying principles, concepts, and their application to enhance the study and understanding of the foundations. By looking at the course contents and learning objectives we note that the course described in this paper again falls into the training category rather than the scholarship category. To sum up, both concerning depth and content the developed computer security course can be classified as a training activity, meaning that the course has been tailormade in order to result in graduates that are prepared for the security challenges they are likely to encounter in their professional roles.

Several articles target issues related to developing security education within the scope of full scale educational programs, see, e.g., [7, 13], but detailed information on security courses of various kinds also exist, see, e.g., [8, 9, 12]. However, specific information regarding courses with similar prerequisites as the one described herein, i.e., a short course especially tailored towards military officers with limited computer knowledge, has not been published widely. In part, this is probably due to that academia traditionally "teaches the why and the what but gives little attention to the how" [4, 10]. Of course, comparable short term security classes given to working professionals exist albeit they have not been reported on in the literature.

The need to build an isolated computer lab where the students are able to use the lab as a playground for trying out various security related tools in a secure fashion have been discussed, and endorsed, widely, and many examples exist, see, e.g., [6, 8, 10]. For the most part, however, development of suitable computer laboratories has been performed by enthusiastic computer science teachers who have focused on the technical issues rather than the educational aspects. It should be noted, though, that the approach taken is an example of the so-called "studio concept" which is a well-documented method for teaching traditional introductory engineering courses [11].

8. CONCLUSIONS

After two years of teaching the computer security class the overall impression is that the involved personnel and the students are fairly satisfied. There is, however, uncertainty regarding the usefulness of non-guided time-consuming hands-on exercises with regard to the officers' future working sites. The teachers, who all were used to teaching at the nearby technical university, were under the impression that non-guided hands-on assignments are the best way to teach computer knowledge—at all times. Some of the students, on the other hand, meant that this way of teaching requires a great deal of time and that it might be better to teach using lab assignments that guide the student towards the solution in a more elucidate way. After some contemplation, however, the "new" way of teaching seemed to have gained approval from most of the students making us think that they slowly had come to the pedagogically well-accepted conclusion that "the greatest enemy of understanding is coverage" [5].

We believe that the course served its purpose in giving the attending officers a reasonable understanding of the difficulties posed by computer security: to attack a system it suffices to find a single vulnerability, but to defend a system all vulnerabilities must be found and repaired. And since the attacker and the defender use the same tools and the same knowledge to find the same vulnerabilities, it follows that it is often easier to attack than to defend.

9. REFERENCES

[1] L. Armistead, editor. *Information Operations: Warfare and the Hard Reality of Soft Power*. Issues in Twenty-First Century Warfare. Brassey's, Inc., Washington, District of Columbia, 2004.

[2] M. Bishop. Computer security education: Training, scholarship, and research. *IEEE Computer*, 35(4):30–32, Apr. 2002.

[3] L. Cohen, L. Manion, and K. Morrison. *Research Methods in Education*, chapter 14, pages 297–313. Routledge, London, sixth edition, 2007.

[4] E. Crowley. Information system security curricula development. In *Proceedings of the Fourth ACM SIGITE Conference on Information Technology Curriculum*, pages 249–255, Lafayette, Indiana, Oct. 2003.

[5] H. W. Gardner. Educating for understanding. *The American School Board Journal*, 180(7):20–24, July 1993.

[6] J. Hill, C. Carver, J. Humphries, and U. Pooch. Using an isolated network laboratory to teach advanced networks and security. In *Proceedings of the 32nd ACM SIGCSE Technical Symposium on Computer Science Education*, pages 36–40, Charlotte, North Carolina, Feb. 2001.

[7] C. E. Irvine, S.-K. Chin, and D. Frincke. Integrating security into the curriculum. *IEEE Computer*, 31(12):25–30, Dec. 1998.

[8] D. Jacobson. Teaching information warfare with lab experiments via the Internet. In *Proceedings of the 34th ASEE/IEEE Frontiers in Education Conference*, pages T3C/7–12, Savannah, Georgia, Oct. 2004.

[9] B. E. Mullins, T. H. Lacey, R. F. Mills, J. M. Trechter, and S. D. Bass. How the cyber defense exercise shaped an information-assurance curriculum. *IEEE Security & Privacy*, 5(5):40–49, Sept.–Oct. 2007.

[10] G. W. Romney, C. Higby, B. R. Stevenson, and N. Blackham. A teaching prototype for educating IT security engineers in emerging environments. In *Proceedings of the Fifth IEEE International Conference on Information Technology Based Higher Education and Training*, pages 662–667, Istanbul, Turkey, May–June 2004.

[11] L. S. Schadler and J. B. Hudson. The emergence of studio courses—an example of interactive learning. In C. Baillie and I. Moore, editors, *Effective Learning and Teaching in Engineering*, chapter 10, pages 156–168. RoutledgeFalmer, New York, 2004.

[12] S. K. Sharma and J. Sefchek. Teaching information systems security courses: A hands-on approach. *Computers & Security*, 26(4):290–299, June 2007.

[13] R. S. Swart and R. F. Erbacher. Educating students to create trustworthy systems. *IEEE Security & Privacy*, 5(3):58–61, May–June 2007.

[14] M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler, and J. B. Ippolito. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. NIST Special Publication 800-16, National Institute of Standards and Technology, U.S. Department of Commerce, Apr. 1998.