Georgia Tech Information Security Center Hands-On Network Security Laboratory

Randal T. Abler, *Senior Member, IEEE*, Didier Contis, Julian B. Grizzard, *Member, IEEE*, and Henry L. Owen, *Senior Member, IEEE*

***Abstract*—An undergraduate internetwork, security-teaching laboratory, which includes both defensive and offensive security laboratory experimentation, is described. This laboratory is oriented toward an introductory internetworking security class and is intended to complement more theoretical network security classes while sparking student interest. The laboratory is unique in that it uses an isolated laboratory network that provides a simple model of the Internet, including an enterprise network component, a university component, a "good" Internet service provider, and a "bad" Internet service provider. This setup is in contrast to typical educational laboratories, which use only a few physical computers with virtual machines. All of the laboratory assignments are available on the Internet for general community use and modification (the Internetwork Security Class Home Page is available at http://users.ece.gatech.edu/~owen/).**

***Index Terms*—Computer network security, educational technology, laboratories.**

I. Introduction

In order to complement the numerous theoretical security classes that exist, a hands-on-oriented, laboratory-based class that allows students to be exposed to the real-world challenges of network security was needed. A common complaint from students who have taken theoretical network security classes was that no apparent way to obtain practical experience, legally and ethically, with network security exists. A large amount of network security course activity was found in literature and Web searches [2]–[11]; however, readily reusable lecture materials or laboratory assignments and laboratory setups that met the goals and objectives of a realistic, hands-on-type learning experience were not found. The existing laboratory infrastructures in the literature consisted of only a few machines and did not approach a "realistic" network topology [4], [6], [7], [10]. Thus, effort was expended to create this laboratory and the associated online laboratory materials [1].

Many groups have explored methods of teaching information security. In [10], the pedagogical issues related to designing and implementing a cyber warfare laboratory exercise for a computer security course is examined. Micco and Rossman [6] discuss using National Science Foundation (NSF) funding to establish a laboratory where students can learn penetration testing techniques, hardening networks against attacks, and logging/audit controls for the purpose of convicting hackers. Ragsdale *et al.* [7] present an information warfare analysis and research laboratory based upon virtual machines. In [11], the pedagogical approach of "active learning and persistent, student-led teams" for learning information security was examined. Reference [5] has a course website that contains complete lecture materials and laboratory assignments for a network security laboratory based upon an "isolated LAN of at least three machines." This teaching laboratory model builds on the previously discussed methods of teaching and also adds unique elements that help build a teaching environment that approaches a real-world, hands-on laboratory that is both fun and inspiring to students.

To strengthen the laboratory design, the industry's best practices and latest developments need to be understood. Organizations that are making important contributions to the network security community and are useful resources in identifying network security laboratory components and teaching objectives include [12]–[14]. These organizations contribute to the community in various ways from informing security professionals of the latest alerts to offering free lectures on information security-related topics.

Building on the various laboratory architectures discussed and the professional security community, a network security laboratory has been created. The goals of this network security laboratory include exposing students to both defensive mechanisms and offensive mechanisms used by the opposition. These goals enable the students to gain a deeper understanding of the real-world threats that exist and how to cope with them. The laboratory was not intended to be a "hacker festival" so that students could learn hacking techniques; instead, the intent was to allow both defensive and offensive strategies to be understood and explored. Better protection mechanisms and strategies may be created and employed when there is a full understanding of how attacks are created and how they work. This laboratory is intended to spark student interest in network security using a realistic environment. The laboratory is intended to motivate students to take additional, more traditional, theoretical, network security classes. The format of this laboratory is one hour of lecture and approximately six hours of laboratory exercises per week.

II. The Network

The effectiveness and the popularity of a hands-on internetworking class [15] were examined to determine desirable char-

Manuscript received August 11, 2004; revised July 22, 2005. The authors would like to acknowledge the CISCO University Critical Infrastructure Assurance Group equipment donation program [17] and training programs, as well as Intel equipment donations, which made this laboratory possible.

The authors are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 USA (e-mail: henry.owen@ece.gatech.edu).

Digital Object Identifier 10.1109/TE.2005.858403

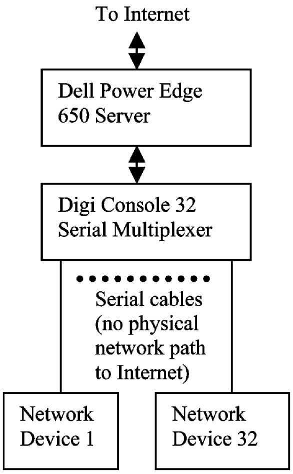

Fig. 1. Administrative interface.

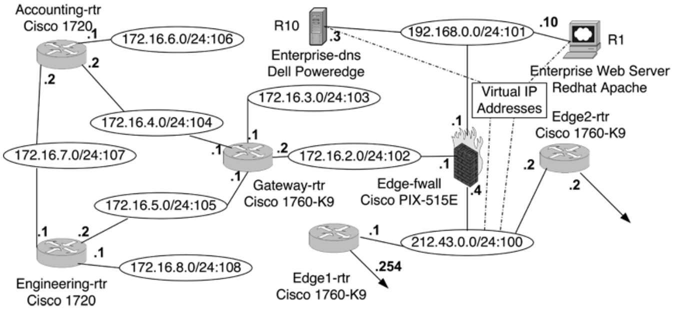

Fig. 2. Enterprise portion of the laboratory network.

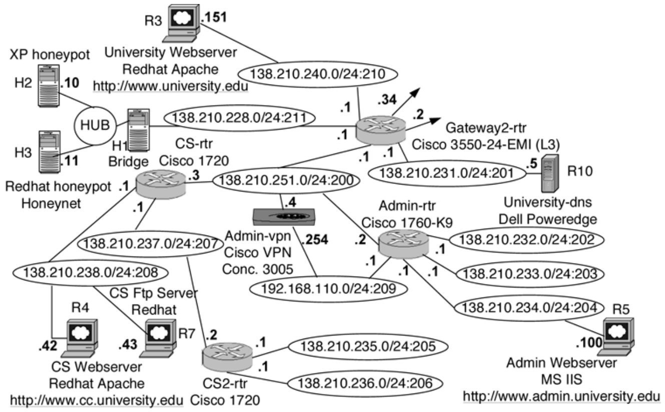

Fig. 3. University portion of the laboratory network.

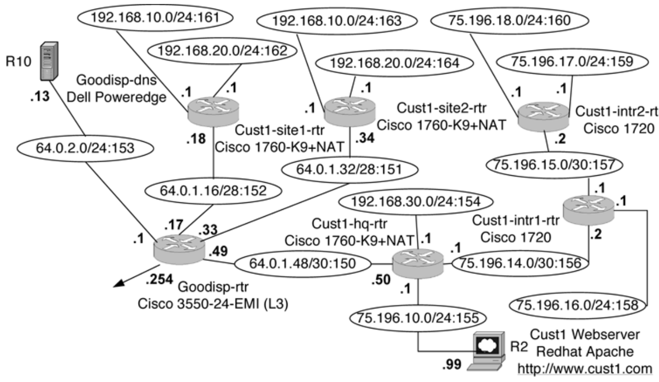

Fig. 4. Good Internet service provided portion of the laboratory network.

acteristics of a new laboratory-based network security class. Student reviews of this existing laboratory-based class indicated that it was a good initial model for the new efforts. Results from this existing class indicated that the new network security laboratory network needed to be as realistic, large scale, and interactive as possible. This type of network structure was not found in any of the published literature. The authors determined that a structure that contained an Internet backbone with distribution routers, an enterprise network with excellent security practices implemented, a university network with a more open network but with some access control, an Internet service provider with good security practices, and a second Internet service provider with no security practices would be the best representation of the Internet for the purposes of this laboratory. This laboratory network architecture represents a very difficult target to exploit (the enterprise network), a network with moderate difficulty to exploit (the good Internet service provider), a relatively easy target (a university), and a very easy target (an Internet service provider with no security). Thus, students can, in practice, learn how very easy targets are exploited and then work their way up the complexity chain as their understanding of exploits and techniques used by hackers increased. In addition, students may encounter good security policies in portions of the network and see the effectiveness of such policies.

The student laboratory network is physically isolated from the Internet so that exploits and information assurance laboratory assignments do not have the potential to escape and proliferate outside the student laboratory. However, one is able to reconfigure the laboratory from the Internet through an administrative interface, which is shown in Fig. 1. This capability allows multiple instructors and multiple teaching assistants to reconfigure the laboratory setup remotely. For example, this capability is used to reconfigure the laboratory network for laboratory assignments in a prerequisite introductory networking course [15]. The laboratory network configurations are stored on a Dell Power Edge 650 server. This server is connected to a Digi Console CM32 console port manager. The Digi Console CM32 is a device that connects to all of the network equipment including the switches, routers, intrusion detection systems, virtual private network devices, firewalls, and any other network device that is incorporated in the future. The combined capabilities of the Power Edge and the Digi Console CM32 enable users to configure the network remotely with the desired topology. One goal of the network is to keep it completely isolated from the real Internet. The access to the Power Edge and Digi Console CM32 does not compromise this goal because the Digi Console CM32 only connects to console ports on the network devices, which are not capable of transmitting network packets. The console ports are serial lines used to configure the devices.

The laboratory network topology is shown in Figs. 2 through 6. The four autonomous systems, an "enterprise" (Fig. 2), a "university" (Fig. 3), a "good Internet service provider" (Fig. 4), and a "bad Internet service provider" (Fig. 5) are federated by a fifth autonomous system (Fig. 6). This fifth autonomous system represents an "Internet backbone" consisting of two "Tier 1" backbone providers. The first "Tier 1" provider consists of one

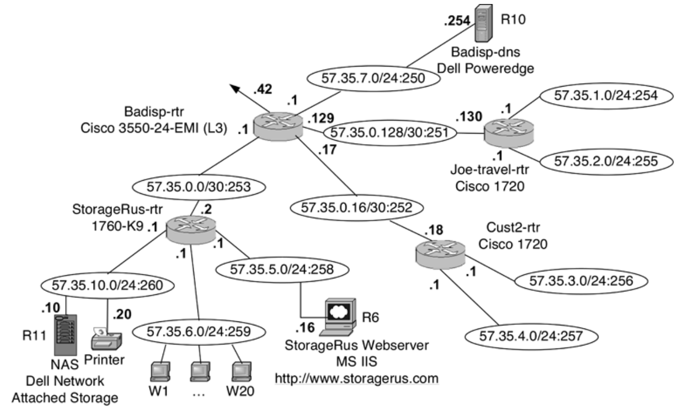

Fig. 5. Bad Internet service provider portion of the laboratory network.

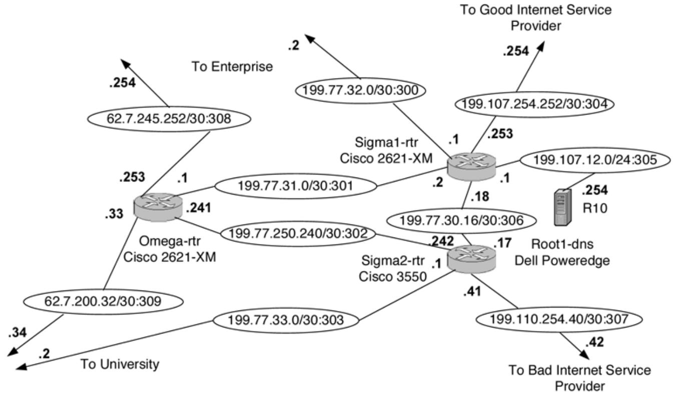

Fig. 6. Backbone portion of the laboratory network.

Cisco 2621XM router and a virtual router on a Cisco Catalyst 3550. The second "Tier 1" backbone provider consists of one Cisco 2621XM router. The backbone routers are used at layer 3 for normal routing. This architecture is a valuable model to use for teaching students and serves as a very small mock-up of the Internet.

Each of the four representative autonomous systems has specific characteristics that model a typical real world scenario. The "enterprise" autonomous system consists of dual-homed Internet connection using two redundant Cisco 1760 routers, a Cisco PIX-515E firewall, an access/edge Cisco 1760-VPN/K9, and two Cisco 1720 access routers. A "demilitarized zone" that contains a domain name server as well as a Web server exists. The "enterprise" autonomous system allows a student to experiment with a realistic enterprise topology. The good Internet service provider autonomous system consists of a Cisco Catalyst 3550, three Cisco 1760-VPN/K9 routers, and two Cisco 1720 access routers. The good Internet service provider is set up so that it may contain remote office enterprise connections through both virtual private networks and clear connections. Network Address Translation is also used inside this good Internet service provider. The "university" autonomous system consists of a dual-connected Cisco Catalyst 3550 and a Cisco 3005 virtual private network concentrator. The emulated "university" has no firewall and terminates virtual private networks from emulated remote users. An access control list is used in the Cisco Catalyst 3550. University use of networks typically entails a large amount of user freedom and, thus, limited network restrictions. The bad Internet service provider autonomous system is a haven for hackers. It consists of a Cisco Catalyst 3550 virtual gateway router and two Cisco 1720s and one Cisco 1760-VPN/K9 for distribution. No access control firewalls nor network filtering is applied internally in the bad Internet service provider. This autonomous system is intended to represent the unrestricted access typical of many Internet service providers.

One of the important features of the setup is its versatility. The use of virtual local area network (VLAN) technology and the combined capabilities of the Cisco Catalyst 3550 equipment that have both layer-2 Ethernet switching capabilities and layer-3 routing capabilities allow multiple logical network topologies to be mapped onto the physical topology. The switches make up the physical backbone of the network. All network devices and computers are connected to the switches, and all of the switches are connected together. Using this physical architecture, an almost unlimited number of virtual architectures may be created. The VLAN technology is used to create virtual switches in which any network device or computer can appear on any virtual switch. This capability is enabled and extended by the Cisco Catalyst 3550s, which are switches installed with an "EMI routing image" yielding both layer-2 switching and layer-3 routing capability in the same box. All that is required to create a new network is reprogramming the switches and network devices, which can be completed remotely.

To enhance this versatility further, custom perl scripts have been developed that can save and restore the network configuration. Network reconfiguration may be necessary as different laboratory assignments or different classes use the equipment. The need to physically rewire the network is essentially gone. One can move various machines around the network, for example, from one autonomous system to another without doing any physical rewiring. One also may change the autonomous system architectures without doing any rewiring. This architecture has been found to be highly effective for a teaching laboratory.

III. Laboratory Assignments

The class typically consists of twelve laboratory assignments and a capstone network security competition, which are all completed in one semester. Table I shows the goals, objectives, and tools used in some example laboratory assignments. All of the laboratory exercises are available online for modification and reuse [1].

One of the most unique characteristics of this network security instructional laboratory as compared with the literature is the level of realism and the scale of the network infrastructure available to students. Various laboratory assignments capitalize and leverage this realistic capability to varying degrees. The laboratory task of network mapping, scanning, and reconnaissance is very realistic because the laboratory is a small mock-up of the Internet. In contrast to traditional network laboratories, the setup enables one to divide the network into different Internet protocol (IP) address ranges, block access to some address by means of a firewall or access control lists (ACLs), have multiple hops and routes between source and destination, and provide various other realistic configurations. In the sniffing labo-

TABLE I
SAMPLE LABORATORY ASSIGNMENTS

Laboratory Exercise	**Goals** (Including Detection and Countermeasures)	**Software** (Used to Support These Goals)
1	operating system installation (Linux as well as Windows XP), network reconnaissance, network mapping, and vulnerability assessment	VmWare [18], Cheops-NG [19], nmap [20], nessus [21], Super Scan 4 [22], Sam Spade)[23]
2	password cracking, sniff network connection between computers, Man-in-the-Middle attacks	L0phtCrack [24], John the Ripper [25], ethereal [26], nmap [20], hunt [27]
3	falsifying identity on a network, denial of service, detecting spoofing	DNSspoof and dsniff [28], arpwatch [29], datapool [30]
4	buffer overflow vulnerabilities in software	C programs used [31]
5	rootkit methodologies for regaining access to systems once compromised and methods of detecting rootkits	lrk4 [32], Knark [32, kern_check [33], chkrootkit [34], strace [35], rootkit Hunter [36], Hacker Defender [37]
6	back doors and Trojans for compromising systems	netcat [38], icmp-backdoor [39], Virtual Network Computing [40], Back Orifice 2000 [41]
7	honeynets and forensics	AIDE [42], "Scan of the Month Challenge" [43], FIRE [44], Coroner's Toolkit [45], Autopsy [46], Sleuth Kit [47]
8	firewalls	Linux firewall *iptables,* Zone Alarm [48], Cisco PIX 515E firewall
9	worm fundamentals, proliferation techniques, and spreading rates	Self-written worm [49], AnnaKournikova [50]
10	wireless security, cracking WEP keys	kismet [51], AirSnort [52]
11	virtual private network security	SSH VPN in Linux, IPSec VPN using a Cisco VPN Concentrator.
12	World Wide Web vulnerabilities	WGET [53], Nikto [54]
Capstone Competition	capture the flag network security exercise	attack and defend using all tools and techniques [55]

ratory, having a large enough network structure to provide background traffic to make sniffing for packets of interest (which are buried in considerable unrelated traffic) very realistic. In the denial of service assignment, the laboratory enables a method to generate a number of diverse denial of service sources, making identifying and blocking those sources more challenging. Releasing a worm on a larger network allows a more interesting study of propagation, while conducting such exercises on only one or two machines does not really allow this study to be conducted. At the other end of the spectrum, laboratory assignments of buffer overflows only require two machines: a victim and an attacker. Not all of the present assignments capitalize on the realistic network architecture; however, the more realistic the network is, the more excited the students are to work and interact in the laboratory environment. The main reason for the realistic design is to provide the infrastructure for challenging and complex security issues. Some of the laboratory assignments can be completed with only a few machines. In fact, using only a few machines is the typical methodology employed in the literature [2]–[11]. On the other hand, a more complex network enables many more possibilities and interesting exercises.

IV. COURSE ASSESSMENT

At the time of writing, this laboratory environment had been used in four semester offerings. Student evaluation of this laboratory is shown in Table II. Results are out of a possible 5.0.

TABLE II
LABORATORY ASSESSMENT RESULTS STUDENT EVALUATION OF CLASS AVERAGE VALUES: 5 = STRONGLY AGREE, 4 = AGREE, 3 = PARTLY AGREE AND DISAGREE, 2 = DISAGREE, AND 1 = STRONGLY AGREE

	Spring 2003	Fall 2003	Spring 2004	Fall 2004	Spring 2005
Lab Assignments Well Planned and Organized	4.4	4.4	4.0	4.4	4.9
Lab Assignments Covering Course Objectives/Content	4.6	4.8	4.3	4.0	4.5
Labs Explained Complex Material Clearly	4.6	4.7	3.8	3.9	4.7
Number of Lab Assignments Reasonable	4.6	4.4	4.3	4.1	*
Labs Covered Course Content/Objectives	4.3	4.4	4.9	4.3	4.0
Labs Appropriate Difficulty	4.0	4.1	4.4	4.4	*
Number of Students Responding to Survey	12	15	10	12	11

* = Institute Survey Changed and No Longer Asked These Questions

These assessment results, coupled with individual discussions with students, indicate that students find it very helpful to see and work with a realistic network topology that is representative of the type of environments they will encounter. Students have indicated that prior to creation of this laboratory that no good hands-on environment was available in which they could ethically and legally experiment and learn. As a result of "unethical attackers" being able to experiment and sharpen hacking skills on the Internet, students who wanted to become "ethical" network security professionals indicated that they believed they were at a disadvantage. They also stated that pure theoretical courses did not really teach them the skills they felt they needed to be competent network security professionals. Feedback has been received from students that this laboratory environment goes a long way toward removing the disadvantage "ethical" students felt they were encountering.

V. CONCLUSION

Having a totally isolated information security laboratory where students are allowed to launch attacks and attempt to defend against them is highly educational and highly motivating. Students having hardened their assigned machines and networks and then seeing them compromised are better prepared to understand how to prevent similar compromises in the future. Having a laboratory environment where students may experiment and be creative in a complex network environment is highly motivating for students.

The reconfiguration capability of the laboratory is highly beneficial in that one can change the network topology by just running a configuration script. One may reconfigure the laboratory for a firewall laboratory assignment without requiring any physical wiring changes or manual configuration changes to reset the firewall laboratory network configuration. One of the interesting capabilities is a “master reset” ability. When the laboratory is completed, one can easily set the network topology back to the original configuration. The laboratory has been used to accommodate up to a total of 90 students a semester. The limiting factor is the number of end station computers (25) that exist at present. The reconfiguration capability allows this laboratory equipment to be shared with an introductory networking class that also requires an isolated network [15].

The laboratory that was implemented has more network equipment and capability than many small companies. These small companies typically have a full-time information technology support person. There is a high workload level associated with maintaining and managing a laboratory of this type. A highly successful information assurance laboratory may be implemented with far less equipment [7]–[16]. What was discovered by implementing this laboratory at the other end of the capability and complexity spectrum is that having this level of complexity enables a level of realism unmatched by the simpler implementations. Exposure to realistic network background traffic, access control lists, firewall rules, network address translation, etc., in a network of the complexity presented here teaches valuable operational issues that theoretical and simpler laboratory implementations never encounter.

ACKNOWLEDGMENT

The authors would like to thank Cisco field representative J. Berg, who was instrumental in helping architect, select, and set up the equipment. The authors would also like to thank M. Nelson-Palmer, who made this laboratory possible.

REFERENCES

[1] The Internetwork Security Class Home Page (2004). [Online]. Available: http://users.ece.gatech.edu/~owen/

[2] A. Yasinac, “Information security curricula in computer science departments: Theory and practice,” in *Proc. 5th Nat. Colloquium for Information Systems Security Education 2001: A Security Odyssey*, May 22–24, 2001, [Online] Available: http://www.cs.fsu.edu~yasinsac/Papers/Yas01b.pdf.

[3] A. Yasinac, J. Frazier, and M. Bogdonav, “Developing an academic security laboratory,” in *Proc. 6th Nat. Colloquium for Information Systems Security Education 2002*, Redmond, WA, Jun. 3–7, 2002, [Online] Available: http://www.cs.fsu.edu/~yasinsac/Papers/YFB02.pdf.

[4] P. Mateti, “A laboratory-Based course on Internet security,” in *Proc. 34th SIGCSE Tech. Symp. Computer Science Education*, Reno, NV, Feb. 2003, pp. 252–256.

[5] Internet Security Lectures Home Page (2004). [Online]. Available: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Top/lectures.html

[6] M. Micco and H. Rossman, “Building a cyberwar lab: Lessons learned teaching cybersecurity principles to undergraduates,” in *Proc. 33rd SIGCSE Tech. Symp. Computer Science Education, Northern Kentucky Convention Center*, Feb. 2002, pp. 18–22.

[7] D. Ragsdale, Lathrop, and R. Dodge, “A virtual environment for IA education,” in *Proc. 2003 IEEE Workshop on Information Assurance U.S. Military Academy*, West Point, NY, Jun. 2003, pp. 17–23.

[8] J. Huss, “Laboratory projects for promoting hands-on learning in a computer security course,” *ACM SIGCSE Bull.*, vol. 27, no. 2, pp. 2–6, Jun. 1995.

[9] C. Frank and G. Wells, “Laboratory exercises for a computer security course,” *J. Comput. Sci. Colleges*, vol. 17, no. 4, pp. 51–54, Mar. 2002.

[10] P. Wagner and P. Wudi, “Designing and implementing a cyberwar laboratory exercise for a computer security course,” in *Proc. 35th SIGCSE Tech. Symp. Computer Science Education*, Norfolk, VA, Feb. 2004, pp. 402–406.

[11] J. Hill, C. Carver, J. Humphries, and U. Pooch, “Using an isolated network laboratory to teach advanced networks and security,” in *Proc. 32nd SIGCSE Tech. Symp. Computer Science Education*, Charlotte, NC, Feb. 2001, pp. 36–40.

[12] SANS Home Page (2004). [Online]. Available: www.sans.org

[13] CERT Coordination Center Home Page (2004). [Online]. Available: www.cert.org

[14] Insecure.org Home Page (2004). [Online]. Available: www.insecure.org/

[15] R. Abler, H. Owen, and G. Riley, “University methodology for Internetworking principles and design projects,” *IEEE Trans. Educ.*, vol. 46, no. 2, pp. 218–225, May 2003.

[16] The Information Warfare Analysis and Research Laboratory Home Page (2004). [Online]. Available: http://www.itoc.usma.edu/iwar/index.html

[17] The Critical Infrastructure Assurance Group Home Page (2004). [Online]. Available: http://www.cisco.com/security_services/ciag/initiatives/education/equipmentdonation.html

[18] The Vmware Home Page (2004). [Online]. Available: http://www.vmware.com/

[19] The Cheops-Ng Home Page (2004). [Online]. Available: http://cheops-ng.sourceforge.net/

[20] The Insecure.org Nmap Home Page (2004). [Online]. Available: http://www.insecure.org/nmap/

[21] The Nessus Home Page (2004). [Online]. Available: http://www.nessus.org/

[22] The Snapfiles.com Superscan Home Page (2004). [Online]. Available: http://www.snapfiles.com/get/superscan.html

[23] The Same Spade.org Windows Home Page (2004). [Online]. Available: http://www.samspade.org/ssw/

[24] The Security Focus Tools Page (2004). [Online]. Available: http://www.securityfocus.com/tools/1005

[25] John the Ripper Password Cracker Page (2004). [Online]. Available: http://www.openwall.com/john/

[26] The Ethereal.com Home Page (2004). [Online]. Available: http://www.ethereal.com/

[27] The Packet Storm Tools Page (2004). [Online]. Available: http://packetstormsecurity.nl/sniffers/hunt/

[28] The Monkey.org Dsniff Home Page (2004). [Online]. Available: http://monkey.org/~dugsong/dsniff/

[29] The LBNL Network Research Group Page (2004). [Online]. Available: http://www-nrg.ee.lbl.gov/

[30] The Packet Storm DoS Tools Page (2004). [Online]. Available: http://packetstormsecurity.nl/DoS/indexsize.html

[31] Smashing The Stack for Fun and Profit by Aleph One (2004). [Online]. Available: http://www.phrack.org/show.php?p=49&a=14

[32] The Packet Storm Rootkits Tools Page (2004). [Online]. Available: http://packetstormsecurity.nl/UNIX/penetration/rootkits/

[33] The Samhain Lab Library Home Page (2004). [Online]. Available: http://la-samhna.de/library/

[34] The Chkrootkit.org Home Page (2004). [Online]. Available: http://www.chkrootkit.org/

[35] The Strace Homepage (2004). [Online]. Available: http://www.liacs.nl/~wichert/strace/

[36] The Rootkit Home Page (2004). [Online]. Available: http://www.rootkit.nl/

[37] The Hacker Defender Home Page (2004). [Online]. Available: http://rootkit.host.sk/

[38] The GNU Netcat Project Home Page (2004). [Online]. Available: http://netcat.sourceforge.net/

[39] The Project-Hack.org Home Page (2004). [Online]. Available: http://www.project-hack.org/back.html

[40] The Real vnc Home Page (2004). [Online]. Available: http://www.realvnc.com/

[41] The cultdeadcow.com Back Orifice Home Page (2004). [Online]. Available: http://www.cultdeadcow.com/tools/bo.html

[42] The SourceForge AIDE Home Page (2004). [Online]. Available: http://sourceforge.net/projects/aide

[43] The Honeynet.org Challenges Home Page (2004). [Online]. Available: http://www.honeynet.org/misc/chall.html

[44] The F.I.R.E. Home Page (2004). [Online]. Available: http://fire.dmzs.com/

[45] The Computer Forensics Home Page (2004). [Online]. Available: http://www.porcupine.org/forensics/

[46] The Autopsy Forensic Browser Home Page (2004). [Online]. Available: http://sleuthkit.sourceforge.net/autopsy/desc.php

[47] The Sourceforge.net Sleuthkit Home Page (2004). [Online]. Available: http://sleuthkit.sourceforge.net/sleuthkit/desc.php

[48] The Zone Labs Home Page (2004). [Online]. Available: http://www.zonelabs.com/store/content/home.jsp

[49] C. Church, T. Schmoyer, and H. L. Owen, “Design and implementation of a simple class room laboratory internet worm,” *J. Security Educ.*, vol. 1, no. 2/3, pp. 39–53, Feb. 2005.

[50] The Symantec vbs.ss@mm Worm Page (2004). [Online]. Available: http://www.symantec.com/avcenter/venc/data/vbs.sst@mm.html

[51] The Kismet Home Page (2004). [Online]. Available: http://www.kismetwireless.net/

[52] The Airsnort Home Page (2004). [Online]. Available: http://airsnort.shmoo.com/

[53] The Wget Home Page (2004). [Online]. Available: http://www.gnu.org/software/wget/wget.html

[54] The Nikto Home Page (2004). [Online]. Available: http://www.cirt.net/code/nikto.shtml

[55] The UCSB Capture the Flag Home Page (2004). [Online]. Available: http://www.cs.ucsb.edu/~vigna/CTF/

Randal T. Abler (M’00–SM’05) received the B.S.E.E, M.E.E, and Ph.D. degrees from the Georgia Institute of Technology, Atlanta, in 1986, 1992, and 2000, respectively.

He is currently an Assistant Professor at the Georgia Institute of Technology with a joint appointment to the School of Electrical and Computer Engineering and to the Regional Engineering Program in Savannah, GA. His research interests include the Session Initiation Protocol, Quality of Service implementations, and Internet technology in support of distributed education.

Didier Contis received the B.S. degree from the School of Mines of Nantes, France, and the M.S.E.E. degree from the Georgia Institute of Technology, Atlanta, both in 1996.

Currently, he is a Research Engineer in the School of Electrical and Computer Engineering, Georgia Institute of Technology. His research interests include network security as well as distributed and embedded intrusion detection systems.

Julian B. Grizzard (S’99–M’02) received the B.S. degree in computer engineering from Clemson University, Clemson, SC, in 2002 and the M.S.E.E. degree from the Georgia Institute of Technology, Atlanta, in 2004. He is currently working toward the Ph.D. degree at the School of Electrical and Computer Engineering at the Georgia Institute of Technology.

His research interests include network and operating system security.

Henry L. Owen (M’00–SM’03) received the B.S.E.E, M.S.E.E., and Ph.D. degrees from the Georgia Institute of Technology, Atlanta, in 1979, 1983, and 1989, respectively.

Currently, he is a Professor in the School of Electrical and Computer Engineering, Georgia Institute of Technology. His research interests include network security and Internetworking.