Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

The Success of the UT IEEE Communications Society

George Chamles and Adam Pridgen, *The University of Texas at Austin*.

Abstract – Over the course of two and a half years, students at the University of Texas at Austin have developed a network and security research group that combines presentations, classes, and projects to produce highly skilled student researchers in a very short period of time. Their program exists independent of any official curriculum and is designed to combine self-motivated students' desire to learn with an environment that allows them to exercise on that knowledge. This paper details the evolution and current structure of the group. It is intended for educators and students interested in creating similar organizations.

Index terms: Honeynets, Student Organizations

I. Introduction

In October of 2001 the leadership of the University of Texas at Austin student chapter of the IEEE Communications Society (Comsoc) fell into the hands of a small group of undergraduate students who shared a growing interest in networking and security. At the time, UT had only a small handful of upper-division courses related to those areas in the Electrical and Computer Engineering (ECE) and Computer Science Departments. The group, primarily sophomores and juniors, did not want to wait until the advanced courses and decided to create an environment where they could learn the material on their own. The new officers inherited a closet-sized office, four ancient 486 computers running Windows 2000, a green leather couch, and a floor safe no one knew how to open.

The primary activity for most of the UT engineering student groups at the time was monthly information sessions presented by local tech-sector companies. While the presentations were often related to engineering, announcement fliers typically only listed the company presenting, the student group sponsoring the event, and the type of free food being delivered at the meeting's conclusion. Student members had little interaction with the student groups outside of the presentations, and the officers spent most of their time finding companies to sponsor their next meeting.

The Comsoc officers were more interested in learning rather than pursuing corporate contacts but recognized that student presentations did have their merits. Unlike their fellow student organizations, they decided that the presentations would be led by the officers themselves. Presenting on technical topics in networking and security would require the officers to learn the material to the point that they felt comfortable passing that knowledge on to others.
.

II. Presentations

Comsoc's first presentation, "Hacking Wireless Networks," was given in November of 2001, the same month UT finished deploying wireless networks throughout the campus. The presentation included a detailed examination of the recently uncovered weaknesses in the Wired Equivalent Privacy encryption scheme used in the IEEE 802.11b protocol [1] followed by several demonstrations of techniques that malicious hackers could use to fool students into disclosing their UT electronic ID and password to rogue wireless access points. Among the attendees was the ECE professor responsible for the creation and maintenance of UT's wireless network system. At the end of the presentation he offered the officers part-time jobs doing security research at IBM and has been the organization's primary advisor ever since.

Comsoc began to grow and expand over the course of the following year. By the fall semester of 2002 the group had moved into an office that was twice the size of their old one and had scrapped everything from the previous room except the leather couch. The group began to build their lab using a set of twelve Pentium 266 computers, surplus from the ECE computer labs, and a pair of faster systems that were constructed using spare parts collected from the officers.

Several of the officers had been busy with part-time jobs and had not taken the time to put together any student presentations during the spring 2002 semester. That fall they decided to get back into the process with a series of

George Chamales is a senior at the University of Texas at Austin and a 2003 Department of Homeland Security Scholar. Adam Pridgen is a junior in Electrical Engineering at the University of Texas at Austin.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

monthly, one and a half hour long presentations on topics in network security.

The three monthly presentations during fall 2002 included "Introduction to Network Security," "Firewall Configuration and Deployment," and "Malicious Code: Viruses, Worms, and Trojans." Each presentation had a significant demonstration component that allowed the attendees to see the topics being discussed in action. During the network security presentation the officers showed the attendees each step of the network attack process culminating in the live compromise of a computer running Windows 2000. In the second presentation they showed how firewalls could be used to prevent attacks by thwarting some of the activities of the previous presentation. In the presentation on malicious code, officers demonstrated the actions of several prevalent viruses then showed how anti-virus software could be used to detect and remove them.

The new presentations, given in the evenings, regularly attracted crowds of over sixty students, faculty, and staff. Each one was followed by a question and answer session that often lasted more than an hour. They were advertised using flyers that listed the topic of the presentation, a brief illustration related to the topic, and Comsoc's name and logo. There were no free dinners.

III. Workshops

That semester several students who had been regular attendees at the presentations asked if they could join the group and begin to learn networking and security. This was an unexpected development for the officers. They had been leading the presentations in order to test their understanding of the material; they had not expected to pique the interest of others. The officers instructed the new students to install and configure spare machines in the office with the Linux operating system. Linux installation allowed the new students to learn the organization's operating system of choice and, more importantly, served as a stopgap measure while the officers decided what to do next.

By the next semester, spring 2003, almost every flavor of Linux had been installed and reinstalled on each of the now twenty-five machines in the Comsoc office by a set of new members nearly twice the size of the original group. Many of the new students were looking for other things to do to occupy their time. The officers decided on a set of introduction workshops on networking and security for that semester's presentation series. Instead of the lecture/demonstration, the workshops brought students into a computer lab to work through the material in a hands-on environment.

The workshop series took place in the evenings in one of the computer labs in the ECE Department and were entitled: "Introduction to Linux," "Introduction to Networking," and "Securing Linux." In the Introduction to Linux workshop students configured their own virtual Linux machine using User Mode Linux [2]. In the networking workshop they examined packet logs and experimented with basic networking connectivity tools. In the final workshop on Linux security they combined the skills from the previous two workshops to secure and defend a Linux virtual host.

To the surprise of the officers the new members internalized the information extremely quickly and, using the workshops as a base, began studying the material on their own. By the end of the spring semester most of them were running Linux as their primary operating system and several of the new members had taken summer jobs running network intrusion detection systems for businesses around Texas.

IV. Projects

The officers had been working on a variety of projects in networking and security since taking over the society. They used the computers in the Comsoc office as a test bed to learn techniques in network design, firewall construction, and intrusion detection system deployment. These projects were useful for learning the basic topics and provided the basis for the presentations and workshops given to the UT community. The officers quickly advanced beyond the introductory material, and in 2002 the officers began three ongoing projects to provide more challenging topics to work on.

Two of the officers built a honeynet in fall 2002 as part of their senior research project. A honeynet is a network of computers placed on the Internet for the sole purpose of being probed, attacked, and exploited by malicious hackers. Behind the scenes honeynet administrators monitor the hacker's actions using a variety of network and host-based tools. A second set of network tools are used to prevent the compromised machines from being used as a launch-point to attack systems that are not inside the honeynet. The honeynet the officres built was connected to the Internet and hacked by a variant of the Code Red worm [3] in less than five minutes.

In January 2003, Comsoc was accepted into the Honeynet Research Alliance [4], an international research organization at the forefront of honeynet development. Comsoc was the tenth member of the Alliance and second university member accepted. At the time, the Alliance was in need of groups to test and debug the tools developed by members around the world. Comsoc volunteered to take part and began testing a suite of tools

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

designed to monitor kernel-level activity on Linux, Windows, and OpenBSD operating systems.

In fall 2001 and spring 2002 a group of seniors in the ECE department had begun working on a voice over IP (VoIP) system using hardware and software donated from Cisco Systems [5]. The VoIP system could allow internet-based phones to replace regular telephone systems throughout the department. Comsoc inherited the system in fall 2002 after the group of students who had started the project graduated. By the end of the semester Comsoc members had completely reengineered the system and had started deploying VoIP phones in offices around the department.

Also in fall of 2002, Comsoc officers began an intra-society hacking competition to provide a safe and legal arena to experiment with offensive security technology. The students felt that the best way to defend against hackers was to understand how they operate; the "know thy enemy" approach. The game, called capture the flag, challenged teams of members to break into hosts on a network and defend those hosts from attack by other teams. The competition was patterned after an event of the same name held at the Defcon security conference in Las Vegas [6]. All offensive attacks took place on a network isolated from the main campus system and the officers established a zero-tolerance policy for any member suspected of using their knowledge of offensive techniques illegally.

The projects gave senior members the opportunity to expand and deepen their knowledge of networking and security and generated a great deal of publicity for the organization. The VoIP deployment introduced members of the ECE faculty to Comsoc's activities. Membership in the Honeynet Research Alliance led to interaction with several security companies around the Austin area and an article in the student paper [7].

V. Problems

The new workshop format and ongoing projects caused an influx of new members throughout the spring of 2003. The new members and the complexity of the main projects quickly led to several problems with the organization of the society.

The ongoing projects required a great deal of experience that many of the new members lacked. This caused a separation between the experienced officers who were busy working on the projects and the new members who were interested in taking part. The new students were discouraged by their inability to work on the more advanced projects.

The projects themselves also had their difficulties. The officers had treated the society's earlier projects in networking and security as part-time hobbies, but the new projects required a high degree of organization and administration. Lacking that organization, progress on the ongoing projects ground to a crawl.

Nowhere was Comsoc's disorganization more pronounced than in the office itself. The 20’x25' office contained nearly forty computers that had been placed in the room with little attention to organization or cable control. The disorganization of the society's working area contributed to everyone's frustration. Comsoc had attracted a dedicated group of members that continued to participate in the organization’s events despite these difficulties. It was clear that Comsoc required a formal organizational structure.

VI. A New Structure

The officers spent the summer of 2003 brainstorming ways to address the difficulties of member participation and project organization. By the fall of 2003 they had sketched out a new structure for the organization. This new structure took a tiered approach to presentations and projects that could satisfy the educational needs of beginners as well as the research interests of the advanced members. Comsoc has used the following structure for the last year.

A. Presentations

Three separate types of presentations are given by the society on a regular basis. Weekly meetings, held on Wednesday's at 7 PM, are used to introduce new students to the society's activities and expose regular members to topics they may not be familiar with. The meetings begin with a thirty-minute presentation by a member of the society on some aspect of networking or security that he or she finds interesting. The second half of the meeting is used by the officers to discuss society organization, review project status, and discuss upcoming events.

The hands-on workshops on Linux, networking, and security are given early in the semester to provide new members with a solid foundation to expand on as they continue to work with the society. The workshops are designed to be repeated every semester and the students are currently working on modified versions that can be done entirely online from a computer with Internet access.

The weekly presentations and regular workshops are designed to attract beginner students and maintain the interest of novice members. A third presentation type, the "hardcore meeting," covers more technically challenging

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

material for the novice and advanced students. The hardcore meetings last approximately one hour and are held at noon on Sundays. All presentation materials from the workshops and weekly meetinsg are archived on the Comsoc website [8].

In addition to the presentations, regular members and new students meet in the office starting at 1 PM on Sunday to work on their various projects. These informal "geek-out" sessions allow students of all experience levels to interact with one another and have led to a solid sense of community in the group. Members occasionally begin the afternoon with a barbecue and often stay in the office until late in the evening.

B. Projects

The society's wide array of projects provide students the opportunity to get involved based on their experience and interests. Newcomers to the group always begin by installing and configuring Linux on their own computer and are strongly encouraged to use Linux as their primary operating system. If a member does not have a computer of his or her own, a spare machine from the office fleet is usually found and the member can come to the office throughout the week to work on it.

Students who have gained a working knowledge of Linux can choose from a set of short-term projects to expand their skills and decide what topics interest them most. The projects are typically thought up by the senior officers and are posted on the Comsoc site. Previous projects have included setting up remote printing from the Comsoc office to the printers in the main IEEE student chapter office, installing an in-office streaming music server, and configuring an office web cam.

Students are invited to take part in the more difficult ongoing projects as they gain more experience. The capture the flag game is an outstanding resource for intermediate students looking to further hone their knowledge of Linux, networking, and security while working with the Honeynet Research Alliance and the VoIP system are typically reserved for more advanced students. By the time the students have begun to take part in the advanced projects they are encouraged to begin presenting at the weekly meetings and to act as proctors in the hands-on workshops.

A team lead, typically an advanced member, oversees each major project. Team leads handle the direction of the project, manage the members taking part in the project, and present regular status reports at the Wednesday night meetings. Members are not allowed to lead more than one project at a time.

The continuum of projects keeps members active in the group and encourages them to continually develop their skills so they can work on more advanced projects. The speed with which studenst progress through the projects is one of the most exciting aspects of the organization. The team leads for both the capture the flag competition and honeynet project as well as the students who currently lead the workshop series all began working with Comsoc during fall 2002.

VII. MOVING FORWARD

Comsoc has evolved into one of the most active student organizations in the UT Austin Electrical and Computer Engineering Department. In the past year, Comsoc members have taken part in presentations by the Honeynet Research Alliance to US and British intelligence and presented to several professional security groups in the Austin area. The members are currently organizing an inter-collegiate cyber-defense exercise similar to their game of capture the flag. The competition will include several universities around Texas and will be the test run for a nation-wide competition being organized by a group of senior faculty and staff from universities around the country. In spring 2004 the members completed the installation and configuration of the VoIP system's voicemail server, allowing the VoIP phones to completely replace regular telephone lines throughout the department.

The society continues to face new challenges. In March of 2004 the officers chose to expel a member who had made several improper remarks concerning the use of malicious hacking technology. Comsoc officers are currently drafting a constitution and code of ethics for the organization in response to this event and other concerns. The Comsoc office has reached a critical mass of fifty computers, a small refrigerator, a microwave, and a leather couch. The society has tripped the circuit breakers for the office several times and is working with the ECE department on a second room to distribute the load. Finally, new projects including an ongoing community service project, establishing an IPv6 node on Internet2 [9], and greatly expanded activities with the Honeynet Research Alliance have senior members of the group concerned that they are stretching themselves too thin. They are looking for ways to balance their time and the variety of interesting projects they could work on.

These difficulties represent the expected challenges of a healthy organization and overall the members are very pleased with the structure and operation of the society. The last of the original officers graduates in May 2004. Replacing the original group is a new set of highly

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

motivated officerss who will continue to expand the society and maintain Comsoc's position as one of the most outstanding student organizations in the UT Electrical and Computer Engineering Department.

VIII. REFERENCES

[1] A. Stubblefield, J. Ioannidis, A. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", ATT Labs Technical Report, TD4ZCPZZ, Revision 2, August 21, 2001. http://citeseer.ist.psu.edu/article/stubblefield01using.html.

[2] User-mode Linux, "User-mode Linux Community Site," March 2004, http://usermodelinux.org.

[3] Carnegie Melon, Software Engineering Institute, CERT Cooridantion Center, "CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL," March 2004, http://www.cert.org/advisories/CA-2001-19.htm.

[4] The Honeynet Project, "The Honyenet Project: Research Alliance," March 2004, http://honeynet.org/alliance.

[5] Cisco Systems, Inc., "Cisco Systems, Inc.," March 2004, http://cisco.com.

[6] Def Con, "Welcome to DEF CON, the Largest Underground Hacking Convention in the World," March 20004, http://defcon.org.

*[7] "UT students hunt down hackers via Honeynet Project," *The Daily Texan*, vol. ***, pp ***, April ***, 2003.

[8] The University of Texas at Austin IEEE Communications Society, "The UT IEEE Communications Society," March 2004, http://utcomsoc.org.

[9] Internet2, "Internet2-Home," March 2004, http://www.internet2.edu

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE