2006-1998: COMPUTER SECURITY SUMMER CAMP FOR HIGH SCHOOL STUDENTS

Douglas Jacobson, Iowa State University

Dr. Doug Jacobson Associate Professor Department of Electrical and Computer Engineering
Iowa State University Ames, IA 50011

Computer Security Summer Camp for High School Students

Abstract

Iowa State University's Information Assurance Center and the Iowa Chapter of InfraGard are collaborating to give juniors and seniors in High School an opportunity to visit ISU for a three day summer camp to gain knowledge in computer security. The camp has been offered twice and is conducted by Iowa State University professors in the security field, community experts, and graduate students that are in the security program at ISU. The camp provides an overview of computer security, educates students on computer networking security concepts, uses of different types of cryptography, and general understanding of how information warfare is conducted. This is a "hands on" lab-oriented camp that provides students an opportunity to work with state of the art equipment and to learn from industrial and academic leaders. Students will work with current technology like firewalls, Virtual Private Networks, and intrusion detection systems. Students setup security systems, analyze attacks, and see equipment in use. The last day of camp the students defend their networks against a red team "hackers" consisting of security professionals. One afternoon the students travel to Des Moines to tour different companies that are related to computer security.

We expect students to gain interest in the area, broaden their knowledge on computer security, have fun, and meet faculty and experts that are able to answer questions about their occupations, and give them insight as to what the future could hold for them in computer security field. The camp will also perk their interest in coming to ISU or other universities after high school.

This paper will outline the camp objectives, the planning process, and the recruitment process. The importance of a partnership between academia, government, and the private sector will be discussed. The changes from the first year to the second year based on feedback will also be presented in addition to plans for the third year.

Introduction

The growing need for information security professionals is well documented. Several universities offer comprehensive programs in information assurance and security, primarily targeted at the graduate level. The number of schools offering undergraduate opportunities is even smaller. The end result is a severe shortage of graduates proficient in the technology and policy issues critical to the security of the information infrastructure. While several universities have started programs to address these needs, this only solves a small part of the problem. According to the National Strategy to Secure CyberSpace[1] released by the President of United States in 2003, "Many cyber vulnerabilities exist because of a lack of cyber security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers, chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructure regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities."

In response to the national need to increase the number of graduates who are knowledgeable about security issues, Iowa State University and its Information Assurance Center have created several initiatives to increase the awareness in computer security and to increase the number of students pursuing a degree with a focus on computer security. These programs include a summer workshop for faculty, a cyber defense competition for college students and IT professionals. We also saw a need to reach out to high schools to try and increase the number of students interested in computer security. To this end the ISU Information Assurance Center and the local chapter of InfraGard[2] created the Computer Security Summer Camp. The camp was first offered in the summer of 2004 and was modified based on feedback and was offered again in 2005.

The Computer Security Summer Camp is synergistic with existing instructional activities at Iowa State University and fits well into our long history of community outreach. Iowa State University has been teaching computer security courses since 1995. Iowa State University has a robust program in computer security and offers two graduate degrees in information assurance. A masters of Science in Information Assurance and a 4 course graduate certificate in Information Assurance. While we do not offer a BS degree in computer security students interested in computer security can take our graduate courses. In our core graduate class about 30 percent of the students are undergraduates. We also offer one undergraduate security course. ISU faculty members are also participating in development of national standards for security education and Iowa State University was named as a Charter Center of Excellence in Information Assurance Education by the National Security Agency in 1999. Our initial target audience for the Computer Security Summer Camp is high school students who will be entering their senior year of high school in the fall.

Goals and Objectives

The primary goal of the computer security summer camp is to raise awareness of computer security issues and career possibilities. When the camp was first designed the goal was to provide students with an overview of many of the important issues in computer security through a laboratory oriented curriculum. From the initial conception of the camp there has been strong industrial support through the local chapter of InfraGard. The role of industry will be described throughout the paper. The goals of summer camp are provided below.

- Convey an overview of computer security
- Educate students on computer networking concepts as they pertain to security
- Instruct students on the uses of different type of cryptography
- Provide an understanding of how information warfare is conducted
- Provide an opportunity for students to interact with security professionals
- Visit several local companies to understand what types of jobs are available in computer security
- Introduce students the concepts of computer forensics.

These goals are achieved through a combination of classroom instruction, hands-on activities, and company tours. One of the goals is to have the students defend networks against hackers in a small cyber defense competition. This activity was added during the second summer camp and will be discussed in more detail later in the paper. In addition to the goals described above we

identified a set of learning outcomes for the camp, which are listed below. The outcomes labeled with a * were new outcomes for the summer 2005 camp.

At the end of the camp the students should be able to:

- Assemble a computer from parts and install an operating system *
- Identify security risks in common computer and network activities
- Sniff network traffic and decode packets
- Setup and configure a firewall and an intrusion detection system*
- Setup, configure, and secure an email server, web server wireless access point*
- Recover data from a forensic image
- Identify possible security jobs
- Hide images within other images and then recover the original data
- Identify the strengths of cryptography
- Defend networks from attacks*
- Understand the ethical issues associated with security and hacking

Even though we have goals and learning outcomes we did not create any formal method to evaluate whether the students achieved the outcomes. We did surveys after the camp and based on the first year surveys we made several changes, which are discussed later in this paper.

Camp Venue

The first camp was housed on the ISU campus with most of the instruction taking place in a computer lab. While it was convenient for the faculty and students to be on campus, it was difficult to reconfigure general purpose teaching labs to support the types of security based activities we wanted for the summer camp. The second year of the camp was moved to the ISEAGE research lab.

Iowa State University has created the **Internet-Scale Event and Attack Generation Environment** (ISEAGE)[3] (pronounced "ice age") facility, which is housed at the Iowa State University research park in a 3000 sq. ft. facility. ISEAGE is a first of its kind facility in a public university dedicated to creating a virtual Internet for the purpose of researching, designing, and testing cyber defense mechanisms as well as analysis of cyber attacks. Unlike computer-based simulations, real attacks will be played out against real equipment. Researchers and vendors are working hard to provide products and services to help defend against cyber attacks, but users of these technologies often do not have any mechanisms to test or even try out these defenses. Law enforcement agencies and forensics analysts have no way to replay attacks or recreate a cyber crime scene. The ISEAGE facility provides a controlled environment where real world attacks can be played out against different configurations of equipment. ISEAGE contains a vast warehouse of attack tools that will be able to simulate point-to-point and distributed attacks. ISEAGE represents a new paradigm in the area of security research, cyber forensics, and will enable new and innovative research needed to solve the current security problems facing the world today.

Figure 1 shows a block diagram of ISEAGE and how it is connected to support the summer camp. As shown in the figure, ISEAGE is a 64 node computer cluster that is capable of representing any IP address space. In addition to IP address space mapping, ISEAGE also provides tools to generate background traffic and background attacks. This helps create a realistic environment where not all traffic seen by the students is coming from the hackers.

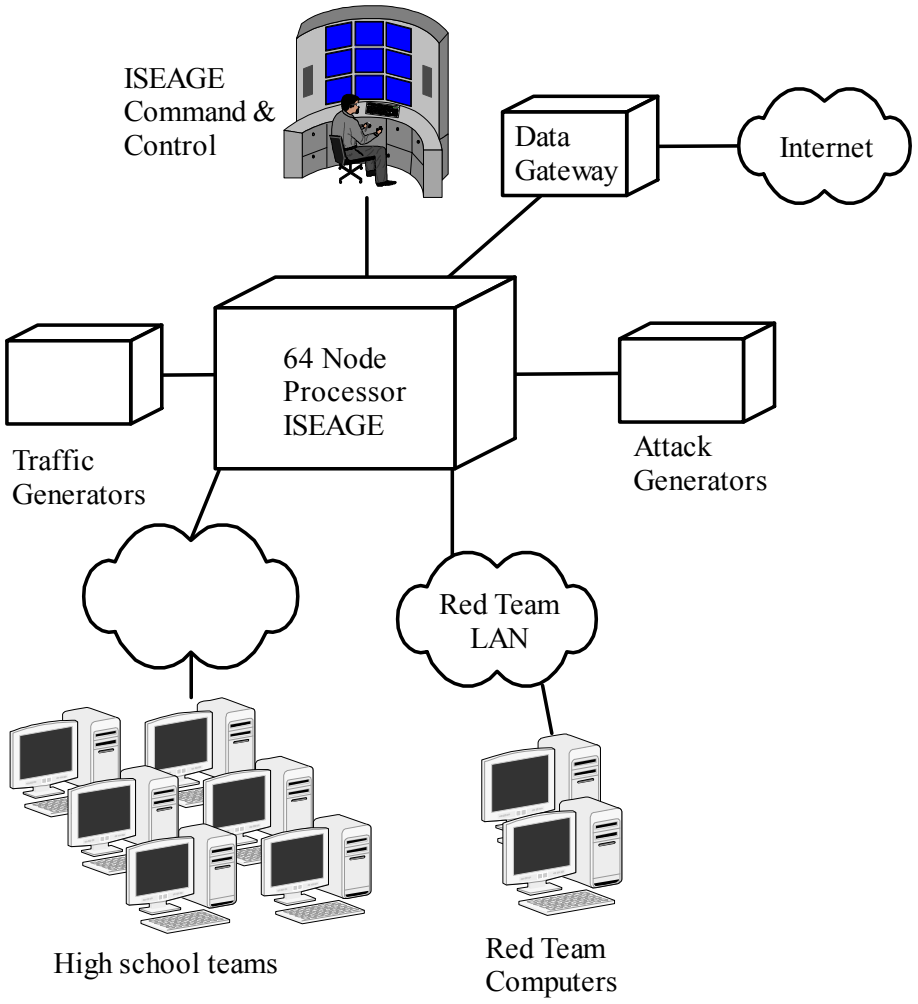

Figure 1. ISEAGE Diagram

Camp agenda and curriculum

The summer camp was designed from the beginning to be three days plus an opening session on Sunday, which allows for easy travel. We also have an open house and dinner the last night to give the students a chance to show their parents and friends what they did during camp. We had talked about making the camp longer than three days, but we decided three days would be long enough to have a meaningful experience and not too long as to being boring. The students live in the dorms on campus with a graduate student mentor. The mentor serves two roles, the first is to watch the students and make sure they have everything they needed. However, the most

important role is to be there to talk to the students about security (or anything else they want to talk about)

The table below shows the agenda and curriculum for the 2005 summer camp. In the following sections of the paper we will discuss some of the lab experiments and provide a description of some of the camp highlights.

Summer Camp Agenda and Curriculum

Sunday:

Time	Topics	Labs	Where
2:00 – 5:00	Check in		Dorm
5:30 – 5:45	Introduction		Dorm
6:00 – 9:00	Build Computers		ISEAGE
6:45 – 7:30	BBQ		ISEAGE
9:00 – 9:15	Travel back to Dorms		Dorms

Monday:

Time	Topics	Labs	Where
8:00 – 8:30	Intro to camp		ISEAGE
8:30 – 9:30	Intro to security concepts		ISEAGE
9:30 – 10:15	Security stories		ISEAGE
10:15 – 10:30	Break		ISEAGE
10:30 – 11:00	Ethics	Group Activity	ISEAGE
11:00 – 12:00	Services (www, email, etc.)		ISEAGE
12:00 – 12:30	Lunch		ISEAGE
12:30 – 1:30	Networking	Sniffing	ISEAGE
1:30 – 2:30	Steganography	Hide your face in a picture	ISEAGE
2:30 – 3:30	Securing your environment	Firewalls, NAT, IDS, etc	ISEAGE
3:30 – 5:30	Plan attack lab		ISEAGE
5:30 – 6:30	Dinner		ISEAGE
6:30-8:30	Movie and games		ISEAGE
8:30-8:45	Travel back to dorms		Dorms

Tuesday

Time	Topics	Labs	Where
8:00 – 9:00	Wireless security		ISEAGE
9:00 – 10:00	Crypto	Crack	ISEAGE
10:00 – 10:15	Break		ISEAGE
10:15 – 11:30	Set up for attack Lab		ISEAGE
11:30 – 12:30	Tour Palisade & Lunch		ISEAGE
12:30 – 8:00	Des Moines tours		
12:30 – 1:30	Travel to Ankeny		
1:30 – 2:45	Tour Cyber Crime Lab		Ankeny
3:00 – 3:45	Tour Principal data center		Altoona
4:00 – 4:45	Tour Farm Bureau		Des Moines
5:00 – 6:00	Pizza		Farm Bureau
6:00 – 8:00	Career discussion		Farm Bureau

8:00 – 9:00	Travel to Ames		
9:00 – 12:00	Set up for attack lab		ISEAGE
12:00	Travel to Dorms		Dorms

Wednesday

Time	Topics	Labs	Where
8:00 – 8:30	Forensics Presentation		Campus
8:30 – 9:15	Forensics Lab	Forensics	Campus
9:15 – 9:30	Tour of Coover Hall		Campus
9:30 – 9:45	Travel to ISEAGE		
10:00-12:00	Set up for attack lab		ISEAGE
12:00 – 1:00	Lunch & final set up		ISEAGE
1:00 – 5:00	Information Warfare	Attack Lab	ISEAGE
5:00 – 6:00	Open house		ISEAGE
6:00 – 7:30	Dinner and awards		ISEAGE

Lab experiments

Feedback from the first year indicated that the campers wanted more hands-on activities. In 2005 we added several additional labs experiments. With the exception of the attack lab the students used the computers they assembled the first night of the camp. These labs are described below:

Networking: The first lab experiments were based around the networking lecture. The students had already assembled computers which they used for the experiments. The computer assembly exercise which was conducted Sunday night will be discussed in the next section of the paper. The networking lectures were designed to give the students an introduction to networking concepts. The lab exercises were intermixed within the lectures. They used a packet sniffing program[4] to watch the traffic on the network and to decode the packets. They looked for packets that contained user names and passwords. We also introduced the idea of encrypted traffic and they saw that they could not longer decode the data.

Steganography: This session was used to show the students how they can hide pictures inside of other pictures and how this can be used in security. They used software that let them experiment different methods of data hiding. Next year we want to take pictures of the campers and then hide them within other pictures. We will then send the pictures home with them. Maybe even a camp group picture done that way.

Wireless Security: This session provided lectures about how wireless worked and how wireless networks are insecure. The students setup a wireless access point and then captured the traffic looking for usernames and passwords. They then configured the access points to provide security and saw that they could not longer decode the data within the packets. We also talked about wardriving (looking for access points while driving around). We saved that experiment for the trip to Des Moines and will be discussed in the highlights section of the paper.

Crypto: This session provided an insight in to how cryptography works and how hard it is to break. The students had several lab experiments where they learned how to encrypt and decrypt data and how to break things like password files.

Forensics: The forensics lab is located on campus and the students were given a lecture on how forensics is used to recover data and to solve crimes. They were given a disk drive with data hidden on it and used state of the art forensics software to find the evidence and solve the case.

Attack Lab: The attack lab is the focal point of the summer camp. We added this lab during the second summer camp. The students were told about the lab on the first night and were given several opportunities to plan their defenses and to implement them. This was the only lab where the students worked in pairs. The goal of the lab is to setup a small network and then defend the network against a group of hackers. The hackers are security professionals from InfraGard. The attack lab is based on the cyber defense competition[5,6,7] we hold for college students. For the summer camp the students were divided into teams of two. The students were given time Monday night to develop a plan for their networks. Monday night we had pizza and a movie where several security professionals attended. They talked to the students about the attack lab and provided some advice about different security methods.

They were given time on Tuesday, before leaving for the tours, to work on the attack lab. After the career night they asked to work on the lab instead of going back to the dorms. They stayed and worked on the lab until midnight. They worked on the lab on Wednesday and the hackers came after lunch. The hackers were local IT professionals and security experts. Several of the hackers were part of the career night panel. The students then spent about 3 hours defending their networks against the hackers. Following the hacking session the students met with the hackers to talk about what happened during the attack lab.

Highlights

In the previous sections of the paper the details of the summer camp were discussed. During the three days of the 2005 camp several events come to mind that highlight the experiences the students had.

One of the several changes we made for the 2005 camp was the first night team building activities. The first night the students were picked up at the dorms and taken to the ISEAGE research facility. They were given a brief tour and then taken into a conference room where on the floor there were boxes with computer cases, motherboards, processors, memory, and disk drives. They were told they need to assemble the computers they would be using during the camp and install the Windows XP operating system. Once they had the systems built and running they could play LAN based games. We had several graduate students that were available to help answer questions, but the campers were pretty much on their own to build the computers.

This activity was a great success; the campers jumped right in and were very focused on putting the computers together. A couple of students had done this before, but the majority of campers had not put a computer together from scratch. While they were working on putting the

computers together we started supper and when it was time to eat, we could not get the campers away from the computers. They had the computers assembled and the software installed after a couple of hours. During that time they were helping each other and working together to get the computers built. This was a great team building exercise. After they finished putting the computers together they challenged the graduate student mentor to play a computer game. This was a great way to have the students interact with the mentor and to get to know him. We had planned to finish by 9 pm, but the campers insisted on staying and playing. We took them back to the dorms around midnight.

Another change we made from the first year was to add a session after the first full day where the students could relax and interact with security professionals. The first year we went to a 4H camp and did various team building activities. The feedback on the outdoor activity was negative, so the second year we decided to have pizza, movies and games. We invited members of InfraGard to come and interact with the campers. This activity was much better received by the campers, the security professionals talked about security issues and we watch a couple of videos that were based on real attacks. The students really enjoyed talking with the security professionals and had lots of good questions. The students also played more LAN games and did not want to leave until midnight.

On Tuesday we started the morning with a discussion on wireless security and then toured an Ames based security company. After lunch we loaded up a van and headed for tour of several companies. The first stop was the forensics lab in Ankeny, which is about 20 miles away. To reinforce the concepts we showed them about wireless security we took two laptops equipped with special antennas that allowed the students to wardrive (see how many wireless networks they can find). Wardriving is legal as long as you don't try to break into any of the networks you find. On the way to our first tour location they found about 100 wireless networks and for the entire 50 mile trip they found over 300 wireless networks. They discovered about half did not security and could easily be compromised. The students had a great time doing this and it helped pass the time in the van. We talked to them about the legality of wardriving and cautioned them about hacking.

During the first year of the camp we had a career night where the students were able to ask questions of a panel of security professionals that represented several aspects of the computer security field. The companies represented ranged from the FBI, military, banking, insurance, to network security companies. It was a great success the first year and we continued it the second year. We were concerned the first year that students wouldn't have very many questions and so we were prepared to ask questions of the panel. Instead the students had a lot of questions and many were very tough questions. The panel members also enjoyed the interaction with the students and several of the panel members were on the panel the second year.

As was discussed above, the attack lab was added in the second year. The students looked forward to the lab from the first night. They enjoyed the idea of defending their networks against "real" hackers. They really started to focus on the lab Tuesday morning before the tour and instead of going home after the career night they wanted to go back to ISEAGE and work on the lab. During the setup times for the attack lab we had several graduate students available to answer any questions and help them find software. For most of the campers this was the first

time they had ever setup web servers, firewalls, and the UNIX operating system. They also spent several hours on Wednesday morning getting ready for the hackers. Once the hackers arrived and started hacking the students had to defend their networks. They were kept very busy for the three hours the hackers were trying to break in.

After three hours of hacking we called a truce and the hackers had a chance to talk with the students. During the debriefing the hackers showed the students some of the tools they used and the methods they tried. Most of the students did quite well against the hackers, but much of this was due to the fact their networks were very simple and they did not have many services for the hackers to attack. The students did enjoy talking to the hackers and were quite excited about the lab. After the debriefing the students had some time to just talk and wait for the dinner and awards. When their parents showed up they were very excited to show them the networks they had built and defended. You could tell by the conversations that they had a good time and were very excited about the lab and the camp. After dinner each student received a certificate and was asked to say a few words about their experience.

Feedback and Lessons learned

After each camp we surveyed the students to determine what to change and what to keep. The surveys were a combination of short answers and questions using a five point scale. The table below shows the results of the survey with the percentage answering each range (1-2 is low and 4-5 is high).

Topics	1-2	3	4-5
Build Computers	0%	17%	83%
ISEAGE		17%	83%
Intro to Security Concepts			100%
Security Stories			100%
Ethics	33%		67%
Services (www, email, etc)			100%
Networking/Sniffing			100%
Stego/Hide your face		50%	50%
Securing your environment		17%	83%
Movie and Games	33%		67%
Wireless	17%	17%	66%
Crypto		17%	67%
Tour/Palisade			100%
Electronic Crimes Task Force Lab		33%	66%
Principal Tour		17%	83%
Farm Bureau Tour			100%
Career Night/Round Table			100%
Forensics Presentation	50%		50%
Forensics Lab	50%		50%
Information Warfare			100%

The students overwhelmingly thought the camp was worth it. We asked them to rate each activity. The most popular events during the second camp were; building computers, career night, networking, information warfare. Many of the comments were used to change the camp. After running the camp for two years we learned a few things that worked and a few that did not. In the previous section of the paper several of the successful activities were highlighted. In this section a couple of things that did not go well are highlighted.

During the first year, we had the students spending time creating a power point presentation with security tips. They then needed to make the presentation to the parents and friends at the Wednesday night dinner. This activity worked fairly well, however it was hard to get them motivated to work on it. To the campers this was also too much like school. The feedback we got from the first year indicated they wanted more hands-on activities and less lectures. We made several changes in the curriculum to introduction more labs including the attack lab.

One of the biggest complaints we got from the first year was all of the team building activities. The first year we had them together the first night and we had dinner and then went on a tour of campus. After the tour we had them doing several team building games. Most of them were physical games and they were not very excited about them. On Monday night in the first year we went to the 4H camp and did several team building exercises, used a low ropes course, had dinner, and played ultimate Frisbee. They seemed to have fun at the time, but the feedback ranked the Sunday night and Monday night activities as the lowest ranked activities (by a large margin). We decided that they wanted more computer related activities. As was discussed above, we added the first night computer building exercise which was a great team building exercise. And the pizza and a movie also was great social activity. In retrospect we should have realized that students come to a computer security summer camp to work with computers.

One of the key aspects of the summer camp has been the involvement of local security professionals. We worked with the local chapter of InfraGard to help define the camp and develop the curriculum. The group helped recruit students and provided 500 dollars the first year for scholarships to students. As discussed above several members of the group provided tours of their companies and spoke at the career night. For the second year of the camp several members also came to the pizza and a movie night and were the hackers for the attack lab. This partnership has been critical in making the camp a success. The InfraGard chapter continues to support the camp and is helping to plan the 2006 camp.

Even though we did not formally assess the learning outcomes we had several opportunities to observe the level of learning. The students were engaged during the entire camp and were excited about what they were learning. The level of questions asked during movie night and career night showed they were obtaining a level of knowledge about security. That fact they were able to design and implement a security network and defend it against hacker shows they had learned many of the intended outcomes.

Recruitment & costs

In order to recruit students we sent an email to a list of high school science, math, and computer science teachers. We also had several members of InfraGard talk directly to schools. We also produced a flyer and a web site[8] that were designed to answer many of the possible questions. We asked the students to fill out an application which included a short essay. We had intended to use the essays to select the students if we had more applicants than spots.

The first year of the camp we expected to have a large number of students sign up for camp. We put a limit of 30 students on the camp. We were also concerned that money might be an issue so we raised money to provide scholarship to the campers and reduced the cost for the camp. We were wrong on both counts. We did not have a large number of students who wanted to come to camp. The first year we only had 25 students that came to camp and we had to work hard to get that many. We found out that most high schools do not have a good method to get this information into the hands of the students. The cost of the camp was not an issue. The first year the fee was $250 and the second year we changed it to $200 and we saw a decrease in the number of students. The decrease was also due to a reduction in the number schools we recruited from. Our goal for the second year was 15 students. We wanted a smaller number since we were trying a more lab oriented camp and we were not sure if we could handle more then 15 students. We only had 9 students attend the camp in the summer 2005. Our only conclusion is that we need to do a better job of recruitment and that we can charge closer to what it costs to put on the camp.

The students came from schools across the state, and the first year we had one student from Wisconsin. Ames is located in the center of the state which meant that most students traveled less than 2 hours to reach the camp. The first year we had one woman and none the second year.

The costs to run the camp are show in the table below:

Year	Total Cost	Number of Students	Cost per Student
2004	$8269	25	$330
2005	$2239	9	$223

There are a couple of factors that changed the cost per student from 2004 to 2005. The largest factor was the change in venue for the Wednesday night dinner. In 2004 we held the dinner at an off campus site that charged $1200 to use, plus we needed to use their caterer. We thought the students would enjoy being at a nice garden area. In 2005 it made more sense to have the dinner at the ISEAGE facility so they could show their parents what they did. Transportation costs were lower because in 2004 we rented a full size bus and in 2005 we used a university van.

Another aspect of recruitment is the number of students that will attend ISU. Even though that was not a primary goal, it is something that we can measure. The table below shows the number of students attending or committed to attend ISU

Year	Number to ISU	Too Young	Unknown
2004	13	5	7
2005	1 + 3	5	3

The number coming to ISU from the 2005 camp is only one so far; however, 5 were too young to attend in 2006. 3 of the 4 students that have been admitted in the fall of 2006 attended the 2004 camp. Out of the 34 kids that came to camp, 17 are or will be attending ISU and 5 are still too young yet to know.

Conclusions and future direction

After two years of camp we concluded that the camp is well worth the time and effort. Our goal is not to make money on the camp, but to provide an opportunity for high school students to experience computer security. The faculty and security professionals volunteer their time to help with the summer camp. The camp does build strong ties between the university and the security professionals. As we have seen the impact on college recruiting is hard to measure. So, the one big question might be why do we hold the summer camp? That question can be easily answered by anyone that spends time with the students during camp. They become excited about security, and they become excited about learning.

The impact of the camp might best be summed up by this excerpt from an email we received in November 2005 (the names have been removed).

> "My son attended your computer security camp last summer. I am very proud as a parent to tell you that he has been admitted to the college of engineering for the fall of 2006. He is thrilled and I know he particularly looks forward to working with you.
>
> My son has a learning disability that was not diagnosed until his sophomore year in high school and is now doing quite well. We submitted on his behalf an application for special consideration. I understand from admissions that one of the reasons that my son was admitted was based on the admissions office communication with you and your support of my son. On behalf of his mother and me I want to thank-you profusely not only for your kind support, but for sponsoring the computer camp and allowing kids like my son to find their careers."

There are several things that are planned for change in the 2006 camp and many things we will keep the same. We are planning for 14 campers in 2006 and we will change the way we recruit. We will be sending out large posters that can be hung on the walls at high schools in an effort to make it easier for high schools teachers and staff to get the word out. We also sent out letters to about 50 high schools in the state. We will charge $300 for the three day camp, which will cover the costs of the camp.

The first night of building computers will stay, we may have to disassemble several computers before hand to have enough computers. With 14 campers we will need to have at least 3 to 4 college students around to help with the first night and with the attack lab. There has been some discussion about having the students build computers they get to keep. We would have to

increase the cost of the camp to provide the computers. We are not sure if this would be a benefit, but we have been asked by the campers where they can get parts to build there own computers. We might put together a part list to they could order a computer on there own. We did provide them with several CDs that had public domain UNIX operating systems. For the 2006 summer camp we will produce several CDs containing public domain software and operating systems.

The attack lab went very well, but was some what over whelming for the campers. A problem was that they did not have time to setup the computers that needed to be defended. They built the defense systems and did not have much to defend. For the 2006 camp we will provide them with several pre-built systems that they would build a defensive system to protect. This would also give the hackers something to attack.

The last thing that we want to change is the companies we visit. We need to find a company with a large data center. It would be great of the company had state of art network management system that would provide an impressive tour.

Bibliography

1. Federal Government "The national strategy to secure cyberspace", http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, February 2003.
2. InfraGard, www.infragard.net
3. ISEAGE, www.iac.iastate.edu/iseage
4. Ethereal, www.ethereal.com
5. Doug Jacobson, "Teaching Information Warfare with a Break-in Laboratory", Proceedings of the 2004 American Society for Engineering Education, Salt Lake City, June 2004.
6. L.J. Hoffman and D. Ragsdale, "Exploring a National Cyber Security Exercise for Colleges and Universities", tech. report CSPRI-04-08, Cyber Security Policy and Research Inst. Aug 2004, www.cpi.seas.gwu.edu/library/docs/2004-08.pdf
7. L.J Hoffman and D. Ragsdale, "Exploring a National Cybersecurity Exercise for Universities", IEEE Security and Privacy, Volume 3, Number 5, September 2005, pg27-33.
8. Summer camp web site, www.iac.iastate.edu/summercamp