Promoting Digital Forensics Awareness through the University of Alaska Fairbanks ASSERT Center

Kara Nance, Brian Hay, Christopher Hecker
ASSERT Center, University of Alaska Fairbanks
ffkln@uaf.edu, brian.hay@uaf.edu, fscrh2@uaf.edu,

Abstract

As a Center of Academic Excellence (CAE) in Information Assurance Education, the University of Alaska Fairbanks is committed to promoting a culture of awareness and advancement of the current state of knowledge in the field of information assurance in Alaska and beyond through dedicated research, education, training, and outreach. The Advanced System Security Education, Research, and Training (ASSERT) Center provides resources and education in information assurance within the University, and also to the Alaskan community, including schools, government, industry, and the general public. This paper presents a survey of the ASSERT Center digital forensics educational resources and outreach activities that are being used to identify and meet the needs of the State of Alaska with respect to the protection of digital assets. These include programs targeting K-12 students, K-12 teachers, business personnel, community members, and higher education audiences.

1. Introduction

Alaska is a land of extremes that play a significant role in shaping the lives and cultures of those who live there. Of those extremes, the most noteworthy is the state's geographic isolation. While faced with unique critical infrastructure issues that are inherent in distributing a small population over an extremely large area, Alaska's digital assets demand the same protection as those in any other state. The lack of commercial industry in the Interior minimizes the potential for partnerships that are so valuable in educating communities about technological issues. While some of the challenges facing Alaskans are unique to the environment, there are many basic issues related to digital forensics awareness that are shared in common with most communities throughout the United States. A focused foundational effort to improve the level of education with respect to digital forensics has been successful and a commitment to continual educational improvement is helping to raise the level of awareness in the field of Information Assurance (IA) at all levels in Alaska and beyond.

2. Issues

Unlike most states, the schools in Alaska are on a wide continuum ranging from large urban schools to rural "one-room" schools that are not on any road system. Since teacher certification in computer science and the safe use of technology is not currently a formal part of teacher training, most K-12 educators do not receive training in associated concepts as part of their academic preparation. While many are competent users of technology, they typically have evolved into their current roles as technological educators through necessity, but without formal training. While we salute these valued educators, we also want to provide them with the underlying foundational information vital to the successful dissemination of critical technological concepts. As the students in the state become community members working in local industry and government with their own K-12 progeny, the educational cycle continues with parents teaching children and children teaching parents.

3. Digital Forensics Outreach Programs

To address the associated issues facing the state, the Advanced System Security Education, Research, and Training (ASSERT) Center at the University of Alaska Fairbanks (UAF) Center has digital forensic outreach programs aimed at identified target audiences including K-12 teachers, K-12 students, business (including industry, government, and law enforcement professionals), the general public, and higher education. In order to promote significant change and the ongoing elevation of technological awareness, these programs are continually being expanded as the needs

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE
1530-1605/07 $20.00 © 2007 IEEE
IEEE COMPUTER SOCIETY

of the individual audiences become clearer and as new potential audiences are identified.

3.1. K-12 Students

The K-12 students in Fairbanks are physically isolated from large industry. They cannot take field trips to IBM, Microsoft, or an FBI forensics lab, and are not generally exposed to digital forensics specifically or technology at all in a more generalized view. To address this issue, ASSERT personnel applied for and were awarded a National Science Foundation (NSF) GK-12 Program grant. This generous grant funds the *Teaching Alaskans...Sharing Knowledge* (TASK) Program.

The TASK Program places graduate students (fellows) from Science, Technology, Engineering, and Mathematics (STEM) disciplines in K-8 classrooms during the academic year. This program is currently in its second year, and has been welcomed by teachers as a way for them to augment their individual STEM related background through interaction with graduate students who act as domain experts. Students in the classroom are exposed to STEM topics through lessons taught by actual practitioners of the discipline, and the graduate students receive teaching experience with guidance from K-8 teachers and UAF faculty mentors, which can be valuable in their future careers.

The current technology fellow, a computer science graduate student, worked with three area schools during the 2005-2006 academic year and was able to present computer forensics content to the students and teachers as part of his extended program. This program exposes K-8 students to a technology expert who is able to address technological issues which are generally far beyond the capability of the teacher in the classroom, and can make digital forensics "real" and exciting for the students by demonstrating activities with which they can relate. One popular example involves the use of digital cameras. The students can take pictures and view them and then delete the pictures. Age-appropriate digital forensics tools are then used to recover the pictures. Exploratory extensions to this exercise include writing over data and analyzing different brands of cameras to determine how they write, erase, and rewrite their digital media. This program provides an age-appropriate experience for a wide range of students in a traditional classroom.

There are other educational audiences in the K-12 arena whose needs are not being met. For instance, it can be very difficult for teachers to meet the needs of the accelerated learners, many of whom have technological backgrounds that exceed the capabilities of their teachers. ASSERT personnel have been asked to work with individual students in these cases on targeted projects in digital forensics. In some cases the projects have covered an extended period of time as students prepare for science fairs at the lower grade levels or Alaska High School Science Symposium at the high school level.

In another program targeted to help to meet the needs of the accelerated learners and to promote the awareness of digital forensics, a Computer Forensics track was offered as part of the Alaska Summer Research Academy (ASRA). ASRA is a two week residential summer science camp in Fairbanks for students in grades 8-12. The application process for the camp is rigorous and students can choose one of 16 fields on which to focus while at the camp. Each field is limited to eight students. The Computer Forensics module introduced students to the field of digital forensics and provided them with the opportunity to use the state-of-the-art professional tools and equipment available in the ASSERT Lab at UAF to explore the exciting world of computer forensics. Topics included "data recovery techniques, erasing disks, reconstructing intrusion methods from system logs, as well as gathering, managing, and using digital evidence." [1] To get the students involved with the forensics process, projects were carefully selected to attract and retain the attention of this challenging age group. For example, while using some of the forensics software to recover hidden and deleted files, a puzzle was hidden in various files for the students to solve while searching for the files. This kept them interested while performing some of the more repetitive tasks. The camp also featured some very well received presentations by law enforcement officers, including representatives from the UAF Police Department, the Fairbanks Police Department, and the local FBI office, in which they discussed their digital forensics work. This opportunity to meet individuals who apply the computer forensics theory covered in the camp to real situations allowed the students to understand some of the legal and technical hurdles that law enforcement must overcome in investigating crimes involving digital media, and the growing number of instances in which digital evidence is relevant to a criminal investigation.

Of the 16 different programs available in the 2006 ASRA camp, computer forensics was the first to meet its maximum enrollment, and in addition had a wait list of 16 students, which is especially encouraging considering that summer 2006 was the first offering of this module. It is anticipated that in subsequent years, the computer forensics module will be split into multiple sections, not only to allow increased

enrollment, but also to provide the option for an introductory track, with a similar focus to the 2006 camp, and an advanced track which allows for an exploration of digital forensics topics in greater depth.

Working with K-12 student in digital forensics provided some unique challenges primarily associated with the ethical maturity of the participating students. For this reason an entire day of the ASRA camp was devoted to a discussion of the ethical issues involved in the field, and with the use of the tools and techniques being discussed in the course. While this had the desired effect on the students, the staff teaching the course were prepared to take action, up to and including removal from the camp, to ensure that students understood the ramifications of the application of digital forensics techniques beyond the ASSERT lab environment, and complied with the stated restrictions both within and outside the classroom. This is a problem not limited to the ASRA age group, and as such the ethical component is also integrated into the graduate and undergraduate IA courses and modules at UAF. To further minimize the risks, most of the ASSERT K-12 outreach activities targeting students focus on disk forensics and data recovery rather than network forensics which can quickly have serious legal implications should an overenthusiastic student attempt to try it on an unauthorized network. When providing important educational experiences that rely on digital forensics, such as discussing and demonstrating how network traffic can be analyzed, presenters are careful to warn students about associated legal issues. They also provide the material in an age-appropriate scope so that students are less likely to violate legal or commercial restrictions. For example, when discussing network traffic analysis with a younger audience, it is not necessary to provide in-depth instructions of how to capture the traffic, which is an activity that could result in significant problems for a curious student with access to a production network. In the ASRA environment, students were provided with sample network traffic to analyze, rather than providing them with the tools and techniques necessary to perform the traffic captures themselves. The sample captures involved real traffic obtained legally by the ASRA staff, and revealed some of the flaws with email and instant messaging while reducing the risk of a student using network monitoring tools to imitate the exercise outside the classroom environment. Embedded JPEGs were also recovered from a sample HTTP capture as a demonstration of data recovery.

The ASSERT K-12 outreach programs have been successful and the ASSERT faculty and staff are working to develop more modules to increase awareness of computer security issues in the K-12 arena.

3.2. K-12 Teachers

While tightly linked to the K-12 student programs, the K-12 teachers have special needs that the ASSERT personnel are working to accommodate. Current teacher programs include the TASK Program, educational modules, and teacher training.

As described in the previous section, the TASK Program places graduate students in K-8 classrooms. While exposing the students to a higher level of technology is part of the TASK mission, there is the additional mission of providing educators with resources that will allow them to continue technology training for students long after the TASK program has ended. During the academic year, the TASK technology fellow is as committed to teacher training as he is to student training. By exposing the teachers, along with the students, to digital forensics concepts, the TASK fellow enables the teacher to see first-hand how digital forensics can be presented in an age-appropriate way and the teacher can then reuse the lessons and materials in subsequent years.

In discussions with teachers, it has become evident that there is a lack of educational resources to help teachers learn about and teach digital forensics topics to their students. To aid teachers, both in the TASK Program and beyond, the TASK website hosts educational modules that teachers can use in their academic programs [6]. Each August, beginning in 2006, each TASK Fellow is responsible for creating and contributing educational modules to the website so that they are available for teachers around the world to use to present topics to their students. Each module provides the teacher with information about the intended audience, foundational concepts, and extension concepts, as well as a complete learning-cycle model of the learning activity. The digital forensics modules will also be available through the ASSERT website and will direct students and teachers to the materials that are available through the site.

In addition to the TASK Program, K-12 teacher training has been presented by ASSERT personnel to numerous audiences around the U.S. The most general presentation entitled “What Every Teacher Should Know about Computer Security” [2] addresses numerous computer security topics selected to raise awareness among teachers and to help identify areas where they need additional training. Digital forensics topics addressed in the standard presentation include secure disposal of data and network forensics

IEEE COMPUTER SOCIETY

awareness. Additional modules are under development for the 2006-2007 academic year to delve more deeply into the topics addressed in the general presentation.

3.3. Industry, Government, and Law Enforcement

Although Alaska has few businesses whose primary field is computer technology, there are many commercial and governmental entities which are reliant on safe use and protection of their digital assets. The geographic isolation of the state, where many towns are not on the road systems necessitates increased usage of networks and computers to complete communication tasks. Law enforcement in Alaska is at a disadvantage with respect to computer crime as they attempt to comply with rules for processing digital evidence without the support of the facilities available in many other states. For example, a local law enforcement officer in a remote rural community is far more likely to be familiar with hunting and trapping laws than the process for the collection of digital evidence. However, in the event that such digital evidence is related to an incident, the option to import expertise from another community to properly collect the data, which can be easily accomplished in other states, typically means flying an expert in from Fairbanks, Anchorage, or Juneau, which can be a costly and time consuming process. Even in the state's three larger communities, the volumes of digital evidence currently being acquired is quickly overwhelming the personnel trained to analyze and present it.

To begin to assess the needs of the state and to disseminate information about the capabilities and expertise within the ASSERT Center, UAF hosts the annual Alaska Information Assurance Workshop each fall [7]. The focus of the 2006 workshop was Digital Forensics and included presentations from leading institutions conducting research and training in digital forensics. There were two major goals associated with the workshop. The first goal was to improve awareness of how the ASSERT Center resources can assist local industry, government, and law enforcement in digital forensics. The second goal was to assess the education and training needs within the state so the development of additional courses and modules in digital forensics are consistent with the needs of the community that the university serves. The workshop was successful with an outpouring of interest in a larger workshop next year with specialized tracks to meet the needs of identified populations including law enforcement, industry, and military.

In addition to the workshop which occurs once each year, the ASSERT Center personnel are available as a resource to answer questions and provide assistance as needed by industry, government and law enforcement. In order to increase awareness of the facilities available to assist this population, a proactive information dissemination plan is being developed that includes information about the physical lab facilities as well as the development of training modules in the use of laboratory equipment and tools. It is anticipated that building stronger partnerships between local business and the ASSERT Center will help improve capabilities in digital forensics as well as to provide targeted educational and training opportunities to meet the needs of these populations.

In addition to this important subset of the population that ASSERT serves, there is a need to work the community as a whole to develop programs to meet the needs of the wider population.

3.4. Community

One of the responsibilities of an institution designated as a Center of Academic Excellence (CAE) is to act as a resource for the community it serves. As the only CAE in Alaska, the goal at UAF is to provide an Information Assurance resource not only within the university itself, but for the wider Alaska population at the statewide level. The ASSERT Center personnel have been working to increase their visibility as an information assurance resource for the community. These efforts include television interviews, articles, and dissemination materials, as well as the other outreach programs described within this paper.

Within UAF, and the University of Alaska system at a statewide level, there are many instances in which Information Assurance expertise is required. Some areas related to computer forensics in which the ASSERT Center has assisted the university include:

- Providing support in the event of system compromise, including the provision of analysis systems to determine the extent of the issue.
- Developing a policy for the safe reallocation of computer systems, including those instances where systems are distributed beyond the university to external organizations, such as local schools.
- Data recovery from various digital media in the case of deletion or corruption. While these tasks are often quite trivial, such as the recovery of deleted digital camera photographs from compact flash media, there

IEEE COMPUTER SOCIETY

is a lack of expertise in Alaska beyond the ASSERT Center.

In addition to the direct contact with the community, the website is being expanded to address community needs and concerns as they are identified. The Fall 2006 workshop focus on digital forensics provided valuable information about the needs of the community which will lead to the creation of additional digital forensics information and educational modules that will be available at the ASSERT website. The needs of the community will also be taken into consideration as UAF continues expanding its courses and modules in digital forensics.

3.5. Higher Education

Over the past five years UAF has significantly expanded its Information Assurance offerings, in part through the development of five new IA specific classes, but also through the integration of IA related modules into classes in the computer science curriculum, and core classes from other disciplines.

When attempting to introduce new concepts into a curriculum, such as IA concepts into the Computer Science Curriculum, there is often the response from educators that the curriculum is already so full that additional content simply cannot be added. An approach to addressing this problem which has been successful at UAF is to provide modules which relate some of the topics already being taught to the new IA concepts that we wish to integrate. One example of such a module which introduces students to some basic computer forensics concepts is currently used in CS 201 (CS1), which is the first programming class for both computer science and electrical engineering students. The class currently uses the C++ language, and the module is typically used as a file I/O exercise, providing the students with an interesting and realistic problem that requires them to utilize file input and output, while also gaining an insight into basic computer forensics and file system concepts.

The module utilizes a set of identical floppy disks which were cloned from a single disk that was prepared as follows:

- Zeroes were written to the entire disk.
- The disk was formatted using the FAT32 filesystem.
- Several JPEG images were saved to the disk.
- Some of the JPEG images were deleted from the disk.
- Some additional JPEG images were saved to the disk.

Floppy disks were chosen, as opposed to hard drives or CD/DVD disks, because they provided enough space to store several images, while remaining small enough that the large volume of data was not the limiting factor in this exercise.

Each student is given one of the floppy disks, and a worksheet which lists the goals of the exercise and provides some information about the JPEG file format, including the start and end of file byte sequences. The worksheet also describes how to create an image of the disk as a file. Each student is then required to write a program which:

- Searches the disk image for the start of JPEG file marker.
- Once the start of JPEG file marker is found, all data should be copied to a new numbered file, until the end of JPEG file marker is found.
- This process should be repeated for each potential JPEG file found on the disk.

At the successful completion of this first task, each student should have several new files which potentially contain recovered JPEG images. They can then attempt to open these files using a browser to determine which are complete JPEG images, partial JPEG images, or invalid JPEG images. This list is then compared with the list of files on the floppy disk as reported by the operating system, and the reasons for any observed differences are discussed.

If there is sufficient time during the lab or homework session, each student can then modify the disk by, for example, saving, deleting, and resaving new JPEG images on the disk. Each student can then exchange disks with another student, and use their newly acquired skills to recover images from the new configuration. This module has also been used with a disk which contained a wider variety of file types, including GIF images and text files, although the basic JPEG exercise has proven to be a sufficiently challenging assignment during the file I/O topic for the CS1 students.

The culmination of this lab involves a discussion of how these techniques can be improved and also potentially extended to other file types, and why this can make the deletion of data from digital media problematic, such as while preparing a computer for resale or reassignment.

IEEE COMPUTER SOCIETY

In addition to digital forensics modules that are used across the CS curriculum, UAF offers classes at the graduate and undergraduate level that are focused on digital forensics. The intent of the classes is to provide students with an understanding of digital forensics from the theoretical standpoint, including some relevant legal and business focused concepts, and the acquisition, analysis, and presentation of evidence.

During the classes, students are given the opportunity to experiment with some current computer forensics tools in the ASSERT Lab, such as EnCase [5] and the suite of tools provided in the Helix distribution [5] although the intent of such exercises is not to provide training in the use of tools, but rather to demonstrate the extent to which today's tools currently implement the theoretical concepts discussed in the lectures. These classes, as well as most of the other outreach programs, rely heavily on the use of the ASSERT Lab facilities to provide hands-on opportunities for students to enrich the learning experience.

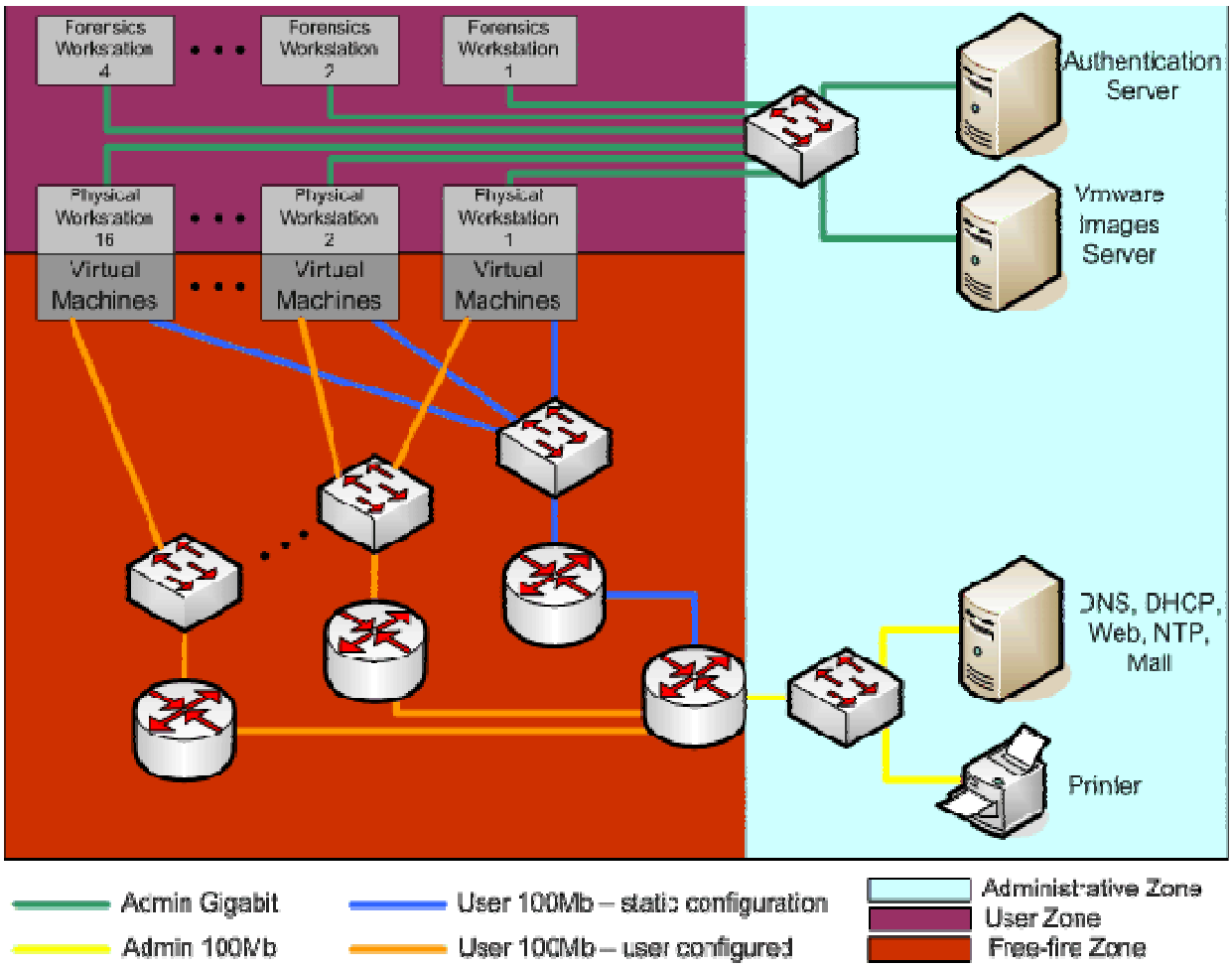

Figure 1 – ASSERT Configuration [3]

4. ASSERT Center

The ASSERT Center is based in the Computer Science Department at UAF, but takes a multidisciplinary and multi-institutional approach to Information Assurance, both in its faculty and staff, and its education and outreach missions. The center coordinates the collaboration of approximately 10 faculty members, drawn from diverse fields including Computer Science, Mathematics, Statistics, Physics, Political Science and Social Sciences. The education and outreach components also extend beyond the core Computer Science based classes to include modules which are presented in many freshman level courses throughout the curriculum, including core classes that are required

IEEE COMPUTER SOCIETY

of all majors on campus. Topics covered in these modules include the selection of good passwords, Internet safety, web research, and techniques for basic computer security.

4.1. ASSERT Lab

The ASSERT Lab is an isolated facility (see Figure 1) which utilizes system virtualization in conjunction with physical networking components to provide an extremely flexible teaching and research environment. The lab features four dedicated computer forensics workstations, on which several common tools are installed. In addition to software, these workstations have FastBloc disk write-blocking devices, Jaz/Zip drives, Floppy drives, CD/DVD drives, and flash card readers installed to allow data to be acquired from a multitude of sources.

In addition to these dedicated workstations, a VMware virtual machine (VM) master image is stored on the lab's images server, and this VM can be cloned and made available to students, staff, or faculty for classwork or research. These VMs can be connected to one of several lab networks, many of which are user-configurable. Using this approach it is possible to gain experience of network forensics concepts, either on a quiet isolated network, or on a more active network with the inclusion of additional virtual or physical systems, or even traffic generators, on the network. Because the ASSERT Lab is physically isolated from any external network, such as the UAF campus networks, actions which take place on the lab network cannot negatively impact any production systems.

5. Conclusions

As a CAE institution, UAF, through the ASSERT Center is working to raise the level of awareness and competence in information assurance both within the university itself, and throughout the community at a statewide level. As part of this effort, digital forensics is presented in several forums with the goal of ensuring that computer systems can be utilized more safely, and that the industry, government, and the public have a resource to which to address their related questions.

6. Acknowledgements

This research sponsored in part through a generous grant by the NSF Graduate Teaching Fellows in K-12 Education (GK-12) Program.

7. References

[1] ASRA (n.d.). *Alaska Summer Research Academy*. Retrieved September 6th, 2006 from http://www.uaf.edu/asra/archives/abstracts2006.html#CForensics

[2] ASSERT (July 26, 2006), *ASSERT Overview*. Retrieved September 6th, 2006 from http://assert.uaf.edu.

[3] ASSERT (July 26, 2006), *ASSERT Resources*. Retrieved September 6th, 2006 from http://assert.uaf.edu/lab/resources.html.

[5] ASSERT (September 5t, 2006). *ASSERT Workshop*. Retrieved September 6, 2006 from http://assert.uaf.edu/workshop.html

[5] E-Fense (n.d.). *Helix Live CD Page*. Retrieved September 6th, 2006 from http://www.e-fense.com/helix/

[6] Guidance Software (n.d), *EnCase Forensic Edition*. Retrieved September 6, 2006 from http://www.guidancesoftware.com/products/ef_index.asp

[7] Possenti, K. (n.d.). *Teaching Alaskans…Sharing Knowledge*. Retrieved September 6, 2006 from http://task.uaf.edu

IEEE COMPUTER SOCIETY