Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

All the News That's Fit to Blog

Richard G. Epstein, West Chester University of Pennsylvania, IEEE Member
Dafan Zhang, West Chester University of Pennsylvania

Abstract – This paper discusses how news stories are integrated into an introductory course on Computer Security and Ethics. The main emphasis in this paper is on two assignments that relate to computer security in the news. Special attention is paid to the second of these two assignments. This requires that students create a blog containing links to security news stories along with commentaries on those news stories. This blog is maintained through the entire semester. All of the students who chose to do this assignment during the fall 2009 semester have expressed enthusiasm for this project.

Index terms – Integrating Information Assurance topics into the undergraduate curriculum, ethics, social implications, scenarios

I. Introduction

The first author teaches an introduction to Computer Security and Ethics course for undergraduate students who are either Computer Science majors or who are pursuing a minor in Information Technology. The two main top-level goals in this course are to provide students with a basic introduction to certain ethical issues in Computer Science (as required for ABET accreditation) and to lay the foundation for an understanding of issues in Computer Security. This course provides a foundation for Computer Science majors who wish to pursue our certificate program in Computer Security, which requires that students take specific security-related courses as they pursue the undergraduate degree in Computer Science.

The main ethical issues covered in this course are privacy, intellectual property, and computer crime. One strategy behind the course is to introduce an ethical issue (like privacy) and then discuss strategies that computer scientists have developed in order to address technical problems relating to that ethical issue. For example, after our introduction to privacy from an ethics perspective, we discuss the Platform for Privacy Preferences (P3P) [1] and anonymous Web browsing using TOR [2].

After our discussion of privacy, we move on to discuss computer crime. The computer crime lectures include a historical introduction to computer viruses and worms, with an emphasis on the historical trends. The computer crime lectures also cover social engineering. We use several scenarios from Kevin Mitnick's book [3] in our introduction to social engineering. After our historical introduction to computer crime, we move on to more recent trends with respect to worms, including a discussion of worm epidemics [4], botnets, and new attack tricks that worms are using [5, 6]. A major focus in this discussion is how sophisticated recent attacks have become and how organized crime is very much involved in some of these attacks.

In addition to lectures materials (which are made available over Blackboard), the course depends heavily upon a "coursepack". The coursepack consists of a collection of papers drawn from publications such as IEEE Security and Privacy, IEEE Computer, IEEE IT Professional and the Communications of the ACM. The coursepack materials are freely available to the students via the IEEE Computer Society and ACM digital libraries. So, for example, references 1, 4, 5 and 6 cited in the introductory paragraphs are contained in the coursepack, as are all of the remaining references found at the end of this paper, except for the references to several books and to one Colloquium paper (12, 25, 26 and 27) . About one half of our class meetings require that students submit reviews for one of the coursepack articles that had been assigned for that particular class. These reviews are submitted via the Digital Dropbox on Blackboard and are usually one to two pages in length (single-spaced). Many of these reviews are very well-written.

After our discussion of privacy and our introduction to computer crime (what the first author sometimes calls "nasty stuff"), we devote some time to how privacy and nasty stuff come together by discussing:

- SPAM [7,8]
- Spyware (maybe a bit less during the past two semesters, because there is so much new stuff to cover) [9]
- Phishing and identity theft [10,11]

Note that the coverage of identity theft includes the topic of social phishing, which is of growing importance. The paper by Jagatic et al. [11] describes an interesting experiment which demonstrated how vulnerable social network users are to phishing attacks.

The course then moves on to discuss additional topics in Computer Security and Ethics. Important references are again included in this bulleted list:

- Intellectual property and piracy

- Information warfare and cyberterrorism [12, 13]
- Cryptography
- Computer Immunology [14]
- The weakest link [15,16,17,18]
- Biometrics [19, 20]
- RFID devices [21]

This semester (Spring 2010) the author intends to devote a class to a fascinating "hot topic": security issues in cloud computing [22, 23]. Another topic we hope to cover at least briefly is what appears to be a growing and scary problem: PIN-stealing attacks at PIN-entry devices (PEDs) [24].

The authors believe very strongly that a basic understanding of computer security is important for citizens in the modern world. (Note that the first author is the instructor for this course and the second author was one of the students who did the news blog assignment which we will discuss in Sections III and IV.) Both authors would like to see more and more colleges and universities devoting time to teaching about these issues to all undergraduate students. The first author was very much impressed with the book Blown to Bits [25] which illustrates how such a course could be designed for undergraduate students with many different backgrounds.

At CISSE 2009 the first author discussed how he integrates news stories into this introduction to Computer Security course [26]. This paper updates that earlier paper, by emphasizing how integrating news stories into an introductory computer security course has evolved and will continue to evolve. In particular, the first author hopes to get more students to pursue the news blog final project option, because the students who have done this (during the Fall of 2009) said it was an excellent learning experience. Indeed, some detailed comments relating to this assignment are included in Sections III and IV of this paper.

Let us conclude this section by indicating how news stories impact the course in general. Then, in Sections II, III and IV we will focus on the two news-related assignments in the course.

Almost every class begins with a news story that is either relevant to that particular class or a breaking news story that the first author wants to share with his students. So, if the first author is going to teach about identity theft on a given day and he has on file a news story from a year or two ago that relates to identity theft, he might start the class with that particular news story. On the other hand, if there is an important security-related news story in the news that emerged just prior to that particular class, he will bring up that news story at the beginning of the class, even if it does not relate to the specific topic to be covered on that day.

In fact, the trend seems to be that hot news stories relating to computer security are in the news almost every day. The first author often begins his workday by going to one of the following Web sites for the latest news stories relating to computer security:

- Dark reading (darkreading.com)
- Threat Level – Wired Blogs (blog.wired.com/27bstroke6/)
- Google News (technology section)
- ComputerWorld (computerworld.com/securitytopics/security)
- Brian Krebs (formerly with the Washington Post, who now has a great security blog at krebsonsecurity.com)

The news stories definitely help to get the message across that computer security is really important stuff. The first author has observed some strong reactions from students to these news stories.

The main emphasis in this paper is on two news-related assignments that the first author has integrated into the course. The first of these two assignments is called "hot topics in the news". This assignment is discussed in the next Section (Section II). All students must do the "hot topics in the news" assignment. The second news-related assignment is the news blog assignment (or, project). Students are allowed to choose the news blog project for their final project. Other options for the final project include a take-home essay exam or a traditional research paper. The author expects that the news blog project will become more and more popular over the coming years. Indeed, while only three students did the news blog assignment last fall (2009), nine students have signed up for the news blog assignment this semester (spring 2010) out of a total enrollment of twenty-six. The news blog project is discussed in Sections III and IV.

II. THE HOT TOPICS IN THE NEWS ASSIGNMENT

One class (75 minutes) is completely devoted to the "hot topics in the news" assignment. All students must do this assignment. This assignment involves writing a short news story which is to be presented in class. Each student hands in the news story that he or she wrote along with references that he or she used to write that story. The references are to be provided as print-outs of the sources that the student drew upon to create his or her news story. In effect, each student acts like a journalist for CNN or NPR, providing information about a development in Computer Security that the student found interesting.

The hot topics in the news class is very informative and usually somewhat provocative. Here are brief descriptions of some of the (over twenty) stories that were presented during the hot topics in the news class last fall (2009):

- Microsoft denies that it built a 'backdoor' in Windows7 for the National Security Agency.
- Using biometrics to perform behavioral screening at airports.
- Cyber Monday: the risks of on-line shopping for the holiday season.
- The US military is developing a portable battle field cyber-warfare device. One use of this device would be to break into the adversary's wireless communications.
- Comcast hackers charged with conspiracy one year after hack. They claim they warned Comcast before they performed the attack.
- A report issued by the US Strategic Command and the US-China Economic and Security Review Commission has revealed that cyber attacks on the US Defense Networks are on a pace to nearly double this year (2009) as compared to last year.
- Several students gave presentations relating to the hack into the Climate Research Unit at the University of East Anglia in the UK. This was a big news story in the media about the time that our hot topics in the news presentations took place.
- Cross-Site Request Forgery, also known as CSRF is an example of the increasing amount of malware aimed at social networking sites. CSRF is a Facebook worm.
- Eleven people are indicted for the stealing, distributing, and purchasing approximately 40 million credit and debit card numbers. This is the largest hacking case that the Justice Department has ever followed and brought to trial.
- Back in June 2009 a new form of malware began spreading through ATM machines in Eastern Europe. The malware records the magnetic strip information on the back of a swiped card as well as the personal identification number.

Again, this is just a sample of the news stories that students presented in this class.

It is worth noting that some of the news stories have an impact on the evolution of the topics covered in the course. For example, the last news story in the above list relates to an important security issue that the first author decided to cover in the computer crime portion of the course this spring (2010). Thus, one of the new papers that has been added to our coursepack is an excellent research paper about stealing PINs at PIN-entry devices by Drimer et al. [24].

III. THE BLOG PROJECT

This section and the following section will focus on the news blog project. Students who chose this option for their final project were required to create a blog and to post several security-related news stories to their blog each week throughout the semester. These posts would include a link to the relevant security news story as well as their own personal response to that news story.

Three students (Dan Arena, Robert Van Zyl and the second author, Dafan Zhang) chose this option. Their blogs were very interesting and they provided very positive feedback on this project as a learning experience. The blogs are available at the following web sites:

- Dan Arena: http://wcu2011.wordpress.com/
- Robert Van Zyl: http://bobvanzyl.blogspot.com/
- Dafan Zhang: http://www.cyberphilly.com/

The handout which describes the assignment suggested that students focus on a particular area of cyber-security that they found to be particularly interesting. None of the three students followed that suggestion, which turned out to be a good call on their part. In retrospect, breadth of coverage, as opposed to a focus on one topic, was a better learning experience for an introductory course of this nature. Each blog covered a range of topics, although different students had different foci. Of course, there were dozens of posting during the course of the semester. What follows is a summary of just a few of the security topics that the students covered in their blogs. This summary includes particular quotes from some of the postings as well as the news source that the students used:

Intellectual property: Some posts related to the Pirate Bay case in Europe. Quoting from Dan Arena's blog: "The world's foremost site for providing a torrent library to copyrighted material will no longer operate its torrents. … The four founders of the site face a year in prison and millions of dollars in fines." [News source: Wired]

Social networking: Quite a few posts related to problems in the social networking sphere. These included postings about malware on Facebook and a law suit which resulted in a $711 million dollar award to Facebook in a spam case. Here is a quote from the second author's blog relating to that case: "A California federal judge found on Thursday that master spammer Sanford Wallace was guilty of bombarding the social networking website Facebook.com. Facebook was rewarded $711 million in damages. The judge also referred the case to the US Attorney's office for further investigations and perhaps federal criminal charges." [News source: CNN]

Other posts related to malware that has had an impact on Facebook users. Here's another quote from another posting on the second author's blog: "Something

interesting developed over at Facebook this week. Some users figured out a security hole in Facebook's group function that allows a group to be taken over by ANYONE once the administrator of the group steps down. Two self-described activists then proceeded to take over almost 300 groups and modified it to display 'Control your info' apparently in an attempt to warn others of this Facebook shortcoming." [News source: CNN]

Cyberterrorism and Information Warfare: There were quite a few posts relating to cyberterrorism and information warfare. One blog post from Robert Van Zyl has the humorous title "Honey, didn't you pay the electric bill?" Here's a quote from this post: "According to the article, the Chinese and the Russians have both penetrated and attempted to map the systems that run our electrical grid. At this point they have not done any damage but they could try if there were to ever be a war. The fact that they have gotten in means that others could as well. The worst part is that the companies responsible for these systems did not detect the intrusions but [they] were detected by US intelligence agencies. Software was left behind by the intruders that could affect the systems that run our electrical infrastructure. Since the start of this class and the mention of the possibility that the MSBlaster worm may have caused the blackout of 2003, this area of Information Security has really interested, and scared me. I'm not out buying a generator yet, but the thought has crossed my mind." [News source: Wall Street Journal]

Bruce Schneier has written about the possibility that the MSBlaster worm caused the massive blackout in the northeast in August 2003 [27]. We discussed Schneier's point of view on this issue during our discussion of worms and worm epidemics.

Security and Cloud Computing: Robert Van Zyl also touched upon the important topic of security and cloud computing on his blog. Here is a quote from Robert Van Zyl's blog posting relating to this issue: "Throughout the semester, while researching articles for this blog, I have run into multiple articles regarding 'cloud' computing. Though this article doesn't exactly discuss security issues with cloud computing so much, it does raise some good questions that a cloud user may ask." The news source for Van Zyl's posting was CNN and the first author watched the video on the CNN interview that Van Zyl used as his news source for this posting. Our course will be covering cloud computing security issues more formally during the Spring 2010 semester. Several articles relating to cloud computing and security have been added to our coursepack [22, 23] (as noted earlier in Section I). This illustrates how the news blog project has helped the first author to introduce new topics into his course.

There were many interesting posts on the student blogs and the quotes given here do not quite communicate the nice job that these students did in creating their blogs. The interested reader should check out the web sites sited above to get a more complete picture of what these students did.

The author received very positive feedback from the three students involved in this assignment. The next few paragraphs contain quotes from Daniel Arena and Robert Van Zyl. More detailed feedback from the second author are contained in the next section.

From Dan Arena: "The introduction of the semester long blog as a final exam option was one of the highlights of my experience in this course. It not only allowed me to spread the work of the hectic finals week out over the semester, but it really did provide me with a valuable experience that better prepared me for the remainder of the course, including the group presentation. [Students work on a team project that leads to team presentations at the end of the semester.] By constantly looking for new things to write about I was able to see how the issues and technologies presented in our course pack have evolved in the modern computer security environment. Beyond this it gave me the opportunity to look at a situation and provide my own opinion on the matter including possible implications.

"This experience also gave me the practical experience of writing a blog and working in the format of an academic article, both extremely valuable skills for security professionals and Computer Scientists in general. The only suggestion I would have about improving the procedure would be to require that students post at least one article on each of the topics covered in the course of the semester to allow them to see the evolution that I was able to see. Honestly, if it weren't for my admittedly over zealous courseload I would still be publishing my blog weekly throughout my academic career, that is how valuable an experience I feel it was. And you can quote me on that."

The first author has decided to take this student's advice and to emphasize breadth of coverage rather than focusing on a particular topic for this blogging assignment. This will help the students to relate topics covered in our course to current events in the realms of computer security and computer ethics.

Here are comments from Robert Van Zyl: "While taking part in the CSC301 course … I was given an opportunity to include, as part of my graded course work, a blog based on news articles related to Information Security. Never did I imagine that this relatively simple task of reviewing

news articles and writing about them would change my career focus.

"I have been in the Information Technology field for close to 15 years, primarily in a role of System Administration and Management. Over the past several years I have been looking for more out of my career then installing and fixing servers and I truly believe this course has helped point me in the direction of Information Security. Enough so, that I will probably delay applying for my degree until I have completed the coursework for the [department's Security Certificate].

"While writing the blog throughout the semester, I looked for topics that were obviously relevant to what is going on in Information Technology today but also that followed the path that the course lectures were taking. Early on in my writings, I found adding a touch of humor here or there made the assignment more interesting and would hopefully alleviate my professor from the doom and gloom that would normally go with this type of assignment. What caught my attention was that my professor was actually reading my work and he wasn't just checking to see that I completed it. As the semester continued, my professor and I would talk more and more about the blog or Information Security related topics and I found myself getting engrossed in the topics we discussed. So much so that the group presentation at the end of the semester that I led could have actually gone on for two or three hours instead of the 30 minutes we were allotted.

"Unlike most courses that when you are done with them you move on, I plan on continuing this assignment on my own. I actually find it worthy of writing about whether or not anyone actually reads it. I believe the topics that I will read and write about will help keep me at least up to date with what is going on in the Information Security world."

IV. MORE DETAILED COMMENTS ON THE NEWS BLOG ASSIGNMENT

This section is devoted to the second author's reaction to the news blog assignment. We have kept the text in the first person.

A. Reason for taking the blogging assignment

During the introduction of the course, we were presented with several final project options in place of a traditional final. I chose the blogging option for several reasons. First, creating a blog and maintaining it throughout the term allows me to spread out the workload throughout the semester, thus lessening the stress and pressure around finals period. Second, since the field of computer security is always evolving, I thought the assignment would be a good way to research the current trends in the real world. Third, it seemed to be a great way to stay involved with the coursework. Studying and writing about current events in computer security would allow me to connect theory with applications.

B. Learning Outcome

Completing the blogging assignment throughout the entire semester was a pleasant experience that I looked forward to. Scanning the news for relevant computer security articles proved to be much easier than I originally anticipated. As the course moved forward, I was able to find news reports corresponding to each new topic we covered in class. Honestly I was slightly surprised at how relevant each of the topics was, as there were plenty of news reports for each topic. It underscored the importance of the course material and the need for every professional to be well educated and prepared in the area of computer security.

The writing of the blog entries also proved to be very valuable. By reporting and commenting on each piece of current happenings I was able to formulate my own understanding of the driving forces in the field of computer security. I came to understand that computer security is much more involved than a fight between the good guys and the bad guys. Each hot issue facing us also involves many other considerations and issues that impact our everyday lives. Aside from the need to secure systems, networks, information, and data, we must also be concerned with privacy, individual rights, ethics, legal issues and many other considerations that are not always clearly forthcoming at first glance. After a semester of researching and formulating responses to current events, I was able to identify some of the trends that are prevalent in the field of computer security. The insights gained from the project have, and will continue to prompt me to keep a keen eye on the current state of computer security as well as future issues and concerns. The experience of the blog project underscored the most important thing that I learned from the course: we need to continue to devote research and education in the field of computer security.

C. Personal Goal Impact

Although I already decided on a career in law prior to enrolling in this course, the course nonetheless greatly raised my interests in studying and practicing law in the technology sector. Furthermore, the blog project and the course as a whole showed that there is a great need to establish more cooperative connections between the legal, governmental and technology sectors in hope of reaching solutions and remedies for the many threats facing us in the realm of computer security. It reaffirmed my career aspirations and perhaps further refined my career objectives. I am very glad that I took this course and took part in the blog project. The whole experience far

exceeded my expectations and will prove to be invaluable in my education and career development.

D. Suggestion on Future Courses

One suggestion I have for future courses is to make more use of the blogs maintained by the students. After reading the blogs kept by my fellow students I was surprised by the variety as well as the common themes between the blogs. I was not aware of many of the news events covered by the other blogs, yet I can spot the same trends and undercurrents that I observed in my own blog. By reviewing or allowing the students to present their blog entries in class, other students can also be exposed to the relevant current events as the students who choose the blog project. Other students will be able to observe the same trends thus making the course more relevant to the entire class. Additionally, since many of the news events involve popular topics to college students such as social networking, personal finance, and career trend in the technology sector, they will help increase student engagement and involvement.

E. Brief Reaction from the First Author

The first author certainly intends to use the feedback he has received from the second author and the other two bloggers. He hopes to continuously improve the course content and to use news stories posted by the bloggers in his course.

The first author would like to close this section with a few remarks about how the news blog projects are graded. Every Monday morning the first author checks each and every blog and reads the postings by the students. The blogs are graded for a total of eleven weeks. Each week the student is given a grade of 0-10 based upon the number of postings (at least two per week) and the quality of those postings. The final grade is based upon the percentage of points (out of 110 possible points) that the student earned during the semester.

V. CONCLUSIONS

Important stories relating to computer security appear in the news every day. This paper focused on two assignments that the first author uses in his undergraduate Introduction to Computer Security and Ethics course. The main emphasis was on the second assignment, which required that students create a blog with links to important security news stories as well as their reactions to those stories. The students who chose to do this project (as opposed to other final project options) clearly enjoyed doing this and learned a lot from the news stories that they posted and reviewed. This assignment gives students an interesting perspective on how the world of Computer Security is evolving and the new issues that we face in this domain. The first author certainly intends to use the feedback he has received from last semester's bloggers to continuously improve the course content and to use news stories posted by the bloggers in his course.

VI. REFERENCES

[1] Cranor, Lorrie Faith, "P3P: Making Privacy Policies More Useful," IEEE Security and Privacy, November / December 2003, pp. 40-48.

[2] Information relating to TOR is available at www.torproject.org/.

[3] Mitnick, Kevin D., The Art of Deception, John Wiley Publishing, Indianapolis, 2002, 352 pp.

[4] Chen, Thomas M., Jean-Marc, Robert, "Worm Epidemics in High-Speed Networks," IEEE Computer, June 2004, pp. 48-53.

[5] Smith, Brad, "A Storm (Worm) Is Brewing," IEEE Computer, February 2008, pp. 20-22.

[6] Heyman, Karen, "New Attack Tricks Antivirus Software," IEEE Computer, May 2007, pp. 18-20.

[7] Pfleeger, Shari Lawrence, and Bloom, Gabrielle, "Canning Spam: Proposed Solutions to Unwanted Email," IEEE Security and Privacy, March / April 2005, pp. 40-47.

[8] Grimes, Galen A., "Compliance with the CAN-SPAM Act of 2003," CACM, February 2007, pp. 56-62.

[9] Ames, Wes, "Understanding Spyware: Risk and Response," IEEE IT Professional, September / October 2004, pp. 25-29.

[10] Geer, David, "Security Technologies Go Phishing," IEEE Computer, June 2005, pp. 18-21.

[11] Jagatic, Tom N., Johnson, Nathaniel A., Jakobsson, Markus, and Menczer, Filippo, "Social Phishing," CACM, October 2007, pp. 94-100.

[12] Denning, Dorothy E., Information Warfare and Security, Addison-Wesley, Reading, MA, 1999, 522 pp.

[13] Lesk, Michael, "The New Front Line," IEEE Security and Privacy, July / August 2007, pp. 76-79.

[14] Forrest, Stephanie, Hofmeyr, Steven, and Somayaji, Anil, "Computer Immunology," CACM, October 1997, pp. 88-96.

[15] West, Ryan, "The Psychology of Security," CACM, April 2008, pp. 34-41.

[16] Cybenko, George, Giani, Annarita and Thompson, Paul, "Cognitive Hacking: A Battle for the Mind," IEEE Computer, August 2002, pp. 50-56.

[17] Thelander, Michael, "The Great Wall Syndrome," IEEE IT Professional, September / October 2005, pp. 25-30.

[18] Gyongyi, Zoltan and Garcia-Molina, Hector, "Spam: It's Not Just for Inboxes Anymore," IEEE Computer, October 2005, pp. 28-34.

[19] Prabhakar, Salil, Pankanti, Sharath, and Jain, Anil K., "Biometric Recognition: Security and Privacy Concerns," IEEE Security and Privacy, March / April 2003, pp. 33-42.

[20] Bowyer, Kevin W., "Face Recognition Technology: Security versus Privacy," IEEE Technology and Society Magazine, Spring 2004, pp. 9-20.

[21] Foster, Kenneth R., and Jaeger, Jan, "RFID Inside: The Murky Ethics of Implanted Chips," IEEE Spectrum, March 2007, pp. 24-29.

[22] Viega, John, "Cloud Computing for the Common Man", IEEE Computer, August 2009, pp. 106-108.

[23] Kaufman, Lori, "Data Security in the World of Cloud Computing", IEEE Security and Privacy, July/August 2009, pp. 61-64.

[24] Drimer, Saar, Murdoch, Steven J., Anderson, Ross, "Failures of Tamper-Proofing in PIN Entry Devices," IEEE Security and Privacy, November / December 2009, pp. 39-45.

[25] Abelson, Hal, Ledeen, Ken, and Lewis, Harry, Blown to Bits: Your Life, Liberty and Happiness After the Digital Explosion, Addison-Wesley, Reading, MA, 2008, 384 pp.

[26] Epstein, Richard G., "News and Notes", presented at CISSE 2009, Seattle, WA, June 2009.

[27] Schneier, Bruce, Schneier on Security, John Wiley and Sons, New York, 2008, 328pp.