An Active Learning Activity for an IT Ethics Course

David M. Woods
woodsdm2@miamioh.edu
IT Services
Miami University
Oxford, OH 45056, USA

Elizabeth V. Howard
howardev@miamioh.edu
Computer & Information Technology Department
Miami University Regionals
Middletown, OH 45042, USA

Abstract

Courses in Information Technology Ethics are often designed as discussion-intensive courses where case studies are introduced and evaluated using ethical theories. Although many of the case studies directly apply to our students' online lives, the stories can sometimes seem too far removed from their own experiences. While we read the news headlines about data being intercepted via networks, students may not fully understand how easy that data is to intercept. Incorporating a hands-on experience using a network sniffing program allows students to actually experience just how easily someone can intercept their data.

Keywords: IT Ethics, Active Learning, Network Sniffing, Interactive Exercise, Experiential Learning, Wireshark

1. THE COURSE

The topic of ethics is an important part of both the IS and IT curriculum (IS 2010; Information Technology 2008), however, there is little literature discussing active learning activities for an IT Ethics course. This paper extends previous discussions (Howard, 2006; Howard, 2007) of an IT Ethics course to discuss how an active learning activity is used to engage students. The IT Ethics course is designed as a discussion and writing-intensive course. We use traditional ethical theories such as Act Utilitarianism, Rule Utilitarianism, and Kantianism to evaluate scenarios on topics ranging from privacy and intellectual property rights to whistleblowing and vulnerable groups. Students participate in discussions both outside of class in online discussion forums using the university's learning management system (LMS) and in-class discussions. Part of the student's grade is based on their participation in the discussions. In addition to discussions, students also write a number of position papers centered around the covered topics and create a final group project on the IT ethical topic of their choice.

The literature suggests that one of the challenges of teaching a discussion-intensive course is the underprepared or unengaged student (Benbunan-Fich, 1998; Greening, Kay, & Kummerfeld, 2004; Sanders, 2005). To help address the challenge of students being prepared to actively participate in class discussions, we provide the students with

specific questions about the chapter of the text (Brinkman & Sanders, 2012) and use a subset of those questions for quizzes. Students are required to prepare two (2) full pages of notes for each quiz and the notes are worth 50% of the quiz score. Students then use those notes during the quizzes. The quizzes and quiz notes are intended to encourage the students to read the text and to be prepared for class discussion. This combination of quizzes and notes seems to be an effective method to encourage student preparedness. Students strongly agree that the quizzes and notes help to better prepare them for the in-class discussions (Howard, 2007). To further encourage students to participate in the class discussions, students must cite their classmates within their position papers (Howard, 2006; Sanders, 2005). Although students find citing their classmates in their papers to sometimes be a challenge, the papers are more interesting and substantive than position papers assigned in other courses. As an added benefit, citing classmates has essentially eliminated plagiarism.

2. WIRESHARK ACTIVITY

Throughout the semester, students engage in online and face-to-face discussions on many case studies and scenarios that are the same type of situations that they face in their daily technology use. For example, students read and analyze examples where network traffic has been intercepted but those scenarios sometimes seem too removed from their personal experience (Greenemeier, 2007; McMillan, 2009). In addition, many students take this course for the general education requirement and are not computing majors and they have not yet seen the type of information that is shared in an internet search. The literature suggests that an active learning opportunity would be more effective than merely lecturing about the information that is transmitted (Schweitzer & Brown, 2007; Gao & Hargis, 2010). As Kolb wrote, "Knowledge is continuously derived from and tested out in the experiences of the learner." (Kolb, 1984). To provide an experience where students could actively consider ethical aspects of technology, a hands-on activity involving network packet sniffing was added to the course. This activity involved having each student run the Wireshark network protocol analysis software (www.wireshark.org) to capture network traffic while the student executed a Google search. Students then reviewed the captured network traffic to explore all of the information sent to Google as part of the search.

This activity provided many technology ethics discussion topics. The first topics came from the need to get permission for the activity from the university's network managers. They approved of the exercise as long as the Wireshark software was not permanently installed on the classroom computers and the exercise was limited to the wired network. Fortunately, the university's switched network design meant that students would not be able to see network traffic from any other computers, which eliminated another potential issue. To avoid the effort needed to install and uninstall Wireshark from the classroom computers, bootable Linux DVDs (http://networksecuritytoolkit.org/nst/index.html) were used. Many of the students were unfamiliar with the Linux operating system and it provided us with an opportunity to discuss various operating systems as well as discussions surrounding open source software

Once students had used Wireshark to capture the network data generated by their search, the next discussion topic was how easy it was to see the specific search term, and by extension any text entered in the browser. Students were surprised at how easy it was to see this text and also by all the additional information such as browser and operating system information that was included. Figure 1 (see appendix) shows a snapshot of the information captured by Wireshark. The search term "wireshark," the type of operating system, the browser used, and other data collected are shown in the rectangles. This provided an opportunity to discuss the ethical practices of the university's network managers in restricting the use of network analysis tools and physically securing access to network switches and other hardware.

The discussion was extended by asking students how they would feel if usernames and password for accessing e-mail, online banking, and other sites could be accessed with the same ease. Most students had never considered this, but in light of what they had seen with the Google search were very concerned. This provided an opportunity to discuss the difference between http and https. While use of HTTPS is an obvious feature for banks, for others, there is a potential trade off between the security of using HTTPS and the additional time required to load encrypted pages. Facebook explicitly discusses this tradeoff in their announcement of the ability

to use the HTTPS protocol for interacting with Facebook (Rice, 2011).

Another follow up discussion topic is the difference between wired and wireless networks, and the additional security risks posed by wireless networks. In the Wireshark exercise, students were only able to see their data due to the switched design of the wired campus network. Due to the broadcast/receive nature of wireless networks all data is broadcast to all users. Poor network security can lead to significant risk for companies and individuals (Greenemeier, 2007). An additional ethical consideration with wireless networks is whether it is ethical to access a wireless network without permission. In every class where this exercise has been used, there has been at least one student who has accessed a neighbor's wireless network without asking for permission. This provides an excellent situation for applying the ethical theories used throughout the course.

During the exercise, many students spend time exploring the Wireshark data and bring up other questions. Figure 2 (see appendix) shows two items that students will often ask about - why the search results aren't actually coming from www.google.com (in Figure 2 results come from "ve-in-f104.1e100.net") or about all of the other network traffic that is captured.

Discussing these questions gives students a feeling for the massive complexity of the internet and the need to consider the interactions between components when discussing ethical considerations. For example, including browser and operating system information seems unnecessary for a simple Google search, but once students see the complexity of network traffic, they begin to appreciate how the additional information could be useful to network administrators.

3. STUDENT REACTIONS

Students have a variety of reactions to the Wireshark exercise. Most students seem to enjoy the opportunity for a hands-on exercise (Howard, 2007) and they are completely engaged during the activity. In course evaluations and in written reflections, students often mention how valuable they found the Wireshark activity. Many students, especially those with less technical backgrounds, are very concerned when they see how easy it is to intercept network traffic and how Google search strings are transmitted in plain text. They often have questions about security of passwords, financial data, and personal information which present an excellent opportunity for a discussion about HTTP and HTTPS protocols and other network security measures.

An interesting outcome of the Wireshark activity is that it prompts many students to think more about the security of their interactions on the web. Many have not previously thought about the security of the data they send across the internet. The discussions during the Wireshark activity provide them with the knowledge needed to think critically about their use of the internet. In our most recent class, one student asked a terrific question, "What are five (5) things that I can do to better protect myself online?" This led to a discussion where other students were able to contribute their own ideas. Ideas included looking for the use of the HTTPS protocol, making use of two-factor authentication where available, keeping anti-virus software updated, using strong passwords, avoiding re-use of passwords, and not doing online banking while connected to public wireless networks. At the end of the class session at least one student typically comments that they plan on reviewing the security practices of web sites they visit for banking.

4. CONCLUSIONS

Including an active learning activity on network sniffing using Wireshark and Linux provided many topics for discussion in our IT Ethics class. Topics such as intercepting network traffic, network security, and open source software suddenly became topics that directly affected the students' lives and not merely stories in an article or case study.

One suggestion that we propose is that instructors be ready to offer tips on safeguarding personal information (Stern, 2013). This would provide information that students could act upon as a result of the Wireshark activity and discussion.

5. REFERENCES

Benbunan-Fich, R. (1998). Guidelines for using case scenarios to teach computer ethics. SIGCAS Comput. Soc. 28, 3 (Sep. 1998), 20-24.

Brinkman, W. & Sanders, A. (2012). Ethics in a Computing Culture. Cengage Learning, Boston.

Gao, J. & Hargis, J. (2010) Promoting Technology-assisted Active Learning in Computer Science Education. *The Journal of Effective Teaching*, 10(2), 81-93.

Greenemeier, L. (2007). T.J. Maxx Data Theft Likely Due To Wireless 'Wardriving.' Information Week. Retrieved on June 15, 2013 from http://www.informationweek.com/tj-maxx-data-theft-likely-due-to-wireles/199500385

Greening, T., Kay, J., and Kummerfeld, B. (2004). Integrating ethical content into computing curricula. In Proceedings of the Sixth Conference on Australian Computing Education - Volume 30 (Dunedin, New Zealand). R. Lister and A. Young, Eds. ACM International Conference Proceeding Series, vol. 57. Australian Computer Society, Darlinghurst, Australia, 91-99.

Howard, E.V. (2006). "Facing the Challenges of Teaching IT Ethics." Proceedings of Special Interest Group in Information Technology Education (SIGITE) 2006, (Minneapolis, MN, October 2006), 95-98.

Howard, E.V. (2007). "Students Respond to IT Ethics." Proceedings of Special Interest Group in Information Technology Education (SIGITE) 2007, (Destin, FL, October 2007), 219-224.

Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. Retreived on Sept. 3, 2013 from http://www.acm.org//education/curricula/IT 2008%20Curriculum.pdf

IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. Retrieved on Sept. 3, 2013 from http://www.acm.org/education/curricula/IS %202010%20ACM%20final.pdf

Kolb, D.A. (1984): Experiential learning: experience as the source of learning and development Englewood Cliffs, NJ: Prentice Hall, p. 27.

McMillan, R. (2009). The NSA wiretapping story that nobody wanted. Network World. Retrieved on June 15, 2013 from http://www.networkworld.com/news/2009/071709-the-nsa-wiretapping-story-that.html.

Rice, A. (2011). A continued commitment to security. Retrieved on June 15, 2013 from http://blog.facebook.com/blog.php?post=486790652130.

Sanders, A. F. (2005). A discussion format for computer ethics. In Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education (St. Louis, Missouri, USA, February 23 - 27, 2005). SIGCSE '05. ACM Press, New York, NY, 352-355.

Schweitzer, D. & Brown, W. (2007). Interactive visualization for the active learning classroom. In Proceedings of the 38th SIGCSE technical symposium on Computer science education (SIGCSE '07). ACM, New York, NY, USA, 208-212. DOI=10.1145/1227310.1227384

Stern, J. (2013). 10 Tips to Protect Yourself Online. Retrieved on June 15, 2013 from http://news.yahoo.com/safer-internet-day-10-tips-protect-yourself-232418764--abc-news-topstories.html.

Appendices

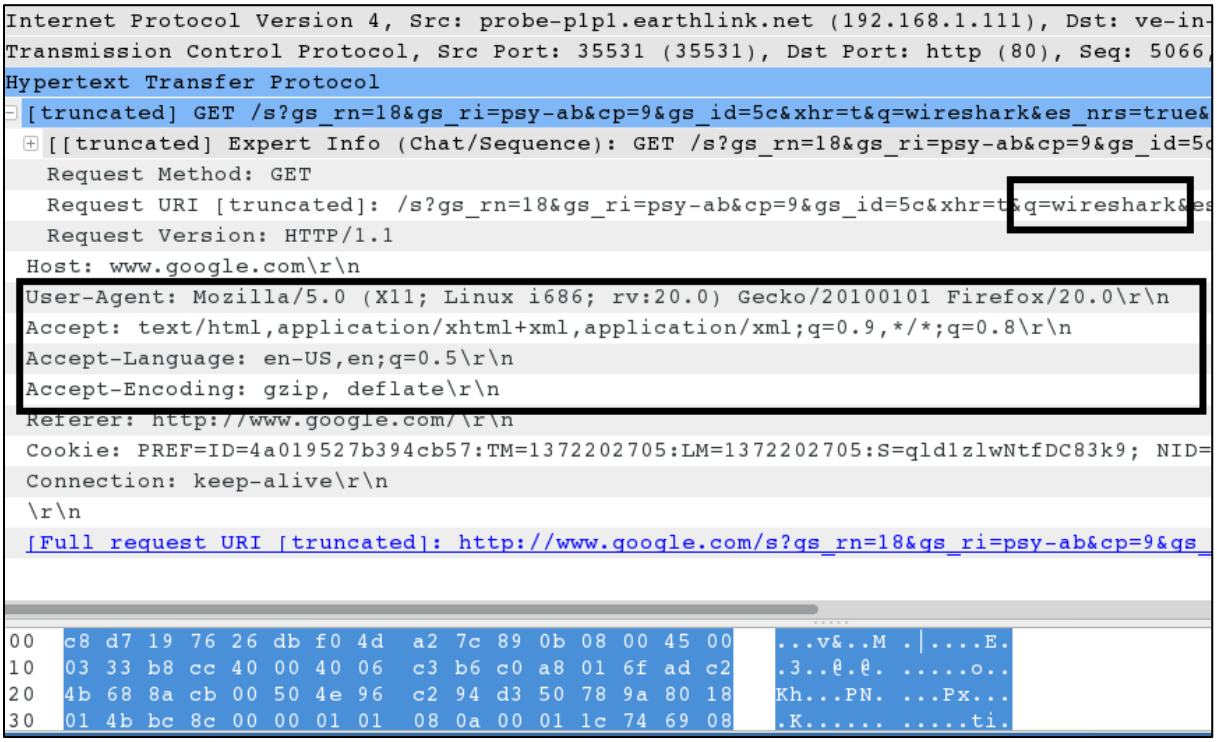

Figure 1. Data collected by Wireshark. The first highlighted box shows the search term used. The second box shows some of the browser and operating system data that is sent as part of the Google search.

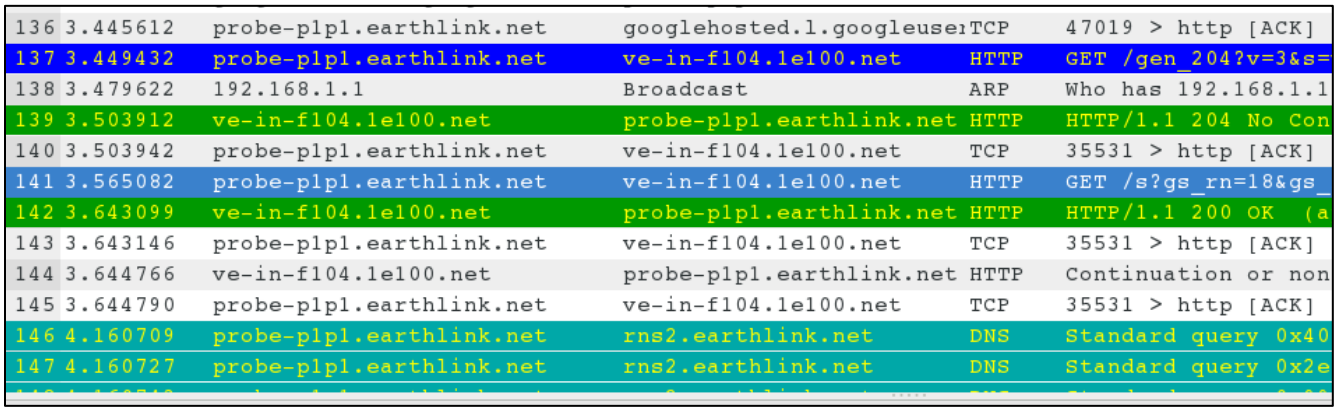

Figure 2. Data collected by Wireshark showing that Google.com search results are actually returned from another address (ve-in-f104.1e100.net in this example). This image also shows the additional network traffic taking place at the same time as the Google search.