Personal Denial of Service Attacks (PDOS) and Online Misbehavior: The Need for Cyber Ethics and Information Security Education on University Campuses

Ashley Podhradsky[1], Larry J. LeBlanc[2] and
Michael R. Bartolacci[3]

[1]*Dakota State University, Madison, SD, USA*
[2]*Owen Graduate School of Management, Vanderbilt University, Nashville, TN, USA*
[3]*Pennsylvania State University, Berks, Reading, PA, USA*
ashley.podhradsky@dsu.edu,
larry.leblanc@owen.vanderbilt.edu,
mrb24@psu.edu

Received 14 August 2014; Accepted 11 September 2014
Publication 7 October 2014

Abstract

The authors examine the need to provide basic information security and cyber ethics training for all university students, not just those pursuing an information security-related degree. The authors also discuss the need to include ethical hacking, as part of an emphasis on cyber ethics, into information security degree programs. Both of these topics are discussed within the context of a new category of cyber crime, a Personal Denial of Service Attack (PDOS) that the authors have identified, along with other types of cyber crime, that are endemic to university campuses.

Keywords: Information security training, Personal Denial of Service Attack, Cyber Ethics.

Journal of Cyber Security, Vol. 3, 339–356.
doi: 10.13052/jcsm2245-1439.335

1 Introduction

The Internet has undeniably become a necessity for many people across the globe. From conducting online banking and paying bills, searching Google, and asking WebMD for medical advice, the Internet is relied upon for a myriad of functions in everyday life. Businesses and governments alike have the same dependency on Internet-based communication, cloud storage, online transaction processing capabilities, and other Internet-enabled tools to keep their entities up and running. With the vast volume of online business transactions today, the importance of securing our online world is more important than ever. Since cyber-attacks have become a fact of life as the Internet grows. Fred Cohen, who is best known for his early work on computer viruses, and Robert Tappan Morris, who created one of the first computer worms, have demonstrated the limitations and vulnerabilities of our networks [1]. Michael Glenn Mullen, retired U.S. Navy Admiral, stated that "the single biggest existential threat that's out there is cyber [2]." Given the importance of deterring and resolving cyber security attacks of varying degrees in the U.S., information security has become a top priority for corporations, government entities, and the general populace. In response to the need for information security education, the U.S. government has created the Comprehensive National Cybersecurity Initiative (CNCI) to expand the nation's cyber security educational capabilities [3]. Initiative #8 of the CNCI identifies that "Billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace; it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success." The initiative further adds that there are not enough cybersecurity experts and "we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees".

As a result, many universities are beginning to implement focused information security programs and are adapting existing curricula to focus on this important area based on standards developed by the National Security Administration [4]. The problem with the creation of just these limited scope programs, from the authors' point of view, is twofold:

- they limit the scope of information security education to a small set of students
- they do not include a sufficient coverage of cyber ethics, instead focusing on more traditional defensively-oriented information security skills

Cyber ethics must also play an equally important role in in cyber security education for all students at a university and would play a crucial role in their

personal information security on campus. This work examines the need for information security and cyber ethics training for all university students and does so in the context of a newly categorized type of cybercrime, the Personal Denial of Service attack (PDOS) [5] and similar forms of online misbehavior. The need for basic information security and cyber ethics training for all students arises from the environment of a highly networked university campus and the close proximity students have with one another in it. The authors posit that this category of Internet crime, the PDOS, and many similar types of online misbehavior are ideally suited for universities' relaxed and social atmosphere of interaction and unlimited Internet connectivity. A PDOS is a cyber-crime in which an individual deliberately prevents the access of another individual or small group to online services. Such an attack can be undertaken using easily obtained information about a target's online services and Internet habits. We developed a survey was and administered it to students at four universities and a fifth non-university control group to help assess student attitudes towards online account security regarding a specific type of cyber crime, an online account breach. This survey provides some evidence that account breaches do occur regularly on university campuses to unsuspecting students and that existing laws do not deter such activity.

Although the initial impetus for this work was to examine the need to include basic information security and cyber ethics training for all students due to their vulnerabilities to attacks such as a PDOS, the authors also realized that information security curricula in the U.S. fell short of our expectations for its cyber ethics content. The scope of our work expanded to also include an examination of cyber ethics in the context of teaching ethical hacking. We argue that cyber ethics must not only be taught in the context of personal information security for the student body as a whole to limit the impact of online misbehavior, but must also exist in specific information security programs and their courses.

2 Student Online Misbehavior

The reliance on the Internet across the world has created a tech-savvy generation of young people who spend a good deal of their time online. "Millennials", as they are called, have grown up with online services such as Facebook, Google, Massively Multiplayer Online Games (MMOG's), online chatting, and social networks as an integral part of their lives. Given such a full time connection to online resources through a wide variety of Internet-connected devices, many users have been tempted to perform activities outside

the boundaries of acceptable online behavior. The darker side of online activity includes more serious offenses such as cyber bullying, online fraud, and hacking, but also includes other types of online misbehavior that are sometimes overlooked or even tacitly accepted by this demographic group. The potential reasons for initiating these activities are myriad, but Routine Activities Theory [6] has been put forth to help explain the origins of crimes such as these. A component of the Routine Activities Theory is the assumption that anyone may commit a crime if given the opportunity or circumstances to do so. An additional assumption that relates to this is that victims of such crimes consciously placed themselves in situations where such crimes may occur. These notions, although controversial to some sociologists and criminologists, set the stage for the discussion of Personal Denial of Service Attacks (PDOS) and other lesser known forms of online misbehavior and their ramifications for students in a university setting.

As previously mentioned, a PDOS [5] is an attack on a person or small group where access to online services is denied through a clever manipulation of existing security procedures implemented by the online service providers. With the dependence on "the cloud" for accessing remotely hosted applications, synchronizing applications between devices, storage, and a myriad of other purposes, continuous access to online services accounts is not a mere luxury, but a necessity for many individuals to live their life each day. A PDOS intentionally seeks to invoke online account security procedures in order to deny a rightful account owner access to the account. This type of cybercrime, while falling short of an actual account breach or what is traditionally defined as cyber harassment, still represents a potentially damaging form of online misbehavior that is relatively easy to perpetrate and difficult to succinctly track. Universities are full of Internet-savvy young people, many with a "gaming" mentality, advanced online technical knowledge, and underdeveloped ethics, who are prime candidates to commit a PDOS attack or similar type of cyber crime. Other types of cyber crime such as theft of intellectual property, the illegal downloading and distribution of copyrighted material, and cyber harassment occur with great regularity on university campuses. Given this environment, and driven by the notions of the Routine Activities Theory, it is more prudent than ever to include basic information security and cyber ethics training as part of the curriculum for all university students.

According to the Privacy Rights Clearinghouse [7], cyber-stalking includes the list of actions detailed below. It should be noted that a PDOS is not directly described by any of the actions in this list. A PDOS attack

does not include sending threatening emails, hacking into an account (in fact in a PDOS, the attacker is intentional not breaching the account in order to activate security mechanisms by the online service provider), creating false accounts, posting messages to online boards, or spamming the victim. Therefore, a PDOS is one form of online misbehavior that university students might engage in with limited fear of legal oversight and policing.
Cyber-stalking actions:

- Sending manipulative, threatening, lewd or harassing emails from an assortment of email accounts.
- Hacking into a victim's online accounts (such as banking or email) and changing the victim's settings and passwords.
- Creating false online accounts on social networking and dating sites, impersonating the victim or attempting to establish contact with the victim by using a false persona.
- Posting messages to online bulletin boards and discussion groups with the victim's personal information, such as home address, phone number or Social Security number. Posts may also be lewd or controversial – and result in the victim receiving numerous emails, calls or visits from people who read the post online.
- Signing up for numerous online mailing lists and services using a victim's name and email address [7]

A PDOS, due to the fact that it is not attempting compromise the integrity of information contained in an online account, would generally fall under the category of cyber ethics for basic information security education on university campuses. It is important to insure that students understand that even an attempt to interfere with the online account of another represents a cyber ethics breach and maybe in fact be a crime in certain jurisdictions. While an information security curriculum teaches students how to deal with the ever-increasing number of ways that systems, networks, data, and organizations can be attacked electronically and how to manage the information security function in an organization, it is very limited in the scope of students that it reaches. We are stressing the need for all students to be given training in best practices for conducting the online portion of their lives which includes basic personal information security and cyber ethics content. Additionally, most information security programs at universities focus on the technical and managerial aspects of information security and do not stress the more ubiquitous societal attitudes towards online conduct and cyber ethics.

3 Need for Cyber Ethics in Information Security Curricula

In addition to the need for basic information security and cyber ethics training for all university students, a concerted effort is needed to incorporate more cyber ethics into information security curricula. While there is an increasing need for cyber security experts, there are limited qualified graduates [8]. There has been a recent increase in such programs in U.S. universities to address this need, but unfortunately the programs are strictly designed around the needs of corporations and government rather than person information security and cyber ethics.

The following is a brief introduction to typical information security curricula in the U.S. which shows that the emphasis is on technical and managerial skills training and not on the ethics of everyday Internet use and interaction with other users of online services. The National Security Administration (NSA) has two core academic accreditation programs: the Cyber Operations Program and the new Cyber Defense Program [8, 9]. These programs replace the existing Center of Excellence in Information Assurance Education (CAE IAE) and Center of Excellence in Information Assurance Research (CAE IAR) [9]. The Cyber Operations designation is seen as a symbol of excellence in offensive-based university curriculum. The program specifies both mandatory and optional knowledge units. Within the accreditation criteria, the university must include certain mandatory knowledge units, and 60% of the optional program content. Of all the required and optional knowledge units for this highly coveted program accreditation, ethics is not specifically listed in the academic content requirements, thus giving it a secondary role in the curriculum at best. Of the mandatory content, accredited programs must demonstrate coverage of low level programming, software reverse engineering, operating systems theory, networking, cellular and mobile communications, discrete math, an overview of cyber defense, information security fundamental principles, vulnerabilities, and legal topics. The optional program content includes programmable logic languages, FPGA design, wireless security, virtualization, large scale distributed systems, risk management of information systems, computer architecture, microcontroller design, software security analysis, secure software development, embedded systems, forensics, systems programming, applied cryptography, SCADA systems, HCI/Usable Security, Offensive Cyber Operations, and hardware reverse engineering.

The content in information security classes taught is always an open topic for discussion. Universities seek to isolate their exposure from the potential

harm such content can wreak on their networks and any liability for cyber crime committed by students in such classes. Any wrong application of the skills learned in such classes may result in very serious consequences (such as expulsion from school, criminal cases, even the cancelation of academic programs, etc. [10]. Cook et al. [10] conducted a series of interviews in eight information security teaching schools at the graduate and under graduate level and discussed real scenarios in which students have misused their cyber security expertise. The research stresses that the students should feel ethical responsibility about application of ethical hacking techniques outside the classroom, but unfortunately such content is overlooked in favor of technical and managerial skill sets. From their interviews, Cook, et al have suggested eleven guidelines from 'hard learned lessons' which include: '(a) providing appropriate context and ethical tone, (b) explain the downsides of inappropriate behavior, (c) policies should be unambiguous, enforced, and legally defensible, (d) encourage students to pause and reflect before acting, (e) avoid stupid mistakes, (f) provide an ethics lesson early in the program, (g) tell the positive story of the program before something bad happens, (h) make students part of the process, (i) provide safe environments for exploration and experimentation, (j) provide leadership, mentorship and role models, and (k) don't crush the enthusiasm of the students". [10]

One methodology for incorporating cyber ethics into an information security program is the introduction of students to ethical hacking techniques. With the growth of the Internet from computers to phones to tablets there is an increase in the types of security threats around the world, challenging the academic world to prepare qualified information security and information assurance professionals (graduates) who also incorporate ethics into their skill sets [11–13]. Such techniques build a sense of responsibility for the security of all online users as a whole and teach students to find vulnerabilities in a responsible manner, including the reporting of those vulnerabilities to the appropriate parties. Teaching students how to attack systems and networks for the purpose of reporting vulnerabilities creates well rounded and ethical hackers who know more than just defensive techniques for information security [14–16]. Trabelsi and Ibrahim [17], researchers from the United Arab Emirates, have created a case study on "implementing comprehensive ethical hacking hands-on lab exercises" which include three Denial of Service (DOS) attacks: the TCP SYN flood attack, the Land attack, and the Teardrop attack. Trabelsi and Ibrahim have also suggested eight steps for educators and academic organizations (that deal offer information security courses) to minimize their liability related to student misbehavior online and stressed the

importance of cyber ethic [17]. Curbelo and Cruz [18], who analyzed topics for the development of information security and information assurance courses, argue that the ethics of offensive hacking cannot be taught as a single course and should be integrated throughout a curriculum. While information security curricula can be improved with more emphasis on cyber ethics, the case can be made for all university students to undergo basic information security training.

Another approach for introducing ethics, in addition to its inclusion in traditional information security programs through ethical hacking training, is the dissemination of information security concepts into other programs and coursework. White, et al. [13] discuss the process by which they changed their existing computer science curricula at the United States Air Force Academy by introducing various security related subjects into their traditional computer science courses. Their work promotes the notion that information security should be introduced throughout all introductory computer science courses with a particular focus on the "ethical and legal issues surrounding hacking and viruses" (White et. al, 1997). AlMalki and Al-Falayleh [19](2013) created an ethical hacking case study for teaching cyber using the systems and networks at the American University in the Emirates (AUE). They sniffed the AUE's network packets using a Man in the Middle attack (MitM) and were able to capture usernames and passwords of various AUE affiliated email accounts, POP3 email accounts, and AUE's Facebook credentials. They were also able to obtain some voice calls of the University's call center. This hacking was done for the purpose of creating the case study as well as exposing vulnerabilities. AlMalki and Al-Falayleh's work represents an example of ethical hacking content that can be incorporated into traditional defensive-orient information security courses for the purpose of a cyber ethics discussion.

The incorporation of ethical hacking into information security curricula does have its potential drawbacks, but in our opinion these are overshadowed by the gains in terms of the skill sets developed by students and the content of cyber ethics exposure they also receive. Many researchers agree that teaching hacking is a dangerous gamble and may involve many legal issues which may allow students to make incorrect decisions thereby creating liability for all parties involved (the student, the instructor, and the university). Separate work by Hartley, Livermore, and Durant [20–22] indicates that 90% of information security attacks happens from within an organization. This leads to the question of whether any "hacking" should be deemed acceptable within a university's network or systems. Wulf [23] indicates that "A problem with

teaching undergraduate students using this (hacking) approach is that the instructor is effectively providing them with a loaded gun". According to Gross [24], "A hacker is anybody looking to manipulate technology to do something other than its original purpose. That's not necessarily a bad thing." There are numerous "grade changing" and similar cases at lower levels of the educational system involving easily implemented technologies, such as hardware or software keystroke loggers, where students took advantage of their technical knowledge in an unethical or criminal fashion. [25–28] As noted previously, although there is some risk involved with the introduction of ethical hacking to students, the benefits outweigh the risks. In addition, the troubling cases described above lend support to the notion that many students possess the technical skills to conduct attacks such as a PDOS or similar unethical online behavior in a university setting.

The Los Angeles Unified School District (LAUSD) recently initiated a $1 billion effort to provide every student in the LA area with an Apple iPad, thereby allowing students from low-income families to have equal access to such technology. [29] The devices were "locked down" so as to restrict access to certain websites and content and also were restricted to the school district's networks. Students were allowed to posses the devices outside of school, but the restrictions were intended to prevent device misuse and limit school district liability for such. In the Theodore Roosevelt High School, one of the first schools to participate in this program, 300 of the devices were hacked within the first week of program implementation.[30] Within this very short time period, students found a way to use their iPads for unrestricted personal use by deleting their personal profile information. Removing the personal profile information allowed the devices to be used on any network and access any website or information they chose. [30, 31] Stories such as these make the case again the teaching of ethical hacking in information security programs, but certainly make the case for cyber ethics and basic information security education for students at the university level.

4 Example of the PDOS Attack: A Need for Information Security Education for all Students

The case of a PDOS attack, as previously defined, represents an example of the type of cybercrime that can occur on a university campus. A cybercrime that is easily perpetrated and very hard to detect until it has been successfully carried out. Such attacks, which utilize online security mechanisms built into services that users access to "lock out" the rightful owner of an account,

are easily perpetrated through a web browser, difficult to track due to IP address masking strategies, and represent an easy cyber crime to perpetrate on a university campus. While a simple PDOS attack can be conducted with nothing more than information that is readily available online, such as an email address, a more targeted PDOS attacks could be conducted when you integrate social engineering practices to acquire additional account information about a potential attack victim. Due to the fact that an attacker intentionally attempting to unsuccessfully login to a victim's online account appears to be normal Internet traffic on a university network, a PDOS, much like a lot of personal information security-related cybercrimes including phishing scams and the like, are not discovered until after it is too late for university network administrators to track properly and identify the attacker. In the book by the famous hacker and security expert Kevin Mitnick, "The Art of Deception: Controlling the Human Element of Security", the author discusses how people can be seen as the weakest link in security. [32] Even with limited knowledge of information security and the technical aspects of the Internet, a university campus environment would allow a student to gain enough information about what online services/websites another student uses in order to carry out an attack such as a PDOS. Gaining information on where an intended victim banks online or what online email service provider they use is as simple as shoulder surfing in a computer laboratory or dormitory room. It does not take a large amount of information, some of which is publicly available such as university email addresses, to conduct a PDOS. Social engineering and security awareness programs must become a common theme in university curricula for all students, regardless of their chosen field of study in order to address the ease with which attacks such as a PDOS can be conducted. Teaching only the technical side of information security in focused programs does not allow for the dissemination of information regarding personal information security and best practices for students when accessing online accounts.

In order to help ascertain the propensity of students to commit a cybercrime such as a PDOS, the authors developed a few survey questions related to account security breaches and attitudes of students towards them. These questions were included in a larger set of survey questions related to information security that were given to classes at four universities as part of a larger body of information security research by the authors. In order to have a "control group" with which to compare student answers to, the survey was also given to a group of law enforcement professionals attending a training seminar on cybercrime. The university students were all undergraduate students with two sets of them

in computing/technical areas of (information science and information security) and two sets of them in business school programs. The goal of this limited survey was "proof of concept" in that the authors sought to support the notion that students do attempt to commit cybercrimes such as an account breaches (which might be considered a proxy for a PDOS), but in general believe that such crimes are not worth investigating if they occur. Some of the results are briefly discussed in an informal fashion below in order to bolster the argument for increased information security and cyber ethics training in universities for all students, not because the survey was the focus of this work.

As an example, a question in the survey was: "Have you ever attempted to login into another person's online account (email, online service, ecommerce website, etc.) without their permission?" In this question, and with the other questions of the survey, the account breach is a proxy for a PDOS. If a student attempts to log on to another's online account without permission, that same student may actually be committing a PDOS through a few unsuccessful attempts. Interestingly enough, 47% of the 115 total undergraduate students who answered this question said yes. In comparison, only 15% of the 60 law enforcement officials said yes. One might infer three possible reasons for the difference between the grouped sets of respondents. The first could be due to an age differential since the students were generally in their teens and early twenties in age while the ages ranged broadly from these same ages to fifties and sixties with the law enforcement officials. The differences in age might be incorporated in the next two reasons though. A second possible reason could be the potentially higher level of skill with respect to the Internet technologies and the ease with which such technology is used by the students when compared to the law enforcement officials. A third possible reason deals with attitudes and cyber ethics and legalities: that the students saw less of an ethical or legal problem with attempting to log onto someone else's account than the law enforcement officials. Regardless of which reason had the most impact on the question's results, it is clear that such an attempted cybercrime (account breach) is one that does occur with some regularity on university campuses.

A second question from the survey was directly related to the one previously described and asked: "If you answered yes to question one, was this attempt done in a joking fashion or as some sort of challenge to see if you could be successful?" Of the students who answered yes to the first question, 70% answered yes to this follow-up one. This is in comparison to 100% of the law enforcement officers. If one is to surmise that attempting an account breach as a joke or a challenge portends no malice towards the account's owner, then

approximately 14 percent (30% of the 47% who answered yes to question one) of all surveyed students attempted at least one account breach with some form of malice as the intent. This result in particular provides support for the inclusion of information security and cyber ethics training for all university students.

A third question asked: "Are you aware of any laws relating to the process of attempting to use another person's online account?" This question is directed at discerning student awareness of the legalities of account breaches (as a proxy for the legalities of personal information security in general). Interestingly enough, 57% of the students answered yes to this question while only 47% of the law enforcement officers did. A greater awareness of the legal ramifications among the students only makes the result of question two even more troubling. The answer to this third question is further illuminated with the fourth survey question: "If you answered yes to question three, do you consider such laws deterrents (meaning that they would prevent you or other people from attempting such an activity because there would be a real possibility of being caught and prosecuted)?" In this case, less than half of the students responding (45%) thought that such laws were deterrents which coincides with the percentage of the law enforcement officials (46%). One can surmise from the results of these two questions that even though laws may exist in certain jurisdictions prohibiting the attempt of an online account breach, students do not take such laws as serious deterrents (and law enforcement does not as well).

Directly related to questions three and four, a fifth question asked: "If no malice is intended when attempting to log on to another person's online accounts, do you think it is a useful activity for law enforcement to investigate and pursue prosecution for such activities?" Again, the answers of the students were similar to those of law enforcement officials: 70% of students answered yes and 76% for law enforcement. This question addresses the sensitivity of students to an attempted breach on their own accounts. In other words, if a student believes that someone attempting to log onto their account without permission is a violation of their person information security, they would most likely answer yes to this question. The answers to this question are also interesting in light of the fact that both students and law enforcement do not believe existing laws to be deterrents. Despite this notion, they still want such breaches investigated and prosecuted if discovered.

A final question explores the propensity of university student to utilize a common tactic for obtaining account information to attempt an account breach. This question asked: "Have you ever employed a social engineering tactic

to acquire someone else's account credentials?" The results of this question show that 16% of the students surveyed answered yes and only 7% of law enforcement did likewise. The 16% is similar to the 14% figure previously derived for the percentage of students attempting breaches with some form of malice. The results of this question make intuitive sense since one would assume that social engineering is the easiest tactic to deploy when attempting to obtain online account information from another student in a university environment.

While these questions were limited in scope and were part of a larger information security research survey, they do provide some evidence that cyber crimes such as a PDOS occur on university campuses. They also provide further evidence that students do not want to become victims of such crimes, as evidenced by the result in question five. These two pieces of evidence, when put together, provide support for the inclusion of basic information security in a personal context for university students. The survey questions also bring to light then need for instruction in cyber ethics. The fact that students do not think laws are deterrents creates the need for developing a sense of personal online responsibility and good practices for the university student body.

5 Summary

In the context of university campuses, where students unlimited access to Internet connectivity and are in close proximity with one another, there is great potential for cyber crime to occur. We examined the need for personal information security and cyber ethics training for all university students. This need is examined in light of the nature of certain types of cyber crime, such as a Personal Denial of Service attack, which are easily perpetrated and difficult to track or prosecute. In addition, the need for increased focus on cyber ethics in information security curricula on these same university campuses, in the form of ethical hacking training, is also addressed by the authors.

References

[1] F. Cohen, 'Computer Viruses', Doctoral Dissertation, University of Southern California, 1985.

[2] M. Zenko, 'Admiral Michael Mullen: Farewell and Thank You', Retrieved from http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/ on May 29, 2014, 2011.

[3] White House, 'The Comprehensive National Cybersecurity Initiative', Retrieved from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative on 29 May 2014, 2012.
[4] National Security Administration, 'National Centers of Academic Excellence', Retrieved from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml on 29 May 2014, 2013.
[5] M. Bartolacci, L. LeBlanc, A. Podhradsky, 'Personal Denial Of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime', *Journal of Digital Forensics, Security and Law*, In Print, 2014.
[6] L. Cohen, M. Felson, 'Social change and crime rate trends: A routine activity approach', American Sociological Review, 588–608, 1979.
[7] Privacy Rights Clearinghouse, 'Are You Being Stalked?', Retrieved from https://www.privacyrights.org/are-you-being-stalked on 29 May 2014, 2014.
[8] M. Schwartz, 'Cybersecurity Expert Shortage Puts U.S. A Risk' Retrieved from www.informationweek.com on May 15, 2014, 2010.
[9] National Security Administration, 'Criteria for Measurement for CAE / Cyber Operations Retrieved from www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml on May 29, 2014, 2012.
[10] T. Cook, G. Conti, D. Raymond, U. Stated, M. Academy, 'When Good Ninjas Turn Bad: Preventing Your Students from Becoming the Threat', Proceedings of the 16th Colloquium for Information Systems Security Education, 61–67, 2012.
[11] S. Bratus, A. Shubina, M. Locasto, 'Teaching the Principles of the Hacker Curriculum to Undergraduates', 31st ACM Technical Symposium on Computer Science Education, ACM, doi:10.1145/1734263.1734303.
[12] D. Carnevale, 'Basic Training for Anti-Hackers: An intensive summer program drills students on cybersecurity skills', Chronicle of Higher Education, 2, 5, 2005.
[13] M. White, D. Ph, C. Gregory, L. Cohen, 'Security Across the Curriculum Using Computer Security to Teach Computer Science Principles' Internet Beseiged, ACM Press, 1997.
[14] K. Arnett, M. Schmidt, 'Busting the Ghost in the Machine', Communications of the ACM, 92–95, 2005.
[15] M. Dornseif, F. Gartner, T. Holtz, M. Mink, 'An Offensive Approach to Teaching Information Security: Aachen summer school applied IT security', Technical Report AIB 205.02.

[16] G. Vigna, 'Teaching Hands-on Network Security: Testbeds and Live Exercises', Journal of Information Warfare, 2(3), 8–24, 2003.
[17] Z. Trabelsi, W. Ibrahim, 'A Hands-on Approach for Teaching Denial of Service Attacks: A Case Study', Journal of Information Technology Education: Innovations in Practice, 12, 299–319, 2013.
[18] M. Curbelo, A. Cruz, A. 'Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems Undergraduates Students', Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology - Innovation in Engineering, Technology and Education for Competitiveness and Prosperity, 1–8, 2013
[19] M. AlMalki, M. Al-Falayleh, 'Ethical Hacking and Security Awareness: An Ounce of prevention is worth a pound of cure', Proceedings of Secure Abu Dhabi Conference, 2013.
[20] R. Hartley, 'Ethical Hacking: Teaching Students to Hack?', Doctoral Dissertation, East Carolina University, 2006.
[21] J. Livermore. 'What are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?', Procedings of the 11^{th} Colloquim for Information System Security Education, 2007.
[22] A. Durant, 'The Enemy Within'. Business *XL*, 2007.
[23] T. Wulf, 'Teaching ethics in undergraduate network', Consortium for Computing Sciences in College, 19(1), 2003.
[24] D. Gross, 'Mafiaboy" breaks silence, paints "portrait of a hacker', *CNN.com*, Retrieved on May 18, 2014, 2011.
[25] AssociatedPress, 'Monroe High School Students Caught Changing Grades' Retrieved from www.KOMONews.com on May 21, 2014, 2014.
[26] M. Birnbaum, J. Johnson, 'Students at Potomac school hack into computers; grades feared changed', The Washington Post, 2010.
[27] C. Gofford, 'Cheating scandal: Newport-Mesa official resigns to protest expulsions', LA Times, 2014.
[28] R. Wilkins, 'Grade-altering scheme sends ex-Purdue student to jail, 2nd student sentenced for hacking professors' computers', Retrieved from Jconline.com on May 2, 2014, 2014.
[29] H. Blume, S. Ceasar, 'Teachers union members, parents protest $1-billion iPad plan. Los Angeles Times, 2013.
[30] H. Blume, 'LAUSD halts home use of iPads for students after devices hacked', Los Angeles Times, 2013.
[31] A. Watters, 'Students Are "Hacking" Their School-Issued iPads: Good for Them. The limitations imposed on these devices inhibit students' natural curiosity', The Atlantic, 2013.

[32] K. Mitnick, W. Simon, The art of deception: Controlling the human element of security, John Wiley and Sons, 2001.

Biographies

Ashley Podhradsky is an Assistant Professor of Information Assurance and Forensics at Dakota State University in Madison, South Dakota. She received her D.Sc in Information Systems from Dakota State, with a specialization in information assurance and computer security. Her research interest include cyber security, specifically digital forensics. She has served as a guest editor for the Journal of Mobile Network Design and Innovation and the Journal of Interdisciplinary Telecommunications and Networking, both were special issues on Cyber Security. She is also the lead investigator at a security consulting firm in the Midwest.

Larry J. LeBlanc is a Professor of Operations Management in the Owen Graduate School of Management at Vanderbilt University. He received his Ph.D. from Northwestern University in Industrial Engineering/Management

Sciences. His research interests include analyzing spreadsheet risk, teaching management science using spreadsheets, supply chain analysis, spreadsheet optimization models, implementation of algorithms for large-scale optimization models, and telecommunication network design/analysis. He has 70 publications in referred journals and also 70 presentations at universities and organizations overseas. Dr. LeBlanc was an invited speaker at the INFORMS workshop on Teaching Management Science and has twice received the Dean's Award for Teaching Excellence. He was a guest editor of the special issue of the Interfaces on Spreadsheet Applications of Management Science and Operations Research.

Michael R. Bartolacci is an Associate Professor of Information Sciences and Technology at Penn State University - Berks. He holds a Ph.D. in Industrial Engineering and an MBA from Lehigh University. He conducts research in Information Security, Telecommunications Modeling, Information Technology Applications in Disaster Planning and Management, and Supply Chain Management.