THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 1 Article 2

2014

Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime

Michael R. Bartolacci
Pennsylvania State University, Berks

Larry J. LeBlanc
Owen Graduate School of Management, Vanderbilt University

Ashley Podhradsky
Dakota State University

Recommended Citation

Bartolacci, Michael R.; LeBlanc, Larry J.; and Podhradsky, Ashley (2014) "Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 1 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2014.1161
Available at: https://commons.erau.edu/jdfsl/vol9/iss1/2

PERSONAL DENIAL OF SERVICE (PDOS) ATTACKS: A DISCUSSION AND EXPLORATION OF A NEW CATEGORY OF CYBER CRIME

Michael R. Bartolacci
Pennsylvania State University–Berks
Reading, PA 19610
(610) 730-7685
mrb24@psu.edu

Larry J. LeBlanc
Owen Graduate School of Management
Vanderbilt University
Nashville, TN 37203
(615) 322-3662
larry.leblanc@owen.vanderbilt.edu

Ashley Podhradsky
Dakota State University
Madison, SD 57042
(605) 256-5821
ashley.podhradsky@dsu.edu

ABSTRACT

The growth of the Internet has created a corresponding growth in Internet-based crimes and online misbehavior, particularly among younger computer-savvy people. Younger generations have grown up in a world where internet access, social networking, e-commerce and smartphones are commonplace. Given this fact, they have learned how to use, and how to abuse, technology. This leads us to define a new category of cybercrime called a Personal Denial of Service attack (PDOS). A PDOS is a cyber-crime in which an individual deliberately prevents the access of another individual or small group to online services such as email or banking. Due to the nature of a PDOS, these acts can be overlooked by law enforcement and organizations that operate Internet infrastructure, such as universities. Our motivation for this work is twofold: to stress the need for cyber ethics education at the university level, and to illustrate how a previously uncategorized type of cyber crime is easily perpetrated in such an environment. To achieve these goals, we define a PDOS attack and discuss how it differs from other categories of attacks. We also examine the motivation for a PDOS attack in the context of the Routine Activities Theory of criminal justice. We further discuss a "proof of concept" survey administered at four different universities to ascertain their attitudes towards online account breaches as related to a PDOS attack. The survey provides initial evidence that account breaches, which are an integral part of a PDOS attack, are a worrisome threat on university campuses and further points to a need for cyber ethics training.

Keywords: Personal Denial of Service (PDOS) attack, Routine Activities theory

1. INTRODUCTION

The explosive growth of the Internet across the world has created a burgeoning generation of young people who are very computer-savvy and that spend a good deal of their time online. Activities such as participating in Massively Multiplayer Online Games (MMOG's), chatting and posting information on Facebook, and managing their bank accounts and financial information online are everyday activities for a generation born in the Internet age. Unfortunately, with the knowledge of how to conduct their lives with devices linked to the vast information superhighway, comes the ability to be tempted by its darker side. Posting child pornography online, cyber bullying, and perpetrating Internet fraud are just a few examples of the unethical and illegal activities that some Internet users engage in. The potential reasons for initiating these activities are myriad, but Routine Activities Theory (Cohen and Felson, 1979) has been put forth to help explain the origins of crimes such as these. Part of the premise of Routine Activities Theory is the presumption that anyone may commit a crime if given the opportunity or circumstances to do so. A related presumption that follows from 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 and analysis of our proposed category of cyber-crime: Personal Denial of Service Attack (PDOS).

A PDOS is an attack on a person or small group where access to online services is denied through a clever manipulation of the security procedures and safeguards used by the online service providers. With the reliance on "the cloud" for using remotely hosted applications (as is the case with the use of Application Service Providers (ASPs) for many businesses and organizations nowadays), synchronizing applications between devices (such as Apple computers and devices), storage (Dropobx and many other cloud or online based storage applications), and a myriad of other purposes, uninterrupted access to online services accounts is not just a luxury, but a necessity for everyday life. Although similar at first thought to a Denial of Service (DoS) attack, a PDOS distinguishes itself through the sequence of actions used to carry it out and through its intended number of victims. Comparisons to other forms of cyber-crime such as cyber-stalking (which includes cyber-harassment as a subcategory) also fall short due to the fact that no private information concerning a victim is necessary to carry out a simple PDOS attack. According to Wikipedia, in the context of cyber-harassment, “the definition of ‘harassment’ must meet the criterion that a reasonable person, in possession of the same information, would regard it as sufficient to cause another reasonable person distress In its simplest form, a PDOS can be performed using public information such as an email address.

This research examines an environment where unlimited Internet access and close proximity to potential victims provides a perfect setting for such attacks to go un-policed. An example of this would be universities, where Internet-savvy young people, many with the "gaming" mentality, advanced online technical knowledge, and underdeveloped ethics, are prime candidates to commit a PDOS attack. While some people may view the results of a PDOS as nothing more than a minor inconvenience, it has the potential for causing monetary and life-changing results. Consider the example of a person who pays credit card and other bills via online banking on the day that they are due. If such a person is denied access to the online banking site on the due date for bills, and does not have the time or means to contact the bank or companies involved to make other payment arrangements, such a person may incur late fees for a late payment, a reduced credit score, an increase in interest rates on credit cards and other financial penalties.

PDOS attacks have the potential to cause further financial harm when they exploit account auto lockout security procedures in online auction sites. Perhaps two users, user A and user B are competing against each other for an auction item. There is potential for user A to lock out user B using publicly available account ID information by simply attempting to log in as user B several times with incorrect passwords. If timed correctly near the end of the auction, user A can ensure that user B does not win the auction, and therefore user A has a greater chance of winning the auction item. This action would not only financially hurt the seller, but the auction site as well since they would receive a smaller commission from the sale assuming that further competition between A and B would have driven up the final auction price.

Pogue points out that with the most recent version of the Apple Macintosh operating system, the synchronization of calendars, address books, etc., with other Apple devices must be accomplished through Apple's iCloud online service (Pogue, 2014). A disruption to accessing one's account on this service could have serious ramifications, both professionally and personally. Another example of the potential harm caused by a PDOS could involve a university student who waits literally until the last minute to turn in a take-home exam or assignment. If denied access to their university account and unable to turn in the exam or assignment before the deadline, the denial of online access could cost the student dearly in terms of their final class grade, their grade point average, their class ranking, their scholarship, and thus their attractiveness to company employment recruiters. Any time-sensitive transaction, be it financial in nature or not, that requires online services to complete, has the potential for disruption by a PDOS. The potentially serious impact of a PDOS, when combined with the possibility of an escalation of a PDOS attacker to more serious cyber-crimes, points out the need for education on online ethics and how to avoid becoming a victim of such attacks.

2. DEFINITION OF A PDOS

The term PDOS should be distinguished from the recently contrived acronym PDoS. This latter type of cyber-crime attack, a Permanent Denial of Service (PDoS) or "Phlashing", is a cyber-security breach that exploits vulnerabilities in network-based firmware updates and attempts to render the target device(s) inoperable. A PDoS is an example of the more general type of cyber-crime called a Denial of Service attack (DoS). Our proposed category, PDOS, is distinct from both a PDoS and its related more general category DoS. In its most general definition, a DoS is an information security breach or attack that attempts to render a device, a network, or a system unavailable to its intended users. The new type of cyber-crime attack we are proposing, a PDOS, is similar in spirit to a DoS in that it attempts to render online services unavailable to a person or small group of people while remaining anonymous, but differs from a traditional DoS attack in several ways. These differences include the intended victim of the attack, the nature of the targeted device or devices, the sequence of actions to conduct the attack itself, the potential results of a successful attack, the nature of anonymity, and the motivation for the attack.

2.1 Intended Victim

While a traditional DoS attack is directed towards the information assets and/or network infrastructure of a company, government, or other type of organization, a PDOS is directed at the online services and accounts used by a single person or small group of people. In a traditional DoS attack, the victim is an organization or company that operates the device, network, or system targeted. Time, money, and human resources must be spent by the victim in order to recover from a successful DoS, or even to react to an attempted one if detected. Secondary victims are possible in a traditional DoS if legitimate outside users or customers are also affected. Unlike a DoS, a PDOS would be intended to have a single individual as a victim or a small group of people. Secondary victims of a PDOS could include the companies providing the online services targeted by the attacker in that resources must be used to create new accounts, change account parameters, and/or deal with the primary victim.

To show the gravity of a PDOS attack and further illustrate the difference between a PDOS and a traditional DoS, we pose two simple questions. The first of these is whether the resources invested to prevent or remedy DoS attacks differ from PDOS attacks in the corporate world. The second is whether the notoriety surrounding, and potential impacts of, traditional DoS attacks differ from PDOS attacks. When potentially thousands of users are impacted by a DoS attack, the resources spent can be quite staggering depending upon the size of the company or organization involved. The costs associated with firewalls, intrusion detection systems, and bringing networks and devices back to fully operational state are not trivial. Resources spent with regards to a potential PDOS attack would only involve policies and procedures that limit personal and account information from being utilized for such attacks. Although the costs associated with putting such policies and procedures in place are not zero, they would certainly not approach those expended for DoS attacks. Furthermore, a DoS is usually newsworthy event where a company’s operations, and therefore its revenue stream and profitability, are adversely impacted. A PDOS would not necessarily affect a company’s operations other than possibly disrupting the life of an employee or small group. It should be clear from this discussion that a PDOS attack is not specifically planned by a corporate information security function in an organization. However, to the person impacted by the PDOS attack, be it a consumer trying to access a website in order to make a purchase, or an employee attempting to access their online banking account during lunch hour, the results are the same. Both are denied access. This research puts forth the premise that a PDOS is a novel type of attack that “falls under the radar”, but has an impact similar to a DoS on a smaller, more personal scale.

2.2 Nature of Targeted Devices

A traditional DoS targets devices (network infrastructure, servers, etc.) operated by an organization in order to limit their functionality. A PDOS does not target a given set of devices, but instead targets the services provided such an infrastructure to an individual or small group, including both local and cloud resources. A clear distinction with respect to this factor is that an attacker must have some minimum knowledge of the devices being attacked for a DoS to be successful. In the case of a PDOS, no such knowledge is necessary to carry out the attack; only knowledge of how to access those services online is required.

2.3 Sequence of Actions to Conduct a PDOS

Unlike a DoS, a PDOS does not attempt to actually manipulate a device, a network, service, or a system to prevent its proper functioning. In fact a PDOS would take advantage of security measures put in place by network, system, and security administrators to mask the PDOS activities to ensure such an attack would succeed. For example, a traditional DoS might flood a given company's web server with excess "useless" traffic in order to overwhelm it capability to serve legitimate online customers. In this case the attacker is attempting to disguise the excess traffic as legitimate traffic until it overwhelms the server. A PDOS takes the opposite approach. It deliberately wants user traffic, or the attempt to access services to be seen as a threat to the online service provider in order to have existing security measures enacted. An example of a PDOS taking advantage of security measures would be the ability to "lock out" an online service user's account by attempting to log onto that account multiple times unsuccessfully. The intent of the PDOS in this case is not to gain actual access to the account, but to prevent the legitimate user from having access to the account for an indefinite period of time. Only after the legitimate user takes certain steps, such as changing a password or contacting the online service provider to provide verification of identity, can the service be restored. Unlike a traditional DoS, one might state that no "hacking" actually occurs against the online service provider in a PDOS; and therefore, it may not be considered illegal in many jurisdictions. A DoS attack requires special knowledge of the network or system being attacked to be successful. Such knowledge is usually gained from one or more smaller reconnaissance attacks that are used to learn about network security mechanisms and technical vulnerabilities of the target. On the other hand, a PDOS attacker can utilize information that is more easily obtained to carry out a successful attack. Information, such as email addresses, may be publicly available; and techniques such as social engineering can be used for gather the requisite information for an attack. Sometimes an action as simple as looking over a person's shoulder as they log in to an online service is all that is needed for a successful PDOS.

2.4 Potential Results of a Successful Attack

A successful DoS renders a web server, a network, a system, etc., (the target of the attack) inaccessible to legitimate users for an indefinite period of time. This period of time can vary and depends on three major criteria:

a. The ability of the organization operating the target(s) attacked to recognize the attack and take remedial action.
b. The nature of the target attacked (type of device or system).
c. The specific technical details of the DoS (which can vary and affect the ability of the organization to recognize the DoS and take action).

DoS attacks are usually recognized and acted upon by the victim in time periods of seconds or minutes and not hours or days. In contrast to the potential for very costly and serious results of a successful DoS, the results of a successful PDOS are much harder to detect and much less evident to everyone, including the primary victim. The inability to access an online service such as banking, email, social media, etc., while creating feelings of frustration or anger from the victim, may be incorrectly attributed to a variety of non-PDOS causes. Some of the possible problems that a PDOS could be attributed to (from the victim's point of view) include excessive network traffic, Internet connectivity problems, web server problems, Domain Name Server (DNS) problems, or a forgotten password. It would take possibly several successful PDOS attacks for a victim to even realize that such an attack has occurred. Even if the victim realizes there is something amiss, it is likely he or she has not documented the attacks or has any true understanding of what a PDOS attack is. Unlike the steps a company or organization would take to remedy a DoS and to prevent another one (such as immediately blocking certain open ports and developing a profile for the traffic signature of the attack), a victim of a PDOS would have little recourse other than to change the parameters of existing accounts (passwords, account names, etc.) and to create new accounts, possibly with different online service providers. It should be obvious that only the most cautious of online service users would take such actions after a single successful PDOS attack. It would most likely take several successful PDOS attacks to prompt such actions from a victim.

2.5 Nature of the Anonymity

A further difference between a DoS and a PDOS is the degree of sophistication for achieving anonymity to which an attacker has to achieve in order to have a successful attack. A DoS attacker would need to have a high level of sophistication in his or her attack in order to remain anonymous if attacking a company or organization with even modest information security protection in place. A Distributed Denial of Service attack (DDoS), which would use remote programs installed on unknowing participants' devices to carry out an attack, in some sense guarantees initial anonymity for the attacker. In this case, anonymity is achieved due to the fact that the actual attack is not coming from the attacker per se, but from other innocent parties. A PDOS would differ from both of these in that the attacker needs much less sophistication to remain anonymous. For instance, the use of a proxy server to access online accounts would only be necessary for an occasional PDOS attack in order to hide the attacker's IP address. Only if an attacker seeks to continue a series of PDOS attacks against a target would more sophistication be necessary. "Criminals hide in cyberspace, but complete invisibility can sometimes be difficult to achieve (Wild, et al., 2011)." Selwyn surveyed university students about online misbehavior and pointed out that "some respondents described such anonymity in opportunistic terms, with the Internet giving users 'the chance to conceal their identity and hence make it easier for them to be deceitful (Selwyn, 2008)." The ease with which a PDOS attacker can initially conceal his or her identity for a few attacks certainly distinguishes this type of attack from a traditional DoS. It would only be after at least a few PDOS attacks that the victim would be suspicious and possibly take action such as having online service providers track attempts to login to his or her account. Such conditions would necessarily force an attacker who wishes to continue PDOS attacks to use more technical and complex means for anonymity.

2.6 Motivation of the Attacker

The motivation for conducting a DoS can vary and includes the following possibilities:

a. Corporate espionage where a hired attacker is paid to attack the e-commerce or other information systems capabilities and functions of a competitor.
b. The making of a political statement against a company or organization through an announced attack.
c. An amateurish "script kiddie" attack for amusement or challenge.
d. Disgruntled employee or customer seeking revenge; and other similar forms of motivation.

Only the last two in this list might be considered somewhat similar to a PDOS. Revenge would certainly be a possible motive for a PDOS; but unlike a DoS where the revenge is directed at an organization, it would be directed at an individual or small group. There are also other factors related to motivation that set the two types of attacks apart. The likelihood that a victim would suffer through several successful PDOS attacks before taking action is an important difference between a PDOS and a traditional DoS. This likelihood would also play a role in the motivation of the attacker. The likelihood of success of a PDOS is high, if an attacker has basic knowledge about the victim, online services and the Internet in general. Some limited knowledge of the victim such as what services are used and possibly a general pattern of when those services are accessed are required for a successful PDOS. This knowledge can be gained in a variety of ways that vary from intimate contact with the victim to social engineering where no relationship with the victim is required. The ease with which this knowledge can be acquired can be additional motivation for this type of attack. Obviously this knowledge threshold is much lower than what is required for a successful DoS, where technical knowledge is required about computer networking and an organization's possible cyber security defenses.

3. CLASSIFYING A PDOS

We propose that a PDOS be considered a new category of cyber-crime. It does not fit in traditional categories such as those proposed by Yar (2006). He defines four categories of cybercrime:

a. Cyber-trespass – crossing boundaries into other people's property and/or causing damage.
b. Cyber-deceptions and theft – stealing and fraud.
c. Cyber-pornography – breaching laws on obscenity and decency.
d. Cyber-violence – doing psychological harm to, or inciting physical harm against others.

One might consider the frustration experienced and time wasted by a PDOS victim when not being able to access online services to be a form of psychological harm, but a PDOS differs from traditional forms of cyber-crime that would fit into the category of cyber-violence. Unlike cyber stalking, in which the attacker often intentionally makes his or her identity known to the victim, a PDOS is carried out in a truly anonymous fashion due to the ability to disguise one's cyber presence as the source of an attack with limited technical expertise. Cyber harassment can loosely define the motivation for a PDOS, but unlike traditional cyber harassment where a person sends disparaging electronic communications or posts such content online, a PDOS has a direct connection to the availability of an online service providers' accounts. For example, it takes little technical skill to post false or disparaging comments on social media such as Facebook about a victim of cyber harassment; but to disguise one's online identity in order to carry out a PDOS to deny a person access to their Facebook account requires a slightly higher level of expertise. What also makes a PDOS a new phenomenon in the context of cyber-crime and information security theory is the use of information security methodologies normally reserved for more serious security breaches of companies (such as the disguising of IP addresses previously mentioned) against an individual or small group of people. Therefore, although one might be tempted to categorize a PDOS as just another form of cyber harassment, the additional technical sophistication sets it apart. A PDOS can be distinguished from cyber stalking because the latter has a more ominous, malevolent, and physically dangerous nature. Generally speaking, a cyber-stalker seeks to use a cyber- presence to exert some degree of control over a person or group and may even threaten or commit physical violence against victim(s). In attempting to exert control, the identity of the stalker may be revealed to the victim(s). Reyns, et al. (2011) define cyber stalking as "the repeated pursuit of an individual using electronic or Internet-capable devices". Unlike a cyber-stalker, a PDOS attacker is not in "pursuit" of a victim. A PDOS also would not want his or her identity known to the victim since it would make future attacks more difficult. While the threat of physical violence is absent in our definition of a PDOS, an attacker's actions could escalate into cyber stalking or other more serious crimes against a victim. Even with the lack of a physical threat and an anonymous attacker, the element of seeking to exert control over a victim(s) is allowed under our definition of a PDOS. It is possible for an attacker committing a series of PDOS attacks to attempt to influence the victim in some way. An example of this would be a series of attacks conducted by an estranged husband against his wife during acrimonious divorce proceedings. Such attacks, if conducted properly (so as to be not traceable back to him) might create such frustration on her part that she is more willing to negotiate during divorce proceedings. Even if she suspected that he is the source of the attacks, without proper evidence, which would be difficult or possibly impossible to collect, no action could be taken against him.

Neves and Pinheiro (2010) define cyber bullying as the use of communication technologies and information to denigrate, humiliate and/or defame a person or a group of people. A PDOS can be distinguished from this definition because the destruction of a person's character or reputation is not the motivation for a PDOS attack. It may become a secondary result of multiple PDOS attacks, but the attacker is not intending such consequences directly.

One characteristic of a PDOS that sets it apart is the necessity to disguise one's electronic identity in order to carry out a series of PDOS attacks. To mask one's Internet Protocol (IP) address, an attacker could use strategies involving proxy servers, onion routing (of which the application Tor is the most popular example), or other similar mechanisms. To mask one's Media Access Control (MAC) address, methodologies exist to "spoof" this factory-set address inherent to all network interfaces of electronic devices that are on local area networks. It should be obvious that although the knowledge of how to hide one's electronic fingerprint is available online, this technical expertise would set it apart from traditional cyber harassment.

4. ROUTINE ACTIVITIES THEORY AND CYBERCRIMES

Cohen and Felson (1979) describe the foundations for what is known as the Routine Activities Theory. "Not only do routine legitimate activities often provide the wherewithal to commit offenses or to guard against others who do so, but they also provide offenders with suitable targets" (Cohen and Felson, 1979). The application of this theory in practice has focused on three necessary, but not sufficient, conditions within a given physical space or arena for crime to occur: the existence of a potential offender, the existence of a potential target, and the lack of authority necessary to prevent a crime from occurring. The application of Routine Activities Theory has been extended and applied beyond traditional high crime rates areas of physical space. It has also been applied across a variety of settings beyond chance physical encounters of an attacker and a victim. Miller posits that "... an individual's activities, regardless of whether unstructured, with friends, or absent authority figures, are carried out in a variety of physical and social settings" (Miller, 2013). Some of these settings the theory has been applied to are general usage of the Internet and computer networks, social media, and online gaming. The linking of Routine Activities Theory to cybercrime was developed by Yar (2005). "In short, the online density of both potential offenders and potential targets is not neutral with respect to existing social ecologies, but translates them via the differential distribution of the resources and skills needed to be present and active in cyberspace" (Yar, 2005). This statement can be simplified to the notion that the more time you spend in cyberspace, the more likely you are to be either an offender or a victim for a cybercrime. Marcum later used Routine Activities Theory as the backdrop for a statistical assessment of cyber-crime and its impact on adolescents (Marcum, 2009).

A corollary also put forth by Yar (2005) is that "the greater the target's accessibility, the greater its suitability, and vice versa". This particular point supports the premise that unlimited Internet access in the relative absence of authority, as is seen on university campuses in computer laboratories, dormitories, etc., provides such great accessibility. Additionally, work by Holt and Bossler (2009) concludes that "committing computer-based deviance (the more formal term for unethical and illegal behavior in the literature) increases one's risk of online victimization, mirroring previous research that has identified an association between real-world delinquent behavior and victimization".

Reyns (2013) analyzed the link between Routine Activities Theory and identity theft. He states that "results suggest that individuals who use the Internet for banking and/or e-mailing/instant messaging are about 50 percent more likely to be victims of identity theft than others". In other words, by merely using such online services, the risk of falling victim to this serious type of cybercrime increases dramatically. Along this same line of thinking, Hutchings and Hayes, in applying Routine Activities Theory to Phishing victimization, found that the routine activities of computer use and Internet banking were risk factors for phishing attacks, another type of cyber crime.

Navarro and Jasinski (2012) analyzed cyber bullying in the context of the Routine Activities Theory. One interesting result coming out of their work points to an increased likelihood of becoming a victim of cyber bullying for young people who spend a good deal of time on "informative" websites, where a two way sharing of information (posting and reading) is conducted. Pratt, et al. (2010) applied the Routine Activities Theory to Internet fraud. They concluded that "to understand the problem of fraud targeting requires an appreciation of how online exposure shapes the opportunity structure for victimization in this context" (Pratt, et al., 2010). We posit that the large percentage of university students who spend a significant percentage of their time conducting these online activities such as banking, emailing, and posting information online, thus exposing themselves to potential attackers, not only put themselves at risk for Internet fraud, identity theft, phishing attacks, or cyber bullying, but are also at risk for a PDOS.

Before focusing on the prevalence of PDOS attacks in light of the Routine Activities Theory described above, an examination of another Internet-based online misbehavior will provide insight. A related, and equally disturbing, type of online misbehavior is called "Kicking". Kicking is a quasi-hacking technique where an online gaming participant, such as an Xbox user, is “kicked” of the online game they are participating in by another participant in that game. Utilizing free software tools, such as OXID’s Cain and Able (OXID, 2012) password recovery tool, the other participant actually crosses the line and becomes a "hacker" in performing such kicking. Using these tools, the other participant is able to gain access to the victim gamer’s IP (Internet Protocol) and MAC (Media Access Control) addresses. These addresses are then exploited to force the victim out of the game and to keep the victim from rejoining the game for some period of time. Under our definition of a PDOS, the denial of participation in an online game created through "kicking" would be considered an example of such a cyber-crime.

Although typically viewed by the online gaming community and the general public as merely a form of malicious harassment, the information obtained through "kicking" can be used to perform more serious spoofs and attacks. Once the other participant has gained access to the target’s IP address, he can then ascertain what city and state the player is located in, determine the name of the service provider, and perform other malicious activities including sending a computer virus directly to the target’s machine or employing further reconnaissance techniques using tools such as Nmap (Nmap.org, 2012) to obtain additional private information about the victim. The escalation of "kicking" into a more serious form of cyber-crime, be it identity theft or some form of malicious hacking, shows the potential for a PDOS to be the precursor to more serious cyber-crimes. The fact that "kicking" even takes place during what is supposed to be a recreational activity also lends credence to the notion that online ethics are viewed in terms of "gray" and not "black and white" by online gamers.

Adding further evidence to the bending of online ethics rules by the online gaming community is the sales of "booting" services. Booting is define as the commercialization of "kicking" where an online gamer can pay a third party to perform kicking against an opponent. This allows players seeking a gaming advantage or a form of revenge to pay for kicking against other online gamers of their choice (BBC, 2009). This type of behavior reminds one of industrial espionage where a company hires a third party hacker to attack a competitor's systems or network to gain a competitive advantage in the marketplace. Such booting services do not target a gaming console such as an Xbox directly, but rather they interfere with the victim’s internet connection (BBC, 2009). For approximately $20.00, some hackers performing kicking are even willing to remotely access their customer’s system and install the software tools for the customer to target players independent of the hacker (BBC, 2009). For a larger fee, some hackers will add the machine to what is termed a "botnet," thus enabling them to perform more powerful buffering or true DOS (Denial of Service) attacks against a targeted IP address (BBC, 2009). Again, the presence of an individual in the online gaming community presents both an opportunity to conduct such online misbehavior and to fall victim to it.

Gaming consoles are typically viewed as entertainment devices by the general public. As such, devices have migrated from single player environments with rudimentary graphical capabilities to powerful communication hubs. This increase in the computing power and communication capabilities of gaming consoles has coincided with an increase in their use for various forms of cyber-crime, including crime within so-called "virtual worlds" that are part of the gaming experience (Pasupathi, 2001; Pew Internet Project, 2008; Prasad, et al., 2013). The technical aspects of the console and related player activities may lead to victimization by other players. For example, Microsoft's gaming console specifically controls certain attributes, or policies, related to the amount of user access to live gaming services. The ports on the gaming platform utilized for these controls are User Datagram Protocol (UDP) ports 3074, 5060, and 5061 (CAI Networks, 2000). Considering that UDP is a connectionless protocol, this could provide hackers with additional vulnerabilities to exploit.

Also, the gaming console is connected to the Internet and therefore is just as susceptible to online attacks. Users need to harden their consoles similarly to how they currently protect their computers. When a participant or hacker attempts to perform kicking activities they target a player's Internet connection and not the actual gaming console. This is possible because the gaming console is vulnerable to attacks involving the UDP 5060 port. Thus, when gamers who are not familiar with such technical details change their gaming console settings in an effort to host games with other players, they are unknowingly introducing more vulnerability into their systems.

5. ROUTINE ACTIVITIES THEORY, PDOS, AND UNETHICAL STUDENT ONLINE BEHAVIOR

As described previously, Routine Activities Theory in the context of a cyber-crime purports that the probability of being a victim is increased by having a greater cyber presence, which equates to a greater exposure to potential attackers. A substantial case can be made that a university environment provides the ideal place for this to occur. Although briefly described in the introduction, a more substantive argument can be made for analyzing the prevalence of cyber-crimes, including PDOS attacks, with respect to students in a university environment. The nature of a PDOS should be viewed in the light of other online misbehavior and unethical activities undertaken by computer-literate young people in their late teens and early twenties. These students who attend institutions of higher education have almost limitless access to high speed networks and Internet resources, and also less direct supervision than they had during their younger years. In particular, this last point fits well with the creation of an environment where potential attackers would feel more at ease than in the more controlled environments of their homes or previous schools where figures of authority had more direct control on their actions throughout the day and night. Reyns, et al. (2011) state that "guardianship, on the other hand, acts as a buffer against victimization by disrupting criminal opportunity structures, thereby decreasing likelihood of victimization".

While computer hacking in general can be attributed to a lack of psychological maturity, it is our position that the demographic of traditional-age university students are particularly predisposed to committing a PDOS attack due to the access to high speed Internet connectivity, close proximity to fellow students' account information in various university settings such as dormitories and computer laboratories, and other questionable online behavior that occurs in such settings. Reyns, et al. (2010) investigated the factors connecting attackers to victims with respect to cyber stalking and university students. Their conclusions confirm that the application of the Routine Activities Theory to this cyber-crime in a university context is valid. Yar (2006) states that "... when applied to computer crime, such understandings attribute youthful participation in hacking to a combination of adolescent 'crisis' and ethical 'underdevelopment'; and conversely they can be used to explain why most individuals 'drop out' of hacking as they reach psychological maturity in their twenties" (Yar, 2006).

University students in the U.S. and some other Western countries already have a general reputation of compromised ethics with respect to their use of the Internet while on campus. Activities involving the illegal downloading of copyrighted material (music, movies, etc.), plagiarism involving websites (copying website content verbatim for assignments) or purchasing fully completed assignments online are not uncommon and often go unnoticed or overlooked by faculty and administration. Williams (2010) and collaborators point out that in the case of illegal downloading of copyrighted material, increased Internet access creates the situation where "consumers will have the ability to download vast amounts of material, illegally or not". Thus, the Routine Activities Theory view of this issue would state that university students are in an environment where they can steal such material or have material stolen from them.

Theft of copyrighted material over the Internet or intellectual property locally (as would be the case if one student copied another's assignment from his or her computer or online data storage without permission) on a university campus is just one example of unethical online behavior present within this environment. Selwyn (2008) surveyed university students and found that 93.9% of the respondents had perpetrated at least one of the following five types of online misbehavior in the year prior to the survey: misrepresentation of self, unauthorized use of another's account, plagiarism of an essay or assignment, unauthorized downloading of music or film, and online pornography use. In relation to a PDOS, 26% of respondents claimed to have used another student's account without permission at least once in the prior year. Additionally, 2% claimed to have done this misbehavior "more than a few times." (Selwyn, 2008). Maimon and collaborators' work that analyzed computer-focused crimes against a large university computer network states that "our findings support the view that the routine-activities and lifestyle perspective could be used to explain cybercrime" (Maimon, 2013). Selwyn explored the propensity of British university students to participate is "lesser" Internet-based online misbehavior (Selwyn, 2008). The study supports the notion that the propensity of such students to participate in unethical or illicit offline behaviors is exacerbated in the online arena. These two works from the literature support the application of Routine Activities Theory to the online misbehavior of university students.

It follows from the application of the Routine Activities Theory that the nearly unlimited Internet access given to university students results in many of them engaging in questionable and possibly illegal behavior with respect to the use of the Internet. One of the activities that university students regularly engage in, whether in computer laboratories, dormitory rooms or other campus areas of Internet access is online gaming. It is our position that this opportunity, when combined with attitudes and behaviors developed in other activities, such as the participation in MMOG's, increases the likelihood that a student would commit a PDOS. If the intent of a PDOS attack is similar to cyber bullying, then the attitudes fostered in MMOG's come to light. Teng, et al. (2012) put forth that "... some online gamers bully other gamers either for fun or to satisfy their needs for dominance". Although online gaming and MMOG's unto themselves are benign upon an initial analysis and can even be used for educational purposes, the lack of authority overseeing these activities and the anonymity while participating online can give way to misbehaviors and abuses by participants.

The participation in computer gaming, particularly MMOG's, can foster attitudes and behaviors that would predispose university students to commit various types of cyber-crime. Chen, et al. (2005) found in their analysis of online gaming crime that 46.7% of the offenders were students and that most of these crimes were committed from public computer use areas such as Internet cafes. In fact, they stipulated in their work, which is now almost a decade old, that "such cyber-criminal activity within online games is increasing at an alarming rate" (Chen, et al., 2005). They found that the use of another person's online gaming account (and subsequent theft of their property within the game) without their permission was 73.7% of all computer gaming crime reviewed. More recent work supports the fact that computer gaming is now conducted by a majority of university students. Hainey, et al. (2011) surveyed 2,218 university students and found that 79.8% of them played some form of computer game on a regular basis. For males this percentage was even higher at 92.6%, as compared to 69.9% for females. This translated to an average of 7.46 hours per week overall with 9.02 hours for males and 4.39 hours for females. Although the percentage playing online games was smaller (38% of surveyed students), this is still a significant portion of the overall student population who are familiar with the use of the Internet to play a game against a distant opponent. Even several years ago, Chen, et al. (2005) noted that with the growth of online gaming, there was a corresponding growth in gaming-related crimes, and particularly in MMOG games.

It is not difficult to visualize the similarities between motivating factors for committing a PDOS and the motivation to participate in an online game. Hainey, et al. (2001) found that "challenge" was the most important reason for playing computer games among the students surveyed. Among online gamers, "competition" was the most important reason found. A PDOS attacker, in the context of a university setting, might be motivated by the challenge to lock another student out of his or her online services much the same way that computer gamer seeks the challenge of besting an opponent through whatever means is necessary. Likewise, competition in a class might tempt a student to lock out another student from student accounts in the hope that their academic standing and grades might be adversely affected. Universities that use course management systems with time-oriented "dropboxes" for assignments or online exams (as is the case with one of the authors) would provide opportunity for such a

PDOS. Tseng segmented online gamers by their motivations:

a. Aggressive Gamers – those who have a high need for both "exploration" and "aggression".
b. Social Gamers – those who have a high need for "exploration" and a low need for aggression.
c. Inactive Gamers – those who have a low need for exploration and a medium need for aggression.

Tseng found that aggressive gamers tended to be male in gender and that inactive gamers tended to be female in gender. Taking this information a step further, it is not difficult to equate an aggressive university-based gamer's high need for exploration and aggression with online misbehavior such as kicking or a PDOS. A single PDOS attack would be of limited value in terms of satisfying the needs of an aggressive gamer; most likely a series of such attacks would be undertaken. It is known that online gamers experience "flow" during gaming sessions. Flow is defined as "... the holistic experience that people feel when they act with total involvement" (Csikszentmihalyi, 1975, 1997). Analogously, the feeling of continually "besting" a victim through a series of PDOS attacks might provide a similar motivation and loss of a sense of surroundings.

Another potential motivating factor for a PDOS attack in a university environment is a form of revenge on a current or former boyfriend/girlfriend. Melander (2009) explored the harassment of intimate partners by university students including methods involving information technologies. "Although it may be overlooked, emotional violence could be as damaging online as it is in person" (Melander, 2009). An intimate relationship, especially in a university environment where students are in close proximity, would allow a current or former significant other to have gained the necessary knowledge of accounts and online habits to perform a series of PDOS attacks.

6. LEGAL ASPECTS OF A PDOS

It should be noted that this research was conducted with the assistance of a law enforcement officer who specializes in the investigation and prosecution of cyber-crime at the local, state, national and international levels. This law enforcement officer is also a college instructor of criminal justice and an author on cyber crime. Officer Samuel Del Rosario of Pennsylvania provided invaluable expert opinion in framing the legal nature of a PDOS and the ability of law enforcement to respond to concerns from a victim of such attacks.

Whether it is the "online gaming mentality," the need for control or revenge upon another, or just the challenge of attempting an attack, the attacker might feel confident that when committing a PDOS he or she will suffer no legal ramifications. Selwyn (2008) pointed out that "... there was a strong sense among respondents that were was 'less chance of you being caught out'." This quote from a respondent in his research deals with what Selwyn calls the "diminished risk of Internet-based action" in terms of accountability for, and the monitoring of, student actions online. He goes on to point out that "perceptions of absolute impunity were recurrent throughout the data". Freestone and Mitchell (2004) state that "the Internet offers the 'advantages' of anonymity, a reduced chance of being detected owing to the difficulty of procuring damning tangible evidence, and convenience to perpetrators, allowing aberrant behavior to remain somewhat faceless". With respect to a PDOS, the fact that it is essentially a hybrid computer crime with a limited impact on an individual or small group allows it to "slip through the cracks" with respect to statutory laws. Additionally, it is very difficult to identify a PDOS attacker who has the requisite technical knowledge to ensure anonymity across several attacks and who plans such attacks to appear random in nature from a temporal point of view. A most worrisome aspect of a PDOS for the Information Security/Information Technology department of a university or institution of higher education is that a PDOS attack is easily accomplished on their networks and would appear to be normal Internet traffic. A traditional DoS attack, on the other hand, would be noticed immediately on a university network, since the traffic would cause access failures for the university community. On the other hand, a PDOS attack would be nearly impossible to distinguish from normal traffic patterns.

Due to privacy rights, information about keystrokes and user activity on university-owned networks and computers cannot be made available to outside entities without getting approval from the judicial system. This means that in the absence of such an allowance, an attacker committing a PDOS on a university computer can only be tracked internally and in a limited fashion. Website browser history and recorded network traffic are very limited in their ability to signal the commission of a PDOS. It would require more sophisticated monitoring such as a keystroke logger or remote desktop monitoring to identify a PDOS. This is due to the fact that even if a given computer user was tracked to a website where a PDOS was attempted or committed, security built into such websites would prevent the university network from seeing the actual keystrokes or seeing encrypted traffic that was part of a PDOS. Only with the use of a keystroke logger or desktop monitoring software could a PDOS be separated from normal website activity by a given user. Furthermore, federal regulations regarding use of the Internet and electronic communication are ambiguous with respect to whether a PDOS is an illegal activity since personally identifying information is not breached, and private data has not been accessed. One of these sets of regulations, the Electronic Communications Privacy Act (ECPA), deals with the illegality of capturing transmitted information and privacy (Reyes, et al., 2007). Since a PDOS is not capturing any information per se and private information is not being obtained, the researchers feel a PDOS would not fall under its parameters. Likewise, it would not fall under the Telecommunications Act or the Computer Fraud and Abuse Act (Reyes, et al., 2007) due to the fact that "protected" computers are not actually being "accessed" as stated in the statute. And even if a PDOS attack against online banking was interpreted to be "accessing" a computer, the scope of the statue is limited to computers of financial institutions and the government.

In the context of using a PDOS attack against a university student, many more types of online accounts and services used by students, beyond online banking, could be attacked by a PDOS without falling under the scope of this legislation. Certainly the Communications Decency Act of 1996 could not be applied either in the case of a PDOS. "This legislation leaves no one legally accountable for cyber targeting (which includes cyber bullying, harassment, stalking, defamation, threats, and so forth)" (Shariff and Hoff, 2011). Given the difficult nature of identifying an attack, the limited logging of user activities, and the limited laws and regulations with respect to this activity, the authors believe that existing legal restrictions will not deter PDOS attacks. Kigerl (2012) makes the case that even if cybercrime laws exist within a country, their effects on the prevalence of cybercrime are difficult to predict and somewhat nebulous). In fact the apparent ease with which a person can commit a PDOS in the U.S. and most of the world, when combined with no effective means to legally regulate such actions, should allow them to continue to grow in popularity. Only through cyber ethics education, and increased awareness of such attacks by potential victims, will this type of cyber crime be combated.

7. SURVEY OF STUDENTS IN FOUR UNIVERSITIES

In order to help ascertain the general propensity of university students to commit a PDOS, we developed a brief anonymous survey consisting of four questions that was part of a larger information security-related paper survey given to undergraduate students across four universities in two countries. The survey was administered to provide a "proof of concept" that a university campus is an environment that would allow a PDOS to be undertaken rather easily both through the attitudes of students regarding laws protecting online account access and their propensity to commit an account breach. The survey was completely anonymous. The gender of each respondent was not tracked because it asked questions about activities that may be considered unethical and possibly illegal, and because the ratio of males to females in the class was not 1:1 (see below). Due to this inequality and in order to avoid any possible incentive for females to mask their answers out of fear of being identified, the question of gender was left out of the survey.

The goal of the survey was to gauge student attitudes towards actions that may be considered part of a PDOS (attempt to breach an online account). The students fell into two main categories with respect to their academic pursuits and the classes utilized for the survey: (1) Information Sciences and Information Security; and (2) Business students. With respect to the first category, Information Security program students were surveyed at Dakota State University in South Dakota and Information Sciences and Technology program students were surveyed at Penn State University in Pennsylvania. Within the second category, business school students taking MIS courses were surveyed at the

New Jersey Institute of Technology in New Jersey and at Sakarya University in Turkey. Although gender was not tracked specifically in the survey, the class rosters revealed the approximate ratio of male to female for each class taking the survey. Both business school classes were approximately a 70/30 percent ratio of male to female. The other two classes surveyed at both the South Dakota and Pennsylvania universities were approximately 75/25 percent male to female. The part of the survey for this work consisted of four “Yes/No" questions related to the unauthorized use of another person's online account and the legality of such actions. The 4 questions in the survey are listed below:

1. Have you ever attempted to login into another person's online account (*email, online service, ecommerce website, etc*.) without their permission?
2. Are you aware of any laws relating to the process of attempting to use another person's online accounts?
3. 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?
4. Have you ever suspected that someone has logged into your account without permission?

Although none of the questions specifically mention a PDOS, attempting to log on to another's online account without their permission (known as an attempted account breach) is used as a surrogate term for a PDOS due to the fact that the term "PDOS" is unknown to students and a complete description of PDOS would not be feasible in the survey. Question 1 directly asks if the student being surveyed has attempted an online account breach. If someone has logged onto another's account without their permission, it can be said then that this person had the knowledge and skills to have committed a PDOS instead. Question 2 seeks to examine how aware students are of cyber security laws related to a breach of a person's online account. Question 3 seeks to ascertain the attitudes of students with respect to being caught after committing an online account breach. If a student believes that an online account breach that is not malevolent in nature should not be pursued by law enforcement, then it can be assumed that either the student sees no wrong in the action or the student believes it is a futile effort or waste of time and resources to pursue the perpetrator. Question 4 looks at the potential vigilance of students against online account breaches. One would expect a student who answers "yes" to this question to be more vigilant and cautious when accessing online accounts, and to safeguard his or her account details and personal information more closely

8. UNIVERSITY STUDENT SURVEY RESULTS

We used the two-proportion test to see if respondents in a given university (location or group of locations) answer "yes" to a given question significantly more often than respondents from another university(s). The results from Question 1 of the survey (Table 1) show no statistically significant difference between the combined American student groups and the Turkish students group with respect to attempting to breach another's online accounts. This result hints at the pervasiveness of the act of attempting to access someone else's account without permission across countries and cultures. The results from Question 2, comparing the sum of the results from the American students with their Turkish counterparts, show a statistically significant difference between the two sets of data with American students being more aware of possible legal implications of using another's account without permission. This comparison is shown in Table 2 and graphically depicted in Figure 1. The results from this question hint at the greater knowledge of information security within the combined American group, and also a greater awareness of cyber-crime in general generated by the mass media in the U.S.

Question 3 is related to Question 2 in that it ascertains student opinions on the severity of an online account breach. This question also showed a statistically significant difference between the two groups. Turkish students wanted law enforcement to investigate account breaches, even in cases where no malice was intended. The more conservative cultural aspects of Turkey could explain this difference in attitudes. Another potential reason could again be that American students are more aware of the pervasiveness of cyber-crime in society as shown constantly in the mass media and feel less threatened by it. The results for Question 3 are displayed in Table 3 and graphically in Figure 2. With respect to

Question 4, American students suspected unauthorized access of their accounts statistically more often than the Turkish ones. These results are displayed in Table 4 and graphically in Figure 3. Again, this could be due to the greater awareness of cyber-crime in the U.S. and the information security knowledge of the students involved in the survey.

Table 1 Awareness of Laws (Hypothesis is not confirmed at Alpha = 0.05)

Hypothesis	U.S. Yes	U.S. Total	Turkey Yes	Turkey Total	P-Value
U.S. students are more likely to have attempted an account breach than Turkish students	31	68	8	23	0.197

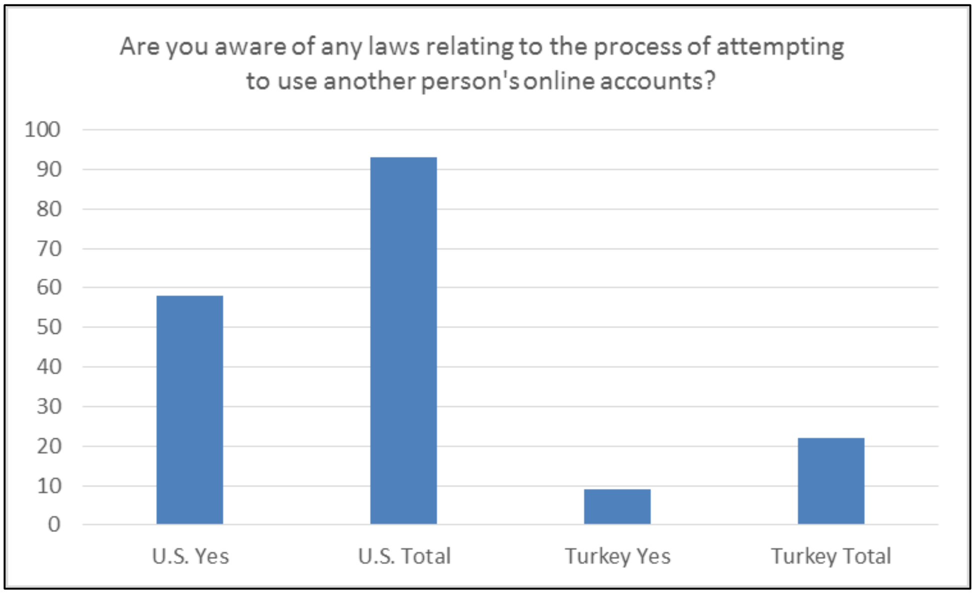

Figure 1 Question 2: Comparison between American and Turkish Students

Table 2 Awareness of Laws (Hypothesis confirmed at Alpha = 0.05)

Hypothesis	U.S. Yes	U.S. Total	Turkey Yes	Turkey Total	P-Value
U.S. students are more aware of laws regarding un-authorized use of others' online accounts than Turkish students	58	93	9	22	0.033

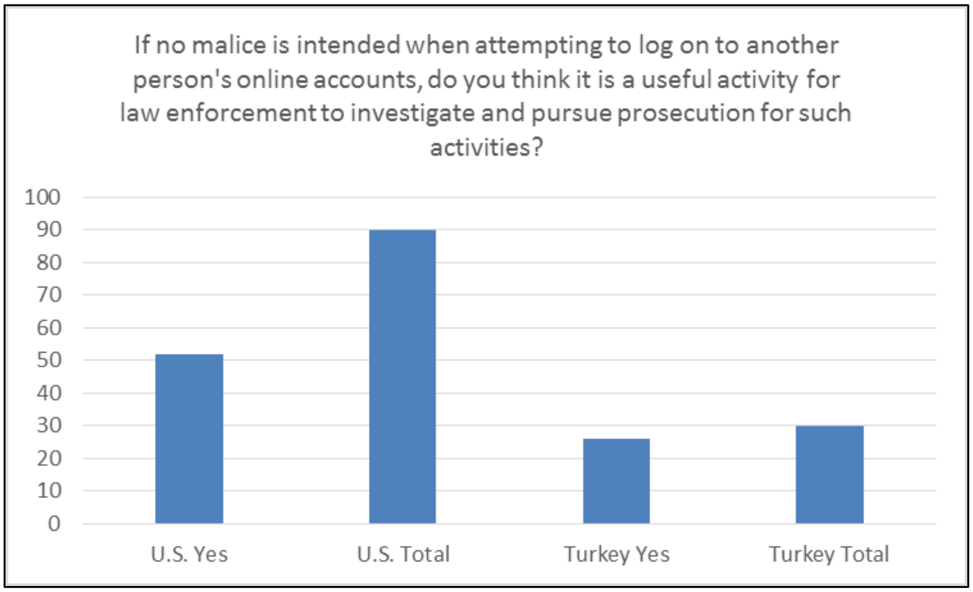

Figure 2 Question 3: Comparison between American and Turkish Students

Table 3 Importance of Prosecution (Hypothesis confirmed at Alpha = 0.05)

Hypothesis	Turkey Yes	Turkey Total	U.S. Yes	U.S. Total	P-Value
U.S. students think investigation and prosecution of unauthorized logins with no malice intended is less useful than Turkish students	26	30	52	90	0.002

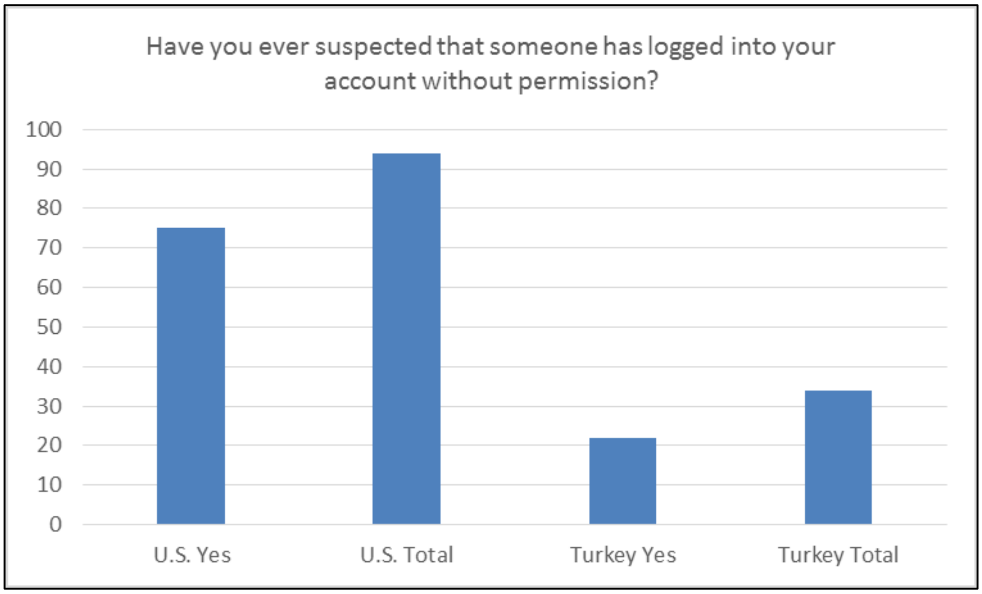

Figure 3 Question 4: Comparison between American and Turkish Students

Table 4 Suspicion of Others Logging In (Hypothesis confirmed at Alpha = 0.05)

Hypothesis	U.S. Yes	U.S. Total	Turkey Yes	Turkey Total	P-Value
U.S. students are more suspicious that others have logged onto their accounts without permission than Turkish students	75	94	22	34	0.039

9. SUMMARY AND RECOMMENDATIONS

The ultimate goal of a PDOS attack is not to gain access to an online account; rather it is to prevent a legitimate online account user from having access to their own account. Therefore, this action would not violate existing federal laws such as the Telecommunications Act or the Computer Fraud and Abuse act. A PDOS attack is difficult to detect given that it relies on what is considered to be normal traffic patterns that would not be seen as out of the ordinary by the intrusion detection systems used by online service providers. A traditional DoS attack aims to stop services for a target device, network, or system and thereby affect as many people as possible. In contrast, a PDOS is limited in scope to a person or small group.

Routine Activities Theory, when applied to cyber crimes such as a PDOS, suggests that university students need to be aware that there is a temptation to commit a PDOS due to the proximity of fellow students and their constant interface with the Internet and their online accounts. As put forth in Pratt, et al, (2010), "... parents, schools, and employers will each be critical to educating citizens on how to reduce their exposure to online risks". We recommend that institutions of higher learning should be providing students with training on how to avoid becoming a victim of cyber crimes, including PDOS attacks. By providing informal training, including methodologies for preventing the transfer of information necessary for a cyber attacks such as a PDOS, the risks of victimization could be reduced. Cesaroni, et al. (2012) described actions taken to prevent cyber bullying ranging from informal education programs to formal policy debates. We believe that mandatory computer-use ethics training for all university students would help to reduce the likelihood of a PDOS or other types of cyber crime being committed. Such training could be included in new student orientations, degree program ethics classes, and similar student learning processes. Routine Activities Theory would dictate that students should be made aware of the fact that just by logging onto online services on campus in the proximity of others, they become a potential victim for a PDOS attack as well as other cyber crimes. The first line of defense for university students is to prevent a common social engineering tactic known as "shoulder surfing". All parents teach their children to "look both ways" before crossing a street. Should not students using online services on university campuses be taught the same principle (to prevent observation of their account names and personal information)? This simple practice of being cognizant of your surroundings and whether anyone is watching could be incorporated into a more comprehensive cyber security awareness plan for students.

From a technical perspective, the authors propose that universities ensure that user accounts are separate from their public personas or aliases. Currently, many university accounts, such as email addresses, give potential attackers all the information they need to perform a PDOS attack. The authors recommend that a separate user ID (or email) is published for external communications with an internal account remaining private with only the student and IT staff being aware of its name and details. This tactic would prevent the initiation of a PDOS attack on a student's university accounts without first collecting this internal account information. It would deter PDOS attacks in much the same way Network Address Translation (NAT) is used to shield internal IP addresses from outside traffic sources to deter attacks on those internal computers. Many active directory accounts at corporations already use this process for account names, and the authors recommend that universities also adopt this approach.

REFERENCES

1. BBC. (2009). *Hackers target Xbox Live players*. Retrieved on May 22, 2012 from http://news.bbc.co.uk/2/hi/technology/7888369.stm
2. CAI Networks. (2000). *Strict, moderate, and open NAT-load balancing Xbox game servers*. Retrieved on May 5, 2012 from http://www.cainetworks.com/support/how-to-NAT-strict-open.html
3. Cesaroni, C., Downing, S., and Alvi, S. (2012). Bullying enters the 21st Century? Turning a critical eye to cyber-bullying research. *Youth Justice*, *12*(3), 199-211.
4. Chen, Y., Chen, P., Hwang, J., Korba, L., Song, R., and Yee, G. (2005). An analysis of online gaming crime characteristics. *Internet Research*, *15*(3), 246-261.
5. Cohen, L., and Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Psychological Review*, *44*(4), 588-608.
6. Csikszentmihalyi, M. (1975). Beyond *Boredom and Anxiety*. San Francisco: Jossey-Bass.
7. Csikszentmihalyi, M. (1997). *Finding Flow: The Psychology of Engagement with Everyday Life*. New York, NY: Basic Books.
8. Freestone, O., and Mitchell, V. (2004). Generation Y attitudes towards e-ethics and Internet-related misbehaviours. *Journal of Business Ethics*, *54*, 121-128.
9. Hainey, T., Connolly, T., Stansfield, M., and Boyle, E. (2011). The differences in motivation of online game players and offline game players: A combined analysis of three studies at higher education level. *Computers and Education*, *57*, 2197-2211.
10. Holt, T., and Bossler, A. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*, 1-25.
11. Hutchings, A., and Hayes, H. (2009). Routine Activity Theory and phishing victimisation: Who gets caught in the 'Net'? *Current Issues in Criminal Justice*, *20*(3), 433-451.
12. Kigerl, A. (2012). Routine Activity Theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470-486.
13. Maimon, D., Kamerdze, A., Cukier, M., and Sobesto, B. (2013). Daily trends and origins of computer-focused crimes against a large university computer network. *British Journal of Criminology*, *53*, 319-343.
14. Marcum, C. (2009). *Adolescent Online Victimization: A Test of Routine Activities Theory*. El Paso: LFB Scholarly Publishing.
15. Melander, L. (2010). College students' perception of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking*, *13*(3), 263-268.
16. Miller, J. (2012). Individual offending, routine activities, and activity settings: Revisiting the Routine Activity Theory of general deviance. *Journal of Research in Crime and Delinquency*, *50(*3), 390-416.
17. PEW Internet Project. (2008). *Nearly All US Teens, 53% of Adults Play Video Games*. Retrieved on May 22, 2012 from http://www.marketingcharts.com/interactive/nearly-all-us-teens-53-of-adults-play-video-games-7114/
18. Navarro, J., and Jasinski, J. (2012). Going cyber: Using Routine Activities Theory to predict cyberbullying experiences. *Sociological Spectrum: Mid-South Sociological Association*, *32*(1), 81-94.
19. Nmap.org. (2012). *Nmap*. Retrieved on May 3, 2012 from http://nmap.org
20. Neves, J., and L. Pinheiro (2010). Cyberbullying: A sociological approach. *International Journal of Technoethics*, *1*(3), 24-35.
21. OXID.com. (2012). *Cain and Abel password recovery tool*. Retrieved on June 1, 2012 from http://www.oxid.it/cain.html
22. Pasupathi, M. (2001). Seeds of wisdom: Adolescents' knowledge and judgment about difficult life problems. *Developmental Psychology*, *37*, 351-361.
23. Pogue, D. (2014) The curse of the cloud. *Scientific American*, February, 28.
24. Prasad, M., Kumar, B., Satish, Y., and Sriraman, K. (2013). Reconstruction of events in digital forensics. *Computer Engineering and Applications Journal*, *2*, 2.
25. Pratt, T., Holtfreter, K, and Reisig, M. (2010). Routine online activity and Internet fraud targeting: Extending the generality of Routine

Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

26. Reyes, A., O'Shea, K., Steele, J., Hansen, J., Jean, B., and Ralph, T. (2007). *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*. Rockland, MA: Syngress Publishing.
27. Reyns, B. (2013). Online routines and identity theft victimization: Further expanding Routine Activity Theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.
28. Reyns, B., Henson, B., and Fisher, B. (2011). Being pursued online: Applying cyberlifestyle-Routine Activities Theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169.
29. Selwyn, N. (2008). A safe haven for Misbehaving: an investigation of online misbehavior among university Students. *Social Science Computer Review*, *26*(4), 446-465.
30. Shariff, S., and Hoff, D. (2011). Jaishankar, K. (ed), *Cyber Bullying: Legal Obligations and Educational Policy Vacuum, Cyber Criminology* (359-392). Boca Raton: CRC Press.
31. Teng, C., Tseng, F., Chen, Y., and Wu, S. (2012). Online gaming misbehaviors and their adverse impact on other gamers. *Online Information Review*, *36*(3), 342-358.
32. Wild, C., Weinstein, S., MacEwan, N., and Geach, N. (2011). *Electronic and Mobile Commerce Law*, Hatfield: University of Hartfordshire Press.
33. Williams, P., Nicholas, D., and Rowlands, I. (2010). The attitudes and behaviors of illegal downloaders. *Aslib Proceedings*, *62*(3), 283-301.
34. Yar, M. (2005). The Novelty of Cybercrime. *European Journal of Criminology*, *2*(4), 407-427.

AUTHOR BIOGRAPHIES

Dr. Michael R. Bartolacci is an Associate Professor of Information Sciences and Technology at Pennsylvania State University-Berks. He also teaches in the Information Security and Risk Analysis Program there. His research interests include information security, telecommunications modeling and analysis, supply chain modeling, and cultural aspects of information technologies. He is editor of the *International Journal of Interdisciplinary Telecommunications and Networking* and also the *International Journal of Mobile Network Design and Innovation*.

Dr. 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 information security, spreadsheet risk modeling, supply chain analysis and telecommunications modeling/analysis. He has over 70 publications in refereed journals and numerous scholarly presentations of his research at conferences, universities, and corporations.

Dr. Ashley Podhradsky is an Assistant Professor of Information Assurance and Forensics and Program Coordinator of the MS Information Assurance and Computer Security at Dakota State University. In addition to her academic roles, Ashley is also the Director of Training for BK Forensics, a cell phone forensics company in Philadelphia and the Lead Forensic Examiner for a security consulting firm in the Midwestern U.S. Podhradsky’s current research focuses on developing digital forensics standards for non-traditional devices, specifically the Xbox 360 and One.