Abstract

This paper discusses the legal considerations for deploying honeypots to combat botnets. The use of botnets is a growing cyber threat and honeypots are being deployed as weapons of defense by companies, law enforcement, and government agencies. Honeypots are designed to track and analyze botnet data. The information gathered through a honeypot can be used for criminal prosecution. As with any weapon used in cyber warfare, there are risks involved. The legal risks associated with honeypot deployment include entrapment, liability, and privacy. The development of technology often outpaces the passage of legal statutes, and it often takes legal statutes time to become equal to technology. The laws applying to honeypot deployment are no exception. This paper discusses the current legal statutes involving entrapment, liability, and privacy and how they can be applied to honeypot deployment. A series of questions were selected as the research focus. Does the use of honeypots constitute entrapment? Is the use of honeypots a liability to those who deploy them? Does the use of honeypots violate privacy rights? It was discovered that there is no clear answer to any of the questions posed. The current statutes were found to be outdated and apply vaguely to entrapment, liability, and privacy. Each current statute has exceptions that can be applied indirectly to honeypots. Each of those exceptions was discussed in relation to honeypot deployment.

COMBATTING BOTNETS WITH HONEYPOTS: THE LEGAL CONSIDERATIONS

By

Carilyn Saul Fennell

A Capstone Project Submitted to the Faculty of Utica College

May 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science Cybersecurity – Forensics

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

I would like to thank my Mom and Dad for supporting me through my educational undertakings. I would also like to thank my Mom for being a fantastic editor. I appreciate the patience of my sister Erin and my brother-in-law Jeremy when I was unable to make plans because all of my free time was spent studying or writing papers. My triplet nieces and nephew Leah, Dylan, and Lilly always kept me motivated by saying “Kee, hurry up and do your homework so you can come back and play.”

To my brother Brian, my niece Victoria, my nephews Ryan and Robbie, and my sister-in-law Kelly; even though I do not see you as much as I would like, you are all a blessing to me. Brian, I thank you for your service to our country.

I would also like to thank Joe Giordano for letting me know about the start of this Master’s Program. I would like to thank Chet Hosmer and Paul Pantani for guidance through my Capstone project. Your feedback was greatly appreciated.

To my friends and fellow cohort 1 members, Kerry and Heather; I could not have gotten through this program without your support. I thank God that I have such great friends.

Finally, I would like to thank my grandma, Christine Saul. You telling me that I needed to find a career that makes me happy was the inspiration behind my new career endeavor. I wish you could have been here to see me graduate.

Combatting Botnets With Honeypots: The Legal Considerations

Among the growing number of threats to government and corporate computer systems, threats from botnets are on the rise. *The Top 10 Botnet Threat Report – 2010,* a report by Damballa, a U.S. based company committed to fighting cybercrime, describes a 650% increase in botnet attacks in 2010. A botnet is a group of interconnected computers that have been compromised through system vulnerabilities. Malicious software (malware) is installed on the group of computers so that they can be run automatically and anonymously (Maughan, 2008).

To combat the growing cyber-threat of botnets, honeypots are being deployed by companies, law enforcement, and government agencies. A honeypot is a type of computer trap that is designed to attract attacks and then monitor botnet activity (Zou & Cunningham, n.d.). The use of honeypots has proven very successful in tracing, tracking, and removing botnets, but there are also issues to be addressed when using them. The purpose of this study was to examine the legal issues relative to the deployment of honeypots.

- Does the use of honeypots constitute entrapment?
- Is the use of honeypots a liability to those who deploy them?
- Does the use of honeypots violate privacy rights?

Entrapment is a consideration when deciding whether to employ honeypots. The legal definition of entrapment is "A person is entrapped when he is induced or persuaded by law enforcement officers to commit a crime that he had no previous intent to commit" (Spitzner, 2002b). A honeypot is designed to attract a bot herder. An allegation of entrapment could be made if the bot herder connects to the honeypot and utilizes it for illegal activity. It is not known if the bot herder would have committed the illegal acts if the honeypot had not been made available.

It is worth restating that a bot herder could use a honeypot to conduct illegal activity. If the bot herder is able to use the honeypot to attack other systems, then the honeypot owner may be liable for any damage to the attacked systems (Sumner, 2002). Honeypot owners may take a variety of measures to mitigate this risk, but this is not a guarantee of complete protection against unlawful activity by a bot herder (Spitzner, 2002b).

The Honeynet Project was founded in 1999 to fight against malware, discover new attacks, and create security tools. They are the leading international research organization continuing to be at the forefront of security research. The Honeynet Project analyzes the latest attack threats and provides education to the public on these threats (The Honeynet Project, n.d.). The Honeynet Project has gone to great lengths to create access controls on the deployed honeypots, but even they acknowledge that one should never underestimate the power of the Black Hat Community (Spitzner, 2002b). Described as a group of hackers and crackers who break into computer systems with malicious intent, the Black Hat Community refers to the days of the wild west when the good guys wore white hats and the bad guys wore hats that were black (Jordan & Taylor, 2004). It is possible that a Black Hat hacker can develop a method or tool that facilitates the bypassing of existing honeypot access control system (Spitzner, 2002b).

Lance Spitzner and the Honeynet Project have become focused on eliminating what they define as upstream liability (Spitzner, 2002b). Upstream liability can occur when one or more Internet connected systems, in this case honeypots or honeynets, are used to attack, probe, or compromise other Internet connected hosts outside of this network or honeynet (LaBella, 2003)**.** An organization can be potentially liable if a honeynet system in their control is used to attack any non-honeynet systems. Organizations must assume responsibility for ensuring that their honeynet does not expose other organizations or individuals to risk (Spitzner, 2002b).

Privacy is an additional concern when deploying a honeypot. Honeypots record all activity occurring on a particular device. Privacy laws relative to this exist in both state and federal statutes (Spitzner, 2002b). One Federal statute that influences the use of honeypots and honeynets in reference to privacy is the Electronic Communications Privacy Act (ECPA) (18 USC 2701-11) (Radcliffe, 2007). A second is the Wiretap Statute (Title III, USC 2510-22) (Spitzner, 2002b). This study found much discussion about whether the recording of all activity of the botnet without the consent violates the Wiretap Statute.

The notion of cybercrime is a relatively new concept. The current legal statutes have not yet been updated to explicitly encompass cybercrime. In many of the cases, it is left to personal interpretation, whether current legal statutes apply to the deployment of honeypots and honeynets. Not much research has been done on the legal considerations of honeypot deployment. Of the research that has been conducted, no clear conclusions have been reached as to the legal implications pertaining to honeypots. In most cases, the general, proactive recommendation is to seek legal counsel before honeypot deployment.

Some honeypot deploying entities believe that the legal definition of entrapment is not relevant to them since their particular organization, government or business, is not acting under the control of a law enforcement agency. In addition, honeypots and honeynets do nothing to persuade attackers to target the systems; rather, bot herders target and attack on their own initiative (Spitzner, 2002b).

As with the previous legal concepts, liability remains open to interpretation. There are statutes in place protecting Internet Service Providers from liability for activity on Internet services they provide. Some honeynet deploying agencies are of the opinion that they fall under the same legal protection. Lance Spitzner (2002b) stated in his book, *Know Your Enemy: Honeypots,*

> While there is case law about the loss of the right of privacy in storing files on a stolen computer, or one that an intruder has compromised and is using without the owner's authorization, there is less case law surrounding interception of communication that is relayed through a compromised host. (para. 47)

Knowledge of legal issues associated with the use of honeypots allows those who deploy them to be more cognizant of the potential ramifications of their actions. It will also facilitate the future creation of smarter honeypots. By improving the ways in which honeypots operate, users will have greater assurance that information collected and actions taken will withstand challenges in court.

This research was conducted through the analysis of current legal precedents as they apply to honeypots. Additionally, past research was examined to find correlations between the deployment of honeypots and honeynets and the legal considerations of deployment.

Literature Review

In the article *Managing a Honeypot,* Peter Mikhalenko (2006) stated,

> It is no secret that many intruders choose their victims by scanning large chunks of addresses and searching for services vulnerable to existing tools and exploits. This can be an effective approach, although there are still some problems for intruders. People employed in IT security must trace bug trackers and the appearance of new exploits. Even open-source code cannot guarantee that the good guys will find vulnerabilities before the bad guys do. However, the good guys have another tool – a honeypot. (para. 1)

The purpose of this research is to examine the legal considerations relative to the use of honeypots and honeynets. The Honeynet Project has been attempting to determine relative considerations and how they apply to most organizations today. Their recommendation is that organizations should review all legal issues with their own legal counsel before proceeding (Spitzner, 2002b). The several legal considerations associated with honeypot deployment include, the use of a honeypot constituting entrapment, the use of a honeypot being a liability, and the use of the honeypot violating privacy rights.

The following literature reviewed by the author will give background information on botnets and honeypots. Also presented are articles supporting the legal considerations of entrapment, liability, and privacy in relation to the deployment of honeypots. Since honeypots are a relatively new technology, no specific statutes apply directly or explicitly to honeypots. Much is left to interpretation by the courts. The author found several ways in which legal considerations are currently being interpreted as fitting the deployment of honeypots.

Botnet and Honeypot Primer

A botnet is a network of compromised machines, or computers, under the influence of malware bot code, which is a form of malware. Malware also includes viruses, Trojan horses, and worms (Nash, 2005). The botnet is controlled by a person known as a bot herder and is utilized as resource or platform for attacks such as distributed denial-of-service (DDoS) attacks, and fraudulent activities such as spam, phishing, identity theft, and information exfiltration (Gu, Perdisci, Zhang & Lee, 2008). The most common type of bot attack can be accomplished in four steps. First, a botnet operator, the bot herder, sends out a virus or worm, the bot, which infects users' computers. The bot is a malicious application. Second, the bot on the infected computer logs into a particular command & control server. Third, a spammer purchases the services of the botnet from the bot herder. In the final step, the spammer provides the spam messages to the operator, who instructs the compromised computers to send out spam messages (Tech Ministries, 2011). This process is shown in Figure 1.

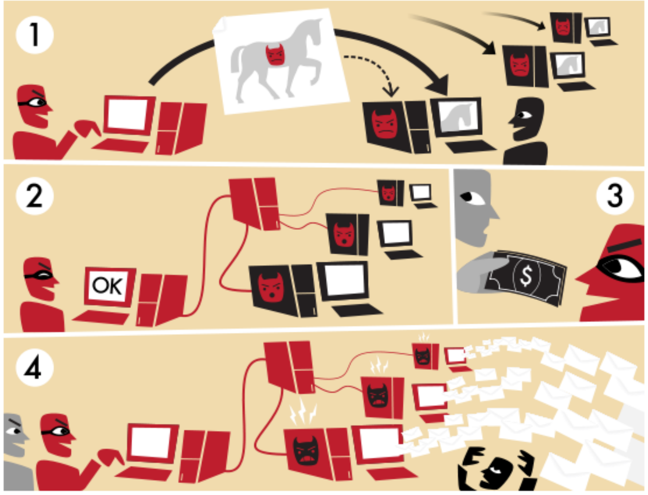


Figure 1 - The Most Common Method Used by Bot Herders to Deploy Attacks (Tech Ministries, 2011)

Even (2000) found that there are two primary reasons to set up a honeypot. The first is to research attackers. Once connected to the honeypot, all of the attacker's activities are monitored and recorded. By analyzing this information, one can gain insight into attacker methodologies and use it to create ways to better protect real systems. The second reason for a honeypot is to gather forensic information. This is often done by, or in cooperation with, law enforcement to gain information about an attacker to be used to prosecute in a court of law. According to Spitzner (2002a), "A honeypot is a resource whose value is in being attacked or compromised. This means that a honeypot is expected to be probed, attacked**,** and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information" (p 50). Appendix A shows a sample of current deployments of honeypots.

There are honeypot systems that are open source, which are free to the consumer, and commercial-grade, which the consumer has to pay to use. There are two primary types of honeypot systems. One is hardware based and the other is software based (Scottberg, Yurcik & Doss, 2002). Appendix B shows representative honeypot systems, including the system platform, vendor, and description.

A honeynet is a group of honeypots designed specifically for research. It is configured to be exactly like the production servers in the organizations deploying them. This network is like a fishbowl, in that everything that happens inside it can be seen. Similar to the fish in the fishbowl, the attacker can be watched and monitored (Spitzner, 2002b). Appendix A displays is a basic honeynet setup.

Entrapment

It is the nature of a honeypot to create an appearance that using lies and deception is acceptable when dealing with botnets. Considering this, the information gathered through the honeypot may not be deemed admissible in court. The SANS Institute develops, maintains, and makes available at no cost, the largest collection of research documents about various information security aspects (The SANS Institute, 2012). Loras R. Even, a court recognized expert witness on forensic data recovery purposes, states in a paper written for the SANS Institute that he has reservations regarding whether or not all courts will accept the honeypot evidence. It may not be deemed admissible due to the circumstances under which it was collected. He also feels that non-technical juries will be able to understand the legitimacy of the evidence and the methods by which it was collected (Even, 2000).

Honeypots have been deemed controversial because they bait and capture an attacker. While they do have benefits, some see them as an unfair entrapment technique. Some experts argue that honeypots give attackers exactly what they want. The primary foundation for the concept of entrapment is to demonstrate that illegal conduct would not be committed by an otherwise law-abiding individual. Even though the vulnerabilities exist, the attacker still has to have the motivation and knowledge to attack the honeypot (Scottberg, Yurcik & Doss, 2002).

The decisions in two United States Supreme Court cases were combined to create the standards of a successful entrapment defense. The cases were Sorrells v. United States, 287 U.S. 435 (U.S. 1932) and Sherman v. United States, 356 U.S. 369 (U.S. 1958) (USLegal, 2012). In Sorrells v. United States, the Supreme Court first recognized entrapment as a defense. In this case, Sorrells, an undercover prohibition agent, went to the house of the defendant with friends and repeatedly asked the defendant for whiskey. When the defendant returned with the alcohol, he was arrested for violating the National Prohibition Act. Twenty-six years later, the Supreme Court reaffirmed the entrapment doctrine in Sherman v. United States. In this case, a government informant met the defendant in the office of a doctor. The informant repeatedly asked the defendant for a source of drugs to negate his tremendous narcotics withdrawal. When Sherman provided the drugs, he was arrested for selling drugs. Sherman was convicted by a jury, but the ruling was unanimously overturned by the Supreme Court (Lord, 1998).

Bradley Schaufenbuel (2008) in the article “*The Legality of Honeypots*” cautioned that it is important to remember that entrapment is only applicable in situations where law enforcement is involved. A member of law enforcement must have induced a defendant to commit a crime that was not having otherwise been committed. When private citizens are involved, it is a similar concept, enticement. Appendix C shows the differences between entrapment and enticement.

Liability

In the 2000’s, the legal focus was on privacy laws on the Internet, but now it has shifted to Internet liabilities. Insurance companies are even offering Internet liability insurance policies (Debus, 2009). Liability implies that if a honeypot is used to harm others, the owner has the potential to be sued. The argument can be made that if an organization has done everything possible to secure its honeypot, then an attacker would not be able to harm another system. That being said, an organization shares fault for any harm done through its system. In the end, liability is an issue of risk (Spitzner, 2010). If a honeypot becomes compromised and outbound traffic is allowed, this traffic can become an attack on others. In this instance, Scottberg, Yurcik, and Doss (2002) found that the honeypot owner may be liable for lacking due diligence of the corporate network. It could also be considered gross negligence because the hazard was deliberately set and not properly supervised.

Privacy

Privacy laws in the United States can limit the information being captured by a honeypot, even if that information is from an attacker of a system. This captured information can be anything from logins and passwords to emails and online chats (Spitzner, 2010). There are several challenges as they pertain to the possible privacy violations when using a honeypot. First is that while there is much case law on the loss of privacy rights in relation to storing files on a stolen or compromised computer without authorization, there are very few cases pertaining to the interception of communications through a compromised system (Scottberg, Yurcik & Doss, 2002).

A second challenge is that it is often difficult to know which privacy statutes apply to a particular honeypot situation. Frequently, state law concerning privacy can supplement a federal statute. For example, a honeypot is located in California and it is attacked by a bot herder from Illinois. What privacy laws apply to this case, Federal, California, or Illinois? To compound the problem of jurisdiction, often the bot herders are located outside of the U.S. When different countries are involved, which privacy statutes apply becomes more difficult to identify (Spitzner, 2010).

Currently, there is no single statute that directly applies privacy rights in the United States relative to honeypots. Two statutes commonly referenced are the Electronic

Communication Privacy Act (18 USC 2701-11) and the Wiretap Statute (Title III, 18 USC 2510-22). Since these statutes only apply to the United States, if a honeypot is being deployed in another country, the privacy laws of that country may be different or potentially non-existent (Scottberg, Yurcik & Doss, 2002).

A portion of 18 U.S.C. 2511(1), better known as the Federal Wiretap Act, states:

> Any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication…intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection… (Cornell University Law School, n.d., para 9)

Walden and Flanagan (2003) state that due to new electronic surveillance technology, there was a need for the U.S. Government to expand the protections of the Wiretap Act. This need prompted the U.S. Congress to pass the Electronic Communications Privacy Act (ECPA) in 1986. The ECPA governs the interception of communications and access to stored electronic communications. This includes electronic communications between machines, including cellular phones, computers, fax machines, and pagers.

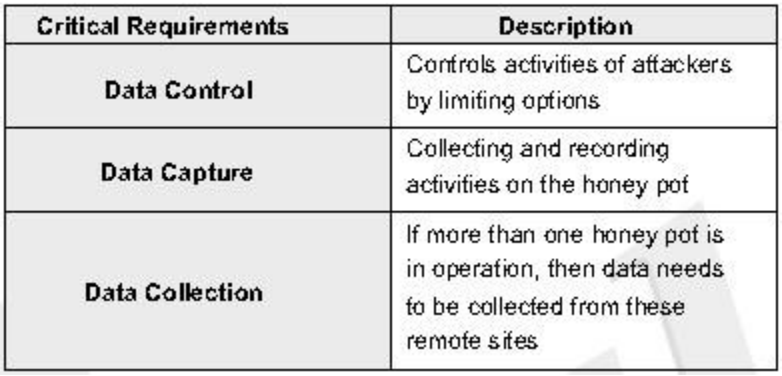
Several elements of the ECPA are applicable to honeypots. One such element protects against the unlawful interception of electronic communications while being transmitted. The interception may be done by any person who knowingly or intentionally intercepts such communications. This statute would include all communications in and out of a honeypot since the definition of electronic communication is “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce….” (para. 86).

Sources that Refute the Issues of Deploying Honeypots

Walden and Flanagan (2003) analyzed previously prosecuted cases involving entrapment and the application of those decisions to honeypots. They found that a successful entrapment defense under Sorrells-Sherman requires two elements. The first is government inducement and the second is a lack of a predisposition to engage in criminal activity on the part of the accused. They discovered that if the purpose of the honeypot operators was not to induce criminal activity under U.S. law, then the predisposition of the accused is irrelevant. The accused must present evidence that a government agent was involved in the inducement into a criminal activity. Accordingly, “if law enforcement officers do nothing to induce a defendant to commit a crime, a defendant can't claim entrapment” (para. 18).

When applying this to honeypots, it could follow that since it is a passive presence and the only lure is that it has less than optimal security, it is in no way inducing an attack. The attacker finds the honeypot using his/her own devices and chooses to connect with it due to the vulnerability of the system. This scenario demonstrates the absence of inducement by deploying the honeynet, and it is unlikely that under U.S. Law it would be considered entrapment.

Spitzner (2002b) documented that it has been established through research that liability can be a legal issue when employing a honeypot or honeynet. Since the use of honeypots has been increasing, so too have the ways to mitigate that risk. Lance Spitzner of the Honeynet Project has made several recommendations in his paper "*Know Your Enemy: Honeynets*." Data control is the key to containing the activity of the honeypot. The biggest challenge during this process is not to incur suspicion of the attacker. When setting up the first honeypot, The Honeynet Project found that if no outbound traffic could be initiated by the attacker, it took less than fifteen minutes for the attacker to figure out something was wrong, wipe the system drive, and disconnect from the network. The trick is to give the bot herder the flexibility to do what they need to, but not allow the honeypot to be used to harm others. Refer to Table 1 for critical requirements of honeypots, including data control, data capture, and data collection.



Critical Requirements	Description
Data Control	Controls activities of attackers by limiting options
Data Capture	Collecting and recording activities on the honey pot
Data Collection	If more than one honey pot is in operation, then data needs to be collected from these remote sites

Table 1 - Critical Requirements of Honeypots (Pinchuk, 2004)

The Honeynet Project created a simple design. A firewall is placed in front of the honeynet and all traffic must go through it. The firewall keeps track of how many outbound connections are made and once the limit is reached, no more attempts can be made. An automated system has been set up to monitor the system and shut down the outbound traffic if it reaches a maximum set. For added security, a router is placed between the firewall and the honeynet. The benefit is twofold. First, it hides the firewall and creates a more realistic environment for an attacker. The second is that router can supplement the protection of the firewall.

Poulsen (2003) addresses the exemptions to the Wiretap Act that may protect the operators of honeypots. One exemption states it is legal if one of the parties gives consent to the monitoring. Kevin Poulsen, from SecurityFocus, found that some experts in the field suggest displaying a banner message on the honeypot warning that the computer is monitored. Once going past the banner, the attacker has consented to monitoring. The main limitation to this is that attackers very rarely enter a honeypot through the standard methods. If they do not see the banner, then they cannot consent.

Another exemption, known as the provider exemption, may be the most beneficial to honeypot operators. This exemption states that if in the process of protecting a system from attack, a honeypot owner is allowed to eavesdrop or monitor activity. Richard Salgado, senior counsel for the Department of Justice Computer Crime Unit, cautions that this exemption may not be applied to honeypots because a honeypot is designed to be attacked. He states, "It's a little odd to say we're doing our monitoring of this computer to prevent it from being attacked" (para. 8). It has been discussed that since honeypots do not provide public accounts for communication purposes and are not fulfilling the functions of a service provider, they are not protected under the Internet Service Provider (ISP) exception (Scottberg, Yurcik & Doss, 2002).

There are also exceptions provided in the ECPA, in which communication interception is not considered unlawful. Some argue that the function of honeypots fall into one or more of these categories. The following are the exceptions and how they relate to the use of honeypots.

The first is the Computer Trespasser Exception. After September 11, 2001, the Patriot Act was created and an amendment was made to the ECPA that stated that a law enforcement agency could aid a private person or organization if that person is acting under the color of the law. In this instance, the person may "intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer..." (Walden & Flanagan, 2003, para. 85). This exception is applicable when the following conditions are met:

- the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
- the person acting under the color of the law is lawfully engaged in an investigation;
- the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
- Such interception does not acquire communications other than those transmitted to or from the computer trespasser.

According to research by Walden and Flannigan, a honeypot would appear to satisfy all the conditions of this exception, since the honeypot only has communications to and from the attacker; and law enforcement can authorize the owner of the honeypot to collect said communications for the purpose of tracking the attacker.

A second exception is the Party to Communications Exception. This exception was relied upon heavily before the creation of the previous Computer Trespasser Exception. This exception permits the interception of communications when one party has given consent. It has been suggested that the owner of a hacked computer could be considered a party to the communication and can give consent to monitoring (Walden & Flanagan, 2003).

Although there are no clear statutes pertaining to the deployment of honeypots, existing statutes do have exemptions under which the honeypots may be considered to fall. Knowing the exemptions and how they apply is essential to honeypot deployment. There are measures that can be taken in order to reduce legal complications such as liability. These measures are addressed in the Discussion of Findings section to follow.

Discussion of the Findings

Sun Tzu, the Chinese warrior and philosopher, stated over 200 years ago, “All warfare is based on deception” (Scottberg, Yurcik & Doss, 2002, para 29).With the rise of Internet threats, an environment of “information war” has been created and deception is a requisite aspect. This type of cyber warfare gives the advantage to the attacker in that the singular requirement is vulnerability. The defender has the difficult job of securing all vulnerabilities on a system. As attacks become more frequent and intricate, the use of honeypots will continue to grow. The use of honeypots allows for early detection and quick analysis of attacks. This prompt action makes honeypots an attractive tool to government agencies such as the Department of Homeland Security since our national infrastructure relies heavily on computer systems (Scottberg, Yurcik & Doss, 2002).

This research concluded that there are always risks when dealing with the Blackhat community. These risks include legal statutes such as liability, entrapment, and privacy. Even though these risks exist, it is not clear how they apply to honeypots. No clear legal precedents have been established regarding honeypots (Walden & Flanagan, 2003). The purpose of this study was to examine the legal issues relative to the deployment of honeypots.

- Does the use of a honeypot constitute entrapment?
- Is the use of a honeypot a liability to those who deploy them?
- Does the use of a honeypot violate privacy rights?

The findings as they pertain to each risk are detailed in the following sections.

Entrapment

Entrapment arises as an issue because a honeypot is designed to attract intruders. Poulsen (2003) describes a honeypot as “a type of hacker flypaper: a system that sits on an organization's network for no other purpose than to be hacked, in theory diverting attackers away from genuinely valuable targets and putting them in an closely monitored environment where every keystroke can be analyzed” (para. 3). Some have compared the use of a honeypot to that of an undercover officer. There are two significant differences. There is no interaction with the individuals acting together with the honeypot; and there is no recruitment of individuals to interact with the honeypot. With no interaction of actual people, an entrapment defense is difficult to establish (Radcliffe, 2007).

The first area of confusion surrounding the concept of entrapment is whether entrapment occurs when law enforcement is not involved. To date, entrapment applies to law enforcement agencies so honeypot operators cannot be prosecuted (Scottberg, Yurcik & Doss, 2002). The Honeynet Project has taken a simple stance on the subject of entrapment. They do not feel it is an issue and the reasoning is straightforward. They are not a law enforcement agency (Spitzner 2002b).

The second area of confusion is that entrapment is only a legal defense. No one can be sued over an entrapment violation. The concept of entrapment is used by an accused individual to avoid conviction. Currently, the U.S. court system sides with the prosecution in that it is assumed that the accused was not entrapped. To prove otherwise, the defense must establish that the accused would not have been involved in the criminal activity without the influence of law enforcement (Radcliffe, 2007). As research suggested, the deployment of a honeypot can still be established as enticement. For now, enticement remains an ethical debate and not a legal precedent (Kabay, 2003).

Privacy

It is very important that all legal aspects addressed when deploying a honeypot; and privacy is one of those aspects. This study found two primary statutes commonly applied to honeypots. They are the Electronic Communication Privacy Act (18 USC 2701-11) and the Wiretap Statute (Title III, 18 USC 2510-22).

The Wiretap Statute has exceptions that may apply to honeypots. One of those exceptions states it is legal if one of the parties gives consent to the monitoring. One way companies show consent to monitoring is by using a consent banner. This can be done both pre and post login on a system. An example of such a consent banner is shown below from the Department of Defense website.

> This is the Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes. (Radcliffe, 2007)

A consent banner is only successful if the attacker enters the system through a method that shows the banner. If the attack occurs in non-traditional ways, the banner may go unseen. An example would be entering a system by bypassing the authentication method. When bypassing the banner by not using standard methods to enter a system, the attacker forfeits the right to privacy. This is because it is illegal to circumvent the authentication process and enter a system (Radcliffe, 2007).

Since the Federal Wiretap Act has both civil and criminal provisions, it is possible that an attacker could file a lawsuit against a honeypot operator. To date, no court case has been seen of this nature, but as criminals get bolder, it is a strong possibility in the future (Poulsen, 2003).

The ECPA has several exceptions that mitigate the risk of privacy violations during honeypot deployment. These exceptions can be easily explained using the diagram in Figure 3 below. A minimum of two individuals must be involved in any communication. In the diagram below, A and B represent the individuals involved in the communication. The method of communication can vary and hold no bearing on the interpretation of the law. In some instances, there can also be a third party indirectly involved in the communication. This third party is represented by X in the diagram. X may or may not be either known to A or B (Radcliffe, 2007).

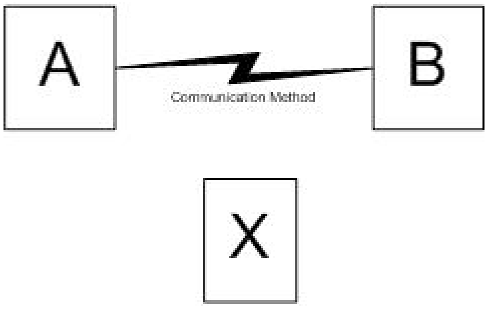


Figure 2 - Communication Method (Radcliffe, 2007)

Using the above diagram to describe honeypot activity, A is the honeypot and B is the attacker. As defined by the ECPA, party A can be considered either a person acting under the color of the law or a person not acting under the color of the law. So as long as A is the owner of the honeypot, according to the ECPA, it is legal to intercept and monitor communications between A and B. At times, other parties may be indirectly involved in the communication, represented by X. Under the ECPA, there are two instances where X may intercept the communication between A and B. The first instance is the Provider Exception of the ECPA. Under this exception, X would represent an ISP. An ISP has the legal right under ECPA to intercept and monitor communications when it owns the infrastructure on which the communication is made. This monitoring and intercepting is legal since it is done to protect the system and scan for quality control issues. The third party X may also have a legal right to intercept and monitor communication between A and B is it is given consent by party A (Radcliffe, 2007).

Liability

Legal experts have been discussing for years the concept of liability. Spitzner (2010) stated in his article *Honeypots: Are They Legal* that to date, there has been no published decision addressing liability when a compromised system has been misused by a hacker. In the same article, Spitzner also asserts that while liability is an important issue, it has been greatly overstated since there has been no recorded case of it occurring. With no current legislation explicitly applying to the deployment of honeypots, the legality of the honeypots is left to interpretation. An owner must take advantage of all precautions available to mitigate the risk of legal action. These measures, as they apply to liability, are detailed in the following sections.

Data Control and Data Capture

Data control is a measure that protects outside systems from becoming a target of an attack through a compromised honeypot. The primary purpose of data control is to protect the honeypot operator from upstream liability (LaBella, 2003). One form of data control is to place a honeywall in front of the honeypot. A honeywall is a firewall specifically designed for a honeypot. The honeywall operates as an entryway from the internet into the honeypot. The honeywall is not only a gateway into the honeynet. It also serves to separate the private network (Krasser, Grizzard, Owen & Levine, 2005). An example of a honeywall setup is shown below in Figure 3 below.

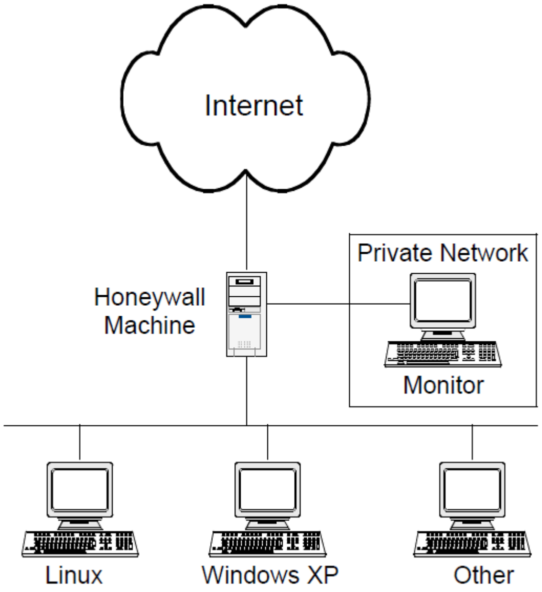


Figure 3 - Basic Honeywall Setup (Krasser, Grizzard, Owen & Levine, 2005)

The honeywall limits the number of outgoing connections and also has the ability to modify malicious data packets targeting non-honeypot systems. Limiting the bandwoidth usage is another form of data control. With less bandwidth, there are fewer network resources available to an attacker (Krasser, Grizzard, Owen & Levine, 2005).

Data capture is another essential part of mitigating liability risk. Data control and data capture function together. Whereas data control involves outbound traffic, data capture involves both inbound and outbound traffic. A 3-layer hierarchy is utilized during data capture. The first layer is the firewall (honeywall) that captures all inbound and outbound traffic. All data, both inbound and outbound, is considered suspicious and analyzed. The IDS component is the second layer of data capture. This layer resides on the target honeypot system and captures all network activity in a hidden manner. The final layer of the hierarchy is the log component. This component logs all activities of the honeypot and stores those logs in a remotely controlled log server. To prevent compromise from an attack, the log server is not only remotely stored, but it is strongly access controlled (Zhang, Zhou, Qin & Liu, 2003).

A disadvantage to using any honeypot is that of possible detection by an attacker. How to capture and store data remains a problem. One solution to this problem was found in the article *Honeypot: A Supplemented Active Defense System for Network Security*.

> Attacker's activity is captured by kernel module of honeypot OS, which encapsulates the captured data with a spoofed IP and common use protocol such as NetBIOS. Honeypot gateway actively captures, decrypts, and reconstructs these data. Capture data in kernel module make it independent of the communication means, such as SSH, SSL, or IPSEC. Spoofed IP and encapsulation are used to trick attackers. (Zhang, Zhou, Qin & Liu, 2003)

Virtual Honeypots and Honeynets

A virtual honeypot is a single computer that imitates a honeynet with multiple honeypots attached. Software such as VMWare can be used to create the virtual system.

As with any honeynet, there are advantages and disadvantages. The primary advantage of using a virtual environment is that it is inexpensive to construct. A disadvantage to this system is that attackers may be able to detect their own presence in a virtual system and cease an attack. In addition, not all computer systems are equipped to set up a virtual environment. An additional consideration is that some computer systems are not able to operate in the same manner in a virtual environment as they operate with a physical setup (Krasser, Grizzard, Owen & Levine, 2005).

Limitations of this Study

The primary limitation of this study is that there is little case law pertaining to the legal implications of deploying honeypots. The literature reviewed for this study reiterated this point. Lakhani (n.d.) summed up the limitations of case law in the doctoral dissertation, *Deception Techniques Using Honeypots*. The dissertation states "… it is hard to define legal boundaries for the 'free and open' usage of honeypots" (p 24). The reasons for the undefined legal boundaries are as follows:

- New technology: As said, when even the people coining this term are in learning curve, the legal framework and its adjudicators are obviously going to take the case in as-and-when circumstances i.e. take it according to the context defined and explained to them.
- Varied applications: Honeypots have not only varied and debatable definitions but also their application too range from a simple port scanner to a virtual machine that is created on demand. A common law, which could then be internationalized, is thus hard to achieve.

- No legal cases: As of yet, there has not been a legal case pertaining to honeypots and its usage, so there is not any pre-established laws directly addressing this concept.
- Concepts already legalized still debatable*:* some issues relating to honeypots like entrapment, enticement etc. themselves have debatable rulings in difference scenarios. For example, while in the case of Sorrells v. United States the court ruled out the possibility of entrapment but in case of Sherman v. United States, it made the government responsible for entrapment.
- Thin line between honeypot technique and unauthorized usage*:* As this thesis further illustrates, there will be applications either by governmental organizations or by obsessive aficionados of spy-work, to track the very nature of hacker activity and their source. This technique, though precious if used by authorized and administrative faculty, could have severe legal obligations. The so-called 'patriotic hacker' term applies to this scenario. (Lakhani, n.d., p 24-25)

Recommendations

In the past, Federal statutes have been adapted to included technology advancements. The same needs to be done for honeypots. Until that occurs, owners of honeypots should proactively consult with legal counsel and risk management professionals. Those persons or companies work with any aspect of a honeypot should then be trained in the legal issues suggested through the consultations. Documentation of all aspects of the honeypot deployment will also be essential. This documentation should include a procedure manual. In addition, in writing should be the justification and intended scope of the honeypot.

> Walden and Flanagan (2003) suggest the following, …carefully consider contemporaneous documentation of the proper operation of the system, the reasons and times of non-operation, the accuracy of the logs and records produced, the expertise of those operating the honeypot system and their ability to explain what the logs and records reflect, and the continuity of the above regarding a specific hacker's period of activity. (para. 1)

Along with documentation, training is an essential element in the deployment of honeypots. Any personnel involved in the deployment of a honeypot should be trained not only in the elements of the honeypot itself, but also in the legal aspects of the deployment. By knowing the proper procedures involved in honeypot deployment, the legal risks are diminished.

Entrapment

According to current statutes, entrapment only applies to law enforcement agencies. In relation to the deployment of honeypots, law enforcement may be involved in the investigation, but the honeypot may not be deployed by an agent of law enforcement. As long as this criterion is met, entrapment is not involved. Depending on the circumstances surrounding the deployment, it may be necessary to consult with legal counsel or law enforcement. Great care should be taken to document all involvement of such consultation, because it could be considered entrapment by the court system. The recommendation is supported in the article *Honeypots: A Sticky Legal Landscape*

(Walden & Flanagan, 2003). Sumner (2002) also added that as long as a honeypot is not advertised and deployed correctly, information gathered could be used as legal evidence.

Liability

There are several recommendations to follow that could result in reduced liability. The soundest way to reduce downstream liability when deploying a honeypot is through data control. Data control will prohibit or greatly reduce outbound connections to third parties and, in turn, will prevent bot herders from launching attacks from the honeypot. Proper implementation is also important since a poorly implemented honeypot that can be easily compromised can lead to liability issues. As mentioned previously, training is also a key an essential part of the implementation. All employees should be trained not only on the legal aspects, but also on the implementation and workings of the honeypot. All activity on the honeypot should be closely monitored and diligently documented. Monitoring protects against the use of honeypots to attack others. Since there is a legal obligation to report criminal activity to law enforcement, proper monitoring and documentation of botnet activity through the honeypot will organize the material when presented to law enforcement. Schaufenbuel (2008) is in agreement with the above recommendation and also suggests that if illegal content has been uploaded to the honeypot by a botnet, it should be purged as soon as approval has been given by law enforcement. This will prevent the illegal content from being used or accessed either by another bot or accidently by a member of the honeypot team.

Privacy

Because no individual statute applies to privacy as it pertains to honeypots, legal counsel should be consulted to determine if the honeypot might fall into exceptions provided by current privacy laws. The operator of the honeypot should fully document all operations. The operations should then be reviewed by legal counsel to make sure the honeypot falls within current statute exceptions. This research has focused on federal statutes, but honeypot operators should also be aware of laws that govern privacy in the state where they operate honeypots.

A honeypot may fall under several exceptions. It would be in the best interest of the honeypot owner to take measures to be protected under each exception. This would include using a consent banner on the honeypot even though attacks rarely happen through traditional entries into the system. In the rare cases where an attack does happen in this manner, the banner serves as a warning of consent. By documenting all aspects of the honeypot deployment, the consent of the honeypot owner is expressly described. This documentation will also verify that the scope of the honeypot deployment is to monitor activity for the protection of the larger network of which the honeypot is a part.

Recommendations for Future Research

As the occurrences of botnet attacks continues to grow, so will the number of court cases pertaining to those attacks. Future research could be conducted on the verdicts of cases involving the deployment of honeypots. The growing number of cases will lead to the adaption of current statues and the creation of new ones. Research of the new statutes could also be conducted.

Currently, there are cyber security organizations voicing the need for changes to current statutes and the creation of new ones. Research could be done on these organizations and their missions. In addition, members of the U.S. Senate have drafted bills that address the limitations of current statutes. If passed, these bills could make the legal considerations of the deployment of honeypots more defined. Research could be done on the bills as they pertain to botnets and the deployment of honeypots. Since statutes will continue to be created and adapted to the changing landscape of cybercrime. The need for research of these statues will continually evolve.

Conclusions

Among the growing number of threats to government and corporate computer systems, threats from botnets are on the rise. *The Top 10 Botnet Threat Report – 2010,* a report by Damballa, a U.S. based company committed to fighting cybercrime, describes a 650% increase in botnet attacks in 2010. A botnet is a group of interconnected computers that have been compromised through system vulnerability. Malicious software is installed on the group of computers so that they can be run automatically and anonymously (Maughan, 2008).

To combat the growing cyber-threat of botnets, honeypots are being deployed by companies, law enforcement, and government agencies. A honeypot is a type of computer trap that is designed to attract attacks and then monitor botnet activity (Zou & Cunningham, n.d.). The use of honeypots has proven very successful in tracing, tracking, and removing botnets, but there are also issues to be addressed when using them. The purpose of this study was to examine the legal issues relative to the deployment of honeypots.

- Does the use of a honeypot constitute entrapment?
- Is the use of a honeypot a liability to those who deploy them?
- Does the use of a honeypot violate privacy rights?

This research was conducted through the analysis of current legal precedents as they apply to honeypots. Additionally, past research was examined to find correlations between the deployment of honeypots and honeynets and the legal considerations of deployment.

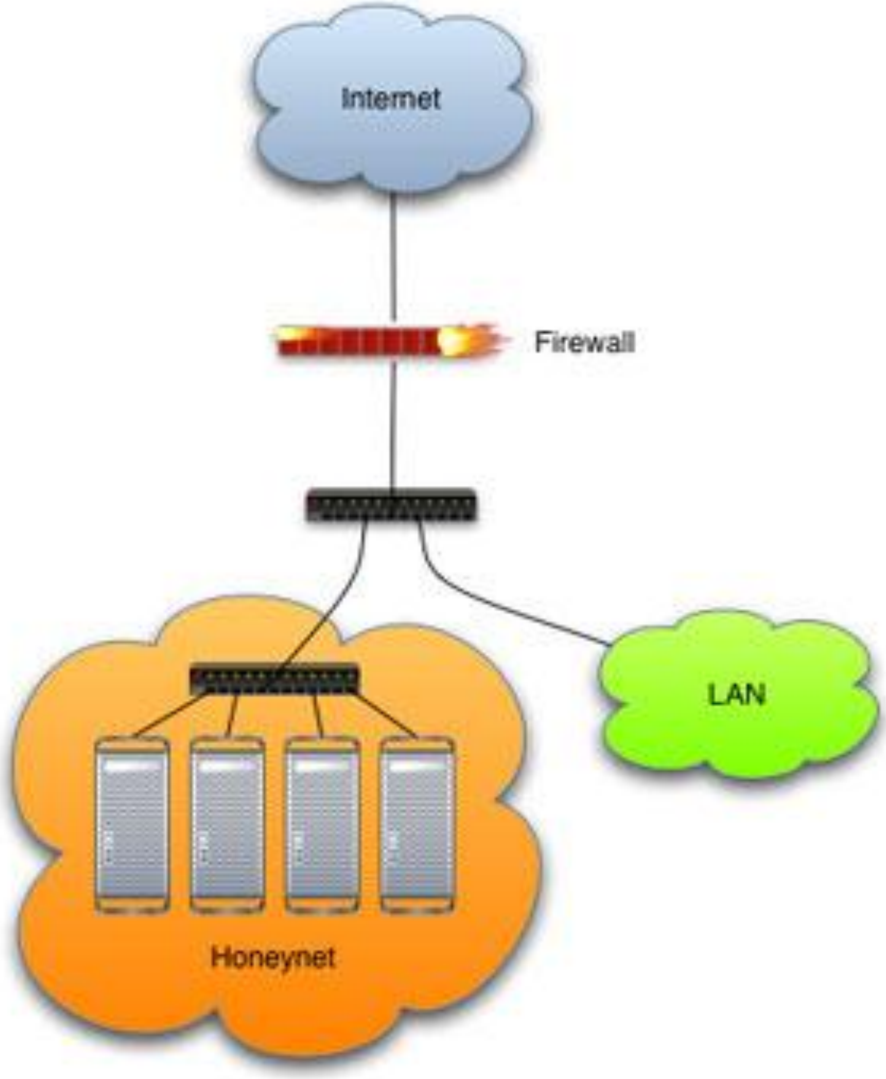
It was discovered through this research that although there are several statutes pertaining to the concepts of entrapment, liability, and privacy, there is nothing that specifically applies to the deployment of honeypots. With botnet attacks being a relatively new occurrence as it relates to cyber-threats, very little case law exists. As stated previously in the Literature Review, certain measures can be taken to limit the legal ramifications, but until specific statues are created, what is legal and what is illegal in relation to the deployment of honeypots is not clearly defined.

There are three common elements found through the research that are essential to avoiding legal complications when deploying a honeypot, legal counsel, documentation, and training. Legal counsel can focus on current and new statutes relating to entrapment, liability, and privacy. The same counsel can also keep abreast of new legislation created and passed. The documentation and training need to be ongoing and occur concomitantly. Taking that advice of legal counsel and adding the parameters and scope of the honeypot, the process and technical information of the honeypot can be well documented. That documentation can then be utilized to train the employees.

As stated in the discussion of findings, there are measures that can be taken to reduce the exposure to entrapment, liability, and privacy. These include using data capture techniques and the use of virtual honeypots. In the cyber security realm, honeypots have become an essential tool for the capture of botnet information and prosecution of bot herders. Without the honeypot, the elements of the working botnet could not be forensically analyzed and dissected. The continued research of current and new statutes relating to entrapment, liability, and privacy concerns related to honeypots will continue to make a honeypot a viable tool for cyber security. With any new technology, current legislation will be needed. It is up to those groups and individuals associated with cyber security and the use of honeypots to be vigilant and keep this subject at the forefront of attention to government law makers so that appropriate legislation can be passed, and that the honeypot can be used as a weapon in cyber warfare.

Appendix A

Basic Honeynet Setup



Source: *Know your enemy: honeynets.* (Spitzner, 2002b)

Appendix B

Honeypot Deployment Strategies

Strategy	Description
“Sacrificial Lamb”	An isolated system that has no entry point to any production systems
“Deception Ports on Production Systems”	Simulated honeypot services submitted for well-known services (www, smpt/pop, dns, ftp)
“Proximity Decoys”	By using port redirection on an upstream router or firewall, you can make it appear that honeypot services are on a production system
“Minefield”	Honeypots (in quantity) placed in forefront to serve as first attack targets to any scans
“Hacker Zoo”	An entire subnet of honeypots with varied platforms, services, vulnerabilities, and configurations’ called a zoo because attackers are in “cages” resembling their natural habitat

Source: *Internet honeypots: protection or entrapment?* (Scottberg, Yurcik & Doss, 2002).

Appendix C

Representative Honeypot Systems

Product	Vendor	Description
BackOfficer Friendly (Windows)	NFR Security	Simulates a BackOrifice Server, listens for BackOrifice (Windows Trojan Program) and responds appropriately while logging various services
CyberCop Sting (Windows)	Network Assoc./PGP	Simulates an entire network segment of routers/hosts on a single system Can mimic multiple OSs, responds appropriately to attacker requests for specific services & log activity
Deception Toolkit (DTK) (Unix)	Fred Cohen & Assoc.	Listens to service requests on ports normally blocked & provides responses to attacker requests while logging activity
NetFacade (Unix-Solaris)	GTE Federal Network Systems	Simulates CiscoIOS, Unix, & Windows (with different versions of the same service) services to mimic the real services Can simulate an entire Class C network of hosts running network services
Mantrap (Unix-Solaris)	Recourse Technologies	Runs a real complete Unix-Solaris OS in a “jail” configuration with no emulation Provides deception hosts with unique/reversible data
Spectre (Windows)	Network Security Software	Dedicated PC simulates multiple OSs and multiple services and variable levels of security
VMware (multiple OSs)	VMware, Inc.	Honeypot OS executing virtually within a HostOS

Source: *Internet honeypots: protection or entrapment?* (Scottberg, Yurcik & Doss, 2002).

Appendix D

Differences Between Entrapment and Enticement

Entrapment	Enticement
It is a protection mechanism by a law-enforcement agent, practicing which the victim does a fraud, but he/she would not have performed it if he were not predisposed by the official.	It is a process by which an intruder is lured to a pseudo or true sensitive area.
It is considered a major legal issue while discussing honeypots.	It has not been able to claim its stand as a major legal issue.
It is a defense that can be sought out by defendants while being acquitted of honeypot related fraud.	It is a tool for the prosecutors to justify their monitoring of communication by the defendant.
Numerous and prominent non-computer legal cases	Various cases but haven’t been prominent enough to grant discussions
Cases defined the basic definition of entrapment and context it has to be used in	Still not a legal definition or the context it has to be understood in

Source: *Deception techniques using honeypots* (Lakhani, n.d.).

Bibliography

Cornell University Law School. (n.d.). *18 usc § 2511 - interception and disclosure of wire, oral, or electronic communications prohibited*. Retrieved from http://www.law.cornell.edu/uscode/text/18/2511

Damballa. (2011). *Damballa top 10 botnet threat report for 2010 shows rampant Increases in internet crime*. Retrieved from http://www.damballa.com/downloads/r_pubs/Damballa_2010_Top_10_Botnets_Report.pdf

Debus, K. (2009, October). Beware of internet hazards enterprises face numerous potential liabilities online. avoiding lawsuits requires a sound cyber risk management plan. *Information Security*, *11*(9), 6-8. Retrieved from http://cdn.ttgtmedia.com/searchSecurity/downloads/F_1009_ISM_eM.pdf

Even, L. (2000, July 12). *Intrusion detection faq: What is a honeypot?*. Retrieved from http://www.sans.org/security-resources/idfaq/honeypot3.php

Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). In Ian Goldberg (Chair). *Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection*. , Washington, DC. Retrieved from http://www.usenix.org/events/sec08/tech/full_papers/gu/gu_html/

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars* (pp. 133-134). London, England: Taylor & Francis Ltd.

Kabay, M. E. (2003, May 22). *Honeypots, part 4: Liability and ethics of honeypots*. Retrieved from http://www.networkworld.com/newsletters/2003/0519sec2.html

Krasser, S., Grizzard, J., Owen, H., & Levine, J. (2005). The use of honeynets to increase computer network security and user awareness. *Journal of Security Education*, *1*(2/3), 23-37. Retrieved from https://docs.google.com/viewer?a=v&q=cache:zKOXim5jN14J:citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.4398&rep=rep1&type=pdf "the use of honeynets"&hl=en&gl=us&pid=bl&srcid=ADGEESiu-qsMMHwNNYA1ZaOBzoL3Jfs9tOmVcbScSmzOY5UmKo6XHfdhSsq2rZ8tU4D5ipkovTH2pmV0Z71lIVGBBfWNT98FoWpGDBEx5EnqDFQD4M3kuV-bF0737-X7uTRJ1EOGz6KE&sig=AHIEtbSiOaD0aZnKVb-tBh-77KnR1duHCQ

LaBella, R. (2003, February 16). *GenII data control for honeynets: Understanding and building snort-inline data control*. Retrieved from http://www.infosecwriters.com/texts.php?op=display&id=64

Lakhani, A. (n.d.). *Deception techniques using honeypots*. (Doctoral dissertation, University of London, London, United Kingdom) Retrieved from http://www.isg.rhul.ac.uk/~pnai166/thesis.pdf

Lord, K. (1998). Entrapment and due process: Moving toward a dual system of defenses. *Florida State University Law Review,* Retrieved from http://www.law.fsu.edu/journals/lawreview/frames/253/lordfram.html

Maughan, J. (2008). *Condenser: A custom tool for capturing and summarizing network traffic for avalanche and iseage*. (Doctoral dissertation, Iowa State University), Available from ProQuest. (1525705051).

Mikhalenko, P. (2006, November/December). Managing a honeypot. *The Developers Group Magazine*, 6-10. Retrieved from http://www.ukbug.co.uk/magazine/dg200605.pdf

Nash, T. (2005). An undirected attack against critical infrastructure a case study for improving your control system security. *US-CERT Control System Security Center Case Study Series*, *1.2*, Retrieved from http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf

Pinchuk, M. (2004). Honey pots - strategic considerations. *The ISSA Journal*, Retrieved from https://www.issa.org/Library/Journals/2004/February/Pinchuk - Honey Pots - Strategic Considerations.pdf

Poulsen, K. (2003, April 16). *Use a honeypot, go to prison?*. Retrieved from http://www.crime-research.org/news/2003/04/Mess1701.html

Radcliffe, J. (2007). *Cyberlaw 101: A primer on us laws related to honeypot deployments*. Retrieved from http://www.sans.org/reading_room/whitepapers/honors/cyberlaw-101-primer-laws-related-honeypot-deployments_1746

Salgado, R. (2004). Legal Issues. In The Honeynet Project (Ed.), *Know your enemy: Learning about security threats* (pp. 225-252). Retrieved from http://old.honeynet.org/book/Chp8.pdf

Schaufenbuel, B. (2008). The legality of honeypots. *The ISSA Journal*, (April), 16-20. Retrieved from http://www.jdsupra.com/post/documentViewer.aspx?fid=cba3901d-d1b2-4da4-9ff2-ba88e3ddfe2f

Scottberg, B., Yurcik, W., & Doss, D. (2002, June). *Internet honeypots: protection or entrapment?*. Raleigh, NC. Retrieved from http://flur.net/archive/research/ISTAS02honeypots.PDF

Spitzner, L. (2002a). *Honeypots: Tracking hackers*. United States: Addison-Wesley.

Spitzner, L. (2002b). *Know your enemy: Honeynets*. United States: Addison-Wesley. Retrieved from http://www.infosecwriters.com/texts.php?op=display&id=31

Spitzner, L. (2010, November 02). *Honeypots: Are they illegal?*. Retrieved from http://www.symantec.com/connect/articles/honeypots-are-they-illegal

Sumner, K. (2002). *Honeypots security on offense*. Unpublished manuscript, Security Architecture, Retrieved from http://sumnerk.tripod.com/mywebsite/courses/secarch/honeypotpaper.pdf

Tech Ministries. (2011, March 21). *Malware - what is it and how to prevent it?*. Retrieved from http://techministries.org/downloads/Malware.pdf

The Honeynet Project. (n.d.). *About the honeynet project*. Retrieved from http://www.honeynet.org/about

The SANS Institute. (2012). *About the sans institute*. Retrieved from http://www.sans.org/about/sans.php

USLegal. (2012). *Sherman–sorrells doctrine law & legal definition*. Retrieved from http://definitions.uslegal.com/s/sherman-sorrells-doctrine/

Walden, I., & Flanagan, A. (2003). Honeypots: a sticky legal landscape?. *Rutgers Computer and Technology Law Journal*, Retrieved from http://www.thefreelibrary.com/Honeypots: a sticky legal landscape?-a0106474528

Zhang, F., Zhou, S., Qin, Z., & Liu, J. (2003). *Honeypot: a supplemented active defense system for network security*. Informally published manuscript, College of Computer Science and Engineering, University of Electronic Science and Technology of China, Sichuan, Chengdu, China. Retrieved from http://folk.uio.no/ingardm/sysarp/honeypot-a_supplemented_active_defense_for_network_security.pdf

Zou, C., & Cunningham, R. (n.d.). *Honeypot-aware advanced botnet construction and maintenance*. Unpublished manuscript, School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL. Retrieved from http://www.cs.ucf.edu/~czou/research/honeypot-DSN06.pdf