Honeypots

by Bob Pelletier
Computer Science Major
Norwich University, Northfield VT

Published in Network World Fusion in 2003
Honeypots, Part 2 (05/15/03) http://www.nwfusion.com/newsletters/sec/2003/0512sec2.html
Honeypots, Part 3 (05/20/03) http://www.nwfusion.com/newsletters/sec/2003/0519sec1.html
Honeypots, Part 4 (05/22/03) http://www.nwfusion.com/newsletters/sec/2003/0519sec2.html

Note from Prof. M. E. Kabay, PhD, CISSP,
Norwich University:

In recent weeks, we’ve been looking at managing vulnerability assessment systems and intrusion detection systems. Norwich University undergraduate student Bob Pelletier is doing some interesting research work on honeypots in the IS406C independent study program with me this term in which he is building a working honeypot system using virtual machines. He did some good background reading about honeypots in the IS340 Intro to Information Assurance and CJ341 Cyberlaw and Cybercrime courses; he has very kindly allowed me to publish his work here as part of the ongoing series. As usual, I’ve made some minor edits for the new context, but all of the following is Bob’s own writing.

* * *

Introduction

With the growing use of computers in today’s society, the protection of information has become of key importance. Malicious hackers (blackhats) continuously try to breach security measures to gain access to protected information. Some blackhats attack computers for fun but others are truly criminals seeking personal gain. The security community is faced with the daunting task of fending off computer attackers and ensuring the confidentiality, integrity, availability, control, authenticity and utility of information. To help better understand the methods used by the blackhat community, a new tool has been developed: the honeypot. The use of honeypots has caused a heated debate within the security field. Many question the legality and ethics of such a system. This series of articles outlines the basic legal issues surrounding honeypots as well as some ethical issues to ponder.

A honeypot is any system designed for the sole purpose of being exploited. This is a broad definition that can be implemented in many ways. Some honeypot systems use software, some use actual production machines, and some even use virtual machines such as with VMware. Whichever honeypot design method is chosen, the underlying goal is to create a system that appears to be vulnerable.

What makes a honeypot different from other vulnerable computer systems is its extensive logging capability. The systems most often include at least four layers of logging to capture attacker activity. Every file accessed, every connection made, every keystroke an attacker makes on a honeypot is logged to a secure location. The advantage of logging attacker activity is the chance to get an inside view of the blackhat community’s methodology. Learning common methods and attack tools of attackers can aid security experts in designing new protection measures. Studying attack trends can also help predict future attacks. The Honeynet Project founded by Lance Spitzner demonstrates the usefulness of honeypots as a research tool.

Honeypots are not only used for research purposes, but also for production. Implementing a honeypot within a company can create a type of intrusion
The design of a honeypot suggests that any connection attempts made with the system are unauthorized. This is because normal business functions do not use the honeypot; only an attacker would be attempting to use the system. Therefore, activity on a honeypot can alert an organization that an attacker is present. From there a company can close the security hole used by the attacker, investigate the incident, and possibly press charges.

**Legal Issues: Entrapment?**

There are many benefits of using honeypots and they are therefore becoming commonplace in many security strategies. However, there are legal issues associated with honeypot technologies. I am not a lawyer and what follows is not legal advice and should not be the sole basis for readers’ decisions in this matter. It is best to consult a lawyer qualified in this area of practice before implementing a honeypot. Many factors dictate whether the use of a honeypot is legal or illegal. These articles do not cover all of these factors, but they do explain precautions that can be taken before implementing a honeypot so that you can comply with applicable federal laws of the United States.

The next step that should be taken before implementing a honeypot is to research the laws and regulations in the particular location the system will be installed. Different countries and even different states will treat honeypots in a different manner. These subtle differences must be studied and understood. Many laws may govern honeypot use, but these articles will cover three general legal issues associated with honeypots. These three categories are entrapment, privacy and liability.

Opponents of honeypot systems often claim that they are a form of entrapment. Entrapment is legally defined as “the conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officers.”[2] This definition implies that a victim of entrapment must be tricked or persuaded to do something that he or she would not have normally done. Honeypots do not persuade attackers to take action against them. The systems are most often discovered through scans by blackhats. In this case, the attacker is taking initiative to find a vulnerable system so therefore cannot claim entrapment after the fact. Some will argue that an attacker would not have exploited a honeypot if it were not there to begin with. However, providing a target for a crime is not the same as encouraging one.

Another hole in the entrapment argument is that it applies only to officers of the law. Private honeypot owners will not be prosecuted with entrapment because they are acting independently of the government. Government agencies and those affiliated with the law can be convicted of entrapment, but only if they encourage attacks as mentioned earlier. Proving an attacker’s disposition to hacking can eliminate most entrapment accusations.

1 Searching and Seizing Computers and Obtaining Electronic Evidence in criminal Investigations created by the Department of Justice for sample banners.[1]

1 Searching and Seizing Computers and Obtaining Electronic Evidence in criminal Investigations.


2 Supreme Court of the United States

Honeypots are under fire for potentially invading two types of user privacy:

- Information privacy protects stored information about an individual [3]. Honeypots are designed with in-depth logging systems that have the ability to capture large amounts of information on its users.
- Communication privacy protects communications by telephone, e-mail and so on. Honeypots are usually set to intercept communication going to and from the system through the use of sniffers and firewalls. Any infringements of these two privacy categories can get the owner of a honeypot in legal troubles.

The governing laws of the honeypot’s location should be reviewed to determine any infringements of the legal definition of privacy. This paper focuses primarily on the governing laws of the United States and other resources should be sought if a honeypot is not within US borders.

One concern that is based on misunderstanding is Fourth Amendment rights. The Fourth Amendment of the US Constitution asserts that “the right of the people to be secure in their persons, houses, papers and effects, against unreasonable search and seizures, shall not be violated.” [4] However, this amendment protects the privacy of individuals from government intrusions. As with entrapment, the private owner of a honeypot is not affected by the Fourth Amendment. As long as they are not acting as government agents, private honeypot owners have the right to search their own systems.

Government agencies and those affiliated with or under the direction of government agencies should include a login-banner that states that privacy protections must be waived when using the system. Take note that a banner is not always affective. For instance, what if an attacker bypasses the login screen containing the consent banner or what if the attacker does not speak the same language the banner is written in?[5] In any case, it is still a good safety measure to include login-banners on all honeypot systems.

Other federal US statutes that are discussed in connection with privacy rights and honeypots include the

- Federal Wiretap Statute (18 U.S.C §§ 2510-22)
- Pen Register Trap and Trace Statute (18 U.S.C. §§ 3121-3127) [6].

None of these poses any serious bar to private use of honeypots when used for serious information security purposes. Nonetheless, one should always rely on a qualified attorney to refer to applicable privacy statutes in one’s own jurisdiction when implementing a honeypot to ensure that it will be operating within legal limits.

### Liability

Another legal issue involving the use of honeypots is called downstream liability. Who is liable for attacks launched from a honeypot, the attacker or the owner of the system? No court rulings have been published yet that directly address this issue. Another difficulty about downstream liability is that it is decided at the state level, not the federal. This can make things difficult because downstream

6 Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections http://www.cdt.org/security/000404amending.shtml


4 What is the Fourth Amendment?

http://www.unc.edu/courses/law357c/cyberprojects/spring01/Carnivore/4th_Amendment.htm
attacks can occur almost anywhere. Deciding if a honeypot owner will be liable for the attack is hard to predict. For the time being, it is best to properly secure a honeypot’s outgoing traffic to prevent downstream attacks. This can be accomplished through such mechanisms as a firewall that properly filters outgoing traffic. Spitzner’s book [5] is an excellent resource to research proper data control mechanisms and practices.

It is not uncommon for an attacker to compromise a computer system and run a FTP warez server on the machine. Who is liable for the contraband on the computer system? Once again, it is best to properly secure a honeypot’s outgoing traffic to safeguard against copyright violation issues.

Ethics

Laws provide guidance but may not suffice in determining whether we ought to do certain things.[7] For example, is it ethically correct to pose a computer system as something it is not? A honeypot poses as just another vulnerable computer system, when in actuality it is a research and monitoring tool. Is this fair to the attacker or do they deserve it? As for entrapment, although this is not a legal problem, this does not mean that the way a honeypot entices attackers is not unethical. Creating a vulnerable computer system on purpose is similar to baiting an animal. The question becomes, do honeypots provoke illegal actions such as hacking? If so, are they not unethical by most standards? It is understood that recording somebody’s conversations without his or her permission is usually unethical. Even if it’s legal, is recording keystrokes from an IRC session taking place on a honeypot ethical? Is it ethical to create a vulnerable system that could potentially be used to harm other computer systems?

* * *

At this point, Kabay intervenes to state that in his opinion, we use deception all the time in information security [8]. For example, we do not label server rooms with signs that say “IMPORTANT VULNERABLE SERVER ROOM.” Instead, we just label them, say, “E-301b.” We remove operating-system identification banners from logon screens and even remove prompts from remote login dialogs to reduce the information flow to potential attackers. So I see absolutely nothing wrong at all with having a system that is clearly marked, “AUTHORIZED USERS ONLY” that is used a honeypot. If thieves break into my home despite the PRIVATE PROPERTY –NO TRESPASSING signs and I have cameras to track their movements so I can help put them in jail, I have no sympathy for whines of dismay about my having invaded their privacy. They want privacy, they can stay out of my computer systems.

I hope everyone understands that the rant in the paragraph above is purely Mich Kabay’s and that no blame for this red-neck arrogance can be assigned to Bob Pelletier.

For further reading:

Honeypots.net: Intrusion detection, honeypots & incident response (resources).
http://www.honeypots.net/


http://www.spitzner.net/honeypot.html

7 What is Ethics?
http://www.scu.edu/ethics/practicing/decision/whatisethics.html

http://all.net/journal/deception/Framework/Framework.html