

Honeypots: Are They Illegal?

Lance Spitzner 2003-06-12

Honeypots are a new and emerging technology for the security community. Many security professionals are just now beginning to understand what honeypots are, their different types, how they work, and their value. As with many new technologies, not only are the professionals attempting to learn about them but so is the legal community. As honeypots and their concepts have grown more popular, people have begun to ask what legal issues could apply. The purpose of this paper is to address the most commonly asked issues. The concepts covered here will be focusing on US statutes, not international, mainly because I'm only familiar with US law. However, these concepts most likely also play some role in the international community. Also, this paper assumes you are familiar with the definition of a honeypot. If you are new to honeypots, I recommend you first read the paper [Honeypots: Definitions and Values](#).

Before we begin, I would like to start off by saying that this paper is based on my opinions. I am in no way an authority on legal issues (heck, I'm a history major who blew things up with M1A1 Main Battle Tanks). However, I feel I have a relatively good feel of honeypots and have worked extensively with several members of the legal community on honeypot legal issues. Before I go any further, I would also like to thank both Jennifer Grannick, Director of Stanford Center for Internet and Society, and Richard Salgado of the CCIPS Department of Justice, for their help in writing this paper.

Precedents

In the past there has been some confusion on what are the legal issues with honeypots. There are several reasons for this. First, honeypots are relatively new. If security professionals are still learning about them, how do you think the legal community feels? Second, honeypots come in many different shapes and sizes and accomplish different goals. We will attempt to identify the different uses of honeypots and how they apply to legal issues. Last, there are no precedents for honeypots. There are no legal cases recorded on the issues. The law in the US is developed through cases. Without cases directly on point, we are left trying to predict, based on cases in other contexts, how courts will treat honeypots. Until a judge gives a court order, we will really never know.

With honeypots, there are three main issues that are commonly discussed: entrapment, privacy, and liability. I'll discuss each of these issues in that order. I will not be covering the

[Digital Millennium Copyright Act](#). I have been asked by numerous individuals how DMCA applies to honeypots. To the best of my knowledge, and that of other legal experts, the DMCA does not affect honeypots. DMCA is focused primarily on circumvention of copyright protection mechanisms and does not apply to honeypot deployments. Keep in mind, this paper represents only my opinions. If you are looking for definitive answers, as always seek the advice of a legal professional.

Entrapment

I'm discussing this issue first because its the simplest. Honeypots are not a form of entrapment. For some reason, many people have this misconception that if they deploy honeypots, they can be prosecuted for entrapping the bad guys. Nothing could be further from the truth. Entrapment, by definition is "a law-enforcement officer's or government agent's inducement of a person to commit a crime, by means of fraud or undue persuasion, in an attempt to later bring a criminal prosecution against that person." [Black's Law Dictionary, 7th Ed]

What this means is that entrapment can only be used as a defense to avoid a conviction. You will not be prosecuted for 'entrapment.' Rather, entrapment is a defense to a criminal prosecution. Second, you have to be law enforcement, or an agent of law enforcement, and prosecute the attacker before entrapment becomes an issue. If you are not law enforcement or not an agent of the law, and you do not intend on prosecuting, then entrapment is not an issue. Last, even if you are law enforcement, and even if you do want to prosecute the attacker, honeypots still are most likely not a form of entrapment.

Think about it, entrapment is when you coerce or induce someone to do something they would not normally do. Honeypots do not induce anyone. Attackers find and break into honeypots on their own initiative. People often question the idea of creating targets of high value, for example honeypots that are ecommerce sites or advertised as having government secrets. Even then, such honeypots are most likely not a form of entrapment as you are not coercing them into breaking into the honeypot. The bad guy has already decided to commit unauthorized activity, you are merely providing a different target for the blackhat to attack. Therefore, in most cases involving honeypots, entrapment is not an issue.

Privacy

Okay, we now go from the easiest legal issue (entrapment) to the most complex, privacy. I'm

not about to begin to cover all the issues of privacy in detail, you could write entire books on the concept. Instead, I will highlight some of the issues (and misconceptions) of privacy and how they apply to honeypots. Privacy laws in the US may limit your right to capture data about an attacker, even when the attacker is breaking into your honeypot. This information could be as simple as his login and password, or more in-depth, such as his emails or online chats. As odd as it may sound, you may not have the right to capture his communications, especially his communications with other people, or other people's communication with each other.

The first challenge we run into is there is no single statute that covers privacy. Instead there are many different legal statutes, including the [Federal Wiretap Act](#) and the [Electronic Communication Privacy Act](#). To make the issue of privacy more challenging, which legal statutes do you apply? In the United States, often state law concerning privacy can supplement Federal law, as it is in the state of California. So if your honeypot is in Chicago, but the attacker is coming in from California, which privacy laws apply, Illinois, California, or Federal? To make matters even worse, what happens if the attacker(s) are coming from different countries, or bouncing through different countries. When different countries are involved, which privacy statutes do you apply? As you can see, things become exponentially confusing. Of all the privacy statutes, the one that most likely applies to honeypots deployed in the US is the Federal Wiretap Act. Under the Federal Wiretap Act it is illegal to capture the communications of an individual in real time without their knowledge or permission, as this violates their privacy. To determine if a honeypot does violate an individual's privacy, there are two major factors: what the honeypot is being used for and how much information it is collecting. These two factors influence the privacy legal implications.

First, the use of the honeypot affects the privacy issues. The reason the use of the honeypot is important is because of something called the exemption under Service Provider Protection. What this exemption means is that security technologies can collect information on people (and attackers), as long as that technology is being used to protect or secure your environment. In other words, these technologies are now exempt from privacy restrictions. For example, an IDS sensor that is used for detection and captures network activity is doing so to detect (and thus enable organizations to respond to) unauthorized activity. Such a technology is most likely not considered a violation of privacy as the technology is being used to help protect the organization, so it falls under the exemption of Service Provider Protection. Honeypots that are used to protect an organization would fall under this exemption. At times, honeypots are used for research purposes, to better understand who the threat is and how they operate. Such honeypots do not directly secure an organization, instead the information they collect is

indirectly used to help defend against threats. The less the honeypot is being used to protect your organization, the less likely it falls under exemption of Service Provider Protection. So the question may become, what is your honeypot being used for?

Second is the type of information that is being collected. There are two general categories, transactional and content. Transactional is not the data itself, but information about the data. For IP, that means transactional data would be IP addresses, IP header information, time and date of the communication, etc. Content data is the actual communication itself, such as IRC chats, emails, and keystrokes. Content data has more privacy issues than transactional data. This distinction can be important, as different honeypots capture different types of information. Honeypots are classified by the amount of interaction they provide an attacker. Low-interaction honeypots limit the amount of interaction an attacker can have. These honeypots emulate services and operating systems, containing the attacker's activities within the emulated services. Examples of such honeypots include [Honeyd](#), [Specter](#), and [KFSensor](#). These honeypots capture mainly transactional information. Some content data may be collected, depending on the honeypot and the extent of the emulated service. High-interaction honeypots are different, they are designed to capture extensive amounts of information. The focus is on not only transactional, but also content data. This is done by providing attackers real systems and applications to interact with. One example of such a honeypot is the [HoneyNet](#). The more content information a honeypot can collect, the potentially greater the privacy implications.

Privacy issues are not limited to service provider exemption or the type of information collected, but there can be other issues. One example is consent. When an individual consents to monitoring, they waive their right to privacy. By placing banners on a honeypot stating an attacker consents to logging, the attacker has waived their privacy rights. Such a banner could look as follows:

```
#####  
#           !READ BEFORE CONTINUING!  
#  This system is for the use of authorized users only.  
#  By using this computer you are consenting to having  
#  all of your activity on this system monitored and  
#  disclosed to others.  
#####
```

The challenge then becomes, which ports do you banner? My opinion is to banner the ports/ services that are normally bannered. This would represent in my mind due diligence. Its

impossible to banner all the ports that are possible for an attacker to break into, not to mention all the different languages that an attacker could possibly speak.

The main point I want to get across is that there are a variety of issues that affect the implications of privacy. To date, many people have been painting a broad stroke against all honeypots, regardless of what the honeypot is doing, or the type of honeypot being used. Honeypots can be used for a variety of different purposes and collect different amounts of information. When used for production purposes, honeypots secure or protect an organization and often capture only transactional information. As such, these solutions have limited, if any, privacy issues. When honeypots are used for research purposes, they are often high-interaction solutions that capture both transactional and content data. To date, the vast majority of discussion has been about high-interaction honeypots used for research purposes, solutions that potentially have the greatest privacy issues. However many people have mistakenly applied the same legal issues of these honeypots to all honeypots. When discussing honeypots and their privacy issues, you want to first define what your honeypot is being used for and the type of information it is collecting. Last, keep in mind that even though these issues potentially exist, to date there has been no public case involving the privacy issues of honeypots.

Liability

The third issue is liability. Liability implies you could be sued if your honeypot is used to harm others. For example, if it is used to attack other systems or resources, the owners of those may sue. Liability is not a criminal issue, but civil. The argument being that if you had taken proper precautions to keep your systems secure, the attacker would not have been able to harm my systems, so you share the fault for any damage occurred to me during the attack. The issue of liability is one of risk. If I deploy honeypots and they are compromised, what happens if they are used to attack someone else? First, anytime you deploy a security technology (even one without an IP stack), that technology comes with risk. For example, there have been numerous vulnerabilities discovered in firewalls, IDS systems, and network sniffers. Honeypots are no different. However, just as in privacy, different honeypots have different levels of risk. Low-interaction honeypots have far less risk, as they do not give attackers a real operating system to interact with. Instead, they contain attackers within emulated services, controlling the actions of the attacker. High-interaction honeypots, such as Honeybots, are different, they provide actual operating systems for attackers to interact with. As a result, most high-interaction honeypots have greater risk. If liability is a concern for you, you most likely want to focus on honeypots with less risk.

One thing to keep in mind. For years legal experts have been discussing possible liability for an organization that has been compromised and in turn was used to attack, compromise, or harm another system or organization. To date, we have seen no published decision addressing whether the operator of an insecure system can be liable to other operators for the misuse of the system by a hacker. So while liability is an issue, it may be an overblown one, as there is no recorded case of it happening with compromised systems.

Conclusion

The views here are my expressed opinions, they in no way represent legal advice. For that, I recommend you go to your legal counsel. My intent here was to raise issues that I have not seen publicly discussed with honeypots and their legal implications. As time progresses, these legal issues will become better understood. If you would like to learn more about the legal issues, chapter 15 of the book [Honeypots: Tracking Hackers](#) is dedicated to this topic. In our next article we look at a new application of honeypots, called honeytokens. While the concept may not be new, the name definitely is. To learn more about honeypots, check out <http://www.tracking-hackers.com>.

[Privacy Statement](#)

Copyright 2006, SecurityFocus