The Legality of Honeypots

By Bradley J. Schaufenbuel – ISSA member, Chicago, Illinois, USA chapter

Deploy a Honeypot – Go to Jail? This article briefly explores the legal issues surrounding the use of honeypots under current United States laws and offers some suggestions for mitigating the legal risks involved.

Since Clifford Stoll first described his attempts to lure a hacker into an environment where he could track his activities in his popular book, *The Cuckoo's Egg* in 1990, researchers and academicians have used honeypots as a tool for understanding the behavior and motivations of hackers.[1] One topic that security professionals, security researchers, and attorneys alike have debated since the inception of honeypots is the uncertainty surrounding the legality of their use. Security newsgroups and blogs contain postings ranging from those titled such as "Deploy a Honeypot – Go to Jail?" to those that dismiss any legal risk whatsoever. This has created uncertainty that has arguably contributed to the slow adoption of this tool within the mainstream security field. This article briefly explores the legal issues surrounding the use of honeypots under current United States laws and offers some suggestions for mitigating the legal risks involved.

Background

A honeypot is a security resource whose value lies in being probed, attacked, or compromised.[2] To be an attractive target for hackers, the honeypot is usually a system that emulates a production host with known vulnerabilities. Its owner places the honeypot on an Internet-facing network segment for accessibility. Unbeknownst to a hacker, the system contains functionality designed to allow a security professional to track the hacker's use of the system.

There are two main reasons to use a honeypot. Most importantly, the honeypot serves as a learning tool. For a security professional to defend his organization against hackers, he must know his enemy. The honeypot allows him to profile the hackers who are attempting to infiltrate his network. Secondly, the honeypot serves as a "decoy," drawing malicious attackers away from legitimate production targets.

Although the benefits of using a honeypot are compelling, so are the risks. The most obvious danger is the additional security risk that it creates. If an organization does not deploy this tool properly, there is a chance that a hacker will compromise the honeypot and utilize its resources to compromise the organization's production systems. While an organization can manage this risk by using experts and deploying a carefully designed solution, the legal risks of deploying a honeypot are less quantifiable and manageable.

Legal issues

There are two broad categories of legal issues related to the use of a honeypot: (1) those involving the liability of the honeypot operator to the hacker: entrapment and invasion of privacy; and (2) those involving the liability of the honeypot operator to a third party or the state: negligence/downstream liability, possession of contraband material, and failure to report a crime. I will discuss each of these issues in turn.

Entrapment

Entrapment is a legal defense that a criminal defendant may advance to avoid conviction. It is only applicable in situations where law enforcement officials have induced a defendant to commit a crime that he or she would not have otherwise committed. It does *not* apply to similar enticement by private citizens.

This defense will fail if the defendant was predisposed to commit the crime or if law enforcement officials did not induce the defendant into committing the crime.[3] Both of these situations are typical of hackers who use honeypots. Although law enforcement officials can provide a defendant with the opportunity and the facilities to commit a crime, the court will dismiss a defendant's entrapment claim if he or she is predisposed to act.[4] Entrapment is really a test to determine whether the defendant had the required state of mind to be criminally liable for his or her actions.[5] Because a hacker finds a honeypot by actively searching the Internet for vulnerable

1 Cliff Stoll, *The Cuckoo's Egg*, New York, New York: Pocket Books (1990).

2 Lance Spitzner, *Honeypots: Tracking Hackers*, Addison-Wesley Professional, Pap/Cdr edition (September 20, 2002), p. 40.

3 *Sherman v. U.S.*, 356 U.S. 369, 373 (1958).

4 *U.S. v. Hampton*, 425 U.S. 484, 488 (1976).

5 *U.S. v. Poehlman*, 217 F.3d 692 (9th Cir. 2000) (held defendant was entrapped).

hosts and then attacks it without active encouragement by law enforcement officials, the defense of entrapment is not likely to be helpful to a hacker.

Privacy

Several federal and state statutes create a right to privacy for a hacker that he or she might use to bring a claim against a honeypot operator. I will discuss the most significant federal acts and Constitutional clauses.

Wiretap Act

Courts may consider sniffing traffic on a network to be an interception of electronic communications that falls within the scope of the Wiretap Act.[6] Violation of the Wiretap Act can lead to a civil suit and may constitute a federal felony punishable by a fine and up to five years in prison.[7] The Wiretap Act only applies when one captures the contents of a communication. If a honeypot operator does not configure the honeypot to capture the contents of the communications of its users, then the Wiretap Act does not apply. However, the value of the honeypot is severely limited without this information.

The Wiretap Act contains multiple exceptions to the prohibition against the interception of the contents of communications. Exceptions that honeypot operators may be able to leverage include the "provider protection" and "consent of a party" exceptions. If law enforcement officials monitor communications, the "computer trespasser" exception may also be applicable.

The "provider protection" exception allows an electronic communication service provider to monitor communications to protect its rights or property.[8] Even if the provider intercepts the communications of a user to assist law enforcement officials with a criminal investigation, the exception is valid if its purpose is to protect the provider's rights or property.[9] The provider can monitor the hacker's communications under the Wiretap Act only if there is a "substantial nexus" between the monitoring it is doing and the threat to the service provider's rights or property.[10] Without this link, the court will not apply the exception. For instance, where a cellular phone company allowed law enforcement officials to monitor the calls of a kidnapper to assist in his capture, the court held that the "provider protection" exception did not apply because the kidnapper was of no threat to the cellular phone company's rights or property.[11] The courts have not addressed whether the "provider protection" exception applies to interceptions of communications to or from a honeypot.

The second pertinent exception to the Wiretap Act is the "consent of a party" exception.[12] If a party to a communication has consented to monitoring and it is performed for a lawful purpose, the Wiretap Act allows the interception. If one party is actually doing the monitoring, then it has consented to it. A honeypot operator may be able to get consent from attackers by placing a "consent banner" on the honeypot. Such a banner should contain language warning the user (1) that he or she has no expectation of privacy, (2) that all activity on the system is subject to monitoring, (3) that the system's administrator may consent to law enforcement searches, and (4) that by using the system, he or she implicitly agrees to this monitoring.[13] A court may hold that the hacker implicitly consented to monitoring even if there is no evidence that he or she read the banner. However, it is preferable if the hacker must take affirmative action upon the appearance of the banner (i.e., "click through"it). Alternatively, when a hacker communicates with the honeypot, some courts may consider the honeypot itself to be a party to the communication that can consent to monitoring.[14]

The third and final relevant exception to the Wiretap Act is the "Computer Trespasser" exception.[15] Congress added this exception as part of the USA PATRIOT Act. It allows law enforcement officials to monitor the activities of hackers on the honeypot when (1) the owner or operator of the honeypot authorizes the interception, (2) the law enforcement agent is engaged in a lawful investigation, (3) the law enforcement agent has reasonable grounds to believe that the contents of the hacker's communications will be relevant to that investigation, and (4) such interception does not acquire communications other than those transmitted to or from the hacker (i.e., that of innocent parties). This exception is most relevant when you have detected illicit activity on your honeypot and wish to turn the situation over to law enforcement to gather evidence for criminal prosecution.

Pen Register, Trap, and Trace Devices Statute

The Pen Register, Trap, and Trace Devices statute applies to the real-time collection of non-content information (or "meta data") associated with communications. Examples include the source IP address of a computer network user or the telephone number of a telephone user. The statute refers to this data as "dialing, routing, addressing, or signaling information."[16]

The statute prohibits the capture of this information unless one of a handful of exceptions applies. The exceptions closely parallel the exceptions in the Wiretap Act. If a honeypot op-

6 *In re Pharmatrak, Inc. Privacy Litig'n*, No. CIV.A.00-11672-JLT, 2002 WL 1880387 (D. Mass., Aug. 13, 2002) *In re DoubleClick Inc. Privacy Litig'n*, 154 F.Supp.2d 497 (S.D.N.Y. 2001)

7 18 U.S.C. § 2511(4) & (5).

8 18 U.S.C. § 2511(2)(a)(i).

9 See *U.S. v. Harvey*, 540 F.2d 1345, 1352 (8th Cir. 1976).

10 See *U.S. v. Auler*, 539 F.2d 642, 646 (7th Cir. 1976) (telephone company); *United States v. Harvey*, 540 F.2d 1345, 1350 (8th Cir. 1976); *United States v. Freeman*, 524 F.2d 337, 340 (7th Cir. 1975); *United States v. McLaren*, 957 F. Supp. 215, 219 (M.D. Fla. 1997).

11 *McClelland v. McGrath*, 31 F. Supp. 2d 616 (N.D. Ill. 1998).

12 18 U.S.C. § 2511(2)(c)–(d).

13 "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," United States Department of Justice – Criminal Division – Computer Crime and Intellectual Property Section, July 2002.

14 *U.S. v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993); *U.S. v. Seidlitz*, 589 F.2d 152, 158 (4th Cir. 1978); *In re DoubleClick Inc. Privacy Litig'n*, 154 F.Supp.2d 497 (S.D.N.Y. 2001).

15 18 U.S.C. § 2511(2)(i).

16 18 U.S.C. §§ 3121–3127.

erator fits within one of the exceptions to the Wiretap Act for intercepting the contents of communications, this statute authorizes the operator to intercept the non-content information related to hacker communications.[17] However, the courts have yet to apply this statute to a case involving a honeypot operator.

Like a Wiretap Act violation, violation of the Pen Register, Trap and Trace Devices statute is a crime. Violations are punishable by a fine and up to a year in prison.[18]

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act creates privacy rights for customers and subscribers of certain computer network service providers.[19] Any company or government entity that provides others with the means of communicating electronically can be considered a "provider of electronic communication service" relating to the communications it provides, even if providing a communications service is merely incidental to the provider's primary function. For example, one court held that a city that provided pager service to its police officers was a provider of an electronic communications service.[20] Another court held that an airline that grants airline agents with network-based access to a computerized travel reservation system is a provider of an electronic communication service.[21] The courts have yet to address whether a honeypot operator is an electronic communications services provider and whether a hacker is a customer or a subscriber. If the courts hold that honeypot operators are electronic communications service providers and that hackers are subscribers, then hackers may be able to sue honeypot operators who monitor their communications for invasion of privacy.

Fourth Amendment

The Supreme Court has ruled that the Fourth Amendment, which forbids the government from conducting unreasonable searches and seizures, prohibits the government from intercepting communications where a citizen has a "reasonable expectation of privacy."[22] Those who hack into networks, on the other hand, have no "reasonable" expectation of privacy in the use of the victim's network.[23] In addition, the Fourth Amendment restricts searches only by law enforcement officials or other government employees. A private individual may implement a honeypot and monitor its users without violating about the Fourth Amendment, unless that individual is acting as an "instrument or agent" of the government.[24]

Liability to third parties and the state

Negligence and downstream liability

If a hacker compromises a system in which the owner has not taken reasonable care to secure and uses it to launch an attack against a third party, the owner of that system may be liable to the third party for negligence.[25] Experts refer to this scenario as "downstream liability." Although a case has yet to arise in the courts, honeypot operators may be especially vulnerable to downstream liability claims since it is highly foreseeable that such a system be misused in this manner. While courts have been largely sympathetic to the plight of innocent victims who lacked the technical sophistication to secure their systems, it is unlikely that the courts will extend the same sympathy to honeypot operators.

Possession of contraband material

A hacker may utilize the honeypot to store contraband material such as child pornography or pirated copies of copyrighted material. If the honeypot operator fails to delete such material from the honeypot in a timely manner, a court could hold him criminally responsible for possession of that material. In the case of child pornography, a violation could result in fines and up to 20 years of imprisonment.[26]

Failure to report crimes

A honeypot operator has an affirmative duty to report certain crimes to the authorities. For instance, those who provide electronic communications services to the public are required to report child pornography violations to the Cyber Tip Line at the National Center for Missing and Exploited Children.[27] Additionally, the court may fine and imprison for up to three years anyone who knows of the actual commission of a felony but fails to report it as soon as possible.[28] Although no one has ever prosecuted a honeypot operator for these crimes and the honeypot operator can avoid them through diligent monitoring and a thorough understanding of its reporting obligations, the risk is nonetheless present.

Suggestions for mitigating the legal risks

Although this survey of U.S. law illustrates the fact that some of the fears associated with the legality of operating a honeypot are either unwarranted or overblown, it also demonstrates that sufficient legal uncertainly remains. Although no honeypot operators have been charged with a crime or sued civilly by a hacker as of yet, the possibility that it will hap-

17 *Know Your Enemy, The Honeynet Project*, Addison-Wesley Professional; 2nd edition (May 27, 2004).

18 18 U.S.C. § 3121(d).

19 18 U.S.C. §§ 2701–2712.

20 *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

21 *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993).

22 *Katz v. U.S.*, 389 U.S. 347, 350 (1967).

23 *U.S. v. Seidlitz*, 589 F.2d 152, 160 (4th Cir. 1978) ("having been 'caught with his hand in the cookie jar,'" hacker has no constitutional right to suppression of evidence gathered from victim computer). See also *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (burglar has no reasonable expectation of privacy while on victim premises) and *Compuserve, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (courts have likened computer hacking and trespassing).

24 *U.S. v. Jacobson*, 466 U.S. 109, 115 (1984).

25 See *American Tel. & Tel. Co. v. Jiffy Lube Intern., Inc.*, 813 F.Supp. 1164 (D. Md. 1993).

26 18 U.S.C.A. § 2252(b)(1).

27 42 U.S.C. § 13032.

28 18 U.S.C. § 4.

pen exists and the law remains unsettled. Information security professionals can leverage the following six suggestions to mitigate some of the legal risks associated with honeypot implementation:

1. **Seek the advice and approval of legal counsel before deploying a honeypot.** Your organization's attorneys are in the best position to understand or research the legal ramifications of your deployment.
2. **Seek out advanced expertise in the implementation and operation of your honeypot.** This is not a project for amateurs. A poorly implemented honeypot that a hacker can easily compromise is a bigger liability to your organization than having no honeypot at all.
3. Where possible, **place a consent banner** meeting the requirements discussed above on all communication services supported by your honeypot. Banners that require actions by users to accept are optimal.
4. **Make sure that you configure your honeypot to prohibit or greatly limit outbound connections to third parties.** The best way to avoid downstream liability is to prevent hackers from having the ability to launch attacks from your honeypot.
5. **Make sure that you constantly monitor the activity on your honeypot** and have established relationships with law enforcement officials so that you can meet your obligation to report felony criminal activity to authorities as quickly as possible.
6. If you allow the uploading of files to your honeypot, **make sure that you purge undesirable or illegal content from the machine as quickly as possible** after receiving the okay to do so from authorities.

Conclusion

Because honeypots have enormous potential both as security research tools and in commercial application as an additional layer of defense, it would be shameful to allow the uncertainty that exists both from the lack of legal precedent and from the proliferation of misinformation to continue to inhibit their deployment. By implementing and operating honeypots in a legally responsible manner, security professionals can effectively manage these risks and fully realize the benefits of this technology.

About the Author

Bradley J. Schaufenbuel, CISM, CISSP, CISA, is Senior Manager of IT Risk & Security at Zurich Financial Services in Schaumburg, Illinois, as well as a JD/LLM candidate in the IT & Privacy Law program at the John Marshall Law School in Chicago, Illinois. Brad is the author of numerous books and professional journal articles on the topics of IT governance, legal and regulatory compliance, and information security. His email address is bradley@schaufenbuel.com.