Honeypots (2):
Entrapment?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University student Bob Pelletier continues his review of the role of honeypots in intrusion detection work. In this article he looks at fears that using honeypots might constitute entrapment. I (Kabay) have made minor editorial changes to his text to fit the format of this newsletter.

* * *

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 first step to insure the legality of a honeypot is to define the goal of the system. Create policies that will outline exactly what information is going to be collected and to what end. There should be no misconceptions about what a honeypot system is being implemented for. Being upfront with the purpose of a honeypot can defuse accusations of secrecy or trickery. This is especially important in a production atmosphere where corporate policies need to be followed. A system banner should also be installed on the honeypot stating that users of the system may be monitored. As will be discussed later, this can eliminate charges of entrapment. Refer to Appendix A of Searching and Seizing Computers and Obtaining Electronic Evidence in criminal Investigations created by the Department of Justice for sample banners. [1]

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.

***

In the next article in this series, Bob Pelletier (mailto:pelletib@norwich.edu) looks at the privacy issues involved in using honeypots.

***

References:


***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Bob Pelletier & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.