Honeypots (3):
Privacy

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 privacy issues surrounding honeypot usage. I (Kabay) have condensed his text (with Bob’s approval) to fit the format of this newsletter.

* * *

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

* Information privacy protects stored information about an individual [1]. 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.”[2] 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?[3] 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) [4].

None of these pose 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.

In the next article, Bob Pelletier (mailto:pelletib@norwich.edu) looks at ethical issues in the use of honeypots.

References:


[2] What is the Fourth Amendment?  
http://www.unc.edu/courses/law357c/cyberprojects/spring01/Carnivore/4th_Amendment.htm


[4] 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

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.