

# Honeypots: The Past, Present and Future

By Lance Spitzner

**H**oneypots are a relatively new technology in the world of information security. While they have been publicly discussed for the past fifteen years, we have only just now begun to see their widespread use, especially in the world of information security research. Honeypots have tremendous potential to help us better understand new and evolving threats and better defend against them. In this article we will start with a review of this technology and its history, then move on to their value to the security community today. We will also cover some of the future roads that we see this technology taking.

## Overview

Before we start talking about honeypots, we need to first define what they are, and their value to you and the security community. As you are about to see, honeypots can be difficult to define, as they come in so many shapes and sizes. The commonly recognized definition of a honeypot is: *an information system resource whose value lies in unauthorized or illicit use of that resource.*

This definition was created by members of the honeypots mail list<sup>1</sup>, a group of over 5,000 security professionals. The first key thing you may notice in the definition is it does not state the problems honeypots solve. That's because honeypots do not solve a specific problem. Firewalls solve a specific problem—host- or network-based access control. Intrusion Detection Sensors solve a specific problem—detection. Honeypots are different; they are a highly flexible tool that can address a wide range of issues. Second, notice we call a honeypot a resource, NOT a computer. In most deployments, a honeypot is a computer. However, they can take on other manifestations, such as digital tokens or client software.

What honeypots do share, and what makes them different from almost all other security technologies, is the fact that you want the bad guys to interact with them. Their value lies in unauthorized activity. The concept of a honeypot is simple. It's a resource that has no production or valid activity. Since no one should be interacting with the honeypot, theoretically it should see no activity, it should not capture any traffic. If it does capture any activity, this is most likely malicious or unauthorized. For example, if you place a computer somewhere on your network, it should not see any connections to it, as no one should know it's there, nor should they have any reason to initiate a connection to it. However, if you did place such a computer on your network, you may be surprised by all the connection attempts it sees. Often these connection attempts are worms, employees scanning where they should not be, third-party vendors probing your network, etc.

Because of this simplistic approach, honeypots excel at capturing information. They only capture malicious traffic. This means they collect small

sets of data, but data of high value. You don't have to weed out the 'good' traffic from the 'malicious or bad' traffic, as it's all malicious. In some ways, honeypots even do data analysis for you, giving you the important data you need to know, right away. Also, honeypots can capture in-depth information at a level few other technologies can. Honeypots can capture the keystrokes, tools, even the communications of threats and attacks, giving us not only their tools and tactics, but their very motives. This demonstrates a honeypot's primary value to the security community—the ability to provide information at a level few other resources can. For example, honeypots gave us the information in the HoneyNet Project and Research Alliance's detailed paper on bots, *Know Your Enemy: Tracking Botnets*<sup>2</sup>. This paper details what Botnets are, who is using them, the systems they target, and why. It's information like this that has tremendous value.

## The Past

The concepts of honeypots were first published in 1989 and 1991 in two different sources. The first is the excellent book, *The Cuckoo's Egg*<sup>3</sup>, by Clifford Stoll. This book recounted the tale of how an academic computer at Lawrence Berkeley Lab was broken into, and how Clifford, a system administrator, tracked the hacker down. The book reads more like a spy novel than a technical manual. The second publication is *An Evening with Berferd*<sup>4</sup>, published by Bill Cheswick in 1991. This was a technical whitepaper, discussing how a system was modified to allow an intruder to break in. While both sources document the concept of a honeypot (its value was in the attacker interacting with it), neither actually used the term honeypot.

For approximately the next ten years, there was little research or publications done in this area. Then, the first honeypot publicly released was Fred Cohen's Deception Toolkit<sup>5</sup>, a collection of Perl scripts designed to emulate certain operating systems and services. This was designed to interact and confuse attackers back in the days when most attacks were manual. Now almost all attacks are highly automated, limiting its deception value. Over the next several years many commercial honeypots were released, including CyberCop Sting and NetFacade. However, honeypots did not really come to public attention until the year 2001, when the HoneyNet Project released the paper "Know Your Enemy: Motives."<sup>6</sup> This paper detailed the activities of an extremely active hacker group out of Pakistan called "Gforce." All of the information, including conversations, were captured with honeypots. This paper, and the HoneyNet Project, opened the community's awareness and acceptance of the power of honeypots. In April 2002, Niels Provos released the OpenSource honeypot Honeyd<sup>7</sup>, considered one of the most powerful and flexible honeypot solutions today.

## The Present

Today, honeypots have become mainstream. They are primarily used by organizations that have a need for information. For example, many universities are using honeypots for research purposes, such as Georgia Tech in the United States, RWTH-Aachen University in Germany, or Peking University in China. These academic organizations use honeypots to collect data, test new application or theories, or for students to gain a better understanding of threats and security in general. Recently the National Science Foundation funded the Center for Internet Epidemiology and Defenses 6.2 million dollars for deploying a large-scale honeypot farm for worm research and analysis. In many ways, their approach to worms is similar to the Centers for Disease Control and Prevention, acting as a clearing house in the collection, analysis, and response to viruses. Some of the most exciting research we are seeing today in honeypot technologies is happening at academic and non-profit institutions around the world.

Government organizations in Brazil<sup>8</sup> and Poland<sup>9</sup> are using honeypots for early warning and prediction purposes. They use honeypots such as Honeyd to monitor a large percentage of IP space, capturing and analyzing all malicious traffic. We are also seeing their use in the commercial sector, especially with security-related corporations. Security companies such as Sophos and Symantec use honeypots to capture and analyze threats, and pass those lessons learned onto their customers. A great deal of Spam and Anti-virus technology and databases are based on the information collected with honeypots. Also, a great deal of the reports you read on attacker and threat activity is based on the information collected from different types of honeypots.

Most non-security related corporations have not invested in honeypot technology, as honeypots may not provide them value. Most commercial organizations are concerned about preventing attacks using technologies such as firewalls, patching, and proper authentication. Honeypots add little value in this area, though solutions such as sticky honeypots can help prevent the spread of worms. At times, it can also be difficult to judge just how widespread the use of honeypots is. Because of the nature of honeypots, some organizations that have deployed honeypots do not make the information public, especially military, law enforcement or government organizations.

## The Future

Honeypots have an extremely exciting future ahead of them. We have only scratched the surface. As attackers have evolved, changed, and advanced, we must also adapt. Honeypots can give us that flexibility. A variety of new concepts are under development around the world. Expect to see these honeypots in the near future in a variety of different organizations. Some of these concepts include:


- ▲ **Client Honeypots:** Traditionally most honeypots have been servers, waiting for attackers to find and break into them. However, attackers have changed. Instead of breaking into systems, they attack the user and their actions. In many ways, it's become easier to hack the end user than a computer. Examples of such attacks include phishing attacks with spoofed e-mails, malicious Web sites that compromise browsers, or Instant Messaging exploits that attack a live connection. Client honeypots can be used to learn more about these threats. These are client-based systems that emulate common behavior, such as searching the Web, reading e-mail, or

instant messaging someone. The client honeypot can then track and capture any attacks or exploit attempts against this behavior and learn more about threats, such as who is doing them, or identify a new exploit.

- ▲ **Application Honeypots:** Many attackers no longer focus on breaking into computers or systems. It's information they want, and it's much easier to compromise an application than it is to penetrate several layers of defense in depth. Applications offer easy, direct, and unfiltered access to many organizations' databases. Attacks such as SQL injection or logic attacks can give attackers easy access with this information, often using nothing more than a Web browser. Application honeypots, designed to look like online targets such as a bank or flower store, can capture and record such activity.
- ▲ **Router Honeypots:** Routers are the backbone of the Internet infrastructure and make them a tempting target. Routers acting as honeypots can capture the attacks against these systems and record the activities and motivations of threats after these systems have been compromised.
- ▲ **Advanced Honeypots:** Little is known about truly advanced attackers, who target specific systems of high value. Expect to see honeypots in the future that replicate all the functionality of a high-value system or even an organization. This type of deployment is extremely complex and would require dedicated resources over a long period of time.

These are just some of the more exciting ideas we will see. As honeypots are very flexible and come in many shapes and sizes, you will be surprised at all the different places and organizations you see them deployed.

## Conclusion

A honeypot is a resource who's value is in the bad guys interacting with it. It is not a solution, but a flexible tool that can apply to a variety of different situations. Its primary value is information, the ability to collect information that few other resources can. Honeypots have come a long way since they were first discussed in 1989 and 1991. We now have a variety of different commercial and OpenSource honeypot options, with widespread deployment by a variety of different academic, commercial, and government organizations. Expect to see honeypots continue to grow in their use and expand in the different ways they are used. For more information on the latest in honeypot technology, I recommend the book *Know Your Enemy: 2nd Edition*,<sup>10</sup> published by the HoneyNet Project. 

---

Lance Spitzner, MBA, is the founder of the HoneyNet Project.

<sup>1</sup> <http://www.securityfocus.com/popups/forums/honeypots/faq.shtml>

<sup>2</sup> <http://www.honeynet.org/papers/bots>

<sup>3</sup> *The Cuckoo's Egg*, Clifford Stoll, Pocket Books Inc, New York, NY 1989

<sup>4</sup> *An Evening With Berferd*, Bill Cheswick

<sup>5</sup> <http://www.all.net/dtk/index.html>

<sup>6</sup> <http://www.honeynet.org/papers/motives>

<sup>7</sup> <http://www.honeyd.org>

<sup>8</sup> <http://www.honeypots-alliance.org.br>

<sup>9</sup> <http://arakis.cert.pl>

<sup>10</sup> <http://www.honeynet.org/book>