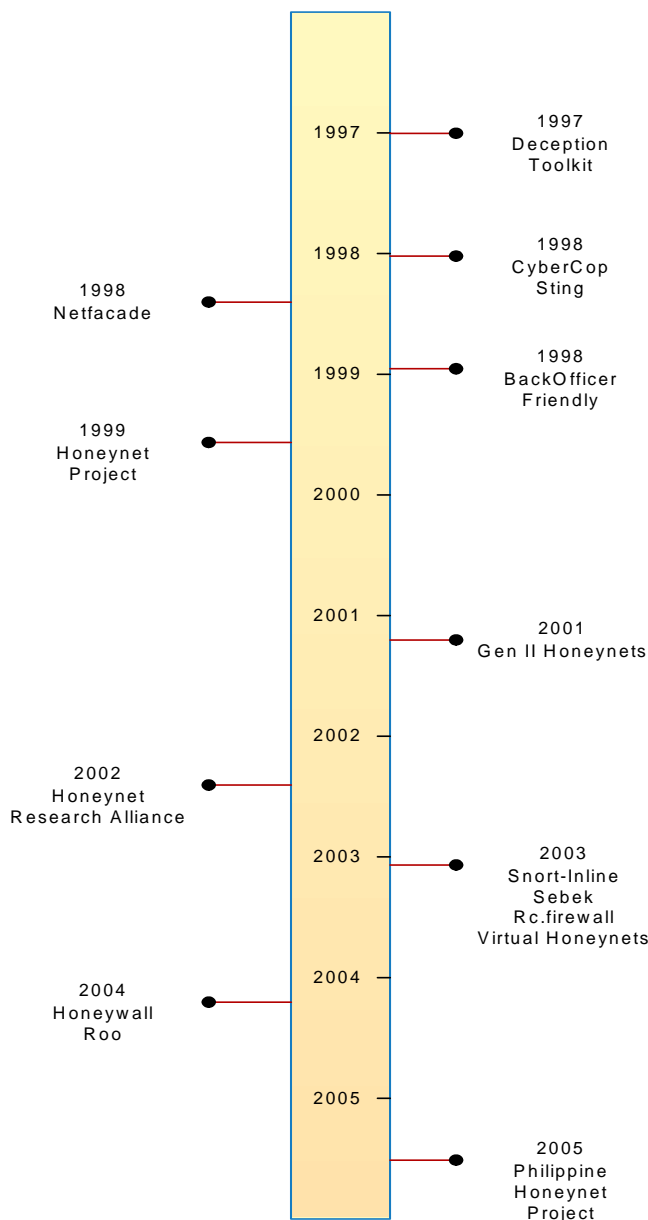




A Student IT Security Awareness Initiative by The Philippine Honeynet Project

Honey pots 101: A Brief History of Honey pots

By Ryan Talabis



As I've said in my previous article¹, the concept of the honeypot is not new. In fact as early as 1991, a number of publications expounded on concepts that were to be foundations of today's honeypot development. Two publications in particular stood out: These were Clifford Stoll's "The Cuckoo's Egg" and Bill Cheswick's "An Evening with Berferd".

Clifford Stoll was an astrophysicist turned systems manager at Lawrence Berkeley Lab. Due to a 75 cent accounting error was able to track down a hacker that was using their computers as a launching pad to hack hundreds of military, industrial, and academic computers in search of secrets for the KGB. His book "The Cuckoo's Egg", published in 1988, detailed his experiences through this 3 year incident where he observed the hacker and subsequently gathered information that led to the hackers arrest. Though it read more like a spy thriller, there were many concepts behind the book that would not be entirely unfamiliar to honeypot practitioners.

The other publication that was of particular note during this period was "An Evening with Berferd" by the well respected Internet Security expert, Bill Cheswick. In the paper, Mr. Cheswick describes how he and his colleagues set up their jail machine, also known as roach motel² in which they chronicled a hackers movements and the bait and traps they used to lure and detect him.

¹ A Honeypot 101: A Honeypot by any other name by the Honeynet Project

² Roach Motel (<http://www.ja.net/CERT/Cheswick/berferd.txt>)

In 1997, Fred Cohen released the Deception Toolkit. The Deception Toolkit is one of the original and landmark Honeypots. It is generally a collection of PERL scripts designed for UNIX systems that emulate a variety of known vulnerabilities. The concept put forward by the DTK is “deceptive defense” which now central in Honeypot concepts and implementations.

The basic idea in the DTK is to use deception to counter attacks. By using the DTK, we can setup a system, which shows up as having a large number of “vulnerabilities”. DTK is able to do this by providing simulated output to the attackers input. For example, If the attacker inputs a known sendmail exploit, the DTK then sends out a corresponding output to the attacker making him believe that his exploit is actually working. So how does this help in defense?

It’s actually pretty simple. Think of it this way, if the attacker falls for our deception not only will it consumes the attackers time and effort trying to exploit our “fake” vulnerability, it also gives us the valuable time to track the attempts at entry and respond to the attack before they come across a real vulnerability that the system is actually susceptible too.

DTK paved the way for more new Honeypot implementations. In fact, 1998 the following year gave us the first commercial Honeypot implementation called Cybercop sting³. CyberCop Sting is a component of the CyberCop intrusion protection software family which runs on NT.

Cybercop Sting has also been referred to as a “decoy server” for it can simulate a network containing several different types of network devices, including Windows NT servers, Unix servers and routers. Each of these decoys had the ability to track, record, and report intrusive activity to network and security administrators. As with the DTK, each of these decoys can run simulated services. However, as with the problem with most simulated or low-interaction Honeypots, you can only only simulate limited functionality with Cybercop sting such as telnet logins or SMTP banners thus limiting its ability to deceive and to study hackers in the long term.

Another commercial Honeypot implementation that came out on the same year was NetFacade⁴. As with Cybercop Sting, it creates a simulated network of hosts, with simulated IP addresses, running seemingly vulnerable services but in a much larger scale. NetFacade can simulate an entire class C network up to 254 systems. It can also simulate 7 different operating systems with a variety of different services. Unfortunately, NetFacade saw little commercial favor but the important side benefit of NetFacade was a network based debugging tool courtesy of Marty Roesch which ultimately led to the Snort IDS⁵ which was to play a major role in Honeypot implementations in the succeeding years.

1998 was a particularly busy year for Honeypot development because after Cybercop and NetFacade, the windows Honeypot “Back Officer Friendly”⁶ came out. This is not to be confused with the very popular back door program called “Back Orifice”⁷. Though totally different, they are in some way related because Back Officer Friendly was in fact made to counter the rising threat of Back Officer Friendly in those days. Back Officer Friendly runs in Windows and was free thus giving more people access to Honeypot technology. Though It didn’t give much functionality it was still a very useful piece of software which demonstrated the concepts of the Honeypot to a lot of people that who were not familiar to Honeypot concepts at that time.

We can say that 1998 proved to be an indication of the rising interest in Honeypot development because in 1999 a group of people led by Lance Spitzner⁸ decided to form the HoneyNet Project⁹.

³ Deception Toolkit (<http://all.net/dtk/dtk.html>)

⁴ NetFacade (http://www22.verizon.com/fns/solutions/netsec/netsec_netfacade.html)

⁵ Snort.org (<http://www.snort.org>)

⁶ Back Officer Friendly (<http://www.nfr.com/resource/backOfficer.php>)

⁷ Cult of the Dead Cow (<http://www.cultdeadcow.com/>)

⁸ Tracking Hackers (www.tracking-hackers.com/)

The honeynet project is a non-profit group dedicated to researching the blackhat community and to share their work to others. Their primary tool for research is the honeynet, an advanced form of Honeybot.

In 2002, another related initiative was born out of the Honeybot Project this time involving the whole security community to further Honeybot related research. This initiative is what we call now the Honeybot Research Alliance¹⁰. The Research Alliance is composed of groups around the world interested in Honeybot research including the Philippine Honeybot Project¹¹. This setup provided a means for Honeybots to be deployed around the world and provided a venue for sharing tools and techniques used in Honeybot research.

A lot of tools used in Honeybot research was developed through the Honeybot project and the Honeybot research alliance. In 2003, several important Honeybot tools were introduced through these organizations such as Snort-Inline¹², Sebek¹³, and advanced virtual honeynets¹⁴. Snort-Inline augmented Snort to block and disable attacks instead of just detecting them. Sebek provided a means to capture hacker activities in Honeybots by logging their keystrokes. Virtual honeynets provided a means to deploy multiple honeynets with just one computer.

Another development of note coming from the Honeybot Project and the Honeybot Research Alliance was the bootable CD ROM Roo¹⁵ which made honeynet deployments relatively simple. This CD ROM was released in 2004 using the tools mentioned above. This tool was particularly noteworthy because it helped start the Philippine Honeybot Projects honeynet deployment.

In 2005, Ryan Talabis and Ateneo Information Technology Institute¹⁶ faculty members John Ruero, Mida Guillermo and Dr. John Paul Vergara together with web-developer Carlo Monteverde started the Philippine Honeybot Project to promote IT security awareness in the Philippines. The initial "proof of concept" honeynet used the bootable Honeywall Roo CD to deploy a honeynet in the AITI campus. The project was accepted into the Honeybot Research Alliance at the same year. Currently the Philippine Honeybot Project is involved in gathering data and developing tools for malicious internet activity monitoring, statistics and trends analysis. We shall be discussing more regarding the Philippine Honeybot Project in subsequent papers.

As you can see, Honeybots have a short but very dynamic history. Though there has been many significant important advancements already, I feel that the best discoveries are still to come. In fact, you and the other people who are reading this article may well be the ones who will be making Honeybot history.

The next paper in this series would deal with the uses and value of Honeybots. In the paper, we will be discussing the myriad fields Honeybots are being used today such as law enforcement, intrusion detection, intrusion prevention, reverse engineering, research and something that the Philippine Honeybot Project is currently involved in namely statistics and trends analysis.

⁹ Honeybot Project (<http://www.honeynet.org>)

¹⁰ Honeybot Project Research Alliance (<http://www.honeynet.org/alliance/>)

¹¹ Philippine Honeybot Project (<http://www.philippinehoneynet.org>)

¹² Snort-Inline (<http://snort-inline.sourceforge.net/>)

¹³ Sebek (<http://www.honeynet.org/tools/sebek/>)

¹⁴ Virtual Honeynets (<http://www.honeynet.org/papers/virtual/>)

¹⁵ ROO (<http://www.honeynet.org/tools/cdrom/>)

¹⁶ Ateneo Information Technology Institute (<http://aiti.ateneo.edu>)

About the author

Ryan Talabis is the founder of the Philippine HoneyNet Project. He is currently working as a web and database consultant for the Asian Development Bank. Formerly, he was the Director of Software Development and Technology for Slingshot Interactive, a start-up web development firm in Manila. He loves to work with honeypots, has a pretty good grasp in making pretty websites and loves to make charts for everything. In his free time, he is an aggressive inline skater and hopes to compete in the X-Games someday. You can contact him at talabis[at]gmail.com.

About the Philippine HoneyNet Project

The Philippine HoneyNet Project (<http://www.philippinehoneynet.org>) is a non-profit, all volunteer group dedicated to promoting honeynet and IT security research in the Philippines. It is a member of HoneyNet Research Alliance (<http://www.honeynet.org>), an organization of HoneyNet initiatives around the world.