Honeypots: Concepts, Approaches, and Challenges

Iyatiti Mokube
Computer Science
Armstrong Atlantic State University
Savannah, GA 31419
im3871@students.armstrong.edu

Michele Adams
Computer Science
Armstrong Atlantic State University
Savannah, GA 31419

ABSTRACT
Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of honeypots. A honeypot is a security resource whose value lies in being probed, attacked or compromised. In this paper we present an overview of honeypots and provide a starting point for persons who are interested in this technology. We examine different kinds of honeypots, honeypot concepts, and approaches to their implementation.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *Security and protection*

General Terms
Security, Legal Aspects

Keywords
Honeypots, Types of honeypots, Legal Issues and Honeypots.

1. Introduction
In this day and age, information security is an ever-increasing concern. The traditional approach to security has been largely defensive so far, but interest is increasingly being paid to more aggressive forms of defense. One of these forms is decoy-based intrusion protection [6] through the use of honeypots and/or honeynets.

A honeypot is tough to define because it is a new and changing technology, and it can be involved in different aspects of security such as prevention, detection, and information gathering. It is unique in that it is more general technology, not a solution, and does not solve a specific security problem. Instead, a honeypot is a highly flexible tool with applications in such areas as network forensics and intrusion detection. For the purpose of this paper, we will use the following definition: a honeypot is a security resource whose value lies in being probed, attacked, or compromised [17].

ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA

Honeypots are closely monitored network decoys serving several purposes that include the following [7]:

1. They can distract attackers from more valuable machines on a network;

2. They can provide early warning about new attack and exploitation trends; and

3. They allow in-depth examination of adversaries during and after exploitation of a honeypot.

Honeypots are a technology whose value depends on the "bad guys" interacting with it. All honeypots work on the same concept: nobody should be using or interacting with them, therefore any transactions or interactions with a honeypot are, by definition, unauthorized.

"Honeynet" is a term that is frequently used where honeypots are concerned. A honeynet is simply a network that contains one or more honeypots. More precisely, it is a high-interaction honeypot that is designed to capture extensive information on threats and provides real systems, applications, and services for attackers to interact with [1].

This paper is organized as follows: In Section 2 we examine different types of honeypots. In Section 3 we provide an overview of the honeypot concept and approaches to their implementation. Section 4 presents legal issues and challenges surrounding honeypots. We then conclude and provide our opinion on the future of honeypots in section 5.

1.1 Related Work
Research in this area has resulted in a number of papers discussing specific topics concerning honeypots and how honeypots can be created and deployed.

Several papers have explored the use of honeynets as an educational tool for IT students and academic institutions [8], [10]. This research indicates that honeynets can be an effective tool in security education. A significant amount of work is available that details the benefits of honeypots [12], [6]. Other papers go into some detail about the strategic considerations involved when using honeypots [12]. There are also papers that describe specific applications of honeypots as building blocks for a system such as a honeycomb, which is used to create intrusion detection signatures [11].

A large amount of helpful information exists on the Honeynet Project at [1]. This website documents lessons learned about security threats through the use of honeypots.
Existing work looks at specific areas concerning honeypots; however it is difficult to find information from a single source that provides an overall picture of honeypots including their benefits, the concepts behind honeypots, the approach to using honeypots, and the challenges involved when implementing honeypots.

The purpose of this paper is to do a survey of honeypots, and provide a reasonable overview and starting point for persons who are interested in this technology.

2. Types of Honeypots

Honeypots can be classified based on their purpose (production, research, and honeytokens) and level of interaction (low, medium, and high). We include honeytokens as another type, because they do not belong to either of the categories mentioned above. We examine each type in more detail below.

2.1 Purpose of Honeypots

2.1.1 Research Honeypot

A research honeypot is designed to gain information about the blackhat community and does not add any direct value to an organization [10]. They are used to gather intelligence on the general threats organizations may face, allowing the organization to better protect against those threats. Its primary function is to study the way in which the attackers progress and establish their lines of attack, it helps understand their motives, behavior and organization Research honeypots are complex to both deploy and maintain and capture extensive amounts of data. They can be very time extensive.

Very little is contributed by a research honeypot to the direct security of an organization, although the lessons learned from one can be applied to improve attack prevention, detection, or response. They are typically used by organizations such as universities, governments, the military or large corporations interested in learning more about threats research.

Research honeypots add tremendous value to research by providing a platform to study cyberthreats. Attackers can be watched in action and recorded step by step as they attack and compromise the system. This intelligence gathering is one of the most unique and exciting characteristics of honeypots [18]. It is also a beneficial tool in aiding in the development of analysis and forensic skills. Sometimes they can even be instrumental in discovering new worms.

2.1.2 Production Honeypot

A production honeypot is what most people think of when discussing honeypots. A production honeypot is one used within an organization's environment to protect the organization and help mitigate risk [10]. It has value because it provides immediate security to a site's production resources. Since they require less functionality then a research honeypot, they are typically easier to build and deploy. Although they identify attack patterns, they give less information about the attackers than research honeypots. You may learn from which system attackers are coming from and what exploits are being launched, but maybe not who they are, how they are organized, or what tools they are using.

Production honeypots tend to mirror the production network of the company (or specific services), inviting attackers to interact with them in order to expose current vulnerabilities of the network. Uncovering these vulnerabilities and alerting administrators of attacks can provide early warning of attacks and help reduce the risk of intrusion [5]. The data provided by the honeypot can be used to build better defenses and counter measures against future threats.

It should be pointed out that as a prevention mechanism, production honeypots have minimal value. Best practices should be implemented involving the use of Firewalls, IDS's, and the locking down and patching of systems. The most common attacks are done using scripts and automated tools. Honeypots may not work well against these since these attacks focus on many targets of opportunity, not a single system.

Their main benefit is in the area of detection. Due to its simplicity it addresses the challenges of IDS's – there are minimal false positives and false negatives. There are several situations where an IDS may not issue an alert: the attack is too recent for your vendor, the rule matching it caused too many false positives or it's seeing too much traffic and is dropping packets. False Positives occur when an untuned IDS alerts way too much on normal network traffic. These alerts soon get ignored or the rules triggering them are modified, but then real attacks may be missed. In addition, there is a serious problem with the volume of data to analyze with IDS's. They can't cope with the network traffic on a large system. Honeypots address these challenges because since honeypots have no production activity, all the traffic sent to a honeypot is almost certainly unauthorized – meaning no false positives, false negatives or large data sets to analyze.

Also, once an attack has been detected the machine can be pulled offline and thorough forensics performed, something that is often difficult if not impossible with a production system.

In general, commercial organizations derive the most direct benefit from production honeypots.

These categorizations of honeypots are simply a guideline to identify their purpose, the distinction is not absolute. Sometimes the same honeypot may be either a production or research honeypot. It is not as much how it is built but how it is used [15].

2.2 Level of Interaction

In addition to being either production or research honeypots, honeypots can also be categorized based on the level of involvement allowed between the intruder and the system. These categories are: low-interaction, medium-interaction and high-interaction. What you want to do with your honeypot will determine the level of interaction that is right for you.

2.2.1 Low-interaction Honeypots

A low-interaction honeypot simulates only services that cannot be exploited to gain total access to the honeypot [13]. On a low-interaction honeypot, there is no operating system for the attacker to interact with [4] (pp. 19). They can be compared to a passive IDS since they do not modify network traffic in any way, and do not interact with the attacker. Although this minimizes the risk associated with honeypots, it also makes low interaction honeypots very limited. However, they can still be used to analyze spammers and can also be uses as active countermeasures against worms [13].

Low-interaction honeypots are easy to deploy and maintain. An example of a commercial low-interaction honeypot is *honeyd*.

Honeyd is a licensed daemon[1] that is able to simulate large network structures on a single network host [3, 13]. *Honeyd* works by imitating computers on the unused IP address of a network, and provides the attacker with only a façade to attack. Another example of a low-interaction honeypot is *Specter*, which is developed and sold by NetSec. *Specter* has functionality like an enterprise version of BOF and only affects the application layer.

2.2.2 Medium-Interaction Honeypots

Medium-interaction honeypots are slightly more sophisticated than low interaction honeypots, but less sophisticated than high interaction honeypots [19]. Like low-interaction honeypots they do not have an operating system installed, but the simulated services are more complicated technically. Although the probability that the attacker will find a security vulnerability increases, it is still unlikely that the system will be compromised [4] (pp. 20). Medium-interaction honeypots provide the attacker with a better illusion of an operating system since there is more for the attacker to interact with. More complex attacks can therefore be logged and analyzed.

Some examples of medium-interaction honeypots include *mwcollect*, *nepenthes* and *honeytrap*. *Mwcollect* and *nepenthes* can be used to collect autonomously spreading malware [3]. These daemons can log automated attacks, and extract information on how to obtain the malware binaries so that they can automatically download the malware. *Honeytrap* dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks.

2.2.3 High-interaction honeypots

These are the most advanced honeypots. They are the most complex and time-consuming to design, and involve the highest amount of risk because they involve an actual operating system [4] (pp. 20 – 21). The goal of a high-interaction honeypot is to provide the attacker with a real operating system to interact with, where nothing is simulated or restricted [19]. The possibilities for collecting large amounts of information are therefore greater with this type of honeypot, as all actions can be logged and analyzed.

Because the attacker has more resources at his disposal, a high-interaction honeypot should be constantly monitored to ensure that it does not become a danger or a security hole [4]. A *honeynet* is an example of a high-interaction honeypot, and it is typically used for research purposes.

2.3 Honeytokens

Simply put, a honeytoken is a fake digital entity that can have many different applications. Although the term "honeytoken" was coined in 2003 by Augusto Paes de Barros [16], the concept of honeytokens is not new. For years dictionaries, encyclopedias, maps and directories have used fake entries or deliberately erroneous entries as copyright traps to facilitate detection of copyright infringement or plagiarism[2].

[1] http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci211888,00.html

[2] http://en.wikipedia.org/wiki/Nihilartikel

In computer security, Spitzner [16] defines a honeytoken as a honeypot that is not a computer, but a digital entity. A honeytoken can exist in many forms such as a credit card number, an Excel spreadsheet, a PowerPoint presentation, a database entry, or even a fake login. Like other types of honeypots, no honeytoken has any authorized use. This gives honeytokens the same power and advantages as traditional honeypots, but extends their capabilities beyond physical computers.

2.3.1 How Honeytokens Work

Whatever you choose as a honeytoken, no one should be interacting with it, therefore any interaction with it is suspicious, if not necessarily malicious. Honeytokens are flexible enough so that you can decide what you want to use as a honeytoken, and how you want to use it; in this regard you can be as creative as you choose. For example, fake credit card numbers can be inserted into a database, file server or some other kind of repository within a network. IDS's can be configured to watch the network so that if these numbers are accessed, you know the data has most likely been compromised.

Like traditional honeypots, honeytokens do not solve a specific security problem. They are a simple and flexible tool with applications in security that include ensuring data integrity, trapping malicious insiders, and detecting unauthorized access to a database. For example, to ensure data integrity, one could use a honeytoken in the form of a fake database entry that wouldn't normally be selected by authorised queries. The use of a honeytoken such as a fake login can help in tracking the activities, and determining the actions, capabilities and intentions of, a malicious intruder.

Honeytokens should not be used by themselves but should be used in addition to other security measures. In addition, the cost involved in the use of honeytokens is minimal because there is no new technology to deploy, no vendors to contact, and no licenses to deploy, which further increases their value.

Further information on honeytokens can be found in [16].

3. Honeypot Concepts and Approaches to their Implementation

We now take a look at the main concepts of honeypots and a few different ways in which they can be implemented.

Honeypots are digital network bait and use deception to attract intruders [12], thereby distracting them from real production systems. A honeypot with several layers can slow down an attack, increasing the possibility of the attack being detected, and the possibility of countering the intrusion before it succeeds [2]. Intrusion detection and logging applications can be deployed within the honeypot to listen for and log unauthorized activity.

Since no interaction with a honeypot is authorized, there is no need to filter through the information collected by a honeypot for suspicious traffic. This information can then be used to learn how the intruders operate, and to come up with suitable countermeasures. In summary, the main concept of a honeypot is to learn from the intruder's actions [12].

Additionally, honeypots are not designed to be the sole source of security for any network; they should be used in conjunction with other security measures.

3.1 Approaches to Honeypot Implementation

To implement a honeypot, some factors you need to consider include:

- **What kind of data that should be made available through the honeypot?**
  For the honeypot to masquerade as an authentic system, realistic data needs to be used. However, there are also the consequences to consider when the honeypot is compromised and the intruder uses the data against the organization [2]. Measures need to be in place to handle such an occasion when it arises.
- **How do you prevent uplink liability?**
  If a honeypot is compromised, it could be used by the intruder to attack other systems (this is known as uplink liability). There are liability issues to consider if this happens, and preventative measures to take. Legal issues concerning honeypots will be covered in more detail in the next section.
- **To build or not to build?**
  The honeypot owner also has to decide between building a honeypot and purchasing a commercially available one. Financial resources need to be considered. In addition, maintenance of the honeypot requires knowledgeable personnel, as well as a considerable amount of time to examine the data collected by the honeypot.
- **Where is the best location for your honeypot**
  Experts suggest isolating the honeypot from your production system to prevent uplink liability [2, 12]. A lot more information on the considerations involved in honeypot implementation can be found in [2].

4. Legal Issues and Challenges

There are potential legal pitfalls that may turn your honeypot into a liability. There are many factors which determine whether or not the use of a honeypot is legal. We provide a brief overview of some of the issues. If deploying a honeypot in the United States, then there are at least three legal issues that you must consider:

- Entrapment - Attackers may argue entrapment
- Privacy – Laws exist that might restrict your right to monitor users on your system
- Liability - Realize that attackers may misuse your honeypot to harm others

We will elaborate on each of these issues as discussed in [14].

4.1 Entrapment

Most articles written discussing legal issues and honeypots consider entrapment a concern for honeypot owners. The Supreme Court defines entrapment 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". Entrapment applies in a criminal case in which the government acted in a manner that actually caused the defendant to commit the crime. It has no application to private honeypot operators. A defendant who is predisposed to commit the crime, or was not induced by the government to commit it, cannot successfully use the entrapment defense.

The defense is unlikely in a pure honeypot case where there was no government inducement and the private honeypot owner is acting independently from the government. When commenting on whether "entrapment" is a concern for honeypot owners, Richard P. Salgado (senior counsel in the Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice) writes that "the issue is overstated" [14].

4.2 Privacy

Although as an owner of a network you have a responsibility to keep it secure, your rights to monitor all the activities of system users may have some limits. There are restrictions that limit monitoring. These restrictions may be in the form of state and federal statutes, privacy or employment policies, terms of service agreements, and other contracts. Depending on the restriction and its source, violating it may lead to civil liability or criminal sanctions. Following are some limitations found in the constitution and federal statutes.

- Fourth Amendment – If you are a government agency operating a honeypot, there is a potential that the Fourth Amendment could limit your monitoring. The Fourth Amendment limits the power of government agents to search for or seize evidence without first securing a search warrant from a judge. Monitoring a user's activities on a network could possibly constitute a "search and seizure". The test for this argument is if the attacker can expect "reasonable expectation of privacy". Hackers do not have this expectation, but other users on a honeypot may. A private organization, not acting at the government's direction can operate a honeypot without worrying about violating the Fourth Amendment.
- Wiretap Act – Essentially, the federal Wiretap Act forbids anyone from intercepting communications (which includes sniffing electronic communications) unless one of the exceptions listed in the act applies. Make sure your organization understands the statute's exceptions and meets their requirements. The exceptions that need to be considered are:

  Computer Trespasser Exception – This exception states that the government may monitor a "trespasser". The operator must authorize the interception and the government must do the monitoring. Only the trespasser's communications may be intercepted and it must be relevant to an ongoing "investigation".

  Consent of a Party Exception – This exception permits an interception if a party to the communication has agreed to the monitoring. It is recommended that you install a system banner to secure consent.

  Provider Exception (System Protection) – To apply, the monitoring must be done to protect the operator's rights or property. Some facts to take into consideration are to associate the honeypot with production servers and to

separate system administration tasks from investigatory functions.

- Patriot Act – A part of the USA Patriot Act, the "computer trespasser" exception authorizes warrantless monitoring of hackers by the government in certain situations. In cases where honeypots are run under the direction of a government entity, this exception could be used. This exception allows someone acting as a government agent to sniff hacker communications if:

  - The network's operator has authorized the interception
  - The person sniffing the hacker's communications is engaged in a lawful investigation
  - That person has a reasonable bias to believe that the communications that will be intercepted will be relevant to the investigation.

4. 3 Liability

Once gaining access to your honeypot, an attacker could possibly use your network and its bandwidth to do harm to others. A neglected honeypot could be used for a variety of illegal purposes. For example, it could become a drop site for contraband such as stolen credit cards, trade secrets, and password files. It could be converted into a warez site or distribution point for child pornography. If situations such as these occur, you may be vulnerable to potential lawsuits from downstream victims. Once your honeypot is set up and deployed, do not neglect it. Be very careful to watch what is happening on your honeypot.

This is just an overview of some of the potential legal pitfalls of operating a honeypot. In addition to these three issues, it is recommended that one of the first steps taken to insure the legality of a honeypot system is to define the goals and strategies of the system. Outline exactly why the honeypot is being implemented and what information is being collected. Document all of these details extensively. There should be no misconception as to what the honeypot is for [9].

For more detailed information on these and other issues, please see http://www.cybercrime.gov. Basically, honeypots are still uncharted legal water so it is highly recommended that you talk to your own legal team when developing a honeypot in order for them to look at your particular circumstances and determine which laws apply to you. The state in which you operate your honeypot may also have its own laws, further limiting its use.

The legal risks are real. However, with a little diligence the potential for legal problems can be reduced to a minor issue.

5. Disadvantages and Advantages

If knowledge is power to the attacker, so is it to the security practitioner. Knowing both the advantages and the disadvantages of honeypots is a must-know. By knowing the inherent risks in honeypots, we can use this knowledge to mitigate these risks and circumvent the disadvantages [20]. We highlight some of these disadvantages and advantages below:

5.1 Disadvantages

Honeypots have several risks and disadvantages. Although few in number, it is these disadvantages that prevent honeypots from completely replacing your current security mechanisms.

- Limited Vision – The only activity tracked and captured by a honeypot is when the attacker directly interacts with them. Attacks against other parts of the system will not be captured unless they honeypot is threatened also.
- Discovery and Fingerprinting – Fingerprinting is when an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviors [15]. A simple mistake such as a misspelled word in a service emulation can act as a signature for a honeypot.
- Risk of Takeover – If taken over, the honeypot may be used to attack other systems, within or outside the organization. The honeypot could be used to store and distribute contraband.

5. 2 Advantages:

Honeypots have several distinct advantages when compared to the current most commonly used security mechanisms:

- Small Data Sets - Honeypots only pay attention to the traffic that comes to them. They are not concerned with an overload of network traffic or determining whether packets are legitimate or not. Therefore they only collect small amounts of information – there are no huge data logs or thousands of alerts a day. The data set may be small, but the information is of high value.
- Minimal Resources – Since they only capture bad activity, they require minimal resources. A retired or low end system may be used as a honeypot.
- Simplicity – They are very simple and flexible [14]. There are no complicated algorithms to develop, state tables or signatures to update and maintain. .
- Discovery of new tools and tactics – Honeypots capture anything that is thrown at them, which can include tools and tactics not used previously.

Reviewing these advantages show how honeypots add value and can enhance the overall security of your organization.

6. Conclusions and Future Outlook

In this paper we have provided a brief overview of what honeypots are, and what they are useful for. We have discussed the different types of honeypots such as production honeypots, research honeypots, and honeytokens. We also looked at factors that should be considered when implementing a honeypot. For example, the level of interaction of your honeypot depends on what you want to use it for. The legal issues surrounding honeypots and their implementation were examined, and throughout we mentioned the advantages of honeypots. An important point to remember is that experts advise using honeypots together with some other form of security such as an IDS.

Honeypots are a relatively new technology that is becoming increasingly popular, and will become even more so as commercial solutions become available that are easy to use and administer. Because they can be used to collect information on attackers and other threats, we believe they can prove a useful tool in digital forensics investigations.

References

1. Know Your Enemy: Honeynets. http://www.honeynet.org/papers/kye.html.

2. SANS Instituite GIAC Certification GSEC Assignment#1.4: Honey Pots-Strategic Considerations, 2002.

3. Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).

4. Baumann, R. and Plattner, C. White Paper: Honeypots, Swiss Federal Institute of Technology, Zurich, 2002.

5. Gubbels, K. Hands in the Honeypot *GIAC Security Essentials Certification (GSEC)*, 2002.

6. Harrison, J. Honeypots, the Hottest Thing in Intrusion Detection. http://www.channelinsider.com/article/Honeypots+the+Hottest+Thing+in+Intrusion+Detection/111384_1.aspx, eWeek Channel Insider, 2003.

7. http://www.honeypots.net/.

8. Jones, J.K. and Romney, G.W. Honeynets: An Educational Resource for IT Security *SIGITE '04*, Salt Lake City, Utah, 2004.

9. Kabay, M.E. Honeypots, Part 2: Do honeypots constitute entrapment? *Network World*, 2003.

10. Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. *Journal of Computing Sciences in Colleges, 20* (4).

11. Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion Detection Signatures Using Honeypots *Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II)*, Boston, 2003, 51-56.

12. Martin, W.W. Honeypots and Honeynets – Security through Deception. http://www.sans.org/reading_room/whitepapers/attacking/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.

13. Provos, N. Honeypot Background. http://www.honeyd.org/background.php.

14. Spitzner, L. The Honeynet Project: Trapping the Hackers. *IEEE Security & Privacy, 1* (2). 15-23.

15. Spitzner, L. *Honeypots : Tracking Hackers*. Addison-Wesley Pearson Education, Boston, MA, 2002.

16. Spitzner, L. Honeytokens: The Other Honeypot. http://www.securityfocus.com/infocus/1713, Security Focus, 2003.

17. Spitzner, L. Open Source Honeypots: Learning with Honeyd, Security Focus, 2003.

18. Spitzner, L. The Value of Honeypots, Part One: Definitions and Values of Honeypots, Security Focus, 2001.

19. Sutton Jr., R.E. DTEC 6873 Section 01: How to Build and Use a Honeypot.

20. Talabis, R. Honeypots 101: Risks and Disadvantages, 2.