# Honeypots: Security by Deceiving Threats

Jared LaBar, Md Minhaz Chowdhury and Mike Jochen

Computer Science Department

East Stroudsburg University

East Stroudsburg, PA 1830

Jlabar7@live.esu.edu,
Mchowdhur1@esu.edu,
mjochen@esu.edu

Krishna Kambhampaty

Computer Science Department

North Dakota State University

Fargo, ND 58102

K.kambhampaty@ndsu.edu

## Abstract

The idea of securing information is nothing new but has increasingly become a large concern in recent years. With the ever-increasing use of technology in nefarious ways, those seeking to defend against these acts are constantly seeking new and improved ways to combat against potential forms of attack. A popular approach to this problem is through the use of deception, using honeypots. Hence, studying and understanding the benefits of using honeypots technology can greatly help to combat against those who would seek to gain access to sensitive information. Honeypots make use of aggressive strategies. When utilizing honeypots, there are many challenges that can arise and need to be taken into account. Honeynets have been explained to be a complex honeypots variety that can lead to even greater benefits, and honeytokens and their ability to be nearly anything have been examined. Whether being used for research, or in production, honeypots and their varieties are a powerful and helpful security tool. This paper expounds upon what a honeypot is, their types, usage, ideas and concepts surrounding them, as well as the challenges faced with their implementation.

# 1 Introduction

The need for more robust forms of securing information has been growing rapidly over the last few years. The latest ideas to protect information have risen in the form of more aggressive techniques rather than pure defensive strategies [1]. Enter in the honeypot, a security technique making use of more aggressive strategies rather than typical passive ones.

To secure the internet, different scientific methods are popular: artificial immune system, machine learning, data mining, deception etc. The Artificial immune system is a sub field of artificial intelligence, focusing on problem solving by mimicking mammals' immune system [2]. Again, the machine learning techniques are techniques applying inference and pattern recognition in problem solving [3-5]. Also, the data mining techniques mines interesting information from large volumes of data [6, 7]. Now, it is true that deceptions are common tools of the deceivers in cyber space and incurs a loss at the victim's end [8-10]. However, such deception can also be used in defending assets. The honeypot is an example of the latter application.

A honeypot is some set of data masquerading as a genuine portion of an information system. These honeypots are set, isolated, and monitored by system administrators for any sort of unauthorized access. The honeypot is a closely monitored computing resource that the individuals monitoring want to be probed, attacked or compromised [11]. The pots are set up to seemingly contain valuable information to lure in potential attackers. Upon accessing the data within the honeypot, the attacker is detected and ideally deflected. This is helpful by allowing administrators to see what methods an attacker is employing to gain access, which provides insight as to what sort of defenses need to be erected in order to protect their real systems and data from the same methods of attack.

Honeypots can serve several purposes; some of the most important include [1]:

1. Honeypots are able to distract attackers from the more crucial machines and resources on a network.

2. Honeypots are able to provide early warning signs about new attack and exploitation trends.

3. Honeypots allow an in-depth examination of one's adversaries during, as well as after, the exploitation of a honeypot.

The main idea of the honeypot is that it should not see any sort of activity. Anyone or anything that interacts with the honeypot is seen as an anomaly. The majority of the time this means that there is some sort of unauthorized or malicious activity on the network [12].

Typically, honeypots fall into one of three main modes of interaction with an attacker. These modes are categorized as low, medium, and high interaction [13]. Each of these modes are discussed further in the background section of this paper. Honeypots are made to be used for two main purposes: production and research. Each of these purposes provide a variety of benefits and is discussed in the background section of this paper.

Expounding upon the idea of the honeypot gave rise to the honeynet. A honeynet, simply put, is a collection of honeypots contained within a network. Also, A more simplistic from of a honeypot is the idea of a honeytoken, which can be any sort of data, small or large, that is placed within a network for the purpose of luring attackers [1]. Both these topics are discussed further in the background section of this paper.

This paper is organized along the following sections: section 2 provides the background information as well as discuss relevant information concerning honeypots in order to better understand them. Section 3 discusses the concepts relating to the purpose and creation of honeypots, some of the various deception techniques used in honeypot deployment, as well as strategies concerning their implementation. Section 4 examines the advantages to using honeypots, as well as the rise of honeypots in the field of information security. Section 5 discusses the main disadvantages of honeypots, as well as some of the most important and noteworthy challenges faced when dealing with honeypots. Section 6 concludes the paper.

## 2 Background

There is such a wealth of information to learn regarding honeypots. This paper, however, touches the most common ideas surrounding honeypots in order to give a decent breadth of knowledge to readers. The following subsections present the description of what honeypots are and can be, as well as few ways honeypots are used in information security.

## 2.1 Modes of Interaction

When an attacker probes a network and ends up initiating an interaction with a honeypot, there are three main classes of which such an interaction can fall under. These three interaction classes are categorized as low, medium, and high interaction. Each of the types of interaction have advantages and disadvantages are discussed below.

1. Low-Interaction Honeypots: Low interaction honeypots are typically the easiest of the three classes to implement. This is because they are the most simplistic. Low interaction honeypots are able to provide only a very primitive emulation of certain services [13]. All the services provided by a low interaction honeypot are emulated, and thus allows the pot itself to be hardened against exploits aimed against an emulated vulnerability. An example of a low interaction honeypot is that of an emulated telnet service with only a login prompt followed prompt for a password where every login attempt is rejected [13].

2. Medium-Interaction Honeypots: Medium interaction honeypots are able to implement a more sophisticated interactions platform for potential attackers [13]. They have been designed to expect activity and are able to respond in ways beyond what a low interaction honeypot can do. Staying true to their name, medium interaction honeypots offer potential attackers a greater ability to interact than a low interaction honeypot, while at the same time providing less complex functionality than the high interaction honeypot.

3. High-Interaction Honeypots: The most complex honeypots are those that fall under the mode of high interaction. Honeypots that are of high interaction typically involve real operating systems or applications. The complexity of high interaction honeypots also causes them to be the most difficult of the three to implement. Once implemented, however, they are able to provide potential attackers with the full functional scope of an operating system, and thus offer the largest surface of attack [13]. Because of their complexity, high interaction honeypots are able to provide administrators with the greatest information regarding how attacks progress. They are also extremely helpful in identifying previously unknown vulnerabilities in a system.

## 2.2 Honeypot Uses

Honeypots are typically used for two main objectives: production and research. Honeypots being used for these purposes are designed and used in different ways.

A honeypot being used in production has the primary objective of detecting and reporting unauthorized access to a system. Production honeypots are typically used by organizations as a way to protect the organization and mitigate potential risks to their systems [1]. They are usually easy to use and most are typically low interaction based honeypots. These honeypots are deliberately placed within a production network; however, they have no production value themselves [13]. By this design, production honeypots should receive no access, and so anyone or anything accessing a production honeypot is seen as suspicious and worthy of being investigated and treated as a potential attack.

Oftentimes, organizations deploy production honeypots to reflect the attributes of their main production network, and so they invite potential attackers to interact with the honeypot. This allows for an organizations' administrators to learn of any vulnerabilities within the system, and thus are able to erect proper defenses with which to protect from like attacks in the future. Though they are able to identify and report potential attacks, production honeypots typically provide less information to administrators than a honeypot being used for research purposes [1].

The second purpose that a honeypot can be used for falls within the realm of research. Honeypots being used for a research purpose have the main goal of trying to find out and learn as much as they can about an attackers' mode of attack and the various tools used by the attacker to commit the attack [13]. They also help researchers to understand an attackers' motives and their behavior. These honeypots, unlike those used in a production network, are typically much more complex for administrators to design, deploy, and maintain [1].

Because of their complexity, however, honeypots used for research are able to capture and provide a much more detailed picture of an attack. This allows administrators to gain a vast wealth of knowledge and intelligence about methods of attack to their systems. Research honeypots are typically implemented and deployed by educational institutions such as universities, as well as the government, military, or large corporations that have interest in learning and studying more about potential current and developing threats [1]. The ability of research honeypots to gather and record vast amount of information regarding threats to security make them an invaluable tool in the ongoing fight to secure information from those that seek to exploit it.

### 2.3 Honeypot Forms

When discussing honeypots, an understanding must exist regarding the main forms that honeypots can take. Other than the typical honeypot that has been discussed previously, there exists the ideas of the honeynet and honeytoken.

The idea of the honeynet is the implementation of a large network of honeypots. The honeynets extend the concept of the single honeypot to a complex and highly controlled network of honeypots [14]. Honeynets, like honeypots, are typically used to discern the various methods and tools used by attackers. The typical honeynet architecture consists of four core elements [14].

1. Data Control: This is the goal of the honeynet to control and contain any potential attackers' activity.

2. Data Capture: Honeynets, like honeypots, should be monitoring and logging all events when interacted with by an attacker.

3. Data Collection: The collection of extensive logs regarding all of an attacker's activities during the interaction with the honeynet.

4. Data Analysis: The purpose of data analysis is being able to examine and analyze any captured and collected data from the honeynet's interaction with an attacker.

The newest form of honeypot implementation is that of that honeytoken. Honeytokens are not computers, and are instead any sort of digital entity, such as a Word document or an Excel spreadsheet [12]. They share the same idea as the honeypot and more complex honeynet in that they no one or thing should be interacting with them, and any interaction seen is automatically deemed suspicious and unauthorized.

## 3 Honeypots: Concepts & Techniques

This section examines some of the central concepts surrounding the idea of honeypots, honeypot techniques, as well as the various ways they can be implemented.

## 3.1 Concepts

The main idea and goal of the honeypot is to sense, identify, as well as confirm the presence of threats to a system. Honeypots are a resource that has no production value. It is there solely for the purpose of being attacked or compromised. The various forms of honeypots discussed previously have proven to be advantageous in improving the efficacy, as well as the productivity, of countermeasures that have been put into place for the defense of a system. Honeypots are of such value because of the information they provide through threats using them. This is quite contrary from most other types of security systems that administrators put into place. Defenders would never want a potential attacker to gain access to a firewall, for example.

This form of security can be used to identify, hinder, or halt automated attacks, as a well as capture information on newly emerging exploits in order to log intelligence on potential threats [12]. A thought-provoking concept concerning honeypots and honeynets is the idea of "adaptive behavior." This method postulates to dynamically change the honeypots based on the actions of an attacker [12].

## 3.2 Techniques

The idea of deception of one of the core principles surrounding the idea of a honeypot. The technique used to deceive must be sufficient enough to mislead an attacker, as well as convince them to initiate an interaction with the honeypot. There are various techniques which defenders can employ when seeking to deceive a potential attacker.

1. <u>Deception Service:</u> One such technique is known as a "Deception Service." A basic honeypot is used to listen to a port and raise an alarm if a certain threshold is exceeded. Deception services has been specifically designed to listen on an IP service port and respond to network requests [11]. If a malicious attacker then gains access to this simulated service, a system administrator will be able to log the individual's movements. An example of this type of deception can be seen with *Honeyd*, which is a virtual honeypot made to look like a real operation system. In *Honeyd*, all TCP ports appear to be running services, and this allows for the honeypot to deceive applications such as Nmap into thinking the pot is a legitimate operating system [11].

2. <u>OS Emulation:</u> Another deception technique deals with the emulation of an operating system. In this strategy, a honeypot is put into place using a virtual machine able to completely emulate a full operating system [11]. Some honeypot examples that utilize

this method of deception are *Vmware* and “Argos”. In this technique, the virtual machine’s operating system is not used for any particular job, and because of this, any sort of interaction with the virtual operating system is deemed suspicious.

3. Digital Bait: One final example of a deception technique used in the implementation of honeypots is the idea of “Digital bait.” This bait is a false digital object created by defenders for the potential discovery of an attacker [11]. The idea of the honeytoken discussed earlier is a form of honeypot that makes use of this deception technique. If there is any sort of interaction with or access to the honeytoken, a potential threat will be shown.

## 3.3 Implementation

The growing attention to cyber security and the protection of information and information systems has caused many system and network administrators to implement the use of honeypots in an effort to entice attackers away from their real systems and toward these phony ones.

There are two main issues that arise when implementing a honeypot. The first is the method of redirecting a potential attacker to the honeypot. The second is being able to create a honeypot that is realistic enough and genuine seeming that it persuades the potential attacker to interact with it. If these two problems have been solved sufficiently, the threat of an attack can be detected as well as confirm who/where the threat is coming from, and what they are doing [12].

In order to redirect any potential attackers away from your real system and toward your deployed honeypot, administrators must create information inside the honeypot that the attacker would want to gain access to. An example of this, in the case of defending against insider attack, is to create information that a potential attacker would not have authorized access to. Honeytokens can be used in this way and can lead an attacker toward a more advanced honeypot, or honeynet system [12]. If a potential attack has been detected, it is beneficial to attempt to redirect the attacker towards a honeynet system. These honeynets can then be used to gather a greater amount of information concerning the attacker.

# 4 The upside to Honeypots

Honeypots are an extremely popular and powerful technology. Their popularity has risen due to the various number of advantages they are able to provide system administrators and others who have worked with them. The following subsections delve into the advantages of honeypots and some of the effects that honeypots have had on the field of information security.

## 4.1 Advantages of Honeypots

Because of the main concept of honeypots being that any sort of interaction with them is to imply some sort of unauthorized or malicious activity, honeypots come with a great number of advantages. Some of the advantages they provide are quite distinct from other commonly used security mechanisms.

Some of the most useful advantages when working with honeypots include:

1. Small Data Sets: The only time a honeypot collects data is when someone or something is interacting with it. Honeypots have no concern with network traffic overloads or determining whether a packet is legitimate or not. This causes the logs they create to be small, high-value, and easy to manage [1].

2. Reduced False Positives: A huge challenge faced when implementing security detection systems is the possibility of false positives and alerts. Use of honeypots helps to curb this challenge as, as discussed previously, any activity with them is, by definition, unauthorized or malicious. Therefore, honeypots are extremely effective at detecting attacks and mitigating the possibilities of false positives [12].

3. Minimal Resources: Because of the fact that honeypots only capture and log unauthorized activity, they require only a small amount of resources. Any sort of retired, or low-end system can be used effectively as a honeypot [1].

4. Flexibility: Honeypots have become a tremendously adaptable and fluid security mechanism. They can be used within a wide range of environments. Also, anything from a SSN embedded within a database, to an entire network of computers can be used as a honeypot [12].

5. <u>New Discoveries:</u> As pointed out in Section 3.1, honeypots have the ability to detect and log anything that is not known to them. This ability allows for intelligence to be gained on newly emerging tools and tactics that had been previously unknown [1].

### 4.2 Effect on information security

The advance of technology has caused potential attackers to grow smarter over time and develop and utilize new ways to exploit vulnerabilities and cause harm. Many mechanisms to alleviate this problem have been created such as firewalls, intrusion detection/prevention systems, and encryption. However, these technologies were not skilled in predicting what would happen to a system when a new type of threat or attack was introduced. The honeypot came into being as a method of information security to solve this specific issue [15].

Because of their effective use in research into discovering new and effective methods of information security, honeypots have also become a splendid educational tool. The honeynet project at Georgie Tech has been used in network security courses as a way of teaching students how to use tools to analyze attack traffic on a network [16].

## 5 The Downside to Honeypots

This section presents the disadvantages of honeypots' use, as well as the wide array of challenges that can be faced when dealing with them. The following subsections discuss the disadvantages of honeypots, as well as the challenges faced when working with them.

## 5.1 Disadvantages of Honeypots

As with any sort of technology, honeypots are not without their own disadvantages. By knowing and gaining information regarding these drawbacks, new technologies can be created in order to alleviate them.

Some of the well-known drawbacks to the use of honeypots include:

1. Restricted Field of View: One of the advantages to honeypots discussed previously was how they produce small data sets because of only collecting information when something is interacting with them. This has also become a disadvantage in that they are unable to capture any sort of attack against other parts of a system. They only have value when interacted with directly [12].

2. Risk: Because of the main concept of a honeypot being that defenders want potential threats to interact with them, there is a risk that comes along it. If an attacker does interact with and gain access to a honeypot, there is a chance they could use the honeypot as a mechanism to attack and gain access to various other non-honeypot systems [12]. The more complex the honeypot, such as a honeynet system, the greater the risk that can arise.

3. Fingerprinting: The idea of fingerprinting is when an attacker can identify that something is a honeypot because they have discovered certain characteristics or behaviors that are expected of a honeypot [12]. Any sort of simple errors or mistakes could be telling to an attacker. A honeypot emulating a web server that responds with a common error message using HTML that is misspelled can identify the honeypot to the attacker. This disadvantage is also quite hindering to honeypots used for a research purpose. If a system designed to produce intelligence has been detected as such, the value completely diminishes.

## 5.2 Challenges

When utilizing honeypots, there are many challenges that can arise and need to be taken into account. The potential for legal issues when using a honeypot is perhaps the greatest of challenge surrounding the deployment of honeypots. Here in the United States, some legal issues that can arise from the use of honeypots are that of entrapment, privacy issues, as well as becoming liable for harm due to your honeypot being used to cause harm to others [1].

The issue of privacy is perhaps the greatest challenge faced when implementing honeypots across a system. There are quite a number of restrictions in place that can limit the ability to fully monitor a system. The violation of such restrictions could lead to legal issues for an individual or company. Two of the most important federal statutes that must be taken into account when dealing with honeypots and monitoring traffic are the Fourth Amendment to the United States Constitution, as well as the Electronic Communications Privacy Act of 1986 [1].

If an attacker is able to gain access to a honeypot, the possibility exists that they could use it to cause harm and damage to others, and thus becomes a liability with the potential to cause legal issues. Neglected honeypots are easy targets that could be used to gain access to a network or bandwidth and cause others damage or be used for a variety of illegal operations [1].

# 6 Conclusion

The growth of technology and the number of advancements of new and improved techniques deployed by hackers and attackers helped to bring about the creation of honeypots. As such growth and advancements continue, the use of honeypots as an aggressive bulwark in the ongoing fight of information security has greatly risen. This research paper has provided and discussed a basic synopsis of honeypots. The main concept surrounding honeypots of their goal being to sense, identify, and confirm the presence of threats to a system has been discussed in detail. Honeypots are such a unique security mechanism in how they are purposely deployed to be tampered with by attackers.

This paper has discussed some of the common types and formats of honeypots. Whether being used for research, or in production, honeypots are a powerful and helpful security tool. The honeynets have been explained to be a complex honeypot variety that can lead to even greater benefits, and honeytokens and their ability to be nearly anything have been examined.

Various techniques have been identified and discussed regarding the use of deception in honeypot design. Though only three methods were presented, there are a multitude of further ways to deceive that are just as effective. This deception helps to realize a honeypots’ goal of redirecting potential threats away from real/valuable systems and toward itself. This paper has also discussed the various advantages gained, as well as disadvantages and challenges faced when utilizing a honeypot.

Though they are a somewhat new tool, honeypots are constantly evolving and gathering us new intelligence. This has caused them to be such a beneficial and popular tool in the field of information security.

## References

[1] I. Mokube and M. Adams, Honeypots: Concepts, Approaches, and Challenges, *The 45th Annual Southeast Regional Conference*, Winston-Salem, North Carolina, 2007.

[2] Md Minhaz Chowdhury, Jingpeng Tang and Kendall E. Nygard, An Artificial Immune System Heuristic in a Smart Grid, *The 28th International Conference on Computers and Their Applications*, Waikiki, Honolulu, Hawaii, USA, December 2013.

[3] Md Minhaz Chowdhury and Kendall Nygard, Machine Learning within a Con Resistant Trust Model, *The 33rd International Conference on Computers and their Applications (CATA 2018),* Flamingo Hotel, Las Vegas, Nevada, USA, March 19-21, 2018.

[4] Rahul Gomes, Mostofa Ahsan and Anne Denton, Random Forest Classifier in SDN Framework for User-Based Indoor Localization, *The 2018 IEEE International Conference on Electro/Information Technology*, Rochester, Michigan, USA, 3-5 May 2018.

[5] Mostofa Ahsan, Rahul Gomes and Anne Denton, SMOTE Implementation on Phishing Data to Enhance Cybersecurity, *The 2018 IEEE International Conference on Electro/Information Technology*, Rochester, Michigan, USA, 3-5 May 2018.

[6] I. Jahan and S. Z. Sajal, Stock Price Prediction using Recurrent Neural Network (RNN) Algorithm on Time-Series Data, *The Midwest Instruction and Computing Symposium (MICS 2018),* Duluth MN, USA, April 6-7, 2018.

[7] I. Jahan and S. Z. Sajal, Prediction on Oscar Winners Based on Twitter Sentiment Analysis Using R, *The 2018 SDSU Data Science Symposium*, Brookings SD, USA, February 11-12, 2018.

[8] Md Minhaz Chowdhury, Kendall E. Nygard, Krishna Kambhampaty and Maryam Alruwaythi, Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm, *The 4th Annual Conference on Computational Science & Computational Intelligence*, Las Vegas, NV, USA, December 2017.

[9] Md Minhaz Chowdhury and Kendall E. Nygard, An Empirical Study on Con Resistant Trust Algorithm for Cyberspace, *The 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing*, Athens, Greece, July 17-20, 2017.

[10] Md Minhaz Chowdhury and Kendall E. Nygard, Deception in Cyberspace: An Empirical Study on a Con Man Attack, *The 16th Annual IEEE International Conference on Electro Information Technology*, Lincoln, Nebraska, U.S.A, May 14-17, 2017.

[11] M. T. Qassrawi and Z. Hongli, Deception Methodology in Virtual Honeypots, *The 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, Volume 02, Pages 462-467, April 24 - 25, 2010.

[12] L. Spitzner, Honeypots: Catching the insider threat, *The 19th Annual Computer Security Applications Conference,* Las Vegas, Nevada, 2003.

[13] M. Valicek, G. Schramm, M. Pirker and S. Schrittwieser, Creation and Integration of remote high interaction honeypots, *The International conference on software security and assurance*, Altoona, Pennsylvania, 2017.

[14] P. Pisarcik and P. Sokol, Framework for distributed virtual honeynets, *The International Conference on Security of Information and Networks*, Glasgow, Scotland, 2014.

[15] R. Tiwari and A. Jain, Improving Network Security and Design using Honeypots, *The CUBE International Information Technology Conference*, Pages 847-852, Pune, India, September 03 - 05, 2012.

[16] K. Sadasivam, B. Samudrala and T. A. Yang, Design of Network Security Projects using Honeypots, Journal of Computing Sciences in Colleges, Volume 20, Issue 4, Pages 282-293, 2005.