A Design of Hybrid Honeypot System for Malicious Code Security

Moongoo Lee

Department of Cyber Security, Kimpo University

yeon0330@kimpo.ac.kr

Abstract —*In order to protect information asset from various malicious code, Honeypot system is implemented. Honeypot system is designed to have attack eliciting purpose in order to not accept internal system attack, or it is designed to purpose of malicious code information collection. Therefore, this study offers hybrid Honeypot that offers internal information system security function and information collection for malicious security. This provides a security preemptive response effect about malicious code but also information security analyze for recent hacking techniques and attacking tool as well.*

Key words —Malicious code, Honeypot, Vulnerable service, Drive-by-download

I. INTRODUCTION

Recent malicious code infection is proliferated through a way of Drive-by download that are infected instantly when the user connect to malicious web site during web surfing instead of vulnerable service attack through network. [1]

Malicious code circulating way through Drive-by-download is possible to infect clandestinely to the user. It is easy to infect web servers at once where a number of users connect by using Drive-by-download as of attacking medium. Through this process, the user who was infected to malicious code can cause the second damage such as personal information extort, DDoS attack, spam mail send. [2]

Those malicious code infect has a possibility to proliferated fast to the public when smart phone to become popular. Therefore, a substitute way of spreading malicious code such as Drive-by download is a honeypot. Honeypot is a system to get actual attack after making security actual vulnerable of computer system in order to offer a good circumstance where malicious code can attack easily.[3][4] As attackers are lead to attack through Honeypot, malicious code information are collected, and through this they offer a detect way against malicious code. In this paper, we suggest an existing type of Honeypot, and a solution to solve these problems such as analysis time delay and separated execution of each Honeypot. And that offered such as hybrid Honeypot operation principle, basis functions and architect design, logic design. In chapter 2, this study introduces operating principle, operation effect that are based on Honeypot category and architect, and the chapter 3 explains hybrid Honeypot compose that this study suggests, and the last chapter 4 depicts hybrid Honeypot strength and expected effects.

II. RELATIVE RESEARCHES

A. *Honeypot operation purpose and expectation effect*

A purpose of honeypot or honey net is to do an advanced detection and advance correspond against security detect standard prepare adaption, attack detection that are not known, and analysis of trend, recent hacking behavior, and malicious code analysis such as hacking action. And the expectation effect has to research internal infra invasion status in order to prepare basis of internal deduction invasion. Thereby, homepage malicious code integrity inspection has to be achieved.

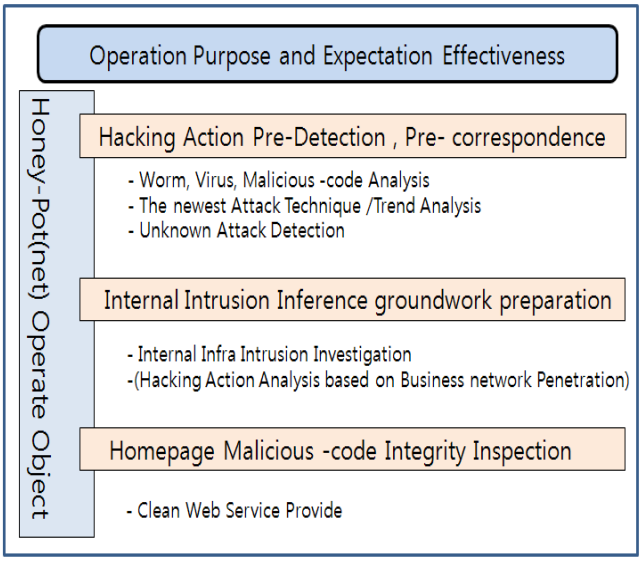

Fig. 1 . Operation Purpose and Effectiveness of Honeypot

B. *The type of Honeypot*

Honeypot can be separated of two categories. One is for honeypot system that purposes to tempted offense in order to not get internal system attack by using honeypot system. The other is a honeypot system, composing of information

collection purpose to study detection technique for corresponding with henceforth attack.

■ A Purpose of Attacking Eliciting

Honeypot that has a purpose of tempted attack disguises client's web page and as offering a camouflaged attractive content is a way of leading attack's inflow actively, and it has a purpose of protecting internal system of information assets that leads attacker's invasion such as hacking and protects itself.

This attack tempted purpose honeypot should be exposed to hackers easily, and it should be looked as weak to be hacked easily. Therefore, it is not easy to tempt for crackers if we do as what crackers do. Therefore, network that is composed of a number of honeypot, in other words, honey net. [5][6]

This honeypot of attack eliciting purpose should be exposed to hackers easily, and it should be looked as vulnerable to be hacked easily. Therefore, it is not easy to tempt for crackers if we do as what crackers do. Therefore, network that is composed of a number of honeypot, in other words, honey net.

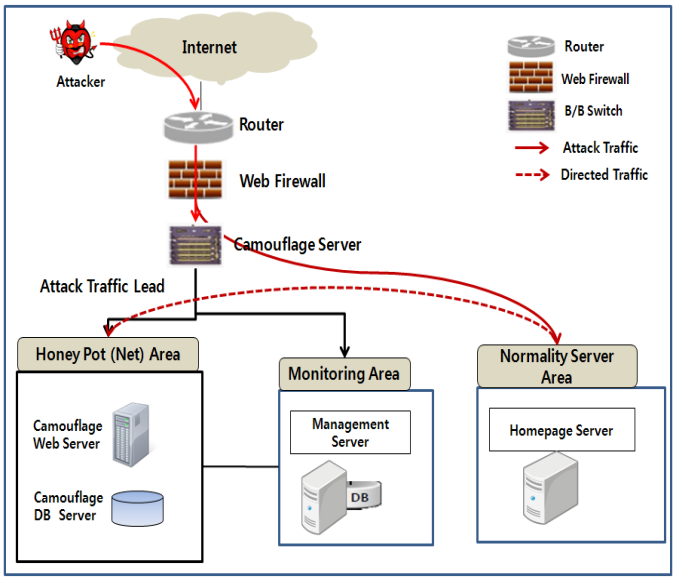

Fig. 2. Honeypot of Attack Eliciting Purpose

An attack eliciting purpose of Honeypot is able to analyze trend with hacking technique detection to strength information collective power, and applying analyze result, it is possible to have a preemptive protective correspondence as inspecting system's vulnerable point in advance and preemptive application of security technique standard detection.

■ A Purpose of Information Collecting

As fraud server in purpose of malicious code information collecting, and as analyzing manually software that is installed in server from outside, malicious code acquires detected information. Due to the fact that this code has a purpose of collecting information about a way and acting of hackers, it is not easy to lead crackers as acting Honeypot itself in order to deceive as of real service network after leading crackers because it has to be isolated from a real service network while it offers the same network environment. Therefore, a network where composed of a number of honeypot, in other words, it has been processing actively to study honey net composition. This honeypot has a purpose of information collection, as shown in Fig. 3.

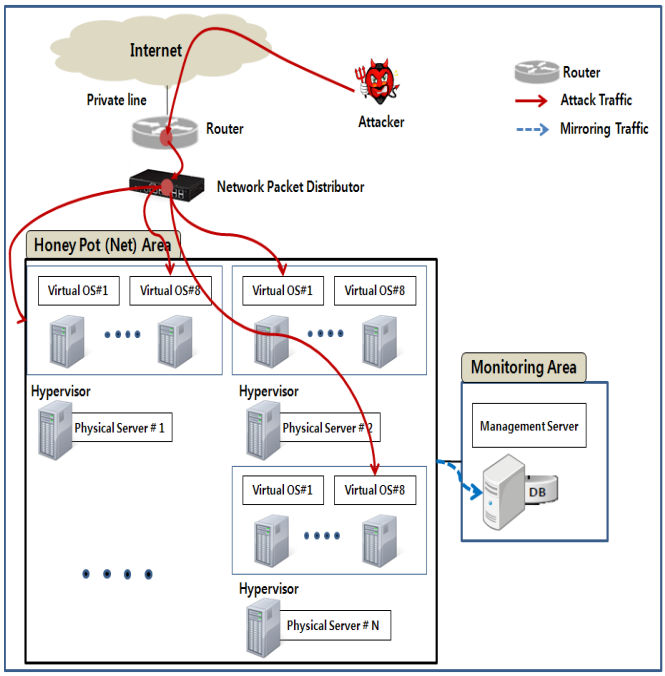

Fig. 3. Honeypot of Information Collecting Purpose (ex1)

Another example of honeypot that has a purpose of malicious code information collection operates disguised client server as we can see in Fig. 4, is an another way of visiting web page in order to analyze and collect of malicious doubtful software.

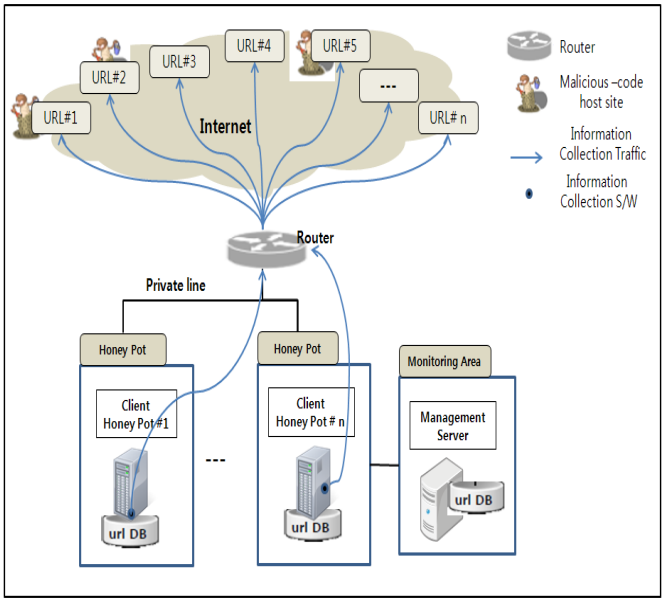

Fig. 4. Honeypot of Active Information Gathering Purpose (ex2)

III. THE HYBRID HONEYPOT

A. A Concept of a Hybrid Honeypot

Since the attacking eliciting and information collection were executed separately in a previous version of Honeypot, it had a problem that a malicious code delayed analysis time. Therefore, we suggested a hybrid honeypot to solve those problems. There exists low-level false response server and high-level real service disguised server in hybrid honeypot. Those hybrid honeypot acting type 1 leads to analyze high level honeypot hacking behavior of attacker and execute its analyze, and the second acting type 2 executes false response through the requests from an attack tool, and analyze attacker's characteristic. Therefore, a hybrid honeypot analyzes internal penetration behavior and collects attack tool information.

B. The 10 Requirements for the Hybrid Honeypot Design

The ten of required condition is organized as Fig. 5 for hybrid honeypot architect. It is a necessary requirement that honeypot has to prepare for the secure of malicious code and hybrid honeypot that is possible to complete information collection and internal system security should be build where it satisfies this necessary requirement.

Criterion	Honeypot System Top 10 Requirement
Faking	1. A component of Normal System has to be prepared, having information and services that lead to attack.
Proactive	2. Active information collection way should be prepared.
Logging	3. Full Packet Dump should be conducted to all traffic that is pass through honey pot
	4. Traffic information and behavior information should be recorded and integrated collection.
Analysis	5. Collected information should be automatic analyzed through system.
	6. Analyzed result should be reported and applied to center security equipment.
Visually	7. Real time monitoring that integrated every honey pot should be executed through single dashboard.
Safety	8. Other system's damage should not spread that is caused by single system accident. (Function unit division to contrast the entire system paralysis, and protection for hacking accident division/barrier obstacles through firewall)
Hiding	9. A way to minimize explosion of operating purpose should be included. (Encryption communication for composition system, process-hidden function related to honey pot, operating system root account change, and etc).
Flexibility	10. A details of composition of honey net should be changed flexible through the need. (Internal invasion inspection requirement and post management according to operation purpose exposure).

Fig. 5. The 10 Core Requirements for Honeypot Design

C. The Architecture of the Hybrid Honeypot

Hybrid Honeypot should be separated by operating system for system management and information collection as well.

Network is also divided up to information collection and network management. For the implementation, as leading attacking traffic as we represent in Fig. 6, it designs low- level interface honeypot and honey wall that is a virtual machine transmitting to the point of high-level interface honeypot. Therefore, information collection and network management system operates as of it is separated.

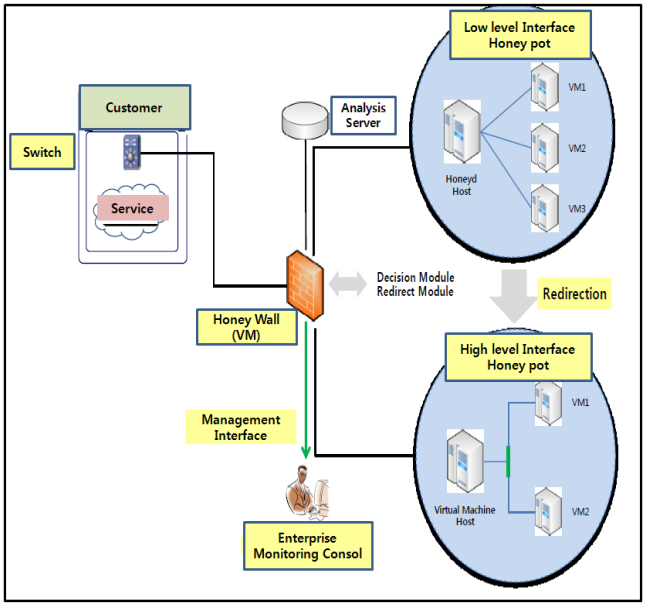

Fig. 6. The Hybrid Honeypot Architecture Design

D. The Logical Design of the Hybrid Honeypot

Hybrid Honeypot executes hacking technique, trend and information analyze, and through that information it offers preemptive security response.

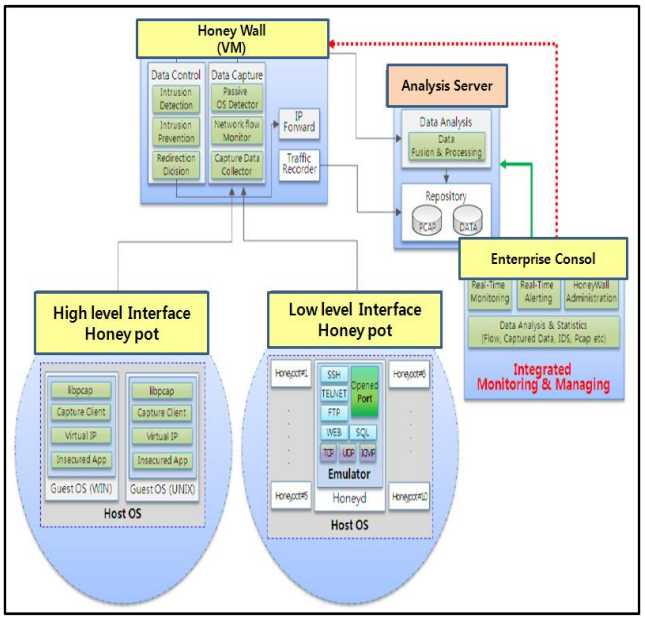

Fig. 7. The Hybrid Honeypot Logic Design

The TABLE I explained for hybrid honeypot configuration and technique briefly.

TABLE I
THE HYBRID HONEYPOT CONFIGURATION AND TECHNIQUE

Division	Module name	Function
High level Interface Honeypot	Host/Guest OS	Service Support of OS Virtualization
	Capture Client	Capture of Malicious behavior and trans Honey wall
	In-secured APP (VM)	Server of Attacker eliciting Purpose
High level Interface Honeypot	Honey demon	Emulator demon
	Honeypot	Virtual Honeypot
	Emulator	Perform of untruth response
Honey Wall	Data Control	Perform of Intrusion detection based on snort
	Data Capture	Perform of Intrusion prevention based on snort-inline
	IP Forward	Attacker traffic transfer low-level Honeypot to high-level Honeypot
	Traffic Recorder	Dump of real-time all traffic
Analysis Server	Data Analysis	Low-level and high-level honey wall correlation analysis and save to repository
	Repository	Save of original data, correlation analysis result, traffic dump
Integrated Consol	Real-time Monitoring	Monitoring real time analysis result of analysis server.
		Monitoring of system status
	Real time Alerting	Real time alert monitoring based on Alert Rule
	Administration	Honey wall management of monitoring, alert rule
		Support of analysis method, statistic management technique

IV. CONCLUSION

Recent malicious code infection is detailed as similar as Drive-by download and threatened with information asset as to proliferate or infect from malicious code once it connects to malicious web sites during the user is doing web surfing.

In order to protect information collection from those malicious codes, there are several ways to implement honeypot system. This study suggested hybrid honeypot where low-level false respond server exists and disguised high-level service.

Therefore, hybrid honeypot analyze not only internal invasion behavior but also collects attacking rate, and it executes information analyze of attacking rate, trend, and hacking techniques. As through that information, it is designed to offer preemptive security response effect. In later, this study will plan to implement a designed hybrid honeypot.

REFERENCE

[1] Empirical study of drive-by-download spyware. http:// cisr.nps.navy.mil/ downloads/ 06paper_spyware.pdf

[2] Niels P., Thorsten Holz, "Virtual Honeypots from Botnet Tracking to Intrusion Detection", Addison-Wesley, 2007.

[3] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser analysis of web-based malware", HotBots'07, pages 4-10, 2007

[4] D. Barroso, ″Botnets-The Silent Threat,″ ENISA Position Paper, Nov. 2007.

[5] ″Know Your Enemy Honeynets,″ http://www.honeynet.org, 2006

[6] ″Honey nets in Universities,″ http://www.honeynet.org, 2004

BIOGRAPHIES

Moongoo Lee became a Member (M) of IEEE and IEIE in 2002. I received B.S. from Dept of Computer Science, Soongsil University in 1984, M.S. from Ewha Woman's University in 1993, and Ph.D. from Dept of Computer Science, Soongsil University in 2000. I am now a full professor in Department of Cyber Security of Kimpo University. Seoul, KOREA. My research interests include Information Security, Algorithm Design, and other fields of Computer Science.