



Politecnico di Torino

# Cybersecurity for Embedded Systems

## 01UDNOV

Master's Degree in Computer Engineering

# Honeypot mechanisms for IoT clusters

## Project Report

Candidates:

De Luca Antonio (s282133)

Guglielminetti Iacopo (s290289)

Manca Edward (s292493)

Silvano Francesca (s282021)

Referents:

Prof. Paolo Prinetto

Dr. Matteo Fornero

Dr. Vahid Eftekhari

---

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Background</b>	<b>3</b>
2.1	Honeypot . . . . .	3
2.2	According to the level of interaction . . . . .	3
2.3	According to the purpose . . . . .	4
2.4	According to the location . . . . .	4
2.5	According to the implementation . . . . .	5
<b>3</b>	<b>A closer look to various honeypot typologies</b>	<b>6</b>
3.1	Malware Attacks and Countermeasures . . . . .	6
3.1.1	Malware attacks . . . . .	6
3.1.2	Malware Honeypots . . . . .	7
3.2	Web application honeypot . . . . .	10
3.2.1	DShield Web Honeypot . . . . .	10
3.2.2	Glastopf . . . . .	11
3.2.3	Comparison between glastopf and DShield Honeypot . . . . .	11
3.2.4	SNARE and Tanner . . . . .	12
3.2.5	Solution of Honeypot with SNARE . . . . .	13
3.3	Virtual Honeypot . . . . .	14
3.3.1	A tool for virtual honeypot: Honeyd . . . . .	15
3.4	DoS attack . . . . .	17
3.4.1	Different type of Dos attack . . . . .	17
3.5	MITM attack and honeypots . . . . .	19
3.6	FAKEHONEYMITM (MITM attacks and honeypots) . . . . .	20
3.7	Eavesdropping Attack and Countermeasures . . . . .	21
3.7.1	Eavesdropping Attack . . . . .	21
3.7.2	Encrypting the channel . . . . .	21
3.7.3	Physical Countermeasures . . . . .	22
3.7.4	Impulsive Statistical Fingerprinting . . . . .	22
3.7.5	Active Eavesdropping - ML approach . . . . .	22
3.7.6	Possible Honeypots . . . . .	23
3.8	Password Attack and countermeasures . . . . .	23
3.8.1	List of counteracts and considerations . . . . .	23
<b>4</b>	<b>Implementation Overview</b>	<b>24</b>
4.1	Case of study 1: Cluster and Honeypot for a Ransomware attack . . . . .	24
4.2	Case of study 2: Cluster and Honeypot for a DoS attack . . . . .	25

---

4.2.1	Structure of the IoT cluster for the project . . . . .	25
4.2.2	DOSPOTPY and climatOffice . . . . .	27
<b>5</b>	<b>Implementation Details</b>	<b>29</b>
5.1	Case of study 1: Cluster and Honeypot for a DoS attack . . . . .	29
5.1.1	Instruments used . . . . .	29
5.1.2	First structure of the IoT cluster . . . . .	29
<b>6</b>	<b>Results</b>	<b>32</b>
6.1	Known Issues . . . . .	32
6.2	Future Work . . . . .	32
<b>7</b>	<b>Conclusions</b>	<b>33</b>
<b>A</b>	<b>User Manual</b>	<b>34</b>
<b>B</b>	<b>API</b>	<b>35</b>

---

# List of Figures

3.1	Gradual responses to file changes according to thresholds set by the admin. . . . .	8
3.2	Example architecture of system with honeypot and machine learning. . . . .	9
3.3	Structure of DShield honeypot . . . . .	11
3.4	Flow of attack in DShield and Galastopf . . . . .	12
3.5	Structure of SNARE and TANNER . . . . .	13
3.6	Structure of the honeypot . . . . .	14
3.7	Structure of the honeyd . . . . .	15
3.8	Implementation of honeyd . . . . .	16
3.9	TCP handshake protocol . . . . .	18
3.10	TCP SYN flood attack . . . . .	18
3.11	An example on MITM attack . . . . .	19
3.12	A possible system structure for the MITM honeypot. . . . .	20
3.13	A possible structure for the fake sensor honeypot and MITM . . . . .	21
4.1	Examble scenario of honypot against ramsonware attacks. . . . .	24
4.2	IoT network scheme with IPS. . . . .	26
4.3	IoT network scheme with IDS. . . . .	27
4.4	IOT network scheme level 2 with IPS . . . . .	27
4.5	An example of the climatOffice IoT cluster . . . . .	28
5.1	Our simple IoT cluster with an high-interaction honeypot . . . . .	30
5.2	Our simple IoT cluster with a low-interaction honeypot . . . . .	30

---

## List of Tables

---

# Abstract

This is the space reserved for the abstract of your report. The abstract is a summary of the report, so it is a good idea to write after all other chapters. The abstract for a thesis at PoliTO must be shorter than 3500 chars, try to be compliant with this rule (no problem for an abstract that is a lot shorter than 3500 chars, since this is not a thesis). Use short sentences, do not use over-complicated words. Try to be as clear as possible, do not make logical leaps in the text. Read your abstract several times and check if there is a logical connection from the beginning to the end. The abstract is supposed to draw the attention of the reader, your goal is to write an abstract that makes the reader wanting to read the entire report. Do not go too far into details; if you want to provide data, do it, but express it in a simple way (e.g., a single percentage in a sentence): do not bore the reader with data that he or she cannot understand yet. Organize the abstract into paragraphs: the paragraphs are always 3 to 5 lines long. In  $\text{\LaTeX}$ source file, go new line twice to start a new paragraph in the PDF. Do not use to go new line, just press Enter. In the PDF, there will be no gap line, but the text will go new line and a Tab will be inserted. This is the correct way to indent a paragraph, please do not change it. Do not put words in **bold** here: for emphasis, use *italic*. Do not use citations here: they are not allowed in the abstract. Footnotes and links are not allowed as well. DO NOT EVER USE ENGLISH SHORT FORMS (i.e., isn't, aren't, don't, etc.). Take a look at the following links about how to write an Abstract:

- <https://writing.wisc.edu/handbook/assignments/writing-an-abstract-for-your-research-paper/>
- <https://www.anu.edu.au/students/academic-skills/research-writing/journal-article-writing/writing-an-abstract>

Search on Google if you need more info.

---

---

## CHAPTER 1

---

# Introduction

This document aims at providing an overview of the state-of-the-art regarding honeypots and provide an implementation of Honeypot inside a cluster IoT.

Due to the fact that exists various type of honeypot, two solutions has been presented for different type of cluster and attack. One solution for a honeypot in a (tipologia?) cluster that protects from Malware attacks and the other for a tree structured cluster that protects from DoS attacks. (Da modificare alla fine) The first chapter shows the criteria according to which you can classify honeypots; the second chapter gives a closer look to some of the possible honeypot typologies and the third chapter described the two use cases; an appendix with useful links is present in the last chapter.

In this first chapter we expect you to introduce the project explaining what the project is about, what is the final goal, what are the topics tackled by the project, etc.

The introduction must not include any low-level detail about the project, avoid sentences written like: we did this, then this, then this, etc.

It is strongly suggested to avoid expressions like ‘We think’, ‘We did’, etc...it is better to use impersonal expressions such as: ‘It is clear that’, ‘It is possible that’, ‘... something ... has been implemented/-analyzed/etc.’ (instead of ‘we did, we implemented, we analyzed’).

In the introduction you should give to the reader enough information to understand what is going to be explained in the remainder of the report (basically, expanding some concept you mentioned in the Abstract) without giving away too many information that would make the introduction too long and boring.

Feel free to organize the introduction in multiple sections and subsections, depending on how much content you want to put into this chapter.

Remember that the introduction is needed to make the reader understand what kind of reading he or she will encounter. Be fluent and try not to confuse him or her. The introduction must ALWAYS end with the following formula: The remainder of the document is organized as follows. In Chapter 2, ...; in Chapter 3, ... so that the reader can choose which chapters are worth skipping according to the type of reading he or she has chosen.

---

## CHAPTER 2

---

# Background

### 2.1 Honeypot

This chapter covers the study of honeypot taxonomy.

A honeypot is an expedient that aims at attracting or tricking somebody or something. It has to be vulnerable and a realistic environment at the same time, resulting in an appealing decoy for attacks. A honeypot could be built for a specific purpose, as well as for more generic ones, it could be implemented exploiting hardware and/or software and disposed in different position inside the network. For what concern IoT systems, a honeypot represents a vulnerable environment that has to be targeted by hackers and then collect data about attacks, study their features and the tools used by the attackers. Many criteria are available to distinguish honeypots, some of which are listed below.

### 2.2 According to the level of interaction

**Low-interaction honeypot:** Honeypots belonging to this category have limited interaction with external systems.

There is no operating system for attackers to interact with, they represent targets to attract or attackers to detect by using software that emulate features of a particular operating system and network services on a host operation system.

The main advantage of this type of honeypot is that it is very easy to deploy and maintain and it does not involve any complex architecture.

On the other hand, it shows some drawbacks: it will not respond accurately to exploits. This drawback lowers the capability of detecting attacks.

Low-interactive honeypots are a safe and easy way to gather info about the frequently occurring attacks and their source. Some examples of low-interaction honeypots are listed below:

1. ADBHoney;
2. Heralding;
3. Honeyppy;
4. HoneySAP;
5. Dionaea.

**High-interaction honeypot:** this is the most advanced honeypot class. These honeypots offer a very high level of interaction with the intrusive system. They give more realistic experience to



attackers and gather more information about intended attacks; this also involves very high risk to catch of whole honeypot.

High-interaction honeypots are most complex and time consuming to design and manage. Also they are very useful when we want to capture details of vulnerabilities or exploits the ones that are not yet known.

**Medium-interaction honeypot:** also known as mixed-interactive honeypots.

Medium-interaction honeypots are slightly more sophisticated than low-interaction honeypots, but less sophisticated than high-interaction honeypots. They provide the attacker an operating system so that complex attacks can be attracted and analysed.

## 2.3 According to the purpose

**Production honeypot:** This honeypot typology is used as a defense instrument by an organization or on networks.

It could be deployed within the production network of the organization where services are placed and exposed.

These honeypots study and analyse attacks received and then help to strengthen the perimeter of the network. Such honeypots could also find and report some vulnerabilities of the environment used in the production network.

**Research honeypot:** Research honeypots are born with a purpose similar to production honeypots, but they have some different features.

Their main purpose is the improvement of defensive and prevention tools, with slightly different strategies with respect to the production honeypots: the latter ones are more generic.

Research honeypots usually look for new types of malware and, moreover, these honeypots are the most used ones when redacting articles and papers for the cybersecurity community, in order to provide the best knowledge.

Research honeypots don't always simulate the environment of an organization network, they search for attacks faded to common infrastructure or solutions.

This type of honeypot could be classified in more categories: the **anti-spam honeypot**, that studies the strategies adopted by spammers, the **malware honeypot**, that is more focused on the analysis of malicious software. In general, they are focused on strategies and techniques adopted by hackers for some specific types of attacks, on the vulnerabilities that these can exploit and on the malicious files that can be diffused.

All the information that can be collected about these attacks assume a fundamental role and need to be saved in ad-hoc infrastructure. A detailed analysis of this data could allow a prevention from future attacks. For example, anti-virus industries use this kind of honeypot to update their database of attacks with the newly discovered malware.

Research honeypot have a more complex architecture. They are usually put outside from the organization network to avoid propagation of possible attacks and to gather all possible information since they are more exposed to attacks. The kinds of services that are exposed by these honeypot types require an accurate selection, the same for tools used and data stored.

## 2.4 According to the location

The honeypot could be placed:

**Outside the network,** before the firewall, in this case the contact with the production network of the organization is null. This approach is used in research honeypots.

**Inside the network:** it emulates the real environments of the production network, and monitor possible attacks that act on the latter.

Here the visibility on attacks is complete, but a risk that the production network is attacked through the honeypot itself needs to be taken into account.

**Inside the demilitarized zone :** DMZ is a network logically divided from the organization network. It has the purpose of offering some services to the public network. This solution is a compromise between the first and the second one.

## 2.5 According to the implementation

**Physical honeypot:** a real system with hardware and software connected through an IP address to the network;

**Virtual honeypot:** a software honeypot that simulates a configuration on an hardware.

In the background chapter you should provide all the information required to acquire a sufficient knowledge to understand other chapters of the report. Suppose the reader is not familiar with the topic; so, for instance, if your project was focused on implementing a VPN, explain what it is and how it works. This chapter is supposed to work kind of like a "State of the Art" chapter of a thesis. Organize the chapter in multiple sections and subsections depending on how much background information you want to include. It does not make any sense to mix background information about several topics, so you can split the topics in multiple sections.

Assume that the reader does not know anything about the topics and the technologies, so include in this chapter all the relevant information. Despite this, we are not asking you to write 20 pages in this chapter. Half a page, a page, or 2 pages (if you have a lot of information) for each 'topic' (i.e. FreeRTOS, the SEcube, VPNs, Cryptomator, PUFs, Threat Monitoring....thinking about some of the projects...).

---

## CHAPTER 3

---

# A closer look to various honeypot typologies

In this section the research focuses on providing deeper details about specific attacks and classes of honeypots used to contrast them:

- Malware Attacks and Countermeasures;
- Web Application Honeypot;
- Virtual Honeypot;
- DoS Honeypot;
- MITM attack and honeypots;
- Eavesdropping Attacks and Countermeasures

### 3.1 Malware Attacks and Countermeasures

#### 3.1.1 Malware attacks

Malware attacks are common cyberattacks that exploit malicious software to execute unauthorized actions on the victim's system.

The burst of the internet contributed to a vast spread of various malware types. Among the most known types, there are:

- **Ransomware**, malware that threatens to publish the victim's personal data or block the access to it unless a ransom is paid, encrypting data with malicious intent. Such attacks are usually carried out using a *trojan* disguised as a legitimate file (for instance, an attachment to an email) and relying on poor social engineering skills of the users. However this is not always the case, as the *WannaCry* ransomware proved, exploiting a vulnerability of the structure it spread across. The user immediately detects a ransomware attack due to payment warnings that pop up.
- **Spyware**, malware that is particularly hard to detect. It collects information about the victim's internet searches or even credit card data. Email attachments or download from file-sharing platforms represent typical injection methods for such malware. The victim usually experiences unusual behaviors of the system, such as new search engine tools.

### 3.1.2 Malware Honeypots

Defending yourself from malware attacks might not be trivial. Many people rely on antivirus software, that offers protection either for free or on subscription.

Many antivirus firms rely on research honeypots to update their knowledge about the software that must be labelled as "dangerous" and create a *malware signature* that can be stored in a database of known threats.

You can use malware honeypots to update such databases, they are supposed to act as a decoy for attackers. In some cases, they should also incentive the attacker to infect a system, in order to study the behavior of the malicious software. This is the case of high interaction honeypots, that can even simulate entire systems in order to be more appealing for attackers.

On the other hand, you can also just use malware honeypots to defend yourself from attackers.

Literature offers multiple ways you can design and deploy malware honeypots, ranging from simple to complex solutions. Some of the studies are listed below:

1. The usage of sentinel files in a network against ransomware;
2. The monitoring of changes in files within a short interval of time;
3. The usage of software diversification;
4. The usage of machine learning algorithms.

#### Sentinel Files

A simple honeypot that intends to defend the system against ransomware, both the ones already known to antivirus database and those not yet listed, could make use of sentinel files.

Such files act as *trip wires* for the trap to be triggered. You keep the original hash digest of the sentinel files aside. Since ransomware tend to encrypt data, if an attack is in progress you will see more and more files changing content. The strategy simply aims at monitoring changes in the digest of the sentinel files, in order to detect a ransomware attack and shutdown services before it spreads. These files do not provide any production value and therefore every interaction with them (changes or removal) is to be considered malicious.

This is one of the few ways to deal with ransomware, since it is a particularly tough malware to defeat, it enters the victim's systems encrypted and so an infection is nearly impossible to prevent.

#### Frequent changes to files

Some malware families aim at making the system busy by performing frequent changes to files within a short time period. For small networks, you can monitor all file accesses and set a threshold above which you can state that probably a malware attack is in progress.

Heuristics can help since setting a low threshold might not allow authorized actions and a high threshold might not detect malware activities properly.

You can link thresholds of file changes to various degrees of response, as shown in the figure below.

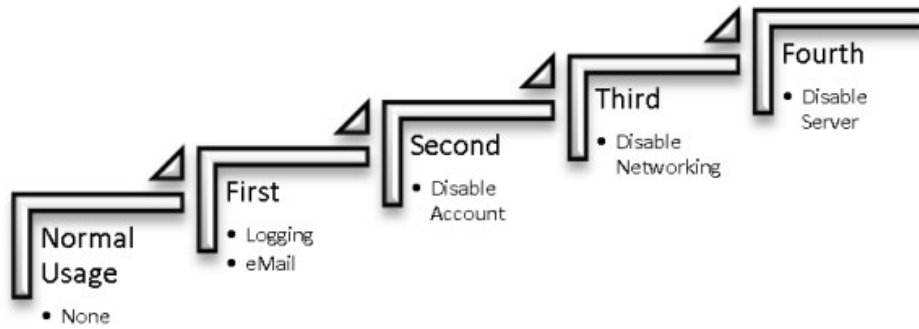


Figure 3.1: Gradual responses to file changes according to thresholds set by the admin.

This mechanism allows you to set your response gradually, avoiding to shutdown all services at once and therefore avoiding to have a large recovery time once the system is restarted.

A proprietary solution called *EventSentry* offers this file integrity monitoring service, letting the user deploy a honeypot that monitors files of interest via GUI.

### Software Diversification

Studies prove that one of the keys for the success of malware attacks is that attackers rely on the so-called "software monoculture". In other words, it is much more likely that an attack is successful when the software implementation of the victim's system or infrastructure is easy to guess.

A *system call* is the way for a computer program to interact with the kernel of the operating system on which it is executed.

Two sets of system calls (well-known ones and hidden ones) can detect attacks if you let the trusted nodes only use the hidden ones, that are less likely to be guessed. Any traffic on the network that relies on the interface of well-known system calls is to be considered as malicious.

This solution allows you to let malware run freely and without any risk to the assets you want to defend. Thus, you can study the behavior of the malware and gather more information about it.

A drawback of this approach is that the malware attack could utilize the code already present in allowed operations.

### Machine Learning algorithms

Literature is full of machine learning-based approaches regarding malware detection. They all use some kind of malware classifier whose purpose is to distinguish between malicious and benign software, with a certain degree of confidence. Here the system exposes some fake service and learns how to defend itself thanks to a training period that exploits a training data set, called "EMBER" as described in the article "The Endgame Malware BENCHMARK for Research" [?], which provides 900.000 training samples.

A classification technique often adopted in malware detection is the Decision Tree Algorithm, that classifies them based on malware features and behavior.

When a malware is detected the honeypot gives some details to the admin, which is supposed to be a cybersecurity expert, who can validate or deny the classification, making the algorithm train even further.

As an example, ransomware always carry a message through which the user is warned that they should pay a ransom (often asked in untraceable currency, like bitcoins) to get their data back from the malicious encryption. This feature could be exploited for defense purposes because as soon as a malicious text is spotted through key words such as "pay", "blocked", etc you stop its spread.

This is clearly just an example since ransomware might not carry this message, or it might be encrypted. A high training period with a wide training data set could help you spot malware by features (e.g., some peculiar file size and code fragments) rather than by a ransom message.

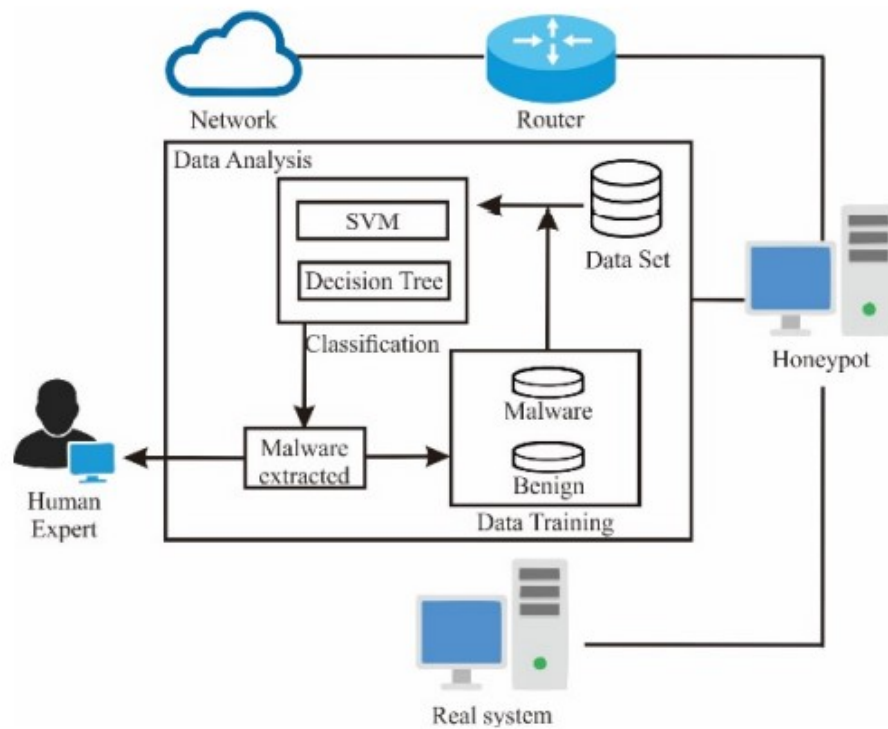


Figure 3.2: Example architecture of system with honeypot and machine learning.

## 3.2 Web application honeypot

End-user applications are an intrinsic part of an IoT infrastructure. These help users in monitoring and controlling IoT devices from remote locations.

These applications transmit user commands to the cloud, and subsequently, to IoT-enabled devices connected to the network.

Mobile apps, web apps and desktop apps are the end-user applications found in an IoT infrastructure. Web applications often get attacked causing a break into confidentiality and integrity of information using:

- **SQL injection:** This is a type of attack granted by the fact that SQL doesn't check that whoever modifies the database has permission and a lack of input validation in web application can cause the success of this attack. The attacker can insert structured Query Language code as parts of final query string into a form that causes a web application to generate and send a query that works differently than the programmer intended;
- **Cross-site scripting (XSS):** An XSS allows a cracker to insert or execute client-side code in order to collect, manipulate and redirect confidential information, or even view and modify data on servers or alter the dynamic behavior of web pages using any language ( example JavaScript, VBScript, Flash);
- **Remote file inclusion attacks(RFI):** This attack is caused when an application builds a path given by the user via variable without checking its origin. The attacker modifies an user variable in the URI (example GET POST in PHP) perhaps adding maligns executable code, the web application downloads and runs the remote file;
- **Local file inclusion attacks(LFI):** This attack is very similar to the previous one, in this case the application only executes files included in the server so the attacker inside the script tricks the application including another malignous script to execute.

In these cases a honeypot can be very useful.

The Honeypot can individuate the IP source of the attack, the purpose of the attack (if there was the intention of destroying or modifying the database etc), which methods are used by the attacker to capture data and what is the most attacked part of the database.

The Web application Honeypot must respond to the attacker in a best possible way to better deceive him/her.

### 3.2.1 DShield Web Honeypot

The idea of this Honeypot starts with DShield, a firewall log correlation system used by the SANS institute to collect logs received by volunteers worldwide and analyze them providing which IPs are more dangerous, which port are more used for attacks etc etc.

The honeypot is a low-latency one that collects logs from web apps adding them to all the logs that already are sent to DShield, this logs contains the URL and header information such as IP address, host, user agent, referring from all requests (even harmless ones) and, after being checked with expressions in *config.txt* file, they are saved inside the logs folder of the honeypot and then posting it to the DShield database (this is done every 30 minutes).

The honeypot works in a simple manner: on the inside it contains a set of templates and a login system; when an attack takes place, the template is chosen checking inside the set if a suitable one is present (if there is no template , it returns a default web page), the honeypot sends the response to the attacker meanwhile the request is logged and sent to the DShield database.

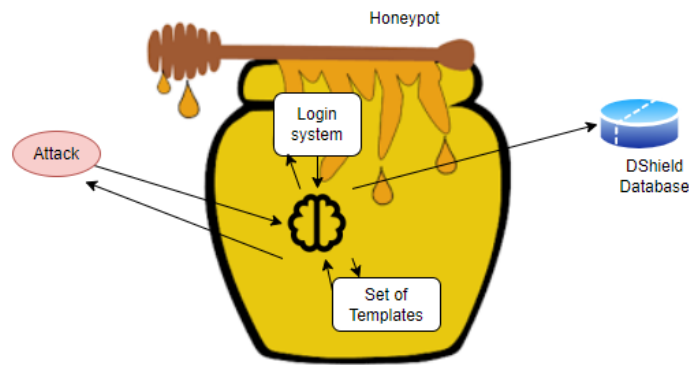


Figure 3.3: Structure of DShield honeypot

All of this idea can be download for free, this because all the logs are useful to the project. It is also used by home connection to collect data (as a peer to peer net "the more the better").

### 3.2.2 Glastopf

Glastopf is a very old Python web application low-interaction honeypot able to produce web applications vulnerable also to SQL injection. Glastopf manages to emulate vulnerability types, this allows us to manage multiple attacks of the same type until the attacker finds another fail in the web application or a new attack method.

Attackers will find the web service and try to attack the system, it is detected and gets logged by the honeypot that inserts all the information in the logs file (or database).

It has a good capability of logging based on the interaction that an attacker would have with the application but it shows some limitations: the front-end part is quite primary and attackers can easily recognize that this is not a real system and it only supports SQL injection, remote (RFI), and local file inclusion(LFI) vulnerabilities.

### 3.2.3 Comparison between glastopf and DShield Honeypot

In the paper of 2014 ,*The Behavioural Study of Low Interaction Honeypots: DSHIELD and GLASTOPF in various Web Attacks*[], the interaction of these two honeypots with various attacks is put in comparison.

DShield and Galastpof have similar working techniques.



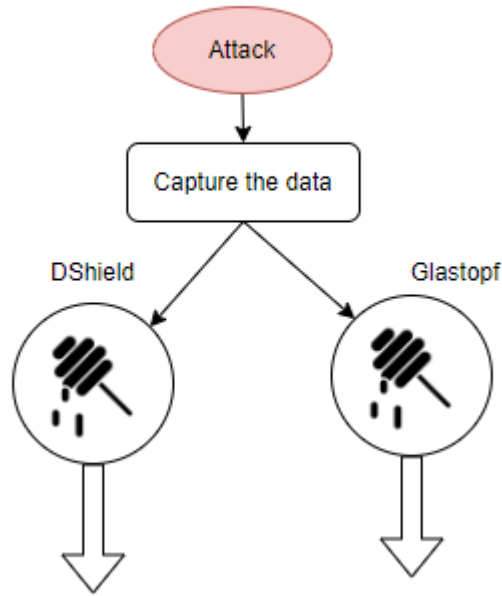


Figure 3.4: Flow of attack in DSshield and Glastopf

DSshield has a better ability to categorize the type of attack and by means of Apache server it is possible to extract a report. On the other hand, it is not easy to go through the logs and understand attacks easily.

Galastopf has logs that are easy to understand and they also capture the HTML information that is posted within the request, the response from the server and response code (200 OK) confirming that the attack was successful on the other way cannot categorize the SQL injection and XSS and the logs generated for Remote File Inclusion attacks were lesser compared to Dshield.

### 3.2.4 SNARE and Tanner

SNARE (Super Next generation Advanced Reactive honEypot) is a web application honeypot sensor attracting all sort of maliciousness from the Internet.

It pays attention to the web site, in fact has an inbuilt Cloner that, invoked before SNARE, clones all the web pages given as input, all the images on the web pages, scripts and action elements so that the clone looks as good as a real system.

SNARE needs TANNER to work. It is a remote data analysis and classification service to evaluate HTTP requests and composing the response then served by SNARE. TANNER uses multiple application vulnerability type emulation techniques when providing responses for SNARE, so it creates each time a new session for a new attack, each session tries to detect the attacker (if it is a tool, an user or a crawler), the location of the attack and shows through the TANNER UI for the administrator statistics regarding how many attacks of that kind have been found; after that, it emulates the response (via an emulator) and gives the attacker the response as the website would do.

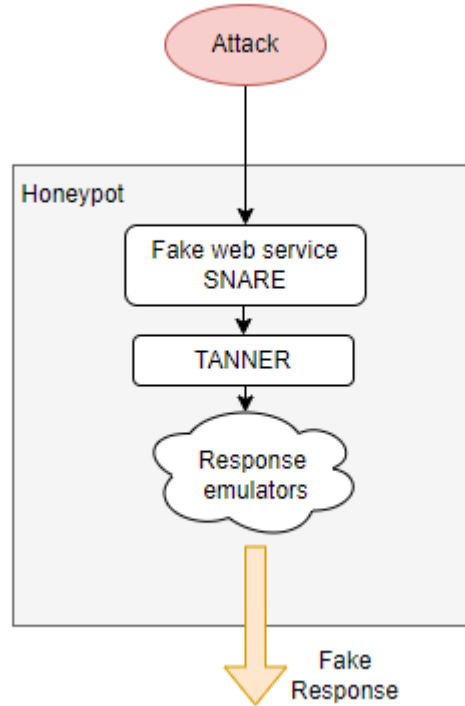


Figure 3.5: Structure of SNARE and TANNER

### 3.2.5 Solution of Honeypot with SNARE

In the paper *An Innovative Security Strategy using Reactive Web Application Honeypot* [?], a solution for a web application honeypot which includes many emulators for very complex vulnerabilities is proposed. Its structure is the following one:

1. SNARE: It serves all the web pages on top of itself, becoming a server and hence monitoring all the HTTP events/flows throughout the application, similar to a real system;
2. TANNER: It analyzes the requests made through SNARE after that it generates the responses dynamically;
3. Database: for attack classifications;
4. Docker: Docker is used to create containers for the emulators; The emulator creates a container for different custom images, executes the payload of the attacker, takes the credible result and deletes the container so that libraries are used inside a container and cannot damage the system, the honeypot remains secure;
5. Emulation engine: every event on SNARE has to pass through all types of emulators: GET, POST and cookies emulators;
6. PHP Sandbox (PHPOX): it returns emulation results for emulators like PHP object/code injection, XXE injection, and RFI;
7. Base Emulator: it manages all the other emulators supporting multiple vulnerabilities and prepares the custom page for the injection;

8. Template Injection Emulator: this emulator imitates the Template Injection vulnerability. The input payload is matched with the element in the database to identify the type of attack, then it is injected into the docker vulnerable custom template of that type and, after the execution, the final results are sent to SNARE;
9. XML External Entity (XXE) Injection Emulator: same story of the Template injection Emulator. It emulates XML External Entity Injection vulnerability and Out of Band XXE Injection as well;
10. PHP Object/Code Injection Emulator: it emulates the PHP Object Injection vulnerability. The injection results are sent to SNARE from PHP sandbox so the code is executed in PHP sandbox safely;
11. Attacker/Crawler Detection: it allows to detect if the attacker is a crawler or a tool and tries to get the owner.

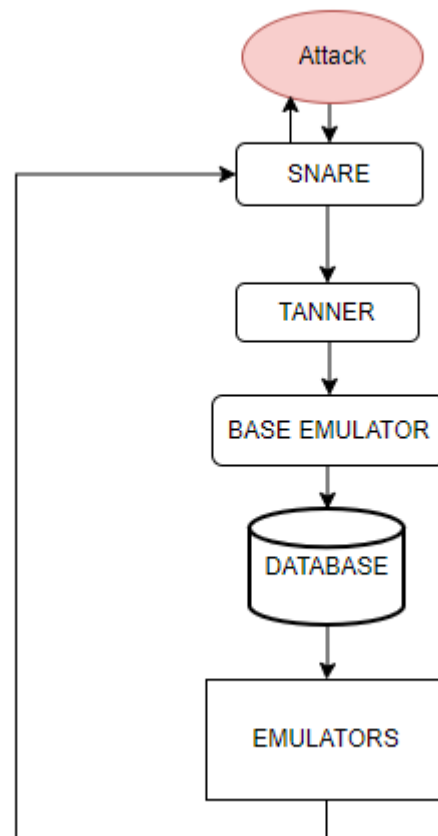


Figure 3.6: Structure of the honeypot

### 3.3 Virtual Honeypot

A virtual honeypot is a software that emulates a vulnerable system or network to attract intruders and study their behavior, It is easy to implement and unlike hardware-based, it can contain in a single

Virtual machine multiple honeypots implemented for different purposes and since it is all emulated it does not allow infiltrations from the outside that can use the same virtual honeypot to attack the system, but because it is completely emulated, a skilled hacker can see the difference from the real system.

### 3.3.1 A tool for virtual honeypot: Honeyd

Honeyd is a small daemon that creates virtual hosts on a network. It creates low-interaction honeypots that emulate service of a real OS. It allows you to create multiple virtual honeypots (each with a different ip) by sharing the resources of the same server.

The server via TCP / IP protocol, based on the destination IP address, chooses which honeypot to serve.

It only supports TCP, UDP and ICMP protocols.

Honeyd, as explained in the article [?] is designed for Unix systems and (as the other low-interaction honeypot) it has no OS installed, it has the advantage of run several different operating systems at the same time, each ip has his port to make the service listen and return different fake message returning them to the hacker, this fake message are generated by personality engine to make it look good and logical according to the template.

The template is a virtual machine where we can set which port are open, which OS is running etc. each port can be set to be open with a script running on it to simulate the service.

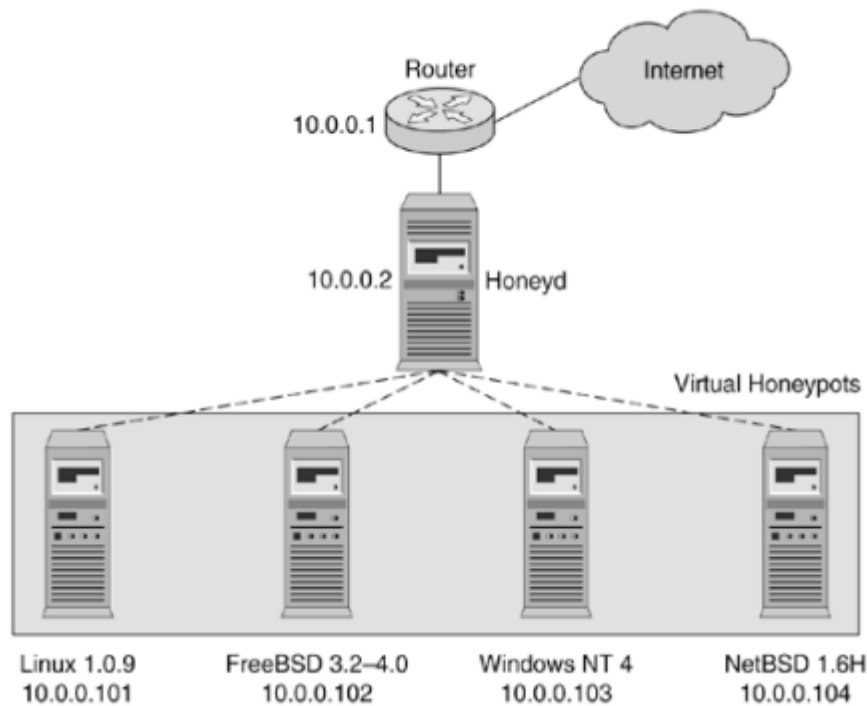


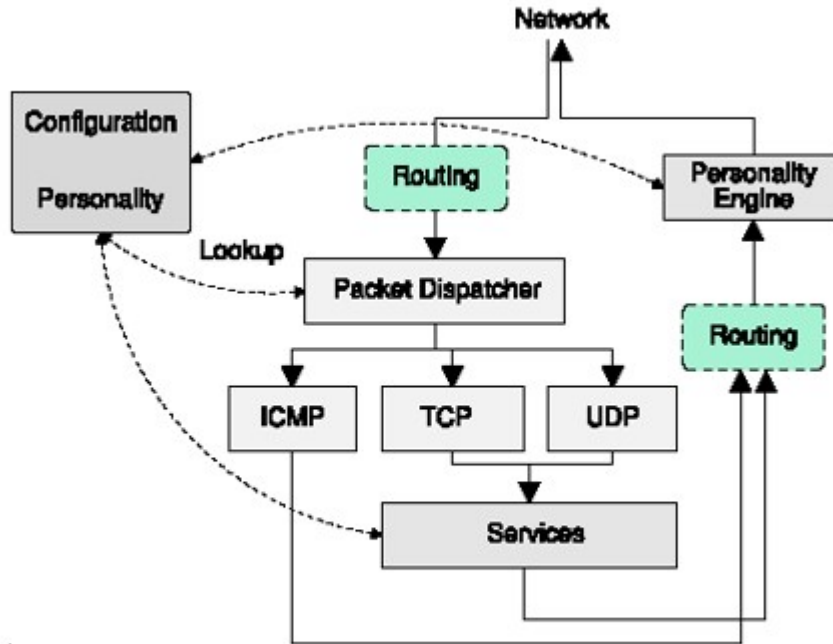
Figure 3.7: Structure of the honeyd

The file Honeyd.conf contains the configuration for the virtual network .

Once the template is fixed we can set the IP addresses, at the end we create a network that seems

real for the attacker.

As soon as a packet arrives, the dispatcher checks that the IP is valid in the configuration file, in the absence of the IP a default model is sent back.



Progetto Honeyd – Architettura di Honeyd

Figure 3.8: Implementation of honeyd

Upon receipt of a request, the framework checks whether the packet concerns an already established connection and in this case forwards it to the corresponding service, otherwise a new process is created for its execution. In addition to local services, a connection redirection mechanism is supported through which it is possible to route a service request to a real system. Personality engine and configuration engine works together to decide the protocol for transferring according to the configuration (transport and link layer), so before returning the packets to the network, the personality engine modifies the headers to make them compatible with the stack used in the machine's SO.

Since attackers often use tools to scan the network and know the operating system running on the system, by default Honeyd uses Nmap's fingerprinting database as a reference for TCP headers and Xprobe's for ICMP headers. In this way he tries to deceive the attackers with their own weapons. Since both the DOS Honeypot and Malware Honeypot works with TCP/IP protocol, we think it should be a good idea to run this daemon inside one Raspberry Pi and generate both the honeypots in virtual. Honeyd is a very interesting low interaction honeypot but its problem is its age, apparently the project is outdated and nobody seems to upgrade it.

Another problem given by age is that hacker tools are evolving during time so identifying this honeypot is not so hard.

Now with a basic scan it is possible to find which ports are open, connect to them and as soon as the connection is established the hacker (based on the response the honeyd provide) understand quickly that something is wrong and abort the attack.

## 3.4 DoS attack

A DoS attack takes place when a client is used by the attacker to flood with TCP and UDP packets one target server overriding the resources of a system so that it cannot respond to service requests of legitimate users. This causes bandwidth saturation and the exhaustion of computing resources, even leading to a server crash.

A DDoS attack takes place when multiple systems target a single system with a DoS attack, more difficult to be tracked because the attack is launched by various positions.

Citing an example, one major use of IoT is home automation systems. If an attacker attacks the main server of such a system with a DoS attack, the whole system tends to shut down and any appliance within the whole house (sometimes even door locks) are made inaccessible. This small example shows the significance of security implementation in IoT. In IoT-based networks new devices that enter the network are configured automatically due to its open nature. This leaves such networks prone to a lot of attacks. The open nature of IoT makes it relatively easy for spammers and attackers to infiltrate IoT networks and launch DoS attacks.

### 3.4.1 Different type of Dos attack

Unfortunately exist very different type of Dos attack, based on the protocol that are using, if the aims is crash services or flood services. For example in a yo-yo attack the attacker generates a flood of traffic until a cloud-hosted service scales outwards to handle the increase of traffic, then halts the attack, leaving the victim with over-provisioned resources. When the victim scales back down, the attack resumes, causing resources to scale back up again. An example of TCP attack is **SYN Flood Attack**. To better understand it we need a closer look on how TCP initialize a connection between a client and a server.

The algorithm used by TCP to establish and terminate a connection is called a three-way handshake. The idea is that two parties want to agree on a set of parameters, which, in the case of opening a TCP connection, are the starting sequence numbers the two sides plan to use for their respective byte streams. In general, the parameters might be any facts that each side wants the other to know about. First, the client (the active participant) sends a segment to the server (the passive participant) stating the initial sequence number it plans to use (Flags = SYN, SequenceNum =  $x$ ). The server then responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, Ack =  $x + 1$ ) and states its own beginning sequence number (Flags = SYN, SequenceNum =  $y$ ). That is, both the SYN and ACK bits are set in the Flags field of this second message. Finally, the client responds with a third segment that acknowledges the server's sequence number (Flags = ACK, Ack =  $y + 1$ ). The reason why each side acknowledges a sequence number that is one larger than the one sent is that the Acknowledgment field actually identifies the "next sequence number expected," thereby implicitly acknowledging all earlier sequence numbers. To better understand the step to establish the connection, please refer to the figure below.

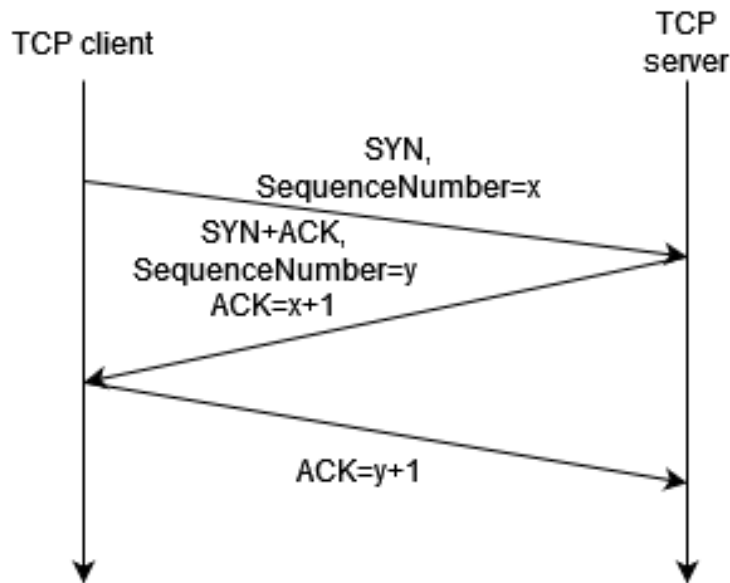


Figure 3.9: TCP handshake protocol

An attacker that want to establish a **SYN Flood Attack** create a bot that create thousands of first segments in the 3-way handshake protocol. Then when the server reply with the SYN-ACK packet, the bot client never reply to it in order to make thousands of incomplete request of connection to the server to slow down it. Please refer to the picture below.

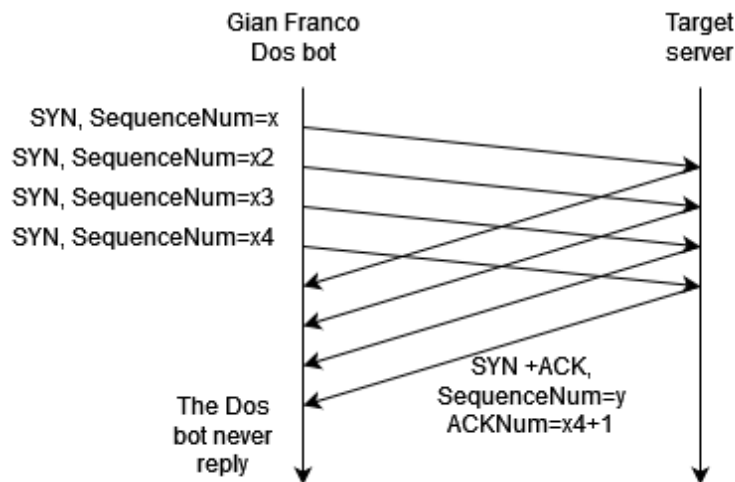


Figure 3.10: TCP SYN flood attack

Now, the following question is, could we use honeypots to avoid this type of TCP attacks? According to what we found on internet, to protect our servers from the **SYN Flood Attack**, is better to:

- Installing an IPS to detect anomalous traffic patterns;
- configure the onsite firewall for SYN Attack Thresholds and SYN Flood protection;
- Installing up to date networking equipment that has rate-limiting capabilities.

So honeypots are not useful to prevent that.

### 3.5 MITM attack and honeypots

In a server-client architecture, a MITM attack takes place when the attacker is inserted inside the communication between client and server. Let's make an example of possible situation that could occur, and a proposal of honeypot that could resolve it.

The normal procedure to avoid MITM attack is to encrypt and decrypt data between client and server. The main steps are:

1. **Use asymmetrical encryption.** First we use an asymmetric algorithm to allow us to send in a secure way the symmetric key that will be used in the future;
2. **Use symmetric encryption.** Now that the symmetric key is shared between the server and the client, the data are sent normally between the ends points and not anyone in the middle can understand them.

What if the first step fails? As an example, our IoT server for example could use a weak RSA algorithm, based on 16 bit key. Our men in the middle could manage to find the private key of the server and decrypt the symmetric key that will be used in the second step, like shown in the figure below.

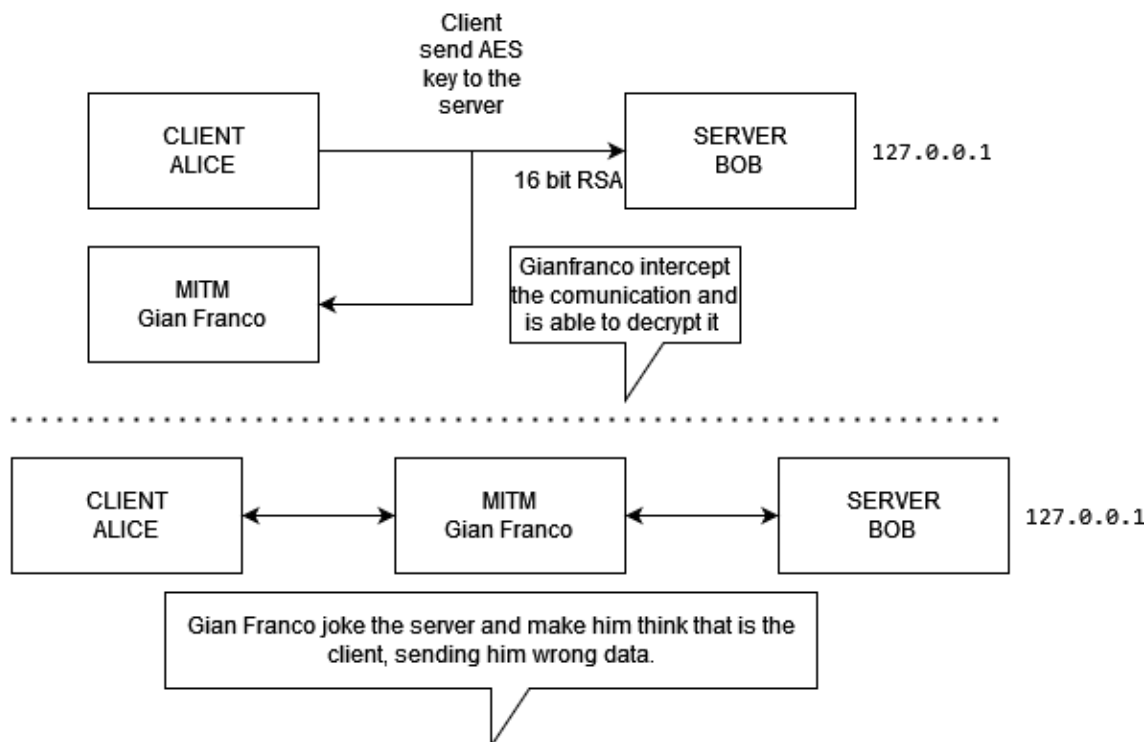


Figure 3.11: An example on MITM attack

How can our system understand that it is speaking to a MITM and not to the client? Our honeypot would intervene right here.

For example, it could first check if the wrong data sent by the MITM makes sense or not. Then it could check if the data of the fake sensor makes sense with respect to a set of data collected from the real sensor in the precedent days. If the honeypot recognizes that a man in the middle is present, it could collect data about the hacker and see what information they are trying to capture, which attacks he/she is trying to inject in to the network, studying the methodology used by hackers. Moreover, a honeypot AP could (at least temporarily) keep the hacker engaged and alert the administrator so



that the actual network can be safeguarded, then close the collection. If no violation is detected, the honeypot sends the data to the real server. A possible implementation is shown in the figure below.

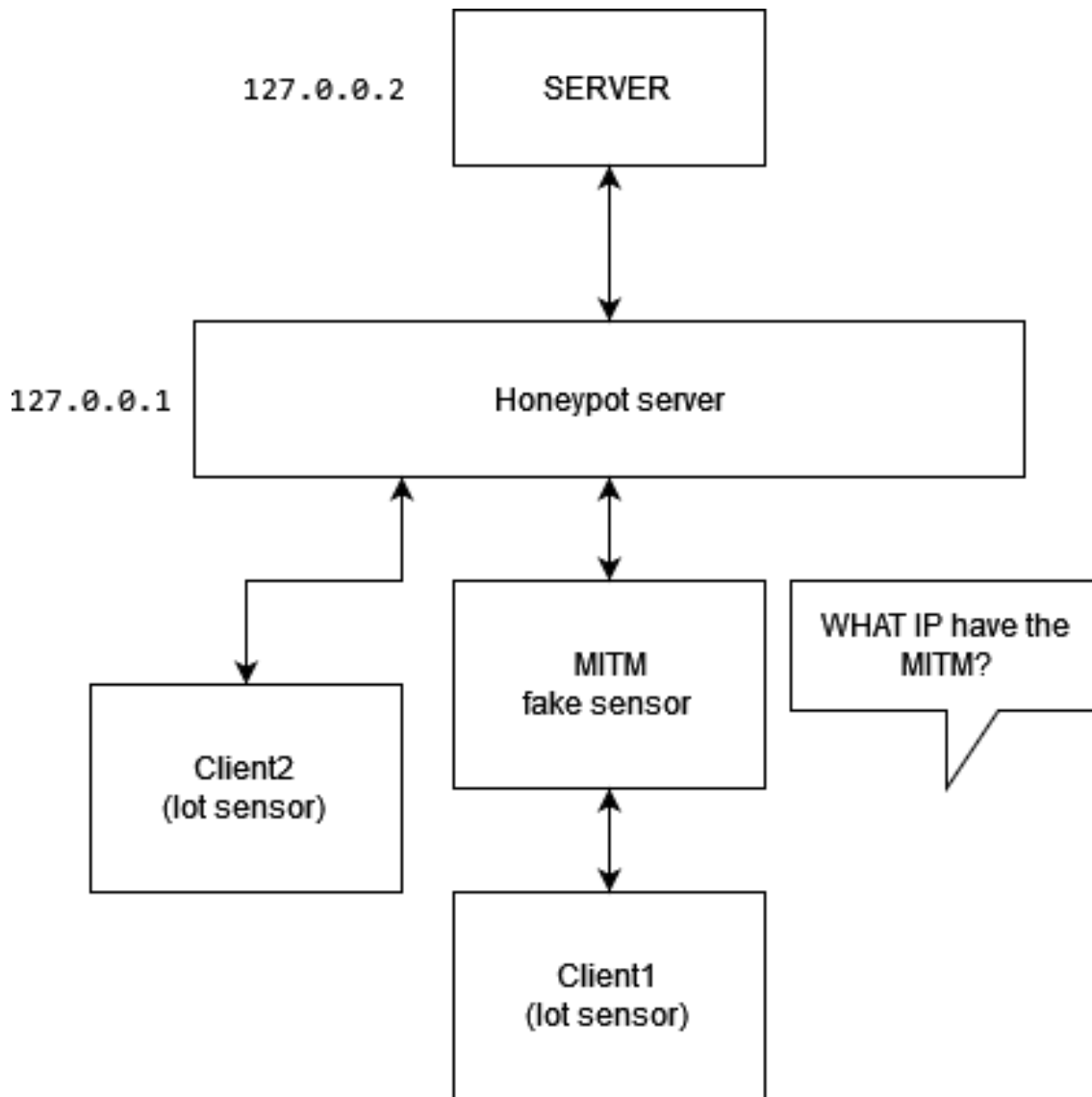


Figure 3.12: A possible system structure for the MITM honeypot.

### 3.6 FAKEHONEYMITM (MITM attacks and honeypots)

Regarding the MITM attack, we have another possible idea to implement. As we know, a man in the middle tries to place himself between the sensors of the IoT cluster and the servers inside the network. He needs to intercept the message from the sensors to the servers and viceversa. But what if the sensor is not real but is a honeypot? For example, our cluster could expose a connection between 2 honeypots, the first one is a fake server, the second one is a fake sensor. But why an attacker would choose this connection for his malicious purpose? Well, this link could work with a weak encryption to seem like a vulnerability of our network. When the MITM manages to put itself between the fake connection, our honeypots could collect data on the activity of the hacker. To better understand this

idea, please refer to the figure (3.13)

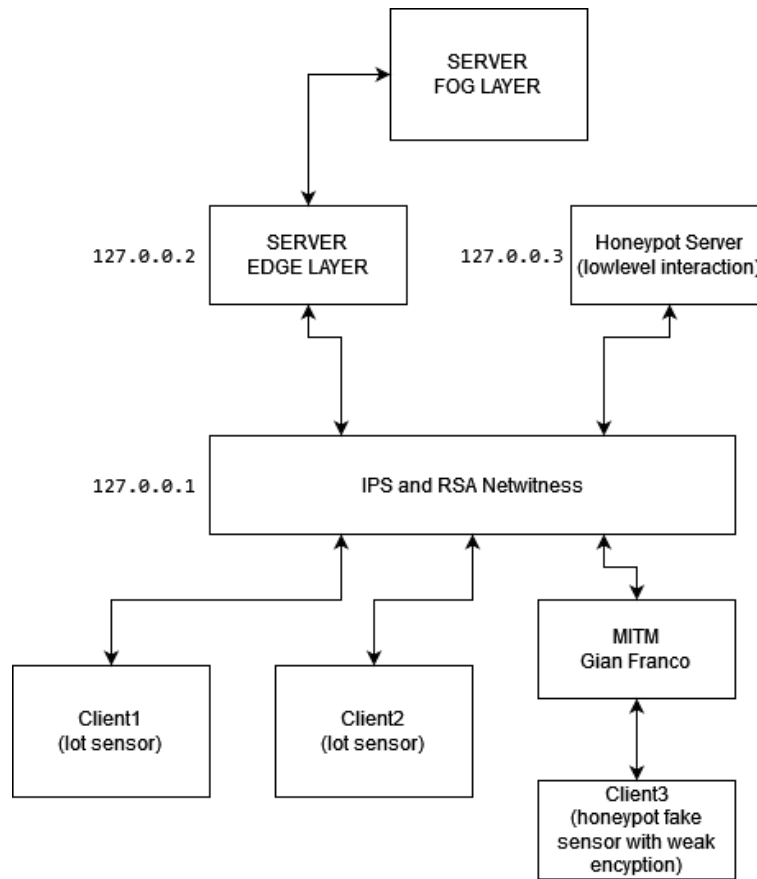


Figure 3.13: A possible structure for the fake sensor honeypot and MITM

## 3.7 Eavesdropping Attack and Countermeasures

### 3.7.1 Eavesdropping Attack

In eavesdrop attack the network is sniffed in order to retrieve information transmitted through the network itself; the process can be classified as passive or active depending on the existence of an interaction of the attacker on the network. Specifically, a passive attack is performed just analyzing packets of information on the eavesdropped network channel, while an active attack is performed requesting directly to the channel information the attacker wants to retrieve.

To counteract eavesdropping phenomena on a network several possibilities are present, always keeping in mind that the desired objective is to maintain secrecy of transmitted information.

### 3.7.2 Encrypting the channel

The most straightforward method to secure a channel communication is to encrypt the transmitted data, in this way even if the channel is sniffed data are secured (assuming a safe key maintenance and management). This solution is great for networks/clusters of powerful computers or for application that require not sending too many data, otherwise the risk is to spent most of the time computing cryptographic algorithms instead of computing for the cluster purpose. Mitigations could be the

design of specific hardware to accelerate those computations; this implies that the applicability of this solution is impossible for most of the cheap low-cost low-power IoT-cluster applications.

### 3.7.3 Physical Countermeasures

#### Intelligent Reflecting Surface

A solution is proposed in the article *"Eavesdropping with Intelligent Reflective Surfaces: Threats and Defense Strategies"* [?] will enhance the point-to-point communication between the sender and the receiver making it impossible for the attacker to read the channel. This result is obtained exploiting properties of reflecting surfaces able to dynamically re-adapt and focus the connection to one specific point. Specifically, the channel for the attacker is worsened to a level of binary gibberish securing the information in the meanwhile.

#### Channel Capacity and Information Freshness

Other techniques are related to evaluating the capacity of the two receiving nodes (the actual receiver and the eavesdropper), CD and CE, and trying to set a network transmission protocol to make the eavesdropper unable to receive the data up to a given secrecy level RS as perfectly described in the paper *"Relay Selection for Wireless Communications Against Eavesdropping: A Security-Reliability Tradeoff Perspective"* [?]

For systems in which the useful information is related to the freshness of the obtained data and the only secrecy that matters is the one aimed in protecting the newest data (we can imagine systems analyzing the position of cars on the road) other metrics have been developed ("secrecy age" and "secrecy age outage") as the article *"Secure Status Updates under Eavesdropping: Age of Information-based Physical Layer Security Metrics"* [?].

### 3.7.4 Impulsive Statistical Fingerprinting

This method is trying to move in the direction of cryptographic methods, without the usage of standard cryptographic algorithms. The point of this technique is to remove information that makes the data understandable before transmitting it. The method relies on the exchange of fingerprints (e.g. time-stamps) between the source node and the destination node. These fingerprints are then used to compute statistics using some algorithms (final results will be mean, std deviation, other order momentum, and so on..) and to manipulate data before transmitting those by manipulations like removing the mean, whitening the data by dividing it by the std-deviation, etc. This method is suitable for the usage on low-performance IoT-clusters; on the other hand it is not mathematically secure: the method relies on the fact that an attacker will not be able to get a sufficient number of fingerprints to then be able to retrieve information on the transmitted data.

### 3.7.5 Active Eavesdropping - ML approach

All of previous remedies are for passive eavesdropping. For active eavesdropping there is the necessity to treat requests through the channel. Common possibility is to reduce the permission of requests from class of nodes. Another approach is to exploit ML to perform anomaly-detection classifying series of actions as normal or anomaly. Algorithms suitable for IoT-class devices can be random trees (random forests in the case of parallel execution on all the IoT-cluster), or comparison based like K-nearest neighbors, or linear methods like logistic regression or Perceptron based approach; in the case of NN (Neural Network) this must be conceived specifically for the device it will be deployed considering HW resources and computation capabilities. In all these cases features can be collected from the normal network traffic in a protected environment and then used to in the training procedure.

### 3.7.6 Possible Honeypots

Honeypots can work together with the identification procedure provided by previous techniques; as an example an useful honeypot approach could be in jamming the channel once the attacker is identified. Or keeping an unprotected (less protected) channel the attacker will try to get access to first and that is sending fake, but coherent, data.

## 3.8 Password Attack and countermeasures

### 3.8.1 List of counteracts and considerations

- Limit the number of attempts and track the requester;
- Since an attacker will try first to use common passwords maybe related to personal accessible info, a possibility is to keep a blacklist of possible passwords created from those personal info (that we also know..) and block the attacker attempts immediately;
- A honeypot approach could be, in the case of previous condition, to give access to a fake shell in order to evaluate requests from the attacker, while taking countermeasures.

---

## CHAPTER 4

---

# Implementation Overview

### 4.1 Case of study 1: Cluster and Honeypot for a Ransomware attack

Let's suppose to have a distributed system as in the following picture.

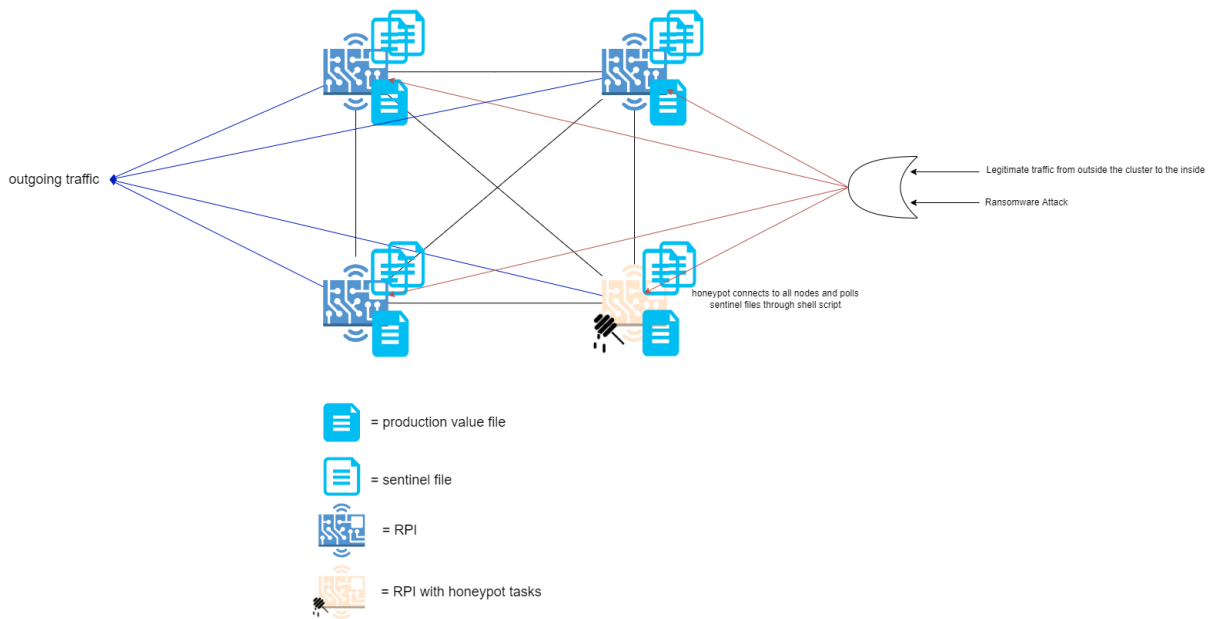


Figure 4.1: Examlle scenario of honypot against ramsonware attacks.

Most IoT solutions include devices that collect data from the environment and send it to more powerful components that gather such information, possibly perform computation and forward data elsewhere. Any Raspberry Pi in the picture represents a server, each connected to more clients (not shown in the picture). Such servers are then connected among each other through a network and a communication protocol.

In this example, the architecture of the network is a full mesh, implying that each server is directly connected to any other. You could think of this network as either a local area network (LAN) or wide area network (WAN). They offer two different flavors of the same problem since in LANs you assume that all devices belonging to the network own a different local IP address and you should deal with

the NAT system, while in a WAN servers have different public IP addresses and you should deal with DNS in order to communicate with each node in the network.

Here, the traffic entering the network can be either legitimate or a ransomware attack, benign or malign respectively.

As to the communication protocol, IoT systems mainly rely on REST or MQTT. In this context we could think of servers as MQTT subscriber & publisher (at the same time), since each server is supposed both to receive and send data. The MQTT broker is the entity through which any data packet has to pass to be forwarded from the publisher to the subscriber.

Even though the underlying hardware is the same for each of the servers, one of them plays a different role: it behaves as a malware honeypot.

All raspberry devices store two distinct types of files: production value files and sentinel files. Sentinel files are spread in the network with the sole purpose of being a bait for ransomware. Such files are useless for production, thus no any trusted node in the network should change their content. Any change should be assumed as malicious.

The task of the honeypot is to monitor the hash digest of sentinel files. If it changed, then there is a very high chance of being under ransomware attack (since sentinel files do not provide production value and therefore are useless for any legitimate operation).

A rudimentary script that analyses differences on sentinel files could be the following:

Heuristics are available since studies show that ransomware tend to encrypt files starting in alphabetical order (or inverse alphabetical order), thus you can name the sentinel files accordingly. As an example, placing files called "####aBaitFile.txt" would be among the first ones to be encrypted with an alphabetical attack.

The computation of hash digests with respect to checking the whole content is a clear advantage regarding speed.

If a difference in the hash digest is present, then a response takes place. The most straightforward response is the shutdown of communication in the whole network and the insertion of the attacker's IP in a blacklist, denying its upcoming traffic.

An improvement with respect to the scenario depicted above could be the deployment of multiple honeypots at the same time, allowing more servers to monitor sentinel files.

The proof of concept can be constructed thanks to a simulated ransomware attack. Some material is available online regarding the creation of simple ransomware via PowerShell, as reported in "How to: Simulating A Ransomware Attack With PowerShell" [?].

## 4.2 Case of study 2: Cluster and Honeypot for a DoS attack

In the paper named *Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks*[?] we found an analysis of the usage of a honeypot to reduce the damage of a DOS attack. One of the several possible attacks on IoT systems, Denial of Service (DoS) attack has been a nightmare for communication networks over the years and they pose a major security threat to IoT systems as well.

### 4.2.1 Structure of the IoT cluster for the project

In order to create the honeypot and check if it works, we would need to create the IoT "cluster" and the DoS client. It is a good idea to start with the most possible structure, and if we manage to create it without any particular difficulty, we could make it more realistic and more complex. So our simple IoT cluster could have very different implementations. We had many ideas, the first of which is reported in the figure below.

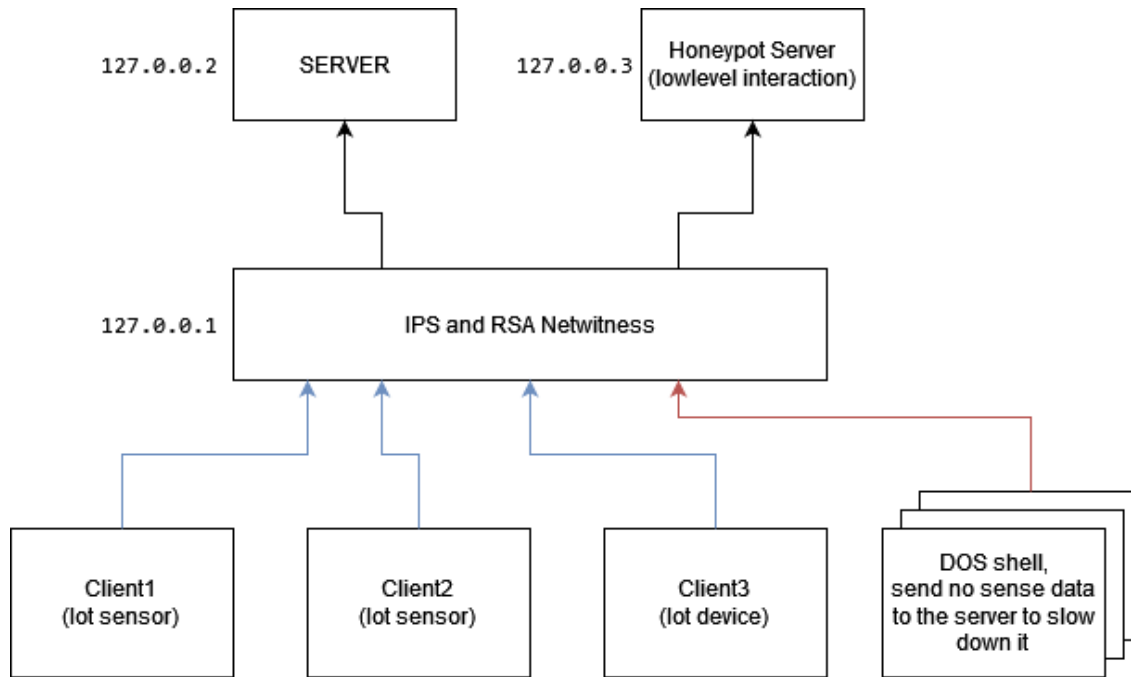


Figure 4.2: IoT network scheme with IPS.

An Intrusion Prevention System (IPS) is an active protection system. It attempts to identify potential threats based upon monitoring features of a protected host or network and can use signature, anomaly, or hybrid detection methods. Unlike an Intrusion Detection System, an IPS takes action to block or remediate an identified threat. While an IPS may raise an alert, it also helps to prevent the intrusion from occurring. An IDS is a passive monitoring solution for detecting cybersecurity threats to an organization. If a potential intrusion is detected, the IDS generates an alert that notifies security personnel to investigate the incident and take remedies against the action.

In our first proposal the system is less complex, because the IPS itself takes the decision on where to redirect the traffic to. If it is a malicious one, to the honeypot that will collect data about it, if it is a normal one, to the server. The IPS needs time to take decisions, so the traffic could be slowed down by it. If the application doesn't require high availability, this solution is acceptable. Our second idea is reported in figure below.

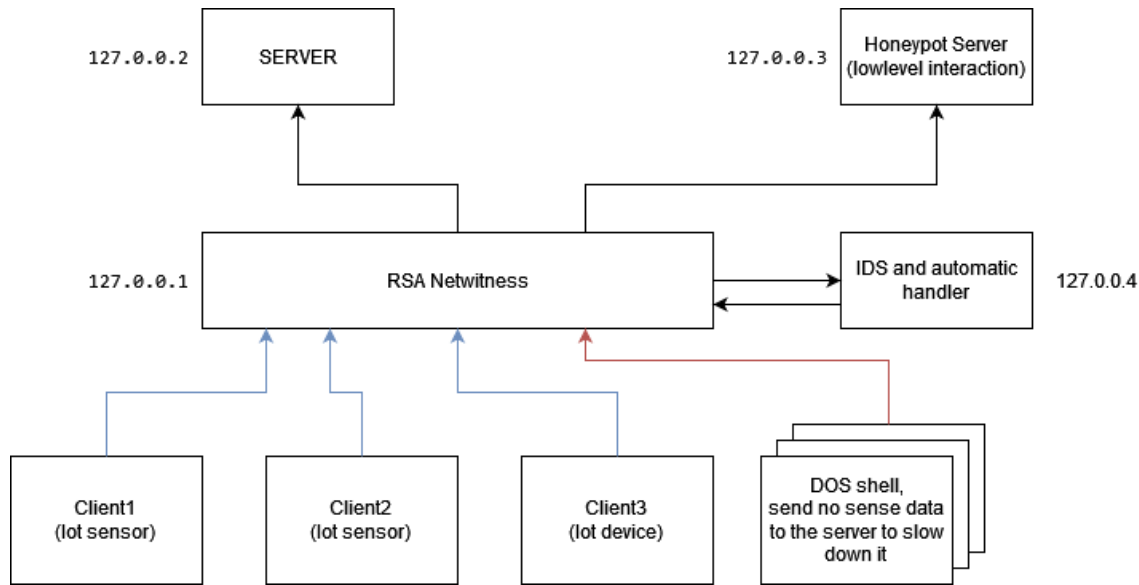


Figure 4.3: IoT network scheme with IDS.

This time an ad-hoc server has an IDS, that arises an alarm when something wrong is happening. Then an algorithm inside the server takes a decision on what to do with this possible malicious connection, and sends a command to the RSA server to redirect the traffic. In this way, the system has an high availability because the RSA server is not slow down by the IDS, that acts in a totally autonomous way. However, this idea requires more engineering effort and hardware. If the implementation of these two systems takes less time than expected, we could try to create a more realistic IoT cluster like in the figure below.

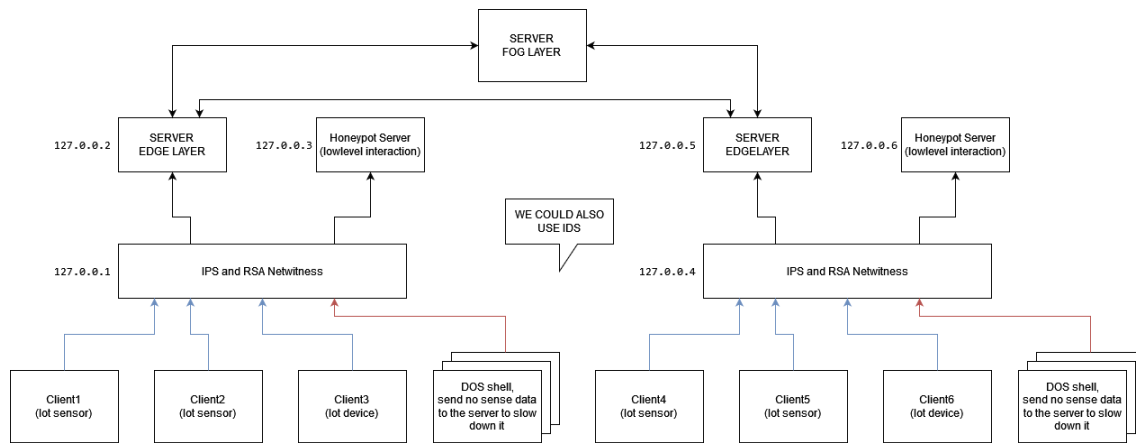


Figure 4.4: IOT network scheme level 2 with IPS

If we didn't manage to do that, we could see this last idea as a possible future implementation.

#### 4.2.2 DOSPOTPY and climatOffice

In the last years it becomes more and more important to avoid waste of energy at home and at work, due to the increasing cost of energy and to the environmental impact from the chain of the energy supply. So a startup develop a new IoT system named climatOffice (This is only an imaginary



company, it doesn't exist in the real life). This solution aims at control the temperature in every office of the company, using  $N$  temperature sensors in every room and at least one air conditioner. The desired temperature could be set by an external terminal to the server that control every room. If there are windows in the room, the system also offer the possibility to control the illumination using automatics roll-up shutter. The last feature of this IoT cluster is to possibly control the accesses to some vulnerable rooms, like the server's farm room. So it can lock or unlock some doors. It can do this last thing automatically or by a command from a terminal. A possible structure of this system is reported in the picture below.

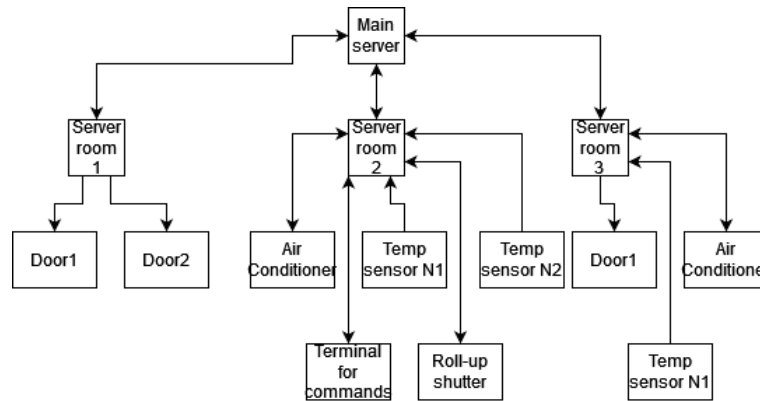


Figure 4.5: An example of the climatOffice IoT cluster

A possible Dos attack could for example avoid the door to close or open, or shut down the air conditioner system. To avoid so we could implement our honeypot and IPS like in the precedent figures. For example, our attacker implement a bot that connect to the system and create thousands of fake temperature sensor that send random and wrong data to the server. Our IPS usually send new traffic connection to the honeypot, that will analyse the data. If this is no sense data, the honeypot will store in a log file the IP addresses of the fake sensor and will told to the IPS to close the connections and to avoid accept new one from that IP.

In this chapter you should provide a general overview of the project, explaining what you have implemented staying at a high-level of abstraction, without going too much into the details. Leave details for the implementation chapter. This chapter can be organized in sections, such as goal of the project, issues to be solved, solution overview, etc.

It is very important to add images, schemes, graphs to explain the original problem and your solution. Pictures are extremely useful to understand complex ideas that might need an entire page to be explained.

Use multiple sections to explain the starting point of your project, the last section is going to be the high-level view of your solution...so take the reader in a short 'journey' to showcase your work.

---

---

## CHAPTER 5

---

# Implementation Details

### 5.1 Case of study 1: Cluster and Honeypot for a DoS attack

#### 5.1.1 Instruments used

In order to simulate our IoT cluster with the honeypot, we decide to implement a simulation using python. The most important aspect to respect when developing a client-server application, like our IoT cluster, is that the servers and the sensors have to be able to exchange data between each others. The module sockets present in the python library allow us to support networking protocols between two or more processes across machines. In this particular case we use TCP sockets, where at one side a process act like a client and on the other side a process act like a server. Also python offer the module selectors that allow us to serve multiple sockets connections. In particular the `.select()` method allows us to check for I/O completion on more than one socket. So we can call `.select()` to see which sockets have I/O ready for reading and/or writing. We also want to underline that with `.select()` we're not able to run concurrently.

#### 5.1.2 First structure of the IoT cluster

In our first simulation we decided to implement an high-interaction honeypot and a cluster reported in the figure below.

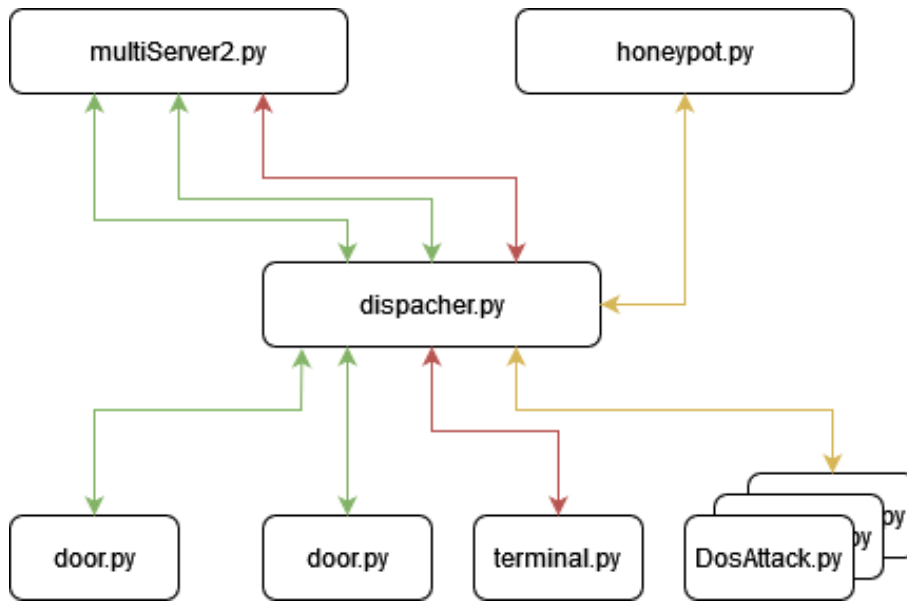


Figure 5.1: Our simple IoT cluster with an high-interaction honeypot

This system help us to underline the difference between the dispatcher and the honeypot. In the other section of the report where we speak about the implementaions of the Dos honeypot, we mention about IPS and IDS, but it turn out that we need only a system that redirect packets from the sensors to the honeypot or to the server. This symple application allow the user to open or close the doors conected to the system. In the nexts subsections we will explain the purpose of every script and how they interact.

### 5.1.3 Door.py

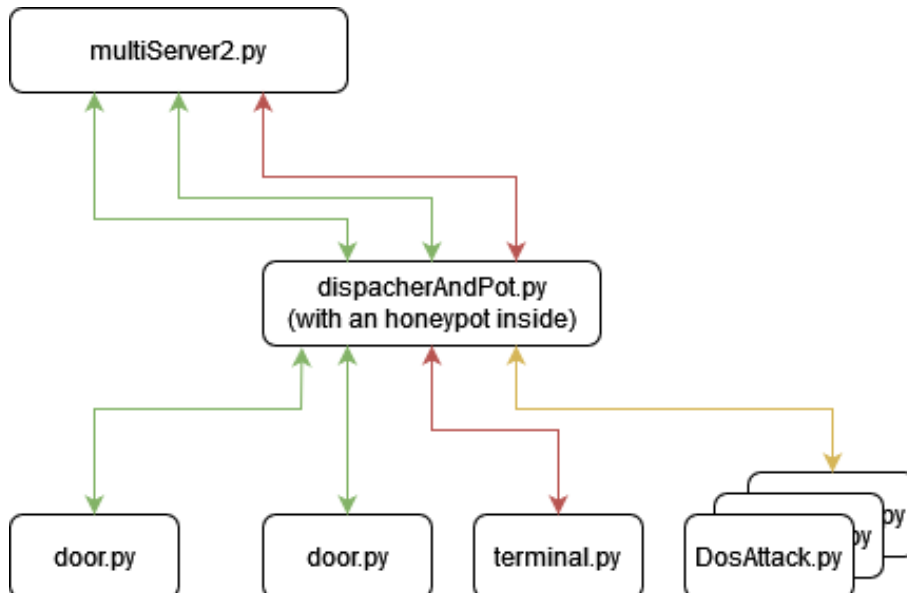


Figure 5.2: Our simple IoT cluster with a low-interaction honeypot

This is where you explain what you have implemented and how you have implemented it. Place here all the details that you consider important, organize the chapter in sections and subsections to explain the development and your workflow.

Given the self-explicative title of the chapter, readers usually skip it. This is ok, because this entire chapter is simply meant to describe the details of your work so that people that are very interested (such as people who have to evaluate your work or people who have to build something more complex starting from what you did) can fully understand what you developed or implemented.

Don't worry about placing too many details in this chapter, the only essential thing is that you keep everything tidy, without mixing too much information (so make use of sections, subsections, lists, etc.). As usual, pictures are helpful.

---

---

## CHAPTER 6

---

# Results

In this chapter we expect you to list and explain all the results that you have achieved. Pictures can be useful to explain the results. Think about this chapter as something similar to the demo of the oral presentation. You can also include pictures about use-cases (you can also decide to add use cases to the high level overview chapter).

### 6.1 Known Issues

If there is any known issue, limitation, error, problem, etc...explain it in this section. Use a specific subsection for each known issue. Issues can be related to many things, including design issues.

### 6.2 Future Work

Adding a section about how to improve the project is not mandatory but it is useful to show that you actually understood the topics of the project and have ideas for improvements.

---

---

## CHAPTER 7

---

# Conclusions

This final chapter is used to recap what you did in the project. No detail, just a high-level summary of your project (1 page or a bit less is usually enough, but it depends on the specific project).

---

---

## APPENDIX A

---

# User Manual

In the user manual you should explain, step-by-step, how to reproduce the demo that you showed in the oral presentation or the results you mentioned in the previous chapters.

If it is necessary to install some toolchain that is already well described in the original documentation (i.e., Espressif's toolchain for ESP32 boards or the SEcube toolchain) just insert a reference to the original documentation (and remember to clearly specify which version of the original documentation must be used). There is no need to copy and paste step-by-step guides that are already well-written and available.

The user manual must explain how to re-create what you did in the project, no matter if it is low-level code (i.e. VHDL on SEcube's FPGA), high-level code (i.e., a GUI) or something more heterogeneous (i.e. a bunch of ESP32 or Raspberry Pi communicating among them and interacting with other devices).

---

---

## APPENDIX B

---

# API

If you developed some source code that is supposed to be used by other software in order to perform some action, it is very likely that you have implemented an API. Use this appendix to describe each function of the API (prototype, parameters, returned values, purpose of the function, etc).