HoneyBot: A Honeypot for Robotic Systems [1]: synthesis

SEUTIN Jeffrey, SOYTURK Okan

Index Terms

Honeypot, Honey-net, Robot, Spoofed, Decoy computer

I. Introduction

A honeypot is a decoy computer which is used in order to delude attackers. This method to prevent hacking our computers allows to trace some information from the hacker, who believe that his attack is a success. HoneyBot is the first honeypot used on a robot device.

But first, we have to explain what a robot is. A robot is a electronic device usually autonomous and used to do repetitive tasks for an human. This need appears with great technological advances since 1950, and in 1961 the first industrial robot was born in General Motors factory [12]. Today robots are mainly used to remove the human factor. The article shows three biggest reasons to explain this:

- To reduce greatly the cost of labor in industries; for example, in a car manufacturing, the price of a robotic arm is less expensive than an workman (about 8 times less expensive according to the article).
- To remove the human error factor in accuracy work; For example to make a microprocessor.
- to avoid a lot of human loss (mainly military).

The aim of this document is to synthesis the article which we have to read. After this briefly introduction, we will see the robots domains of application, then we will see the purpose of the article to introduce the different approaches tackled in the article. Next we will see positive and negative point of the article and conclude with future trials and advances since the release of the article.

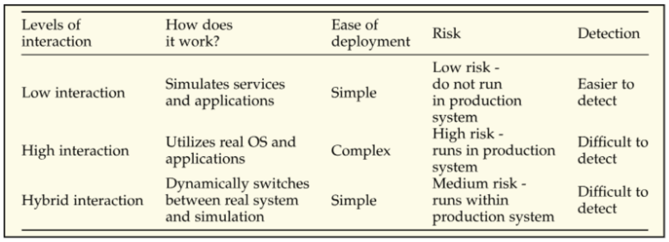
II. Domains of Application

Today, we use robot more and more because of the evolution of jobs. This reality is more visible in particular in manufacturing sector because of redundancy and repetition of boring tasks. But this change is as interesting to the employer as it is to the employee : this makes live easier for employee who will be able to do less repetitive tasks and better for the employer by saving money.

To illustrate this economy for a company, we have to compare the difference of cost between human and robot. A very popular robot in industry is Baxter : he is able to reproduce most of human gesture and can be used in different sector, so he can replace many position. Its price is $32000 and entry-level factory employees is around $25,000 a year. So the robot will be profitable from the second year of operation. Of course, robot will need electricity, some maintenance and be programmed by an operator which cost more than a entry-level factory employee, but the advantages take over because he can work every day and even night. He doesn't need beaks, don't go on strike, won't get injured and will never complain.

As we said it before, honeypot is a decoy computer used to delude attackers. The method consists to convince hacker that his attack succeed. The first honeynet (a network of honeypots) was created in 2004 by Pothamsetty and Franz of the Cisco Infrastructure Assurance Group (CIAG) [11]. According to the article, their aim was to simulate a programmable logic controller services to help researchers to better understand the risks of exposed system devices. Today the honeynet is used to simulate a lot of industrial networks.

According to the article, there is several different classes of honeypot. The next table, which comes from the article, illustrates differences, risks and works of each classes.



Levels of interaction	How does it work?	Ease of deployment	Risk	Detection
Low interaction	Simulates services and applications	Simple	Low risk - do not run in production system	Easier to detect
High interaction	Utilizes real OS and applications	Complex	High risk - runs in production system	Difficult to detect
Hybrid interaction	Dynamically switches between real system and simulation	Simple	Medium risk - runs within production system	Difficult to detect

Fig. 1. Interaction level of honeypot

Honeypots are classified under their level of interaction. Additionally of low-interaction and high-interaction classes, the previous work of authors allowed to include a third classes, called ”hybrid” interaction classes which allow to dynamically swap between real system and the simulation.

III. Purposes of the article

This article presents the robot software HoneyBot, the first honeypot used on robotic system, and why the HoneyBot device was created for. As we said it before, robotic systems today is no longer isolated from the internet. We have to consider that robot is vulnerable to cyber-attacks as a computer, so we need to protect their embedded-systems with an ”anti-virus” . Especially, the consequences of a pirated army drone for example could be a disaster.

We have to explain why the honeypot device is especially used to be adapted for robotic systems. We had already define a honeypot, but we hadn't already explain how the device work. To delude attacker, the network redirect attack toward a decoy computer and spoof the hacker that his attack succeeded. To adapt this kind of technology for a robot and according to the article, we have to spoof attacker with wrong information, and for that the next paragraph will detail the different parts of robots.

To understand how the HoneyBot exploits the different parts of the robot to delude the attackers, the article have to explain the work of each different interfaces used to get information to the environment and how those data are computed:

- Sensors allows robots to get data from the environment. Those data are crucial for the robot in order to adapt itself.
- Actuators allows robots to modify the environment and move.
- Controller allows robots to parse commands and to send signal to other components.

Finally, the global aim of the article is, according with it, to present a technology which allows to notify the system administrator that his system is corrupted, and to get information from the attackers. To our mine the article prevents people to the danger of non-protected robot. For example, an random enterprise can be unfair toward its competitor and hack one of the manufacturing robot to destruct many products. The need to protect robotic system today is primary and the article shows us a solution and how this solution works, the HoneyBot device.

IV. Approach

A. Scientific approach

Research about trap attacks has long been concentrated in the computer field, but since robotics has become more and more important in our lives, researchers have to take the lead before hackers get ahead. It's in this context that engineers at the Georgia Institute of Technology have developed the HoneyBot, a decoy robot (as a honeypot is a decoy computer) totally inoffensive which can trick hackers that they control their target (mainly a manufacturing robot). So, HoneyBot is based on the concept of honeypot that are used by IT firms to lure hackers, but with some modifications to adapt them in the robotics fields.

HoneyBot is based on the HoneyPhy software[7], which allow its different inter-modules to communicate, because most of CPS (Cyber-Physical System) neglect that robotics system can alert attacker about the physics of the device that interact with the process. According to the thesis, the HoneyPhy software allows to investigate how attackers exploit the vulnerability of a network system and how far they succeed to penetrate the system, which allows to build the honeypot device by the way. So

HoneyBot adapt this framework to specifics of robotics system.

To successfully trap someone, the HoneyBot must be able to make the hacker believe that he listens to his instructions and execute them. This is where this device is very effective because the idea behind this honeypot is that the hacker should never know he is in a honeypot.

HoneyBot is a small rolling robot that receives instructions, executes them and sends back data from its sensors (characteristics in the following section). The robot always executes the commands it receives, but when one of them does not correspond to an expected behavior, it will act differently : the HoneyBot will not allow the action to be performed but will send data as if action has been performed to persuade hacker.

For example, to check if robot is moving in the way that he want, the hacker will probably check the position of the robot thought differents sensors which are on the robot, like an accelerometer or speedometer. To detect that the system is penetrated by an unusual user, it becomes very simple: when the robot detects a command different from that of the owner, it first returns fake data from its sensors, then alerts the real owner. The bad guy thinks he just hacked a robotic system when he just warned the cyber security team about his presence, because it's impossible for him to distinguish between simulated data and real data.

The next figure which comes from the article illustrate the processing of safe and unsafe logs in a network robotic system which uses HoneyBot.

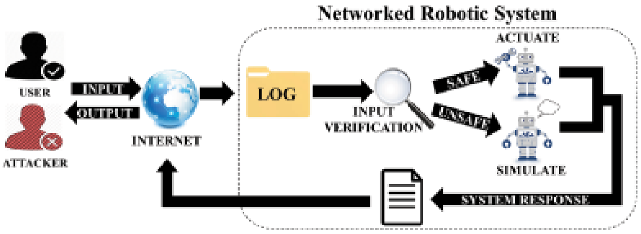


Fig. 2. HoneyBot system

B. Technical approach

The HoneyBot project is based on a robot with 4 wheels and multiple sensors. Any robot is composed of 3 distinct modules:

- the sensors: it's the eyes of the robot. They allow to collect information on its environment and its state. It's thanks to these sensors that he will make decisions, and especially to warn the user that everything is going according to plan. There are many sensors that can provide a different variety of information: accelerometer, thermometer, camera, IR, magnetometer, ...
- the actuators: they allow to modify the environment of the robot, so they are mechanical elements: motor, robotic arm, loudspeaker
- the controller: it's the brain of the robot. He will have to make decisions thanks to the different inputs of the sensors and then send commands to the actuators.

To prove the feasibility of this concept, the team decided to deploy this HoneyBot on a GoPiGo[5], a programmable robot which uses a Raspberry Pi 2[3] as the robot's brain. The advantage is they can use a sensor board GrovePi[6] on which they can connect many sensors.

Then what is left to do is to have the best software to detect intrusions and act accordingly. Indeed, HoneyBot must absolutely know when a command is not normal to generate "spoofed" responses, but contrary to what we can think, it's not that hard. Taking an example which comes from the article, let's suppose that HoneyBot was implemented in military drone and some attackers try to perform malicious unsafe actions by directing it in a no fly-zone, it's very easy for the controller to know that something suspicious is happening and so to not performing the move. But don't forget that we have to trick attackers, and what is much less obvious, it's to return false data of the sensors so that everything is coherent between them. First, the drone have to mark the action as unsafe, and then maintain its position in the authorized zone. Afterwards it must return the

coordinates that the attacker wants to see, but also make the link with other sensors, such as velocity or distance. This requires a lot of calculation to respect the correlation between several sensors.
To conclude those two parts, HoneyBot use a hybrid interaction level, meaning a combinaison of unsafe commands with safe actions to delude attackers. The hybrid interaction class of a honeypot imply a easy deployement in a production system with a difficult way to detect the trick.

V. Critique

A. *Positive*

The next part will contain some positive points that we found during the reading part. First, the full article allows us to understand why a protection device for robotic system will be useful, especially the honeyBot system.
We consider this article as a popularizing science article. They are able to reach anyone to prevent the most people of the danger of unsafe network of robotic system. We are able to understand how the GoPiGo robot use its component to delude hacker.
The article explains perfectly why the honeypot technology is used to be adapted for robotic system and how the HoneyBot device works. The article specifies how the honeyBot device is effective, supported by lot of concrete results, for example the HoneyBot simulator.

B. *Negative*

This article is of course not perfect, and here we will explain some points that we found negative. First, as we said in the last part we consider the article as a popularizing science article. In fact, we learn about why robots are created and how the GoPiGo robot tested for experience works, and how the honeypot device is used to be a synchronize to a robot device.
The main part of the article is dedicated to the three main parts affected by the device, and it explains how they work. Nonetheless, we would have preferred more detailed paragraph about honeypot or honey-net specification. The article doesn't explain especially the difference between drone and robot application of the HoneyBot device.
Moreover, the article doesn't really explain any algorithm. We can't reach algorithmic boundary about the only framework showed, the HoneyBot simulator, an experimental tool developped in order to test the HoneyBot device before to apply it. The weakness of the software aren't showed in the article, and neither future trials is presented, for example a future collaboration with a robotic enterprise would be really interesting to follow.

VI. Future trails

According to the article, the HoneyBot is first decoy robot which use the honeypot technology to trick hackers. Since the release of the article, we have neither found any advancement about any other honeypot systems used in robotic system, nor about any technology which is adapted to be use on a robotic device.
According to an article wrote by the Robotic Business Review staff [9], some components use to build computers are already industry-tested and safe to be adapt to build robots, like many QorIQ multicore processors [8]. But of courses, it will be really expensive to change component with newest in a manufacturing robots industries.
According to a study done by a Trend Micro's research team in collaboration with the polytechnic school of Milan [10], industrial robots are more and more targeted by hackers due to the lack of security.
With those both information we can deduce that the HoneyBot solution is the best choice for a manufacturing robots enterprise, if one day the project would be commercialized.

VII. Conclusion

To conclude this synthesis, we found just few information about the advancement of the HoneyBot. It seems that the HoneyBot project is still an experimental and private tool, according to this recent article which present the device as would do a popularizing science article [2].
Even if the article doesn't specify it, the GoPiGo robot constructor, Dexter industries [5], presents its product with a HoneyBot video presentation [4]. We can consider they obtain the collaboration that they needed, highlighting the work done.

References

[1] Samuel Litchfield Raheem Beyah Celine Irvene, David Formby. Honeybot: A honeypot for robotic systems. *Proceedings of the IEEE*, 106(1):61–70, 2018.

[2] digitaltrends.com. Meet the HoneyBot, a decoy robot designed to trick hackers. https://www.digitaltrends.com/cool-tech/honeybot-decoy-robot/, 2018.

[3] R. P. Foundation. Raspberry Pi Foundation — Raspberry Pi. https://www.raspberrypi.org, 2016.

[4] D. Industries. Dexter Industries — Robots in Higher Education. http://info.dexterindustries.com/dexter-higher-ed/.

[5] D. Industries. Dexter Industries — GoPiGo. http://www.dexterindustries.com/gopigo/, 2016.

[6] D. Industries. Dexter Industries — GrovePi. http://www.dexterindustries.com/grovepi/, 2016.

[7] Samuel Litchfield. *HoneyPhy: a physics-aware CPS honeypot framework*. PhD thesis, Georgia institute of Technology, 5 2017.

[8] nxp.com. QorIQ Processing Platforms: 64-bit Multicore SoCsks. https://www.nxp.com/products/processors-and-microcontrollers/power-architecture-processors/qoriq-platforms:QORIQ_HOME.

[9] roboticsbusinessreview.com. Robots vulnerable to hacking. https://www.roboticsbusinessreview.com/unmanned/robots_vulnerable_to_hacking/.

[10] trendmicro.com. Rogue Robots. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security, 2017.

[11] Matthew Franz Venkat Pothamsetty. SCADA HoneyNet Project: Building Honeypots for Industrial Networks. http://scadahoneynet.sourceforge.net/, 2004.

[12] World-Information.org. 1961: Installation of the first industrial robot. http://world-information.org/wio/infostructure/100437611663/100438659325.