HoneyBot, a Honeypot for Robotic Systems

Celine Irvene, David Formby, Samuel Litchfield, Raheem Beyah

---

synthesis wrote by SEUTIN Jeffrey and SOYTURK Okan

Supervising teacher: M. Chaumette

University years: 2018 - 2019

Outlines

1. Introduction
2. Domains of application
3. Purpose of the article
4. Technical and scientific approaches
5. Positive and negative critiques
6. Future trials
7. Conclusion

Introduction

- Why?
  - To reduce the cost of labor in industries
  - To remove human factor in accuracy works
  - To avoid a lot of human loss (mainly military)
- Honeypot: a decoy computer to delude attackers
- Honey-net: a network of honeypots

Domains of application

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 - run within production system	Difficult to detect

Purpose of the article

- To prevent people to the danger of an unsafe system
  - To notify the administrator when the system is corrupted
  - To get information about the attackers
- To offer a solution for that issue: HoneyBot
- How the device exploit different components of the robot

Technical and scientific approaches

Scientific approach:

- HoneyBot is based on HoneyPhy researches done by S. Litchfield
  - inter-communication between components in the machine
  - high interaction between processor and interfaces with the environment
- HoneyPhy allows to investigate about the attackers
  - how far they penetrated the system
  - how attackers exploit the vulnerability of the system
- Trick attackers with wrong data

Technical and scientific approaches

Technical approach:

- Sensors, the eyes of the robot
- Actuators, modify the environment and allow robot to move
- Controller, parse command and send signal to other components

- GopiGo robot and GrovePi sensor

Positive and negative critiques

- ✓ Explicit, perfectly understandable for everyone
- ✓ Utilities of the HoneyBot device explained
- ✓ How GoPiGo components are used to delude
- ✓ Awareness of the importance of a protected system, robotic or not.

- ✗ Popularizing science article : some points unexploited
- ✗ Some technical points still obscure
- ✗ Can not prove results exposed (robots are expensive)
- ✗ Can not really test neither algorithm used nor simulator (experimental tool).

Future trials: today...

- HoneyBot stays the only one and the first honeypot for robotic system
- Components used to craft robots are safe and certified
- Manufacturing robot industries more and more targeted by attackers
- HoneyBot can be the solution and gets a good success

Conclusion

- Just few information are diffused about HoneyBot
- Dexter Industries presents their GopiGo robot with a HoneyBot video
- Not yet commercialized, maybe already tested

References

The full article: https://github.com/jefseutin/HoneyBotIR/blob/master/article.pdf

Safe components, the QorIQ processor: https://www.nxp.com/products/processors-and-microcontrollers/power-architecture-processors/qoriq-platforms:QORIQ_HOME

HoneyPhy: https://smartech.gatech.edu/handle/1853/58329

Dexter Industries, GoPiGo, GrovePi: http://www.dexterindustries.com/

HoneyNet work: http://scadahoneynet.sourceforge.net/

Recent publish about HoneyBot: https://www.digitaltrends.com/cool-tech/honeybot-decoy-robot/