OPEN ACCESS

2nd International Electronic Conference on Sensors and Applications 15–30 November 2015

www.mdpi.com/journal/sensors

Conference Proceedings Paper–Sensors and Applications

Honeypot Wording and Definitions in Wireless Sensor Networks

Jürgen Markert [1,*] and Michael Massoth [2]

[1] Centre for Security, Communications and Network Research, School of Computing, Electronics and Mathematics, Plymouth University, Drake Circus, Plymouth, PL4 8AA , UK; E-Mails: jurgen.markert@plymouth.ac.uk

[2] Computer Science Department, Hochschule Darmstadt - University of Applied Sciences, Haardtring 100, 64295 Darmstadt, Germany

* Author to whom correspondence should be addressed; E-Mail: jurgen.markert@plymouth.ac.uk

Published: 9 November 2015

Abstract: Wireless Sensor Networks (WSN) as emerging technology are becoming even more important through the technisation of industry, our mobility driven lives and our "smart homes". In a world where a plethora of our devices interact to serve our purposes, it's clear that competing groups may want to use these devices for their own objectives. Therefore we focus on honeypots for WSNs as an opportunity to become acquainted with the techniques used to misuse or even to take-over WSNs. This knowledge has the potential to improve the WSN designs and even those already deployed in the field. Honeypots in information security can be found in computer networks where a client-server model is applied and client-honeypots are very different from server-honeypots. In WSNs the client-server model is not applicable. This was the motivation behind determining whether it would be a honeypot at all if brought into this domain. What if we have to call it something else? The uncertainty of a missing naming convention leading to ambiguous conversations about this new topic needs discussion. In this paper we show the classic definition, discuss the categorisation and give recommendations for further use as well as the wording that will be used further on in the following research.

Keywords: Honeynet, Honeypot, WSN, Wireless Sensor Network, Network Security, IDS, Intrusion Detection System

---

1. Introduction

Honeypots for WSNs [1] are an emerging and mostly unexplored research field. We give an overview on the topic of honeypots and compares honeypots with the purpose of starting a discussion on the differences between WSN honeypots to wireless ones as well as those in wire-bound networks. Numerous definitions and terminology exist. This discussion is on their use in WSN and offers guidance or recommendations for further use in the field of honeypots for WSN. This clarifies our description of a WSN honeypot. The meaning of the term WSN honeypot is established, because, so far, a concise definition does not exist.

A honeypot is a well and widely known term in information security. Like the authors of [2] have practised, it stands for a computer system that is closely monitored, reachable as a decoy and has only one purpose: to entice the bad guy into this pit trap. The result is knowledge. It is important to understand there was (an entity with) the intention to utilise the system for (its own) other purposes. Additionally, a closely monitored system will also give valuable data for analysis, for instance the attack vector, the strategy, or the tools and techniques used. A set of more than one honeypot acting jointly is called honeynet [3].

Classically, the discussion is about high-interaction honeypots vs. low-interaction honeypots, when speaking about honeypots in wired network environments [4]. These are then further divided into client-side and server-side honeypots, depending on the deployment of the honeypot as being a client system or a server system [5]. This detail is very important since a client is exposed to other threats than a server system. As an example, on a personal computer client an attack vector is triggered when a malicious website is visited (e.g. by a drive-by-download). On the other hand, a server system offers services likely to contain vulnerabilities, that can be exploited to gain control of the system or deploy other malware for further attacks.

High-interaction server honeypots are set up to focus on attacks carried out manually and new methods of the attacker. Therefore a highly interactive honeypot is set up in a way that achieving control of it appears very desirable, i.e. it would offer significant bandwidth for a potential attacker or seem to contain documents or data of interest. High-interaction honeypots are often set up in the same network as the “normal” server. The normal server is hardened as good as possible and the honeypot is under continuous monitoring. There are honeypot software solutions for these monitoring purposes. Highly interactive honeypots are very resource-intensive in maintenance, repair and operations (MRO) [4].

On the client-side the high-interaction honeypots are partly automated web crawling systems with real client software. They are configured to visit websites and capture incoming attacks as well as their payloads in a sand-boxed system. These honeypots preferably run on a virtual machine for convenience. Further their web browsers are designed to run in sandboxes.

Low-interaction honeypots are defined as systems that emulate one or more systems [4],[5].

When regarding low-interaction server honeypots, these are services that are emulated. A single interaction with them is enough to capture an intrusion attempt. A low-interaction honeypot could also seem to be a whole network, emulated by a single honeypot system. The emulated services offer only a subset of the features that would be available on a real system. Those systems are most often used to capture packets of automated or new attacks, to get new variations of computer network worms and to get

the latest version of a malware, this could for instance be a software trojan application. An attacker has various possibilities to detect being connected to a honeypot, but this fact could be ignored completely, because the intrusion detection attempt is already valuable information enough at a low-interaction server honeypot.

A low-interaction client honeypot is for example a web crawling client emulation that visits websites to capture drive-by-download attempts of infected malicious websites.

2. Discussion

For the start of a naming discussion after a preliminary short summary of the various details of established honeypot concepts. With the established fact that a honeypot has no other purpose than to attract and monitor an attackers' behaviour (compare to honeypot definition by Spitzner [4]) We compare the WSN honeypots to this, exactly this is what is done with the "Honeypot Framework for Wireless Sensor Networks" [1]. Due to this fact that every connection to a honeypot is by definition an attack, because it has no other purpose than to attract and to monitor the attack, an intrusion detection attempt is already valuable information enough. So if the name "honeypot" is indeed the right term for a honeypot independent of being in a wired-network, a wireless network or a meshed network like a WSN is, it can be called a honeypot, but not something else. Despite the fact, that in a WSN the routing is different compared to IP networking and we don't use ports and services, so a service like a honeypot daemon for a single networking service is not used, it will be called honeypot.

2.1. Low- and high-interaction honeypots

With the definition that a honeypot in a WSN is a generally accepted term for a system that attracts an attacker and otherwise has no real use for the original purpose of the WSN, can a statement be formulated to say something about the fact of it being a high-interaction honeypot or is it a low-interaction honeypot?

Like it was shown in the introduction, that low-interaction honeypots are simulating services on real systems, but they are not physically there, they are not real hardware. It is abundantly clear, that the devices in a WSN do not offer services like a mail- or web-server in an IP based network does. Due to the fact that a node in a WSN is real hardware and does not emulate anything, a honeypot in WSN must be a high-interaction honeypot.

2.2. Honeypots form a honeynet

Likewise it was stated in the introduction, that more than one honeypot working together is called honeynet, this goes further on. Is it a honeypot if it is distributed and should it be named a honeynet or is a swarm of nodes that ba acting together are the honeypot? In a WSN all the sensors of the network together have the honeypot capabilities. A WSN covers a geographical region, its nodes can only transmit and receive signal within a limited radius. Therefore the taken approach due to the physical region a WSN can only be is that this WSN running honeypot routines and algorithms should together be called a WSN honeypot. A single node of the WSN is not the honeypot, it is all the nodes working together. Our recommendation here is to stick to the naming convention that is already established; a set

of honeypots working together is called a honeynet. More than one WSN honeypot acting together may then be called a WSN honeynet.

This is also how a honeynet for wire-bound networks is designed. Numerous systems work together to collect the attacks, honeynets can work together globally. This design can be adapted for a WSN honeynet, consisting of WSN honeypots.

The WSN honeynet is a solution that can be reached by numerous WSN honeypots, for instance one in every metropolitan region, sending their distributed alerts to a database for analysis. In this setup the analysis of attacks is possible and therefore new improvements can be developed for securing the WSNs.

2.3. Client-Server Model

In a discussion whether it is a client or a server honeypot the classical definitions of client and server help us to come to conclusion. We assume that the WSN honeypot functionality is put (among others) in an end-device node of the WSN. As a result, this is by definition not a client honeypot. WSNs don't have clients comparable to those on a personal computer. Each of the nodes in a WSN has networking capabilities and offers services e.g. being an actor for controlling the heating control unit of a radiator. But is it a server? A server offers services and responds to requests.

With regard to the commonly known wording for the client-server model, the WSN do not fit there. One of the comparable models is the peer to peer networking architecture that has a decentralised organisation where every node can communicate to every other, directly or indirectly via hops. Looking at other networking models, a WSN is rather either a peer to peer or a meshed network.

So a WSN honeypot is neither a client nor a server honeypot.

2.4. Physical or virtual honeypot

Is it a physical or a virtualised honeypot? With regard to the scarce resources in a WSN it will most likely in any set-up be a physical honeypot. This can be stated, because research on virtualised wireless sensor network nodes is further ongoing.

2.5. Effectiveness on different layers

Likewise a honeypot needs directed interaction so that if an event is triggered, a WSN honeypot has the same premise. It waits for interaction, so that the event can be analysed.

An estimated effectiveness discussion was previously already discussed and we would like to give a reference to this [6].

3. Results and Discussion

So as a matter of fact it has to be stated, that it is neither a client nor a server honeypot, but a WSN honeypot, nonetheless, this results in:

1. A honeypot in a WSN should be named what is is: a WSN honeypot.

2. The WSN honeypot is most likely a high-interaction honeypot, nothing is emulated.

3. All the nodes are physical, nothing is virtualised.
4. A differentiation between client and server is impossible, a WSN is different in this aspect.
5. A WSN honeypot needs direct interaction to be triggered.

4. Conclusion

Therefore the fact of matter is, as the result of the discussion on the naming conventions for honeypots in WSNs it has to be stated, that it is neither a client nor a server honeypot, but a WSN honeypot, nonetheless. Its use is worthy and needed, paying attention to honeypots shall be on every organisations list.

Acknowledgments

The authors would like to thank the CSCAN, Centre for Security, Communications and Network Research and the GSD, Graduate School Darmstadt.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Markert, J.; Massoth, M. Honeypot Framework for Wireless Sensor Networks. Proceedings of International Conference on Advances in Mobile Computing & Multimedia; ACM: New York, NY, USA, 2013; MoMM '13, pp. 217:217–217:223.
2. Cheswick, W.R.; Bellovin, S.M. Firewalls and Internet Security: Repelling the Wily Hacker, 1994.
3. Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*; Addison-Wesley, 2001.
4. Spitzner, L. *Honeypots: Tracking Hackers*; Addison-Wesley, 2003.
5. Provos, N.; Holz, T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*; Pearson Education, 2007.
6. Markert, J.; Massoth, M. Honeypot Effectiveness in Different Categories of Attacks on Wireless Sensor Networks. Proceedings of Database and Expert Systems Applications (DEXA), 2014 25th International Workshop on. IEEE, 2014, DEXA '14.