Did you really hack a nuclear power plant? An industrial control mobile honeypot

Emmanouil Vasilomanolakis[a,b], Shreyas Srinivasa[b], Max Mühlhäuser[b]
[a]AGT International, Germany
[b]Telecooperation Group, Technische Universität Darmstadt / CASED, Germany
{manolis, max}@cased.de, shreyas.srinivasa@stud.tu-darmstadt.de

***Abstract*—The emerge of sophisticated attackers and malware that target Industrial Control System (ICS) suggests that novel security mechanisms are required. Honeypots, can act as an additional line of defense, by providing early warnings for such attacks. We present a mobile ICS honeypot, that can be placed in various network positions to provide security administrators an on-the-go security status of their network. We discuss our system, its merits in comparison to other honeypots, and provide preliminary results towards a large-scale evaluation.**

***Keywords*—industrial control systems, honeypot, mobile honeypot**

I. Introduction

Over the last years, the number and the sophistication of ICS-specific malware [1] has increased. Moreover, the rise of search engines such as Shodan [2], that focus on the discovery of on-line devices, and specifically ICSs, highly increases the attack surface and creates additional security challenges. It is evident that networks that were traditionally considered secure or air-gap, can nowadays be reached and thus attacked.

Honeypots can work as an additional line of defense and early warning systems both in traditional networks as well as ICSs. In fact, over the last years several honeypots have been proposed for such purposes, e.g., [3], [4]. Nevertheless, many of these proposals are either hard to deploy, or do not support ICS protocols in an efficient or holistic manner.

We extend our previous work on *HosTaGe*, i.e., a lightweight mobile low-interaction honeypot [5], by including support for ICS protocols. We argue that our honeypot brings a multitude of merits with most important ones being:

- *Easiness of deployment and usability*: Network administrators can quickly choose between various systems profiles and the honeypot adjusts itself without additional effort.
- *Interoperability and modularity*: New protocols can be easily added to the honeypot, while existing ones can be customized for creating new emulated systems and profiles.
- *Support for various ICS protocols and entities*: In contrast to related work that focuses usually only on the PLC level, we provide support not only for emulating Programmable Logic Controllers (PLCs), but also for master controllers. Emulating master controllers is particularly important as the majority of attacks is targeting them. Furthermore, besides ModBus, we provide support for TELNET, SMB, as well as upcoming support for SNMP and the S7 protocols.

II. ICS-specific mobile honeypot

HosTaGe, which stands for Honeypot-To-Go, is an open source low interaction mobile honeypot. Currently it supports the emulation of various protocols, e.g., SMB, SSH, HTTP, TELNET, ModBus, FTP, SIP, MySQL, etc. The honeypot utilizes the idea of profiles of systems (see Figure 2) to automatically enable the required services and protocols.

Figure 1, depicts the architecture of the possible network positions that *HosTaGe* can have. For instance, the honeypot can be placed outside of firewalls, thus directly facing the Internet. This is useful for measuring the automated attacks from malware that spread randomly in the IPv4 address range by attacking well known ICS protocols and ports. Furthermore, in corporate networks, one can decide between placing the honeypot either inside the corporate intranet, i.e., behind the main firewalls, or even inside highly protected DMZ networks that are not supposed to communicate with the outside world. The latter provides the ability of even detecting targeted internal attacks, e.g., manifested by infected USB drives.

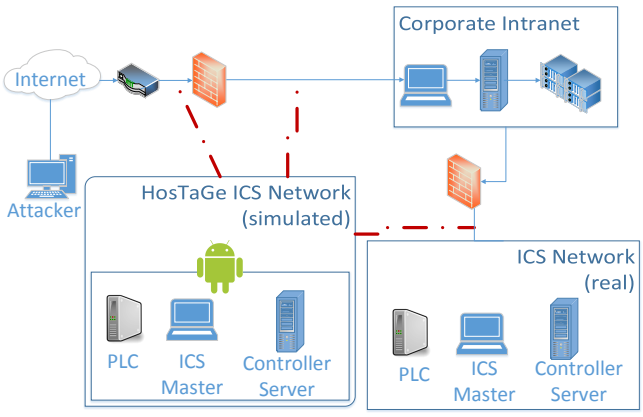

Fig. 1: HosTaGe network positions architecture

Figure 2, shows two examples of the GUI of our system. The user can navigate between different profiles, e.g., a profile

emulating a Nuclear Power Plant, a Water Distribution Plant, a Microst Windows system, etc. When a profile is selected the system adapts itself, and utilizes specific protocols. For instance, when the user switches from the *Apache server* profile to the *Nuclear Power Plant* the port 80 emulation changes from a simple HTTP server to one that appears to be a Siemens PLC control server. Likewise, additional protocols, i.e., SMB, TELNET and ModBust, are activated.

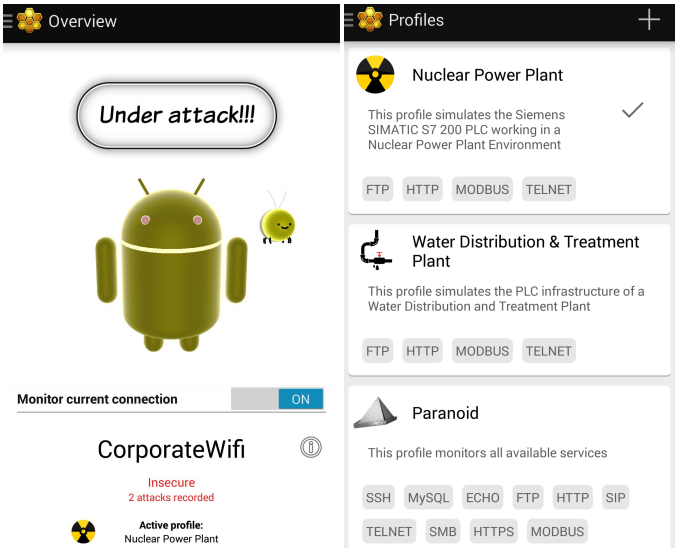

Fig. 2: GUI views of HosTaGe

III. Preliminary Results

We present a short evaluation and comparison of *HosTaGe* along with Conpot, that is considered the state of the art in ICS honeypots. In more details in Table I, we present some preliminary results from the deployment of HosTaGe and Conpot for a weekly period during July 2015. Both honeypots were outside of any firewall, directly facing the Internet, and had similar IP addresses in the sense participating in the same /24 sub-network. We should note that no advertising, e.g., to Shodan, of the IP addresses of the honeypots was made, as our main focus was to investigate automated malware propagation rather than targeted attacks.

Our analysis shows that both HTTP and TELNET protocols cannot provide useful conclusions in the context of ICSs or for directly comparing the two honeypots. First, Conpot does not support TELNET which is however present in most ICS networks (research shows that and most PLCs make use of TELNET without any kind of authentication). Second, for both protocols the attacks that we recorded cannot be considered as ICS-specific. For instance, some attacks on TELNET appear to be malware that try to propagate via password brute-forcing. Likewise, HTTP connections as a result of crawlers and spiders cannot be easily distinguished. Therefore, we believe that it makes sense to only consider attacks in such protocols, in the context of ICSs, only when they are second-stage attacks, i.e., attacks on ModBus have already been detected from the same adversary in a certain time-frame. Moreover, after analyzing our results on the ModBus protocol, it became evident that many of the attacks on it were part of research-related Internet-wide scans, e.g., via [6], from various institutes. Nevertheless, a number of attacks appear to be from malicious entities that were trying to connect to ModBus by specifically targeting the respective port, i.e., 502, (yet, to the best of our knowledge, no further action was taken from their side).

Simulated Protocol	Conpot Honeypot	HosTaGe ICS profile
HTTP	38	83
TELNET	-	177
ModBus	9	9

TABLE I: Comparison of detected attacks on HosTaGe and Conpot in a weekly period

IV. Conclusion and Future Work

The increase of attacks in ICSs indicates the need for novel security mechanisms. Honeypots, can act as an additional line of defense for corporate networks. We present a mobile ICS honeypot that supports the major ICS protocols and is able to provide an on-the-go security status of monitored networks. Our preliminary results suggest that our tool is able to detect attacks on ICS protocols as efficiently as other state of the art stationary honeypots, and even without advertising the IP address of the honeypot.

With regards to future work, we are finalizing the support for various additional ICS protocols, e.g., SNMP and S7. Moreover, we plan to further deploy honeypots that publicly face the Internet for investigating the propagation of ICS malware. In addition, we are working on a module that will support the identification of captured malware via the utilization of the VirusTotal API [7]. Finally, with respect to our analysis of the recorded HTTP and TELNET attacks we plan to introduce multi-stage detection in our honeypot to reduce false positives when emulating an ICS.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, no. June, pp. 49–51, 2011. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5772960

[2] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, "Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 2, pp. 114–123, 2014.

[3] L. Rist, D. Haslinger, J. Smith, J. Vestergaard, and A. Pasquale, "Conpot honeypot," 2013.

[4] M. Winn, M. Rice, S. Dunlap, J. Lopez, and B. Mullins, "Constructing cost-effective and targetable industrial control system honeypots for production networks," *International Journal of Critical Infrastructure Protection*, 2015.

[5] E. Vasilomanolakis, S. Karuppayah, M. Fischer, M. Mühlhäuser, M. Plasoianu, L. Pandikow, and W. Pfeiffer, "This Network is Infected : HosTaGe - a Low-Interaction Honeypot for Mobile Devices," in *Security and privacy in smartphones & mobile devices*. ACM, 2013, pp. 43–48.

[6] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *Proceedings of the 22nd USENIX Security Symposium*, 2013, pp. 605–619.

[7] V. Total, "Virustotal-free online virus, malware and url scanner," 2012.