HoneyPlant: A Distributed Hybrid Honeypot System for ICS Security

Sam Maesschalck
Security Lancaster
Lancaster University
s.maesschalck@lancaster.ac.uk

Vasileios Giotsas
Security Lancaster
Lancaster University
v.giotsas@lancaster.ac.uk

Benjamin Green
Security Lancaster
Lancaster University
b.green2@lancaster.ac.uk

Nicholas Race
Security Lancaster
Lancaster University
n.race@lancaster.ac.uk

Industrial Control systems are a vital component within critical national infrastructure such as the power grid, water treatment and nuclear power plants [1]. The criticality of these systems makes them an attractive target for cyber-criminals and state-sponsored adversaries, which is highlighted by the increasing number of serious incidents [2]. Timely detection of intrusion attempts is critical for preventing attackers from reaching sensitive parts of ICS networks. Honeypots are part of the best practices, as they can provide valuable threat intelligence and slow down or even completely misdirect attackers. Nonetheless, ICS-specialized honeypots are sparse and not widely deployed [3]. Poorly configured honeypots or honeypots that lack realistic interactivity can be easily avoided or even exploited by skilled attackers [4]. Additionally, even when honeypots are successfully used to trap an attacker, analysing and correlating the collected data and reconfiguring the network accordingly can be a time-consuming and largely manual process. The overheads of honeypot data analysis may inhibit timely and proactive attack mitigation [5, 6].

The proposed system aims to address the shortcomings of the current industrial honeypot implementations, by combining a network of honeypots distributed across the Internet, with honeypots situated within the ICS network. Distributed honeypots are used to gather threat intelligence on botnets and scans in-the-wild such as patterns of targeted services and ports and source IPs where these scans originate. Together with blacklists, the data captured by these honeypots, are used to calibrate firewalls and IDS and ensure no device within the protected network has the same signatures as the attacked ones. The internal honeypots are divided between a compartmentalized honeypot network and the operational network. The honeypot network hosts several high-interaction honeypots including ICS and standard IT infrastructures such as domain controllers, web and email servers and clients. These honeypots are designed to lure attackers to them instead of the operational network [7] and should be configured as if it was one. Data gathered from these honeypots provide data on current forms of malware and new exploitable vulnerabilities [8]. The honeypots within the operational network will be used to gather current threats mitigating within it and will allow administrators to gain valuable knowledge about the security of their network and systems. We suggest these honeypots to be low-interactive, to limit risks as high-interaction honeypots can be taken over by malicious attackers [9]. The collected data will be automatically fed to a cloud-hosted server to store and analyse the captured traffic using state-of-the-art machine learning techniques [10]. Due to the nature of the process, the accuracy will improve over time. This analysed data can then be fed into an SDN based network controller which will automatically reconfigure the network to mitigate potential detected vulnerabilities.

References

[1] B. Green, M. Krotofil, and A. Abbasi, “On the significance of process comprehension for conducting targeted ICS attacks,” CPS-SPC 2017 - Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, co-located with CCS 2017, pp. 57–68, 2017.

[2] Humayed, A., Lin, J., Li, F. and Luo, B., 2017. Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), pp.1802-1831.

[3] Iturbe, M., Garitano, I., Zurutuza, U. and Uribeetxeberria, R., 2017. Towards large-scale, heterogeneous anomaly detection systems in industrial networks: A survey of current trends. Security and Communication Networks, 2017.

[4] Mokube, Iyatiti, and Michele Adams. "Honeypots: concepts, approaches, and challenges." Proceedings of the 45th annual southeast regional conference. 2007.

[5] McGrew, Robert. "Experiences with honeypot systems: Development, deployment, and analysis." In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), vol. 9, pp. 220a-220a. IEEE, 2006.

[6] Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C. and Schönfelder, J., 2016. A survey on honeypot software and data analysis. arXiv preprint arXiv:1608.06249.

[7] The Honeynet Project, Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Addison-Wesley, 2001.

[8] M. Skrzewski, “Network Malware Activity – A View from Honeypot Systems,” in Computer Networks , A. Kwiecien, P. Gaj, and P. Stera, Eds. Berlin: Springer, 2012, pp. 198–206

[9] A. Vetterl and R. Clayton, “Bitter Harvest: Systematically Fingerprinting Low-and Medium-interaction Honeypots at Internet Scale,” 12th USENIX Workshop on Offensive Technologies (WOOT 18), 2018.

[10] Yen, Ting-Fang, and Michael K. Reiter. "Traffic aggregation for malware detection." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 207-227. Springer, Berlin, Heidelberg, 2008.