Hasso Plattner Institut
Digital Engineering · Universität Potsdam

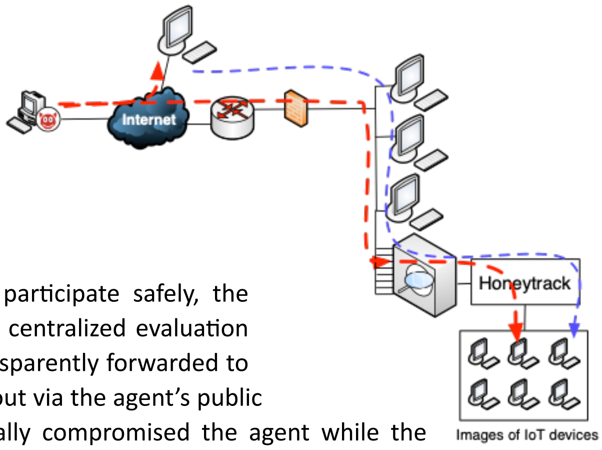
Master Project WiSe 2022/23

Distributed High-Engagement Honeypots

FG Cybersecurity and Enterprise Security, Prof. Dr. Christian Dörr

Project Goal

While defenders typically collect and mine connection attempts to servers and workstations as a measure to quantify exposure, this analysis provides only limited insights into how malicious actors are trying to compromise a system and what they are subsequently trying to do. For instance, an increased volume of connections to TCP 443 could potentially indicate a new vulnerability on a web server software, but only by posing as a potential victim, negotiating a connection and recording the interaction with the victim the defender can likely learn the real intentions behind the connection attempt. As it is prohibitive to deploy "real" vulnerable services, defenders typically turn to honeypots as decoys, which do not risk exposure of valuable data and may be disposed afterwards.



In this project, we are going to evolve existing specialized research prototypes into a multi-purpose distributed honeypot framework for high-engagement honeypots on different platforms. With this framework, researchers can efficiently deploy victim systems at scale by providing container or virtual machine images, which are dynamically spun up whenever an adversary connects to them.

To encourage community involvement and allow users to participate safely, the framework is comprised of two systems, a local agent and a centralized evaluation environment. Connection attempts to the local agent are transparently forwarded to the central honeypot installation and results are routed back out via the agent's public connection, so that it appears that the adversary has actually compromised the agent while the experiment is safely running within the central enclave of our honeypot system. The framework controls the entire stack of the communication, and is thereby able to let the exposed victims appear as legitimate servers or as obvious decoys to determine the sophistication and level of interactions of attackers with the honeypots. The key engineering components of transparent tunneling of adversary connections to images has already been successfully validated.

As an open platform for adversarial research, the platform has be hardened against malicious agents, apply rate limiting and selective filtering to prevent potential abuse against third parties, and allow to save state so that adversaries can return to "their" machine to continue an ongoing compromise. In the last stage of this project, we will deploy a vulnerable router firmware, a vulnerable VPN service, and the SMB file sharing service, three types of services that currently see majorly exploitation campaigns on the Internet for a peek into the current threat landscape.

Contact Information

Prof. Dr. Christian Dörr christian.doerr@hpi.de Haus III, G-3.1.09