Cybersecurity Internship (M2)

EP CIDRE Inria / CentraleSupelec / CNRS / Univ. de Rennes 1 – IRISA

Test coverage of an attacker's capabilities

Gilles Guette, Valérie Viet Triem Tong
EPC INRIA CIDRE, Rennes, France
gilles.guette@univ-rennes1.fr
valerie.viettriemtong@centralesupelec.fr

Keywords: Security - Tactics, Techniques and Procedures (TTP) - Test - deception

An advanced persistent threat is a stealthy threat actor, which regularly targets or involves nation-states and large companies. An Advanced Persistent Threat (i) pursues its objectives repeatedly over an extended period of time (ii) adapts to defender's efforts to resist it and (iii) is determined to maintain the level of interaction needed to execute its objectives. The attacker's lifecycle can be divided into three operational phases: Initial compromission, exploration phase and exploitation phase [1].

During each of these phases, the attacker exposes its operational capabilities which are techniques similar to those listed in MITRE ATT&CK matrix and represents a part of its Tactics, Techniques and Procedures (TTP) [2, 3].

The level of threat posed by the attacker is measured by the variety of attack techniques he masters. These techniques can be qualified by their technical complexity, their efficiency, their novelty, their stealth. Most of these techniques are reported in the MITRE ATT&CK^{TM} framework. This matrix is a knowledge base that reports tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.

In this context, it is crucial for the defender to quickly measure the attacker's capabilities. A defender can use a honeynet: a computer network that's intended to attract cyberattacks[4, 5]. Such a network can be used to observe the actions of an attacker and allows to measure his technical skills. To this end, the honeynet has to expose services that are susceptible to be attacked. The attacker's abilities that can actually be observed are therefore directly related to the exposed services.

The question explored in this internship is define and measure the coverage of attacker capability tests covered by a deceptive architecture.

The purpose of this internship is to model, specify and start to implement, an architecture designed to test the concrete capabilities of an attacker.

To achieve this objective, the intern will have to propose a model allowing to deal with the technical skills of the attacker, the vulnerabilities of a service and a system architecture exhibiting those vulnerable services. The trainee will be able to draw on research work on decoy networks, on MITRE's knowledge bases. The student will be able to rely on research works in progress in the CIDRE team in collaboration with the cybersecurity office of the Institute for Radiation Protection and Nuclear Safety (IRSN). In particular, the intern will be able to rely largely on a first developed prototype.

Location The internship will be granted and will take place in Rennes on the Beaulieu campus within the Inria CIDRE project team, starting in February 2021 for a duration of 5 to 6 months. It will be supervised by Aimad Berady, Gilles Guettes, Valérie Viet Triem Tong of the Inria CIDRE team in collaboration with Mathieu Jaume (LIP6) and Olivier Fichot (IRSN).

Contacts Gilles Guette `gilles.guette@univ-rennes1.fr`
Valérie Viet Triem Tong `valerie.viettriemtong@centralesupelec.fr`

References

[1] Aimad Berady, Valérie Viet Triem Tong, Gilles Guette, Christophe Bidan, and Guillaume Carat. Modeling the Operational Phases of APT Campaigns. In *CSCI 2019 - 6th Annual Conference on Computational Science and Computational Intelligence*, Las Vegas, United States, December 2019. IEEE.

[2] F. Maymí, R. Bixler, R. Jones, and S. Lathrop. Towards a definition of cyberspace tactics, techniques and procedures. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 4674–4679, 2017.

[3] The MITRE Corporation. The mitre att&ck matrix for enterprise, 2018.

[4] Timothy Barron and Nick Nikiforakis. Picky attackers: Quantifying the role of system properties on intruder behavior. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, pages 387–398, 2017.

[5] Chris Moore. Detecting ransomware with honeypot techniques. In *2016 Cybersecurity and Cyberforensics Conference (CCC)*, pages 77–81. IEEE, 2016.