Risk-Based & Honeypot-Informed Moving Target Defence (RB&HI MTD)

Ronny Blostein, Natalija Vlajic
Department of Electrical Engineering and Computer Science, York University, Toronto, Canada

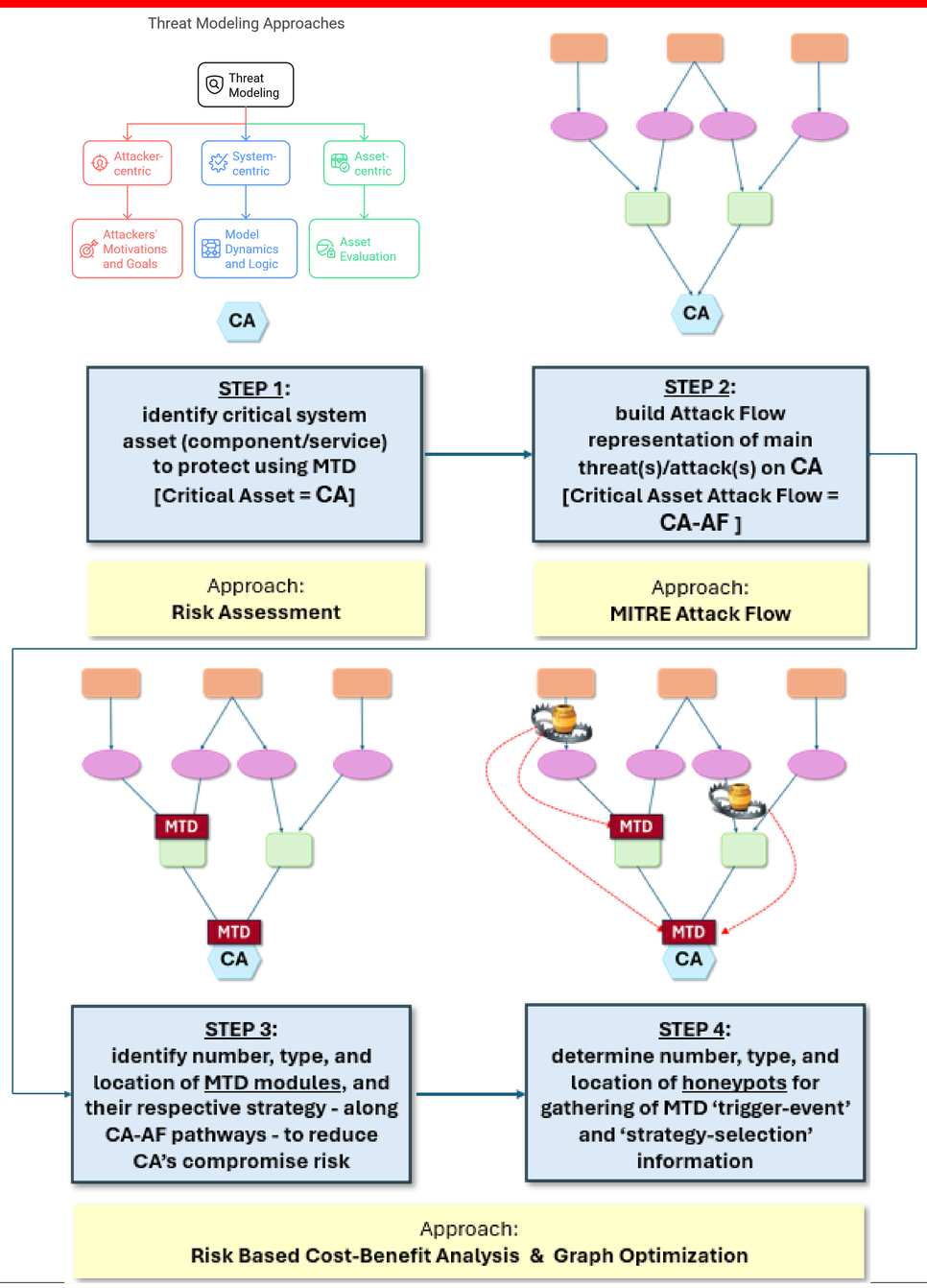
Moving Target Defence (MTD)	Cyber-Deception (Honeypot)
Altering properties of a system either randomly, regularly, or upon event-detection with little to no effect on performance. Main objective is to increase complexity for attackers by decreasing attack opportunities and exhausting adversarial resources. Relies on three design principles: • What to move – which property to manipulate • How to move – shuffling, diversity, redundancy, and hybrid. • When to move – periodical, event-based, hybrid. Examples IP shuffling/mutations/host randomization, port hopping, packet header randomization, network topology shuffling, VM/proxy migrations, code/programming language diversity, redundancy of software components of network sessions.	Deception-based measures attempt to draw attackers away from the target system and take in/actions that would benefit the system. Honeypots are deception-based tools that aim to waste attacker resources by mimicking systems or modules of a system. This tool offers three functionalities – detection, prevention, and research. They are often categorized by their characteristics such as interaction level, implementation, activities, etc. Examples SIPHON portrays physical IoT devices, HoneyIo4 simulates partial capabilities of a chosen device, HIoTPoT occupies attacker in a fake environment, IoTPOT emulates Telnet services.

Objective

Use the Information from the honeypot to calibrate the MTD

Risk-Based & Honeypot-Informed MTD

Deployment



Details

Taking high interaction research honeypot such as HoneyPLC, not only with high level of adversarial deception, but also data collecting abilities. The logs produced from a honeypot such as this contain every interaction that takes place during the (suspected) attack on the decoy. These logs are then analyzed by the MTD and can lead to three possible attack scenarios.

Scenario 1: Honeypot thwarts attack	The attacker fails to proceed past the honeypot phase, either believing the decoy is the real system, or all of the attacker's resources have been exhausted. Data is gathered from the honeypot for further MTD calibration and attack analysis.
Scenario 2: Bypassed Honeypot, attacking real system	a) Honeypot is compromised; Intrusion Detection System noticed the attack and the MTD is calibrated using the collected information. The attacker is now attacking the real system.
	b) Honeypot is compromised; Attack is undetected by the IDS. Data relating to the attack is analyzed later for better MTD calibration.
Scenario 3: Honeypot was never attacked	Honeypot was never attacked, no data collected. MTD runs at default settings.

In our **Adaptive HI-MTD** system, the volume and type of data gathered by the honeypot determines the 3 key MTD parameters: nature (what), type (how), and frequency (when) of deployed system changes.
E.g., higher activity observed by the honeypot will/should result in an increase in the frequency of MTD changes.

References
Rongbo Sun, Yuefei Zhu, Jinlong Fei, and Xingyu Chen. 2023. A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive. MDPI Journal of Applied Sciences 13, 9 (2023). doi:10.3390/app13095367

Amir Javadpour, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaï d. 2024. A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers Security 140 (2024), 103792. doi:10.1016/j.cose.2024.103792

Mengmeng Ge, Jin-Hee Cho, Dongseong Kim, Gaurav Dixit, and Ing-Ray Chen. 2021. Proactive Defense for Internet-of-things: Moving Target Defense With Cyberdeception. ACM Trans. Internet Technol. 22, 1, Article 24 (Sept. 2021), 31 pages. doi:10.1145/3467021

Xupeng Luo, Qiao Yan, Mingde Wang, and Wenyao Huang. 2019. Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT. In 2019 Comput- ing, Communications and IoT Applications (ComComAp). 392–395. doi:10.1109/ ComComAp46287.2019.9018775

Amal O. Hamada, Mohamed Azab, and Amr Mokhtar. 2018. Honeypot-like Moving- target Defense for secure IoT Operation. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 971–977. doi:10.1109/IEMCON.2018.8614925

Efrén López-Morales, Carlos Rubio-Medrano, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Gail-Joon Ahn. 2020. HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 279–291. https://doi.org/10.1145/3372297.3423356