Guaranteed Trade-Offs in Dynamic Information Flow Tracking Games

Kush Grover

Technische Universität München

Advanced persistent threats (APTs) are targeted attacks in which the attacker gains illegitimate access to a system and stays there undetected for a long period of time. Attackers use prolonged and stealthy incursion techniques, which are customized to specific targets in order to gather confidential data and sabotage critical infrastructures. Such an attack was carried out in 2013, when Target corporation's network was breached, resulting in 40 million credit and debit card details along with 70 million records of personal information being stolen [1]. In this case, the attackers entered the system by compromising a third party vendor and stayed there undetected for about two weeks while gathering sensitive information. APTs are methodically designed to bypass conventional security mechanisms making them difficult to detect.

Even though detecting APTs is difficult, their interaction with the system creates information flows such as data-flow and control-flow commands, which are recorded in the system logs. Dynamic Information Flow Tracking (DIFT) is a widely used mechanism to analyze these information flows. DIFT "tags" suspicious input/output data channels and traces the propagation of the tagged information through the system. However, this increases the memory and performance costs on the system since it involves tracking and analyzing large number of innocuous flows [2]. Our aim is to optimally select where to perform the security analysis on, for resource-efficient detection.

In this work, we model the strategic interactions between APT and DIFT as a game on the information flow graph (IFG). The position of the information on the IFG along with the actions of the attacker and defender yields a probability distribution on the transitions in the game. This game is concurrent since the probability of a successful attack by APT and an effective defense by DIFT depend on the actions of both the defender and the attacker. Also, it's a non-zero-sum game since it captures the trade-off between DIFT's resource efficiency and detection effectiveness. Overall, the interaction was modeled as non-zero-sum concurrent stochastic games.

We give a gadget to convert this concurrent game into a turn-based one and we also convert the non-zero-sum game to a multi-dimensional (zero-sum) game. This more interpretable formulation allows us to ask and answer questions such as "What cost does the defender need to pay to achieve the maximum probability of trapping the attacker?", "What is the highest probability to trap the attacker by a defence cheaper than 10" or what the possible tradeoffs are. In contrast to the previous learning-based solution [3], we provide a guarantee on the result in the form of a probably approximately correct (PAC) best-/worst-case analysis.

This is a joint work with Maximilian Weininger, Shruti Misra and Jan Křetínský which was accepted for presentation in CDC 2021.

References

[1] Xiaokui Shu, Ke Tian, Andrew Ciambrone, Danfeng, and Yao. Breaking the target: An analysis of target data breach and lessons learned. 01 2017.

[2] Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alessandro Orso, and Wenke Lee. Rain: Refinable attack investigation with on-demand inter-process information flow tracking. pages 377–390, 10 2017.

[3] Shruti Misra, Shana Moothedath, Hossein Hosseini, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran. Learning equilibria in stochastic information flow tracking games with partial knowledge. pages 4053–4060, 12 2019.