STIXChecker: From STIX sharing to Automated Threat Intelligence and Response

Cyber threat intelligence and information sharing with peers and partners is becoming an emergent necessity and a key success component for organizations to use their cyber defense efforts productively and efficiently in the face of adversary. STIX is an evolving, collaborative effort to develop a language that provides structured threat information representations.

Security administrators strive to protect networks against cyber threats. However, STIX contains wealth of attack information and utilizing this information to make cyber defense decisions such as using the appropriate counter measures and network reconfigurations to provide defense on the basis of this information is a difficult process and requires extensive network and threat analysis. Also, blindly fixing all vulnerabilities and reconfiguring the network in a way to protect it against attacks is very expensive strategy. Security requirements are not the only aspect of the problem; there are mission and usability requirements to consider as well. Thus, finding a solution that resolves the contention between security and mission requirements within a given budget, is a challenging and complex problem.

In this work, we analyze, extract and formalize STIX attacks in a symbolic logic-based notation and augment it with the enterprise network configuration to (1) provide risk analytics imposed on the enterprise network by these attacks. To this end, we propose a new metric to quantitatively measure the impact of each attack kill chain phase to the assets and mission of the targeted network. (2) devise a plan to reduce the risk by containing the impact and/or stopping the attack progress considering the trade-off between the attack prevention cost and impact. For this purpose, we encode the system model, mission and security requirements, and counter measures as a constraint satisfaction problem using SMT logics solver. Namely, Microsoft efficient SMT solver Z3, which solves large numbers of constrains in a timely manner [SMT][Z3 Java API].

We model (i) the attacks from STIX feeds, (ii) the network configurations using ConfigChecker, (iii) the system mission and security requirements, and then implement our proposed metric to provide a holistic view of the system's proactive resilience in the face of cyber-attacks.

We devise a plan with the optimal (i.e., minimum) vulnerability fixes and reconfiguration of the network to achieve an acceptable level of security, while satisfying the mission requirements in the face of attacks. For this, we provide cost-benefit analysis for the impact induced by each threat kill chain phase to the network and mission assets, and the cost to prevent each phase from progressing to the next one.