Chris Curry

Threat Modeling: Concepts and Actions

Organizational resources devoted towards cybersecurity, no matter how robust, will always have limitations. These limits may be a result of manpower, computational complexity, cost, time, knowledge, etc. Therefore, it is existentially vital that these assets are operationally employed to protect the organization and its stakeholders against the most dangerous and most likely adversarial threats. Threat Modeling, when properly executed, can uncover these attack vectors where defensive resources should be concentrated. Furthermore, threat modeling can highlight those critical nodes in which security controls must be tested. Likewise, these nodes provide realistic targets to enhance attack scenarios for tailored adversarial simulations. The end result is an organization with critical systems hardened against their most probable threats, and equally important, heightened confidence held by those that rely on the organization. For this session, threat modeling concepts are reviewed and evaluated. Methods to mature our model using attack frameworks and threat intelligence are discussed. Next, a notional organization, attack framework, and threat intelligence are given, and a concise threat model is constructed. Finally, security solutions tied to the threat model are constructed from the mindset of a Blue Team, and an adversarial attack plan is constructed from the mindset of a Red Team. The end result is a mature model constructed by security professionals with a thorough understanding behind the emplacement of defensive controls and the attacker's courses of action.

Biography is available on the next page

Biography

Chris Curry is a Cyber Operations Officer in the Delaware Air National Guard, specializing in cyber capability development, vulnerability research, and security assessments. His work with security assessments is coordinated with the Delaware Department of Technology & Information (DTI), where he joins a cadre of National Guard members and DTI's Security Operations team to war game the range of cyber threat scenarios scoped to protecting the State's critical infrastructure. Additionally, Chris works full-time for ICR, inc. as a computer engineer and reverse engineer specializing in embedded and Radio-Frequency (RF) systems. With ICR, he continues to serve as project lead and lead engineer on myriad projects supporting technical research and perpetual capability development for the company's government customers. Prior to joining the Air Force and ICR, Chris served as an active-duty officer in the Marine Corps, leading the operations element for a cyber operations unit at Fort Meade, MD. Before specializing in cyber operations, Chris was an AV-8B Harrier II attack pilot supporting multinational and joint engagements while deployed on shipborne expeditionary tours. Prior to transitioning to the computer security world, Chris earned a graduate degree in Computer Science from the Whiting School of Engineering at Johns Hopkins University in his home state of Maryland.