CrossTalk would like to thank DHS for sponsoring this issue.

Protecting Our Cyber Infrastructure From Predatory Practices

Part of our role at DHS is to better enable all stakeholders to secure their part of cyberspace. Given that our adversaries will exploit even the smallest weakness, identifying and mitigating exploitable weaknesses before they become a pathway for attack is vital to the defense against predatory practices. One weak link in the chain can compromise an entire software application and degrade our enterprise capabilities.

Organizations must understand their information asset vulnerabilities. In order to assess the nature and extent of these vulnerabilities, organizations must first collect a consistent set of metrics. The Federal Government is collecting metrics with the help of the CyberScope Initiative, which mandates that federal civilian agencies report cybersecurity data using standardized formats. The CyberScope application is a web-based interactive tool that allows agencies to report data that complies with Federal Information Security Management Act (FISMA) rules. Ultimately, this tool helps federal agencies identify weaknesses, thus enabling the cyber enterprise to better defend against predatory attackers by making their assets more resilient.

Successful collection and analysis of metrics relies on standards. One standardized reporting format, a dictionary of software flaws called the Common Weakness Enumeration (CWE), provides required information feeds for FISMA reporting. The DHS National Cyber Security Division, through its Software Assurance (SwA) program, facilitates public-private collaboration that advances CWE. CWE now includes the Common Weakness Risk Analysis Framework (CWRAF) and the Common Weakness Scoring System (CWSS), which provide consistent, flexible means for identifying and mitigating the highest priority risks. CWRAF enables users to incorporate the CWSS scoring criteria to identify the most exploitable software fault patterns for web applications, control systems, embedded systems, end-point computing devices, operating systems, databases, storage systems, enterprise system applications, and cloud computing services. Identifying and mitigating exploitable software weaknesses before they become vectors of attack are some of the most effective means for addressing predatory practices.

The SwA program also sponsors other security automation enumerations and languages that enable consistent, interoperable reporting among IT security tools and services. These open, voluntary standards accelerate actionable information exchange within the incident response community. The set of standards include the Open Vulnerability and Assessment Language, the Common Attack Pattern Enumeration and Classification, and the Malware Attribute Enumeration and Characterization. These languages and enumerations are resources that help software engineers and enterprise IT security managers to identify and correct errors early in and throughout the software lifecycle. Integrating security into the software lifecycle is a critical practice and vital to the safety and resilience of our software-enabled systems.

Powerful tools and services that use these enumerations and languages already exist–and the ranks of users are growing quickly. This CrossTalk issue will alert participants in the software lifecycle of certain predatory practices and enable them to arm themselves with means that efficiently find and assist in mitigating software security flaws.

Roberta "Bobbie" Stempfley
Acting Assistant Secretary,
Office of Cybersecurity and Communications
Department of Homeland Security