Security Metrics

Estimating a System's Mean Time-to-Compromise

Mean time-to-compromise is a comparative security metric that applies lessons learned from physical security. Security architects and managers can use MTTC intervals to intelligently compare systems and determine where resources should be focused to achieve the most effective cost/MTTC ratio.

David John Leversage
British Columbia Institute of Technology

Eric James Byres
Byres Security

One of the challenges network security professionals face is providing a simple yet meaningful estimate of a system or network's security preparedness to management, who typically aren't security professionals. Although enumerating system flaws can be relatively easy, seemingly simple questions such as, "How much more secure will our system be if we invest in this technology?" or "How does our security preparedness compare to other companies in our sector?" can prevent a security project from moving forward.

This has been particularly true for our area of research—the security of Supervisory Control and Data Acquisition (SCADA) and industrial automation and control systems (IACS) used in critical infrastructures such as petroleum production and refining, electricity generation and distribution, and water management. Companies operating these systems must invest significant resources toward improving their systems' security, but upper management's understanding of the risks and benefits is often vague. Furthermore, competing interests for the limited security dollars often leave many companies basing decisions on the best sales pitch rather than a well-reasoned security program.

The companies operating in these sectors aren't unsophisticated. Most have many years of experience making intelligent business decisions on a large variety of multifaceted issues on a daily basis. For example, to be profitable [illegible] well-reasoned decisions on global operations without getting mired in the details.[1]

In our discussions with management and security administrators at these companies, they repeatedly pointed out those similar types of performance indicators could be useful for making corporate security decisions. What these companies wanted wasn't proof of absolute security, but rather a measure of relative security. To address this need in the SCADA world specifically and the corporate IT security world more generally, we propose a mean time-to-compromise (MTTC) interval as an estimate of the time it will take for an attacker with a specific skill level to successfully impact a target system (see the "A brief history of MTTC" sidebar). We also propose a state-space model (SSM) and algorithms for estimating attack paths and state times to calculate these MTTC intervals for a given target system. Although we use SCADA as an example, we believe our approach should work in any IT environment.

Lessons learned from physical security

Determining a safe's burglary rating is similar to determining a network's security rating. Both involve a malicious agent attempting to compromise the system and take action resulting in loss. Safes in the US are as-