Chapter 107
Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments

Eric D. Vugrin
Sandia National Laboratories, USA

Jennifer Turgeon
Sandia National Laboratories, USA

ABSTRACT

Cyber resilience is becoming increasingly recognized as a critical component of comprehensive cybersecurity practices. Current cyber resilience assessment approaches are primarily qualitative methods, making validation of their resilience analyses and enhancement recommendations difficult, if not impossible. The evolution of infrastructure resilience assessment methods has paralleled that of their cyber counterparts. However, the development of performance-based assessment methods has shown promise for overcoming the validation challenge for infrastructure systems. This article describes a hybrid infrastructure resilience assessment approach that combines both qualitative analysis techniques with performance-based metrics. The qualitative component enables identification of system features that limit resilience, and the quantitative metrics can be used to evaluate and confirm the effectiveness of proposed mitigation options. The authors propose adaptation of this methodology for cyber resilience analysis. A case study is presented to demonstrate how the approach could be applied to a hypothetical system.

INTRODUCTION AND BACKGROUND

Cybersecurity is generally acknowledged as a critical priority within the national, homeland, and business security communities. This sentiment has been echoed at the highest levels of the U.S. government, with President Obama (2009) stating that "cyber threat is one of the most serious economic and national security challenges we face as a nation."

Fortunately, the concept of cybersecurity is not new to the academic and research communities.

DOI: 10.4018/978-1-4666-5942-1.ch107

Cyber security standards and guidelines have been developed (e.g., see Smart Grid Interoperability Panel, 2010; IEEE, 2000, 2010a,b; NERC, 2002; ISO/IEC, 2000). These standards typically list best practices and provide guidance for securing various systems. Existing standards generally focus on mitigating system vulnerabilities to prevent a successful attack from occurring. Some guidelines, such as Guidelines for Smart Grid Cyber Security: Volumes 1-3 (Smart Grid Interoperability Panel, 2010), recommend prioritizing vulnerability mitigations by performing a risk assessment to determine which threats are of most significant concern. Within current standards, the primary focus is on preventing a successful attack. The current cybersecurity philosophy, as represented in these standards, centers on the detection and prevention of an attack.

However, over the past decade, a small but emerging movement within the cybersecurity community has voiced the opinion that cybersecurity strategies must expand beyond the protection-centric focus to incorporate cyber *resilience* principles. Cyber threats are constantly evolving and increasing as the number of cyber assets and system vulnerabilities continues to grow. As Goldman (2010) states, "The notion that we can achieve 100% protection is not only unrealistic but also results in a false sense of security that puts our missions and businesses at serious risk." Franklin D. Kramer (2011), Vice Chair of the Atlantic Council and former Assistant Defense Secretary for International Affairs, affirms that statement and adds that "we cannot assume protection and prevention will be adequate. And so we need resilience. " Similarly, the private sector has recognized the need for resilience, as evidenced by the launch of the World Economic Forum's Cyber Resilience Initiative. This initiative is aimed at creating partnerships within the public and private sectors to foster cyber resilience (World Economic Forum, 2012). Similar opinions are becoming more common with events such as the STUXNET virus, the Chinese attack on Google, and suspected attacks on power grids. Hence, many have called for cyber resilience to become a primary system objective in cybersecurity activities.

Cyber resilience can be described as a cyber system's ability to function properly and securely despite disruptions to that system. Disruptions can be cyber or physical; they can also be intentional, accidental, or random. Over the past decade, organizations such as the Carnegie Mellon University's Software Engineering Institute and MITRE Corporation led efforts to develop cyber resilience management and design practices. These ground-breaking efforts are significant advances toward the development of resilient cyber systems. However, they have the same limitation that cybersecurity standards have: that is, they are descriptive methods that recommend approaches for increasing resilience, but the emerging cyber resilience standards have yet to be validated.

In parallel to cyber resilience-related efforts, the infrastructure protection community is developing infrastructure resilience assessment methods. Similarities exist between the evolutions of cyber and infrastructure resilience assessment methods. However, a class of infrastructure resilience assessment methods, termed performance-based assessment methods, overcame the validation limitation by evaluating system outputs rather than system structure and design. By measuring the performance of infrastructure systems rather than system structure and attributes, performance-based assessment methods address the central resilience issue: can the infrastructure system continue to deliver critical services in the presence of disruptive events?

This article presents a particular performance-based infrastructure resilience assessment framework that shows promise for extension to cyber resilience. In the following section, the article reviews recent resilience assessment methods from the cyber and infrastructure communities and the parallel evolution of their respective assessment methods. The article then introduces a performance-based infrastructure resilience as-