

Cyber Resilience-by-Construction

Ehab Al-Shaer and Yasir Imtiaz Khan

The need of cyber security is increasing as cyber attacks are escalating day by day. Cyber attacks are now so many and sophisticated that many will unavoidably get through. Some of the broad impacts of cyber attacks are subject to denial of services, theft of intellectual property, credit card breaches, national security, and health care. The employment of intrusion detection systems and secure perimeter firewalls provide no full immunity to network from sophisticated attacks. Therefore, there is an immense need to employ resilient architectures to defend known or unknown attacks. The central idea of cyber resilience is to avoid or minimize the potential damage that may be caused by the cyber attacks instead of blocking or stopping them. Engineering resilient system/infrastructure is a challenging task, which implies how to measure the resilience and how to obtain sufficient resilience necessary to maintain its service delivery under diverse situations. This proposal has following research objectives; the first is to propose a formal approach to measure cyber resilience from different aspects (i.e., attacks, failures) and at different levels (i.e., pro-active, resistive and reactive). The initial version of a formal framework named as: *Cyber Resilience Engineering Framework (CREF)* has been proposed [1]. The second objective is to build a resilient system by construction. The idea is to build a formal model of a cyber system, which is initially not resilient with respect to system mission (to be measured by CREF). The system mission refers to the preservation of confidentiality, availability and integrity properties. Then by systematic refinements of the formal model and by its model checking, we attain resiliency. For the experimentation purpose, we are interested to take firewalls and network configurations case studies.

1) Khan, I, Yasir. Alshaer, E and Rauf, U. "Cyber resilience by construction: Modeling, measuring and Verifying" to appear in SafeConfig 2015: Automated Decision Making for Active Cyber Defense, The Denver Marriot City Center, Denver, Colorado, USA October 12, 2015.