ASYMMETRIC RESILIENT CYBERSECURITY

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Asymmetric Resilience in Cyber Systems

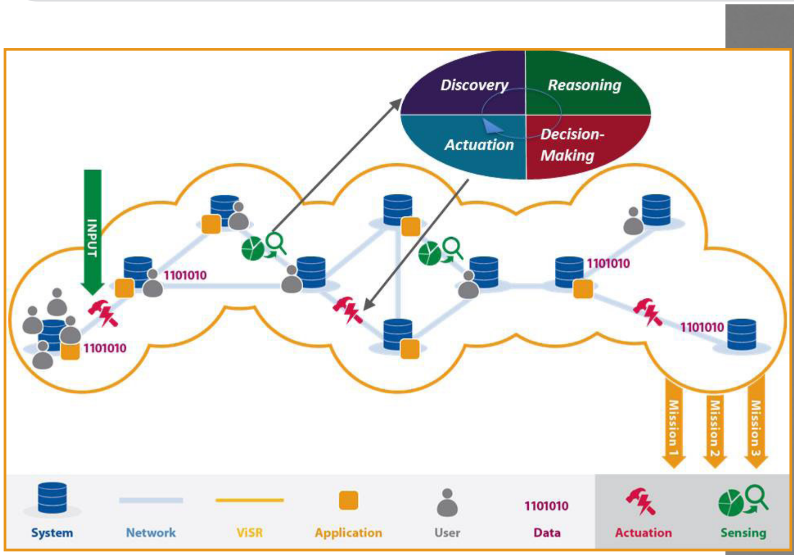
CHALLENGE

Traditional approaches to cybersecurity allow asymmetry in favor of the adversary by requiring the defender to successfully respond to each adversary attack while allowing a persistent adversary to learn from each failure and ultimately succeed in their objective. This project will work towards developing and evaluating an integrated methodology for demonstration of asymmetric resilience in cyber systems that will shift the focus from the unrealistic goal of a perfect defense to resilient technologies that maintain in the face of impediments in contested systems. These technologies respond to adversaries when necessary, and quickly recover when degraded below an acceptable threshold. Success of these technologies may be able to move the asymmetric advantage from the adversary to the defender.

Developing and evaluating an integrated methodology for demonstration of asymmetric resilience in cyber systems

CURRENT PRACTICE

Resilient cybersecurity in enterprise systems is not the state-of-practice today. Traditional cybersecurity has primarily focused on the strategies of detection, deterrence, denial, delay, and defense of adversaries. However, this method has not been very successful in preventing novel attacks, and there is little-to-no objective evidence that such practices allow the cyber system to maintain mission capability in a contested environment. Further, this approach allows an asymmetry in favor of the adversary by requiring the defender to successfully respond to each adversary attack while allowing a persistent adversary to learn from each failure and ultimately succeed in their objective.



Conceptual integration of asymmetric resilience technologies with operational cyber systems.

Building secure, resilient systems requires multiple disparate technologies, and is complex, time consuming, and expensive. Research to-date has focused on specific aspects of resiliency, and most

U.S. DEPARTMENT OF
ENERGY

approaches depend on some form of redundancy and transparent state migration. Solutions that address fault-tolerance are generally focused on providing resiliency to a specific type of fault and do not address all possible faults or hazards.

APPROACH

Developing resilient cybersecurity requires:

1. Categorization of available technologies, both Asymmetric Resilient Cybersecurity (ARC) and non-ARC developed, by functionality and assigning these technologies to one or more parts of the Discover-Reason-Decide-Act loop. This stage also enables requirements definition and a gap assessment of these technologies.
2. Design of the integrated technology stack that leverages current technical developments within the ARC initiative and incorporates specific complementary technologies where gaps exist.
3. Implementation and evaluation of integrated technology. The evaluation of the integrated approach to asymmetric resilience depends on the specific impediments (i.e. attacks or hazards) that impact the cyber system under test. A series of impediments, progressing from simple to complex, are used for this purpose and provide the basis for demonstration of an integrated suite of technologies for asymmetric resilience of cyber systems in a repeatable, scientifically defensible manner. This enables the design and evaluation to show quantitatively that a given technology stack has one of three impacts on a system: it improves resiliency, it does not improve resiliency (i.e. resiliency is unchanged), or it degrades resiliency.

The ARC initiative has resulted in the development of a publication-subscription communication paradigm between the various technologies of the ARC stack. This communication paradigm is being leveraged during the integration process, as it allows a non-linear workflow and also allows technologies or additional input to be easily integrated.

IMPACT

Successful integration and demonstration of a suite of technologies for resilience is expected to benefit a number of entities. Given the ubiquitous nature of cyber systems today and the increasingly common nature of breaches in cybersecurity, the ability to integrate and demonstrate in a repeatable, and scientifically defensible manner, a set of technologies for resilient cyber system operations is necessary before such solutions are deployed with the goal of improving cybersecurity and cyber system mission performance. The outcomes of this current effort will also provide a common, theory-derived framework for quantification of resilience and insights into the impacts of such technologies to operability and security of cyber systems, as well as insights into generalizability of parameters (threat-agnostic vs. threat-specific), bounds of applicability of resilience technologies, and qualitative information on criticality of specific technologies for achieving asymmetric resilient cybersecurity.

Contact

Pradeep Ramuhalli
Principal Investigator
(509) 375-2763
pradeep.ramuhalli@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*