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

The Defender's Role in Resilient Cybersecurity

CHALLENGE

Situational awareness for network defenders is a challenging problem today, even with mostly static networks and well-understood architectures. Resilient technologies, while promising, will likely increase complexity, transitivity, and automation of the network, further compounding the problem of awareness. In order to have a road map for adoption of resilient technologies; it must be shown how those technologies will reduce and not increase the burden of network defense. To do that, we must deeply understand the roles of defenders, how they manage a network given resilient technologies, and the effect of those resilient technologies on defense.

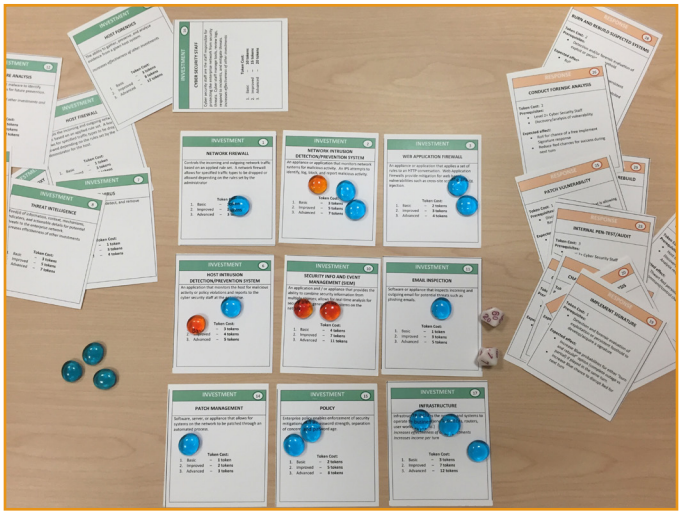
CURRENT PRACTICE

Today, defense and operations focus on a primarily static infrastructure, with many applications built on the assumption that the network is "clean". As we transition to resilient infrastructures, and the assumption that the network is never clean, there is a gap in providing awareness and investigation into resilient environments. Current tools will not provide adequate information given the additional complexity of the system.

APPROACH

To evaluate the impact of resilient infrastructures, we are conducting a human subjects study that tracks cost of implementing technologies, the complexity of those technologies, and evaluates the chosen technologies through an attack scenario. The outcome is a cost function for each study, allowing comparisons between groups of participants, and between the technologies that are available to participants. The study is being conducted in two parts, resilient and traditional

Evaluating how resilient technologies will change the cost and decision making for cyber network defense



An example game board, with selected technologies and investment tokens

Red Rolls:

Stage	1	2	3	4	5	6	7	8	9	10
RECON	10	76	53	70	54	0	0	0	0	0
WEAP	1	27	71	37	8	0	0	0	0	0
EXPLOIT	42	24	82	8	79	0	0	0	0	0
PERSIST	26	60	84	67	48	0	0	0	0	0
C_C	76	27	60	79	44	0	0	0	0	0
ACTIONS	8	11	47	32	97	0	0	0	0	0

Blue Rolls:

Stage	1	2	3	4	5	6	7	8	9	10
RECON	18	25	91	66	63	0	0	0	0	0
WEAP	45	87	66	30	87	0	0	0	0	0
EXPLOIT	57	42	65	99	94	0	0	0	0	0
PERSIST	2	78	2	1	60	0	0	0	0	0
C_C	26	5	43	58	74	0	0	0	0	0
ACTIONS	5	25	88	96	37	0	0	0	0	0

	1	2	3	4	5	6	7	8	9	10
Red Start:	RECON	RECON	C_C	WEAP	ACTIONS	RECON	RECON	RECON	RECON	RECON
Red End:	RECON	RECON	RECON	WEAP	ACTIONS	RECON	RECON	RECON	RECON	RECON

An example of game status tracking. Green cells are success, while red are failures; in this example the red team wins in round 5.

infrastructures. By conducting the study with and without resilient technologies, we aim to evaluate the differences for organizations between the two types of infrastructures.

Understanding that hardly any decision in cyber network defense is made by a single person, we conduct the study using a group of participants, rather than any individual participant. By doing so, we are able to explore the network defense problem space using a distributed representation for group problem solving. This allows us to ensure the complexities of balancing various responsibilities (business, defense, engineering, and intelligence) are captured in the study. This approach has been utilized successfully in many domains, including disaster management and pandemic research by leveraging a table-top exercise to facilitate the group reasoning space.

IMPACT

By conducting the studies focusing on the defender's roles in resilient cybersecurity, we will be providing a valuable foundation for those who wish to develop resilient capabilities. We will identify the impact resilient security has on defense, defender roles, and situational awareness. We look to identify new or potentially disappearing roles; from this, we build a foundation of next generation defensive constructs.

Additionally, we will push the boundaries further by exploring the correct role of defenders in resilient cybersecurity. Assuming advantages in defense are gained through resilient technologies, we explore what roles defenders can play that provide the greatest impact.

Contact

Rick Riensche
Principal Investigator
509-375-4535
rmr@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*