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

Asymmetric Resilient Cybersecurity Overview

JOHN R. JOHNSON

The Cyber Challenge

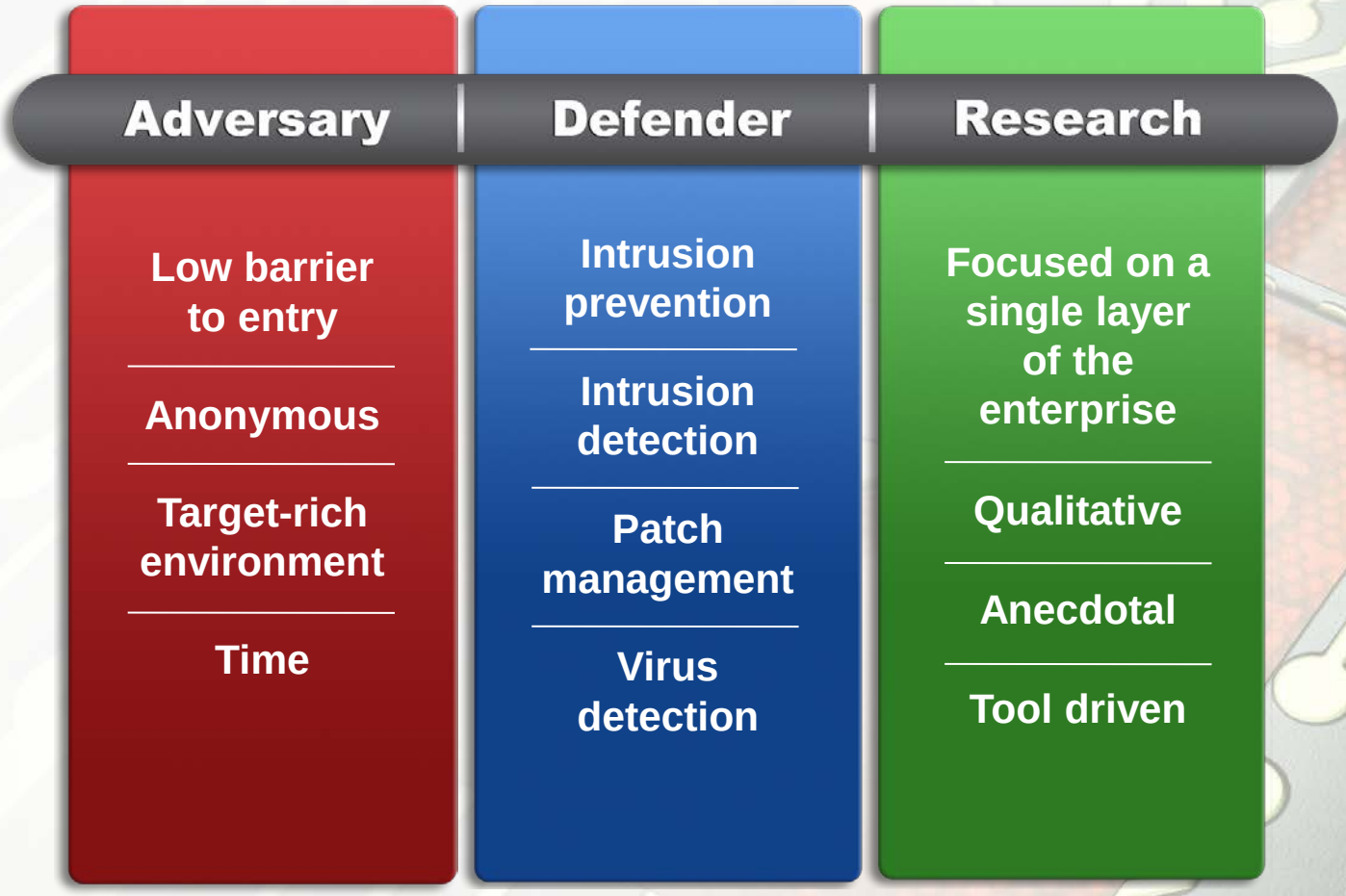
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Adversaries will always have a presence in the enterprise; so why is there so much focus on defending the perimeter?

- Current understanding of cyberspace by practitioners is incomplete
- Defenders rely upon art, practice, and guessing to inform defensive decisions
- The research community lacks a foundational scientific understanding of the cyber domain and security
- Defender costs are grossly disproportional to the cost of an attack
- Infrastructure fragility is commonplace

Today's Landscape

Current enterprises are attack focused, lack resilience, and attackers have an asymmetric advantage.



Asymmetric Resilient Cybersecurity (ARC)

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Our approach is interdisciplinary, holistic, and threat neutral.

ARC's three-pronged approach to science-based resilience comes from research and development in:

- Theory of resilience that allows us to manipulate asymmetry
- Models and metrics that inform the quality of resilience
- Methods that provide validation of the approach

Benefits

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Decision makers will be able to measure and quantify enterprise security posture enabling cost-effective actions.

- Scientific understanding of cybersecurity for enterprise systems and system resilience
- Quantifiable security posture

That will

- Enable resilient cyber systems to fight through an attack
- Disrupt asymmetric advantage by raising the cost and exposure of the attack at an acceptable cost to the defender