Pacific Northwest
NATIONAL LABORATORY

TMBR – Threat Model-Based Response

The challenge/need

Cybercriminals are always evolving. Threats change frequently and quickly. Analysts and defenders require extensive resources to determine exactly what mechanisms are needed to defend against a particular type of malware.

The skill set needed for proper analysis is time-consuming and difficult to acquire for human analysts. Defenders need an automated or semi-automated framework to build a knowledge base for keeping up with novel malware samples.

APPROACH

Pacific Northwest National Laboratory has developed a new, model-based approach to automated threat detection through an investment in its Proactive Adaptive Cybersecurity for Control (PACiFiC) project.

PACiFiC combines adaptive principles, cross-domain information, and classic security best practices to deliver measurably more secure, reliable, robust, and resilient control systems while maintaining business performance.

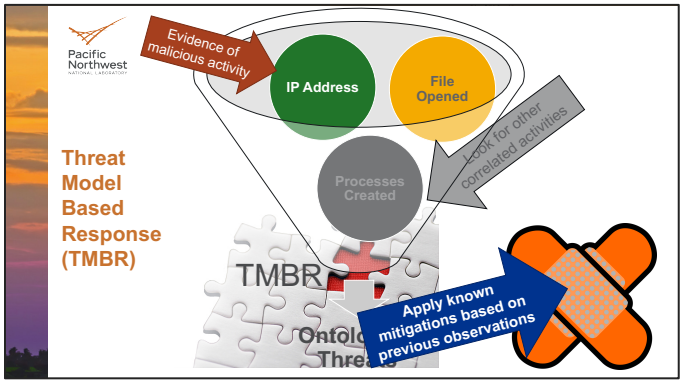
By unifying disparate data from multiple domains, including human, cyber, communications, and process physics, PNNL has defined and established secure design principles for use in all operational technology systems across multiple critical infrastructures.

TMBR is a machine-learning-based approach to malware triage and analysis that augments human analysis to improve threat detection and response.

HOW IT WORKS

TMBR analyzes samples of malware to generate behavior profiles, file information, and mitigation techniques, and makes them available in a database. Through correlation of disparate data points into behavioral fingerprints, TMBR enables cyber analysts to identify potential threat actors and actions, and populates them into a ready to use, automated database that supports queries from analysts and defenders.

- TMBR uses machine learning to identify similarities between known and new malware samples.
- TMBR supports insertion of new behaviors or threat signatures.
- TMBR arranges behaviors into hierarchical relationships and stores behavioral traits and patterns in semantic models.



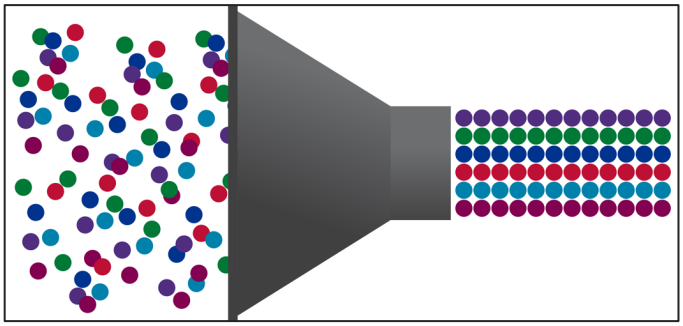
The Threat Model-Based Response active database provides analysts with critical information on similar cyberattacks.

BENEFITS

- TMBR links seemingly unrelated data to specific actors to identify and mitigate malicious intrusion into operational settings that manage critical infrastructure.
- The TMBR database helps determine the best course for defending the system.
- TMBR analyzes behaviors of interest and intruder actions to provide contextual knowledge.
  - Are there co-occurring behaviors?
  - Are there mitigations for known behaviors?
  - What existing threat agent information is available?
- The TMBR project has developed industrial control system-specific malware samples and behavioral analysis.
- TMBR is broadly deployable regardless of network type or malware analysis techniques.
- TMBR's abstract semantic model enables continual enhancement of the database information.

IMPACT

- TMBR enables faster and semi-automated response to potential threat actions.
- Defenders and analysts get prioritized information through machine-learning-based approach to malware triage.
- TMBR improves formulation of defensive mitigations by providing deeper understanding of tools, techniques, and processes.



The TMBR database correlates and organizes suspicious activity or intrusions with identical or similar attacks, helping defenders decide on a course of action.

For more information, contact

Kristine Arthur-Durett
Cybersecurity Researcher
National Security Directorate/Computing & Analytics
Pacific Northwest National Laboratory
509.371.6068 | Kristine.Arthur-Durett@PNNL.Gov

Mark Rice
Electrical Engineer
Energy & Environment Directorate/Electricity Infrastructure
Pacific Northwest National Laboratory
509.375.2435 | Mark.Rice@PNNL.Gov

www.pnnl.gov

PACIFIC

PNNL-SA-148200 | 10/1/2019

U.S. DEPARTMENT OF ENERGY