CRII: SaTC:

Creating and Managing Structurally-Morphing IT Systems – Moving Targets

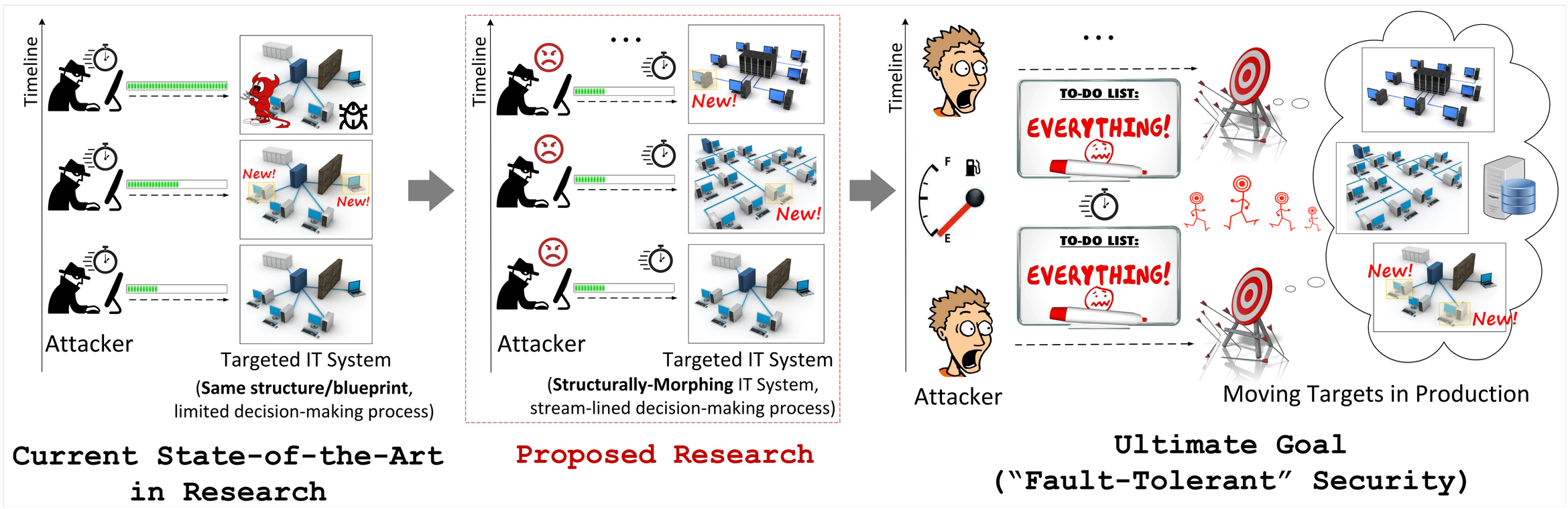
Alexandru G. Bardas, University of Kansas (www.alexbardas.com)

Moving Target Defense (MTD) techniques have been proposed as a way to rebalance the security landscape by increasing uncertainty and apparent complexity for adversaries, reducing their window of opportunity, and raising the costs of their reconnaissance and attack efforts. Intuitively, the idea of applying MTD techniques to an entire IT system should provide enhanced security; however, research in this area is still in its initial stages.

The **overarching goal** of this research is to develop a novel, comprehensive framework for creating and managing structurally-changing (morphing) IT systems in real-world scenarios.

The framework/platform will be composed of:

- a high-level multi-layered abstraction
- a "compiler" that converts the abstract requirements into actual IT systems



Building blocks:

- virtualized infrastructures (e.g., OpenStack and VMware vSphere Enterprise),
- containerization techniques such as Docker,
- configuration management tools (e.g., Ansible, Puppet), and
- hardware enclaves (e.g., Intel SGX for vital component MTD operations).

Impact on Society

Operational dynamic, structurally-morphing IT systems will force a change in the current modus operandi of cyber-attackers:

Impose a change from "compromise and persist" to the more challenging obligation of repeatedly attempting to compromise a constantly-changing IT system.

Outreach and Education

Working with a diverse student organization, the Jayhackers, and coaching them in cyber-defense or capture-the-flag competitions.

Goal: Deploying the proposed automated framework along student teams as part of cyber defense competitions (e.g., regional competition and workshop CANSec)