SAND2019-8018D

The Center for Cyber Defenders

Expanding computer security knowledge

Analyzing APTs with GAMES

Michael Rausch, University of Illinois at Urbana-Champaign

Project Mentor: Vincent Urias, Org. 9315

Problem Statement:

Sophistication and stealth are hallmarks of *Advanced Persistent Threats* (APTs). Stuxnet, perhaps the most famous of the many known APTs, demonstrates how impactful and damaging APTs can be.

Care must be taken to ensure that cyber infrastructure is designed to defend against APTs.

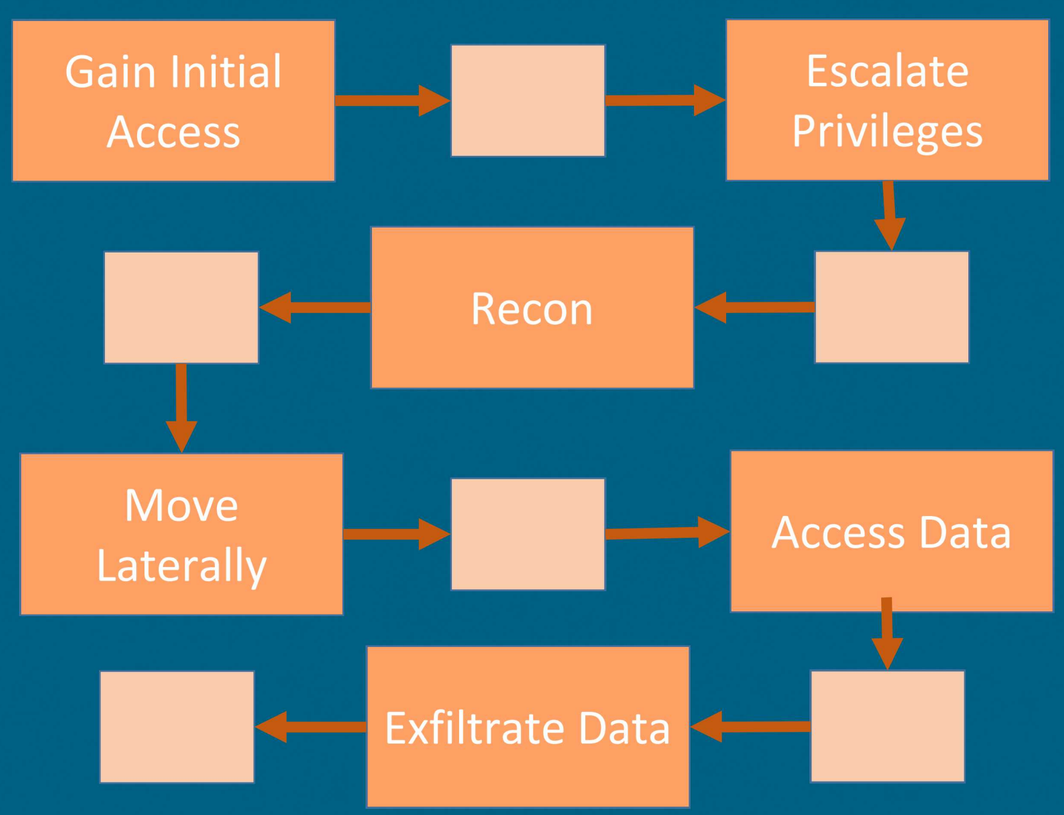
Objectives and Approach:

The overall objective is to help architects to design systems that are able to mitigate APTs.

Our approach is to develop realistic models of enterprise networks using the GAMES formalism, and then simulate APTs given different network architectures and defenses.

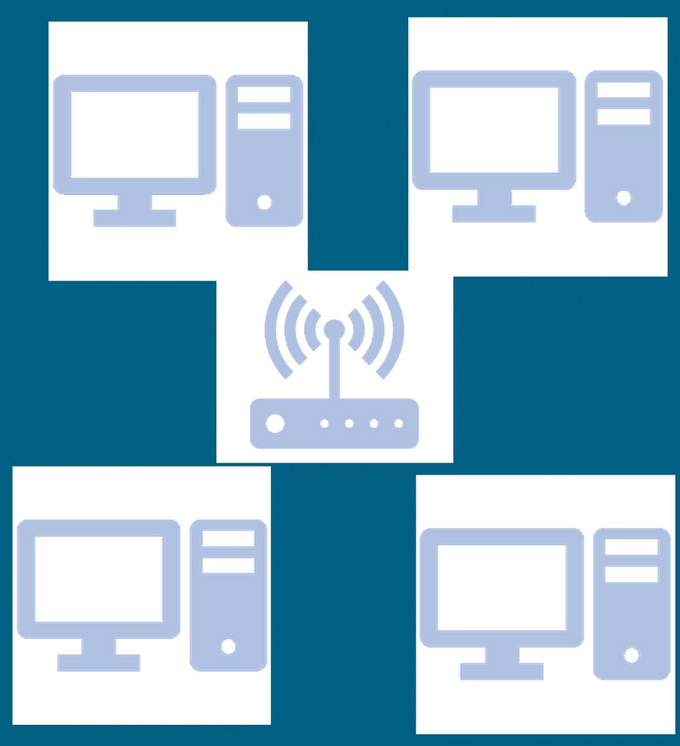
Simulations and emulations validate each other in iterative model-test-model loop.

GAMES Model



Validation Loop

Emulation



Impact and Benefits:

The use of modeling will help system architects:

- Create secure system designs
- Determine cost-effective defenses to invest in
- Develop effective policies and strategies

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.