SAND2019-8165D

The Center for Cyber Defenders

Expanding computer security knowledge

Using PRESTIGE to Assess Risk of Cyber Physical Systems

Dustin Campbell, Georgia Institute of Technology, M.S CmpE May 2020

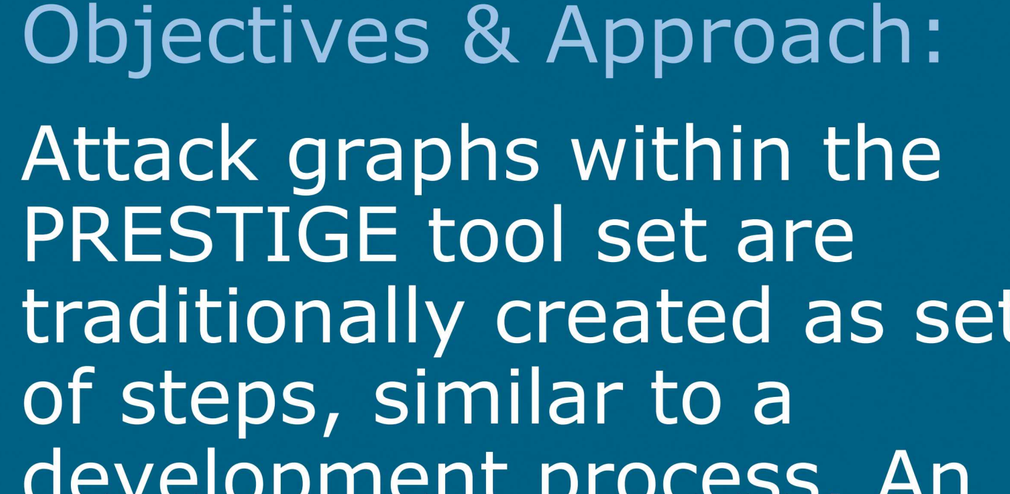
Project Mentor: Brandon Eames ORG 5838

Problem Statement:

The goal of this project is to extend the modeling features of the PRESTIGE tool set to be able to model attacks against critical cyber physical systems, such as the power grid. Simulation of models like the power grid will help identify how to optimally use defensive resources.

Objectives & Approach:

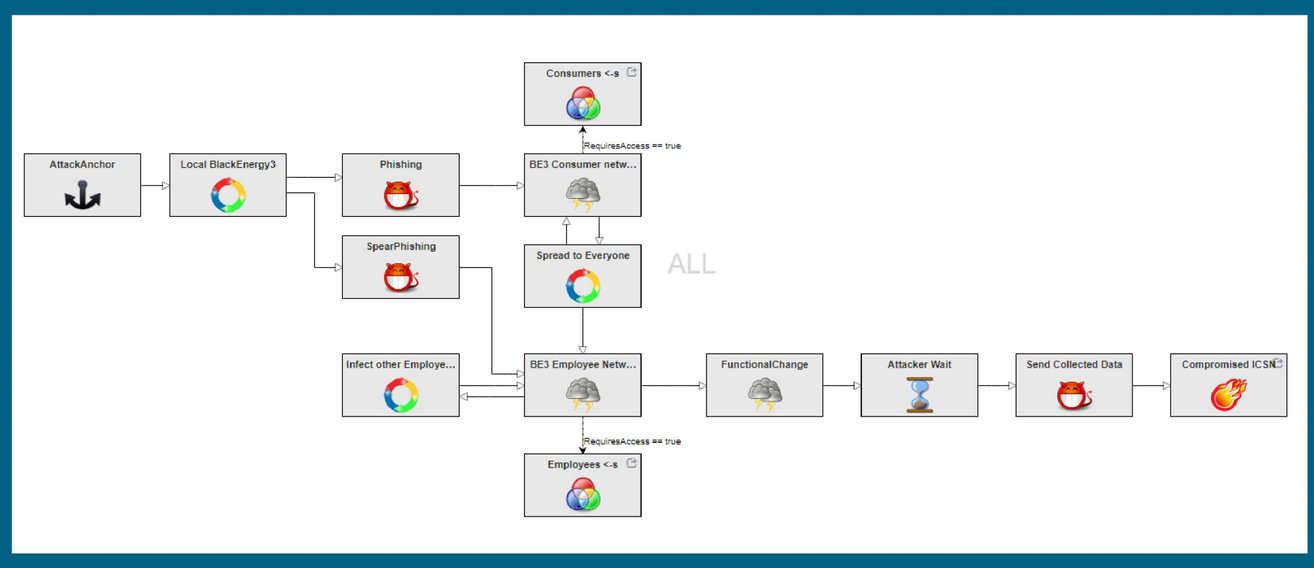
Attack graphs within the PRESTIGE tool set are traditionally created as set of steps, similar to a development process. An example of a “normal” attack graph can be seen below:



Attacks such as these are linear and the attacker succeeds upon reaching the final node.

Results:

A new method of modeling attack graphs was proposed to support generative attacks.



In this attack graph the attacker continuously creates “workers” to complete a desired task. Once any single “worker” achieves the shared goal, the attacker can move to the next node.

Impact and Benefits:

The proposed attack node would allow modelers to represent attacks, such as a botnet spreading through the network. As more devices are compromised the attacker’s probability of success increases.

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.