SAND2014-16446PE

Exceptional service in the national interest

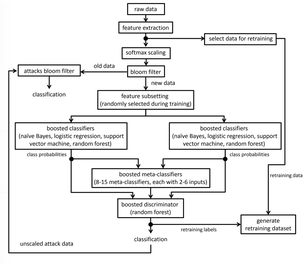
Sandia National Laboratories

Dynamic Defense and Network Randomization within Industrial Control Systems

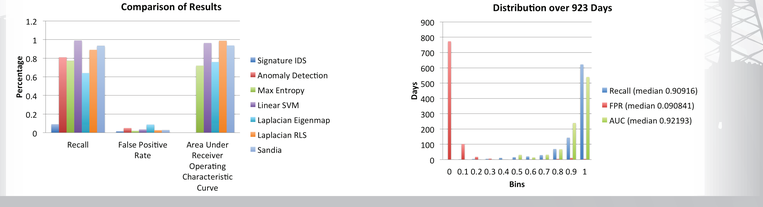
Contact:
Adrian R Chavez | adrchav@sandia.gov | (505)284-6664

Detect

Currently, it is extremely difficult to detect an attack on control system networks until it is too late. Using dynamic defense, SNL has developed a set of machine learning algorithms that recognize active attack patterns in real-time and respond in an appropriate manner depending on the scenario.



The knowledge gained from attack patterns during a training phase is used to generalize and dynamically recognize future attack vectors. Additionally, responses to these attacks provide situational awareness to operators and uncertainty of the true state of the system to an adversary.



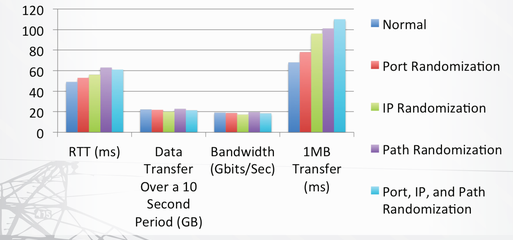
Respond

Automatically reconfiguring network settings and randomizing application communications dynamically is one possible response to a targeted attack. Introducing artificial diversity converts control systems into moving targets that help mitigate the early reconnaissance stages of an attack. This will help eliminate the class of adversaries who rely on known static addresses of critical infrastructure network devices for attack.

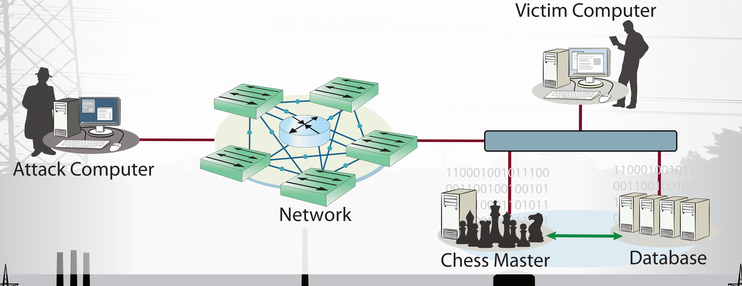
We are currently focused on creating uncertainty and unpredictability for adversaries by randomizing the following:

- IP Addresses
- Application Port Numbers
- Paths packets take through the network
- Application Randomization

Mitigate



The performance metrics gathered are compared against a network without any randomization applied. The network without randomization was the fastest, followed closely by each of the randomization schemes applied for each test performed. The differences that account for the increases in time are attributed to the time it takes to lookup the random mappings, to take additional hops through the network, and the management of the random algorithms in a single centralized controller



Sandia National Laboratories is a multi-program laboratory operated and managed by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

TVA

Sandia National Laboratories