Cyber Operations Analysis and Research Group
Risk and Infrastructure Science Center
Global Security Science Division

Argonne NATIONAL LABORATORY

MOVING TARGET DEFENSE

Security through Dynamic Software

SUMMARY

Moving target defenses are a collection of technologies that seek to increase resilience and availability of an application through increasing diversity of software and network paths. Argonne is currently working on three projects that employ this technique.

MODELS

Multiple Operating System Rotational Environment (MORE)

MORE is a project that controls multiple machines running a diverse set of operating systems. These operating systems serve the same content making their rotation transparent to the end user. In the event that an attacker is successfully able to exploit one of the machines serving content, it will be taken out of rotation in order to isolate any user's further interaction with a vulnerable machine.

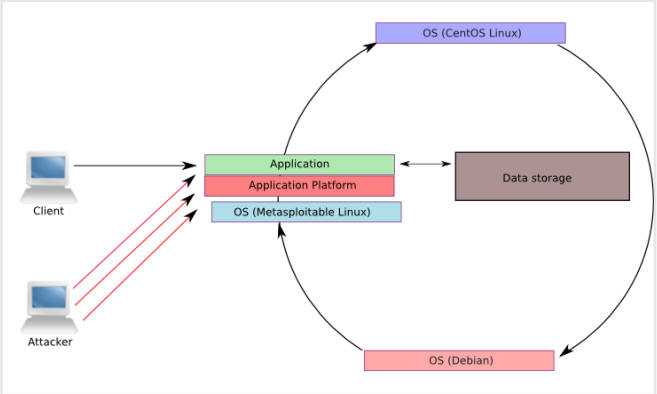

Figure 1. MORE MTD

Dynamic Application Rotation Environment (DARE)

DARE is a project that rotates software providing the same service on a host. Our current research involves rotating web servers in order to provide resiliency against exploits that compromise performance or security. By rotating the software that serves users, an exploitation of one of the pieces of software in rotation can be mitigated by reducing the vulnerable software's exposure to attackers.

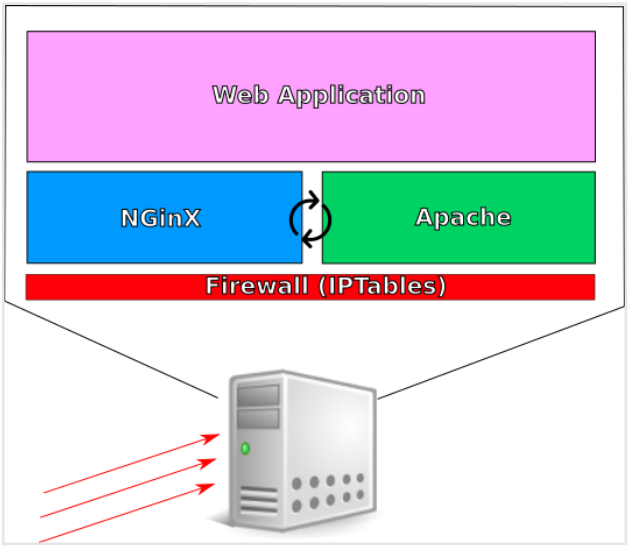

Figure 2. DARE MTD

Stream Splitting

Stream splitting is a project that sends data across multiple geographically diverse media (cellular, fiber, radio, DSL) in order to provide redundant links to the internet, prevent traffic correlation between hosts by using intermediate nodes, and mitigate useful traffic interception by preventing any one link from having all contents of a network communication. In the event that one of these links becomes constricted or fails, stream splitting can automatically reroute traffic through higher bandwidth links to maintain connectivity and availability. The division of traffic across links makes it more difficult for an attacker to obtain all pieces of a communication by requiring them to have access to all links used in stream splitting in order to reassemble the complete message.

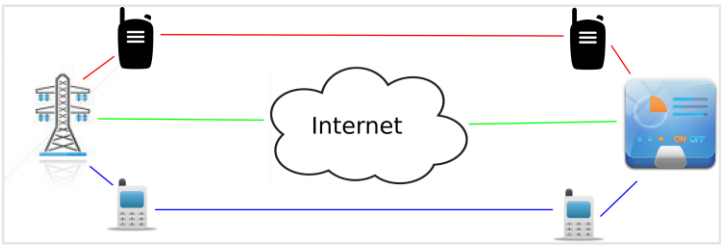

Figure 3. Stream Splitting MTD

LONG TERM GOALS

With the enhancements and validation to data, owners and operators can become more prepared and educated on their current dependencies. SimDependency can allow for a connected dependency map that would not only benefit the owner/operators of the facilities but also the federal and state governments in the event of a major event.

Contact: Nathaniel Evans
Phone: 630-252-3733
Email: nevans@anl.gov
https://coar.risc.anl.gov

THE UNIVERSITY OF CHICAGO
U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.