

Time Series Graphs of Clustered Human-Network Behavior

Scire

Objective

In order for the ARC Initiative to have significant impact, its work must be validated. The cybersecurity field is still struggling with developing methods and procedures to discover generalizable and future looking knowledge. The Scire project is designed to assist other ARC projects in performing rigorous science such that their results are well understood and defensible.

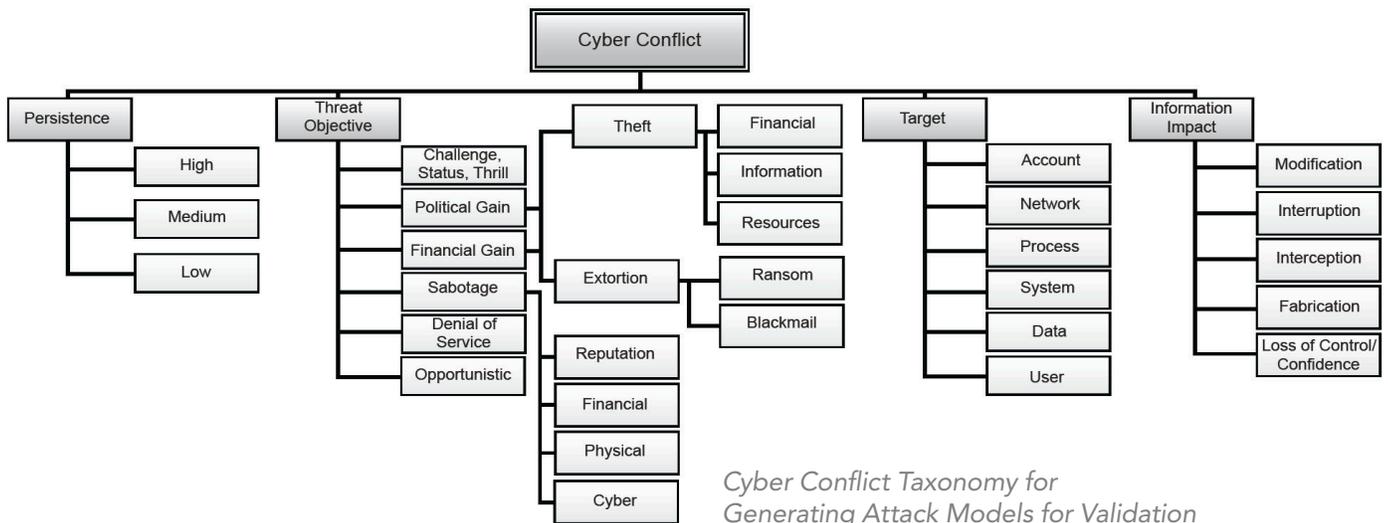
Approach

In addition to operating the Science Council, the Scire project is addressing two key validity challenges that projects are experiencing. The first is developing sufficient user models for simulation in experiments. We are performing statistical cluster analysis on real network traffic to develop a process and example models for experimentation. The second task is to provide

methods of integrating synthetic adversaries into experiments to validate the ARC hypothesis of being threat-agnostic. The Scire project is developing a cyber conflict taxonomy to define different variations of adversaries and a survey of methods to integrate them into experiments.

Achievements

- Instantiated the Science Council
- Statistically cluster analyzed ICIR and PNNL datasets to develop user models
- Developed cyber conflict taxonomy
- Surveyed adversary integration approaches to help validate ARC projects.

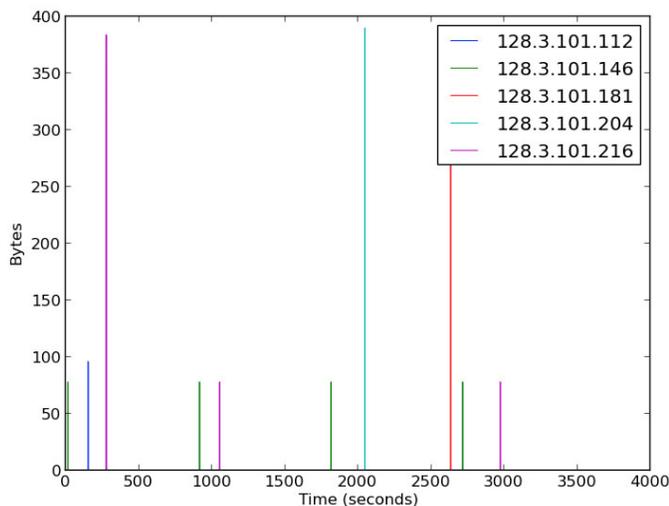


Impact

The Scire project developed a methodology by which projects can scientifically validate their claims. The Science Council was instantiated to steward this methodology and work with ARC projects to integrate it into their approaches. In addition, the Scire project is helping close technological gaps necessary to evaluate the rest of the initiative. The user modeling process and examples will provide the necessary rigor in the background noise present on an enterprise network and the adversary integrations will provide projects a toolbox of methods to leverage when testing their hypotheses. The Scire project enables the initiative to be successful.

Future Work

The Scire Scientific Council will continue to steward the scientific methodology developed under this project and will work with projects to be rigorous and scientific. Our hope is to further develop this material outside of the ARC Initiative into a textbook and a university course to spread the impact of the developed approach.



Data Density of ICIR Dataset

ABOUT

The Asymmetric Resilient Cybersecurity Initiative

Researchers at PNNL are delivering the theory, processes, methodologies, and algorithms that will enable a resilient cyber infrastructure with an asymmetric advantage to thwart adversaries who seek to infiltrate and damage our national security through digital means. This exploratory science in Laboratory Directed Research and Development effort is made possible by the Pacific Northwest National Laboratory through funding provided by the U.S. Department of Energy.

For more information on the science you see here, please contact:

Thomas Edgar
Pacific Northwest National Laboratory
P.O. Box 999, MSIN: K3-12
Richland, WA 99352
(509) 372-6195
thomas.edgar@pnnl.gov



Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by **Battelle** Since 1965