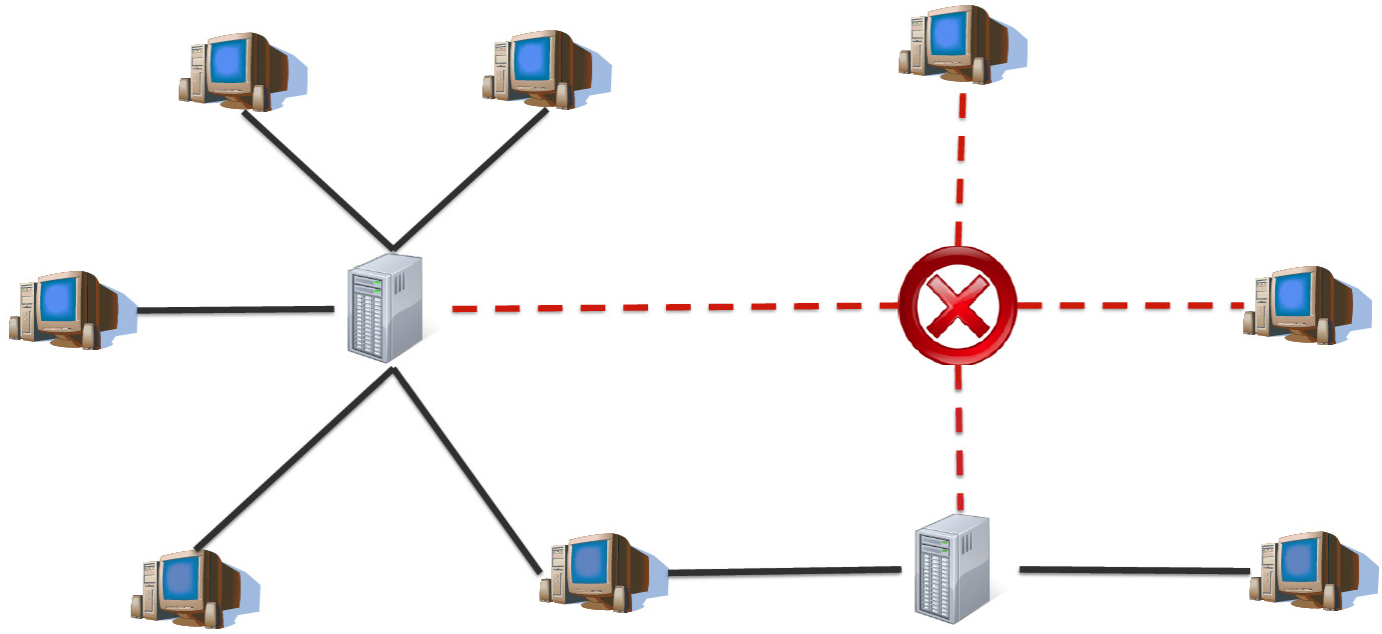
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



# Cyber Contingency Analysis

## Objective

It is often difficult to come up with metrics to describe the resiliency of a cyber system. We might feel a system is in a good state currently but does it remain so when an element becomes compromised or disabled?

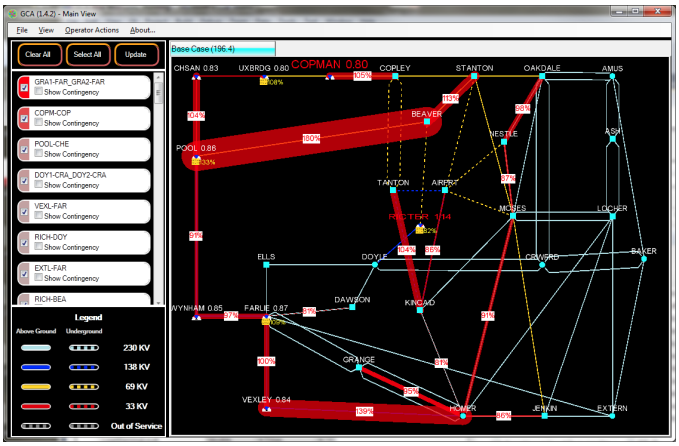
A similar problem exists with power systems. To deal with this, power grid operators use a technique know as contingency analysis. By observing what the system might look like given a list of possible contingencies, they adjust the system so that no violations will occur. This makes the system resilient against any one element becoming disabled.

**Can we apply this same concept to improve the resiliency of cyber systems?**

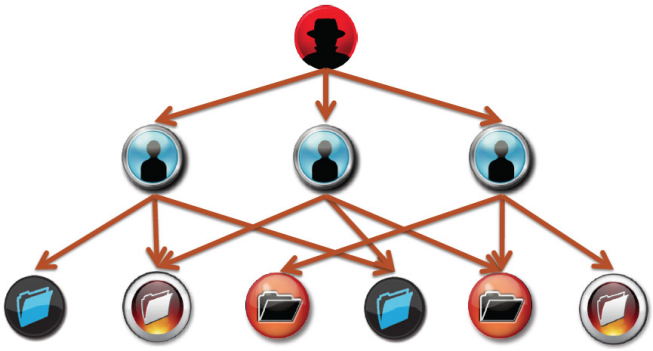
## Approach

For our cyber contingency analysis, a contingency can be either a user account or network resource that may become compromised. We examine all possible contingencies and then calculate the severity of each in regards to:

- Confidenciality: What confidential data can be read?
- Integrity: What intregal files can be written to?
- Availabilty: How many mission critical paths are disrupted?




*Graphical Contingency Analysis Tool for Electric Power Grids*



*Each Account Has Access to Files with Different Confidentiality and Integrity Concerns; the More Access Available, the Greater the Potential Liability Is*

## Achievements

- Implemented a graph based algorithm for availability that runs in $O(n^{k+1})$, where k is the number of simultaneous contingencies being studied
- Parallelized algorithm for multicore CPU, with linear speed up
- Implemented software for computing confidentiality and integrity measurements for Windows and Linux systems
- Used metrics from confidentiality and integrity scores to improve security on a real world system.

## Impact

If successful, we hope to :

- Have a real tool useable by practicing cybersecurity operators
- Improve security before attacks occur
- Take confidentiality, integrity, and availability into account
- Create a holistic picture of cyber health
- Develop an approach that is useful for both planning and daily operations.

## Future Work

- Implementing a user friendly graphical interface for cyber contingency analysis
- Creating metrics that are useful even when the model of the system is incomplete or inaccurate
- Developing more automated ways for establishing system topology and mission critical paths
- Performing empirical studies to demonstrate the usefulness of the technique, regardless of deficiencies in the model and probabilities.

## 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:

**Patrick Mackey**
Pacific Northwest National Laboratory
P.O. Box 999, MSIN: J4-32
Richland, WA 99352
(509) 372-6778
patrick.mackey@pnnl.gov

Pacific Northwest NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

*Proudly Operated by* Battelle *Since 1965*