



Network Intelligence for Measuring & Improving Resilience



Jonathan Ganz*†

Domingo Colon†

Sean Peisert*§

Celeste Matarazzo†

*University of California, Davis

†Lawrence Livermore National Laboratory

§Lawrence Berkeley National Laboratory

Introduction

Resilience is a developing field of Computer Security that seeks to minimize the amount of damage that attacks can effect on a network. Common resilience-providing techniques include redundancy, diversity, and increasing entropy. However, researchers in the field often disagree on which properties constitute a resilient system. This project seeks to reconcile these views by developing software that measures properties on the network to evaluate its resilience and software that can autonomously change configurations in order to improve resilience.

Measuring Resilience

Robustness

- Resistance to damage from malicious activity

Detection

- The ability for a system to discover malicious activity before or after it causes damage

Recoverability

- Time since an operation-impacting event occurs to the point at which different quality of service levels are reached

Evolution

- Learning from previous experience to improve future operations involving the same activity and, desirably, involving similar activity

Optimization

- Balancing various potentially incompatible goals based on their priority and feasibility

Improving Resilience

Redundancy

- Critical systems should have duplicates to increase reliability

Diversity

- Duplicate systems should be fundamentally different (Architecture, Language, Dependencies, Control Flow, etc.)
- Vulnerabilities in one system should rarely exist in the duplicate

Communicate Security Status

- Systems report current/future configurations to ensure diversity
- Attacks & vulnerabilities should be reported to relevant systems

Systems Respond to Change in Network

- Systems react to reports, improving high priority characteristics

Analyze Damage Over Time

- Determine how effective defenses were during attack
- Adjust recovery/response procedure for future attacks

Experiment

Redundant Links

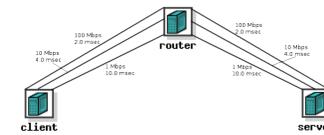


Figure 1: A network of redundant & diverse links

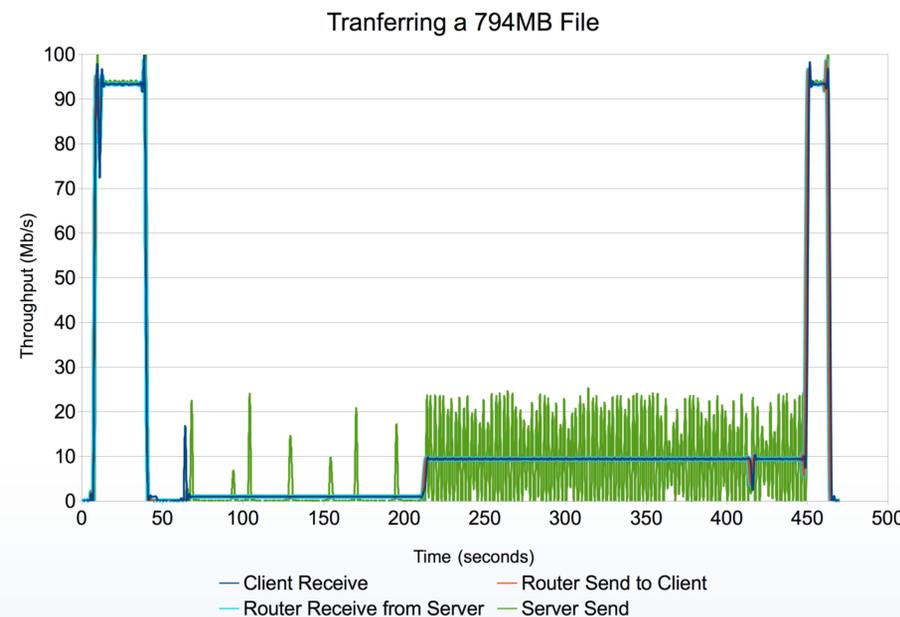


Figure 2: File transfer over the network in Figure 1

When a utilized link is brought down, a redundant link is chosen to continue the file transfer. The throughput of the file transfer changes based on the maximum throughput of the currently active link.

Results

The experiment described above was performed on the DeterLab Experimentation Facility. The networks created in this environment are a combination of real hardware and virtualized components. This can reduce the realism of such experiments and prevent certain features from being properly implemented. The quality of service on each link is controlled by the addition of delay nodes which can affect traffic patterns in ways that real physical limitations would not. The routing is virtualized so that although all links exist, the real paths are abstracted away from the experimenter. Routing and redundancy techniques are limited to what the network testbed framework supports.

Prototype Metric

$$Adv_N^\tau = \min_{cfg_A} \begin{cases} h = \frac{Pr[dtk_p|cfg_N] \times \delta(atk_\tau|cfg_A)}{Pr[atk_\tau|cfg_A] \times \delta(dtk_p|cfg_N)} & h > 1 \\ \frac{Pr[dtk_p|cfg_N]}{\delta(dtk_p|cfg_N) + \delta(rcvr_\tau|cfg_N)} & h \leq 1 \end{cases}$$

Figure 3: Generic resilience metric designed for customizability

A network's resilience in the presence of attacks of type τ (Adv_N^τ) depends on the network's ability to detect and respond to the attack. The top equation represents the network's ability to detect and block an attack before it finishes running. If the network is unlikely to block such attacks, the bottom equation representing the network's ability to recover from successful attacks will be used.

$Pr[dtk_p|cfg_N]$ – Network's ability to detect process p in configuration N
 $Pr[atk_\tau|cfg_A]$ – Ability for attack in configuration A to damage network
 $\delta(atk_\tau|cfg_A)$ – Time required for attack in configuration A to succeed
 $\delta(dtk_p|cfg_N)$ – Time required for Network N to detect process p
 $\delta(rcvr_\tau|cfg_N)$ – Time required for Network N to recover from attack

Conclusion

The network testbeds available for performing experiments are useful for many types of tests. But low-level experiments in which protocols are being modified may require a greater level of fidelity. In order to advance network resilience, the type of virtualization and simulation allowed in the networks examined must be carefully evaluated.

Future Work

Resilience Testing Framework

- Centralized server for monitoring status over a network
- Capable of performing common network attacks
- Records specific damage to resources & recovery over time

Resilience Communication Protocol

- Protocol for communicating network status
- Systems respond to changes in security

Reproducible Experiments

- Networks comprised entirely of real hardware
- Better control over network connections
- Ability to perform physical attacks as well as cyber attacks