



CASE STUDY

BreakingPoint Keeps the Louisiana National Guard a Step Ahead of Cyberattacks

The National Guard symbolizes being ready for anything and everything, including the latest cyberattacks. Several years back, the Louisiana (LA) National Guard began operating a state-of-the-art cyber range facility to conduct training, test innovations, and build prototypes at Louisiana State University (LSU).

The team engaged Stephenson Technology Corporation (STC) to design cyber range training featuring Keysight's BreakingPoint Security Testing and PerfectStorm hardware. Trusted by world-leading network security providers and Fortune 100 companies, BreakingPoint simulates more than 400 legitimate application traffic protocols and some 38,000 exploits including malware, viruses, and distributed denial of service (DDoS) attacks.

Validating a security infrastructure with BreakingPoint has been shown to increase an organization's attack readiness by nearly 70 percent. In designing a curriculum to master basic cyber skills and techniques, STC chose the Keysight solution to generate realistic mixes of application and attack traffic.

"BreakingPoint gives us the ability to recreate real-life scenarios as closely as possible to see how different types of attacks affect various machines," says Major Alan Dunn, commander of Louisiana National Guard's Cyber Protection Team. "Soldiers can not only spot attacks; they get to see what's behind them and do deeper exploration."



Company:

- Louisiana National Guard

Key Issues:

- Training cybersecurity teams on the latest best practices
- Securing small businesses, IoT, active oil/gas locations
- Putting defenses to the test

Solutions:

Using BreakingPoint to:

- Build and operate a state-of-the-art cyber range
- Test security for the Department of Defense (DoD) supply chain
- Simulate IoT environments at scale

Results:

- Cyber range training improving response times
- IoT lab detecting malicious attacks
- Security testing being extended across LA



Early cybersecurity initiatives spearheaded by STC include creating a small business security operations center (SOC) to strengthen cyber defenses across the Department of Defense (DoD) supply chain and infrastructure. The project gives analysts greater visibility into the traffic feeding into military bases from small family-owned shops, and veteran- or minority-owned businesses that might not employ cybersecurity experts.

The National Guard team also leveraged BreakingPoint in developing sensor technology that would help defenders spot and explore anomalies that might trigger alerts if left unaddressed. The research included testing multiple remote sensor hardware platform configurations to gauge their bandwidth and threat preprocessing capabilities.

“BreakingPoint was the only platform that could manage the throughput and realism we needed to conduct this research which benefits both state and national security,” Major Dunn says. “The system enables realistic framing to help recognize and identify something that looks odd instead of simply feeding a bunch of numbers to analysts.”

STC also employs BreakingPoint at a “smart house” test lab at LSU designed to improve security for the Internet of Things (IoT). According to Dunn, the house was originally designed to withstand the impact of a category five storm following the cataclysmic Hurricane Katrina. “We converted the building into a ‘smart house’ environment with a system that lets us test all the things in a house that might connect to the Internet — garage door openers, appliances, baby monitors — and see how they’re communicating on the back end.”

Quickly paying dividends, the testing conducted at the new IoT lab showed that sensors attached to a popular brand of baby monitor were sending data to foreign countries unencrypted and automatically clicking on ads to generate revenues for hackers.

The LSU team also conducts innovative research on securing active oil platforms. Research takes place at a dry oil well used for training to secure petroleum engineering sites and energy grids. STC’s Secure the Energy Grid (STEG) efforts employ BreakingPoint to simulate regular business traffic as well as communications using the Modbus protocol from specialized oil field and Industrial Control System (ICS) devices.



The ICS platform is utilized to improve security at premier petroleum companies like Shell and Valero as well as at various utility companies. “We’ve built an ICS ‘trainer in a box’ that mimics water, electrical, and natural gas environments,” says Dunn. “We use Keysight to simulate denial of service (DoS) attacks against the infrastructure to see how well it performs.”

The LA National Guard and STC now maintain multiple cybersecurity teams with more than 50 experts conducting research and training at the LSU facility. Group leaders recently decided to extend BreakingPoint test coverage across Louisiana using the software-based version at remote sites. BreakingPoint Virtual Edition (VE) makes it easier to add new users as the program expands, with testing of up to 20,000 concurrent connections per test and per seat.

STC is also contemplating adding greater network visibility at operations centers. “Our results have definitely improved with BreakingPoint,” Major Dunn reports. “Next we plan to explore other options such as Keysight’s network packet brokers that might also improve operations and keep us a step ahead of new threats and attacks.”

Cultivating cyber skills and honing processes require two things: continuous testing and comprehensive training. Central to the cyber range, IoT, and secure energy research taking place at LSU, BreakingPoint equips STC and the LA National Guard to defend and aid local and homeland security.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

