Addressing Cybersecurity

March 17, 2016

Recent cyberattacks in the private and government sectors have shined a spotlight on cybersecurity and the challenges organizations face in trying to protect their data. According to Experian, the risk of a data breach is higher than ever with almost half of organizations suffering at least one security incident in the last 12 months. It's no wonder industry and government are looking for more tools to keep their data safe.

To this end, in 2015, Los Alamos National Laboratory partnered with two private sector companies to bring cybersecurity technology developed by the lab to market. The first partnership, with Whitewood Encryption Systems, Inc., developed a quantum random number generator in an effort to address a key fundamental flaw in all cryptosystems: predictability. The security of electronic messages depends on the unpredictability of the random numbers used to scramble the data. Modern data centers have very limited access to true random numbers because computers do not generally do unpredictable things. To provide truly secure data communications, systems need a reliable source of unpredictable numbers that aren't generated by a set of mathematical operations.

This is where the laboratory's experience in security and pushing the limits of computing comes into play. From the physicist's point of view, the only true unpredictability comes from quantum mechanics. So Los Alamos physicists developed a quantum random number generator and a quantum communication system, both of which exploit the weird and immutable laws of quantum physics to improve cybersecurity.

These physical laws state that events at the subatomic level cannot be predicted; random quantum events lie at the root of the universe. From that starting point, Los Alamos developed a revolutionary method to generate unpredictable, theoretically unhackable random numbers. Quantum mechanics itself guards the secret. Unlike current math-based encryption keys, which are derived from random numbers generated by a potentially knowable algorithm, a quantum key can't be determined through calculation, no matter how powerful a computer one uses.

Quantum random number generation technology, commercialized by Whitewood under the name Entropy Engine, is a plug-and-play computer card that fits most network servers and creates truly random numbers at a rate of up to 200 million bits each second and can deliver them on-demand over a network to existing encryption applications and devices performing cryptographic operations across datacenters, cloud computing systems, mobile phones and the internet of things. Entropy Engine is more than ten times higher performing than other quantum devices currently on the market and is one of the world's most cost-effective, quantum-powered random number generators.

The second alliance, between Los Alamos and Ernst & Young, commercialized PathScan, a network-anomaly detection tool that searches for deviations in normal communication patterns

that might indicate a cyber intruder. Unlike traditional security tools that look for malware or network signatures, PathScan searches for deviations from normal patterns of communication that are indicative of an intruder's presence. By creating a deep behavioral model of a network, it can expose intruders and insiders causing local anomalies during their activity.

PathScan's three-step approach builds statistical models to characterize the normal flows of traffic between each pair of communicating computers; actively enumerates multi-hop paths of communication; and passively monitors each path and tests whether the flows observed are expected in the context of the statistical models or whether they are unlikely and, therefore, indicators of a possible adversary moving through the network.

The tool's modeling capabilities are dynamic: continuously updating parameters in step with the non-stationary use of the network, thus reducing alerts due to unusual but non-threatening behavior. PathScan was also designed to work with an organization's legacy information security framework and does not require significant infrastructure development or vast stores of data to operate. Its network collection is passive, with limited impact to operations.

Both projects were initially funded through the Laboratory Directed Research and Development fund. Later, the Intelligence Advanced Research Projects Activity (IARPA) helped fund the applied demonstration work for our quantum encryption technology, while the National Nuclear Security Administration helped support Pathscan. The Department of Homeland Security's Transition to Practice program within the department's science and technology directorate helped bring the technology to market.

Each project illustrates a different, yet equally important, role government can play in bringing lab technologies to market. In the case of Whitewood, we see the bridging role national labs can play between government and industry. Quantum encryption is a technology Los Alamos spent decades developing and, through Whitewood, it was brought to the commercial sector.

The Ernst & Young alliance, on the other hand, demonstrates how national labs can leverage private investment in technology for its own benefit. We develop the technology; industry deploys it; and then we get to do the next generation of analytics. It allows us to see how industry is addressing their cyber issues and then put that technology to work for the government.

This article originally appeared in Innovation Magazine. Written by Duncan McBranch, chief technology officer at Los Alamos National Laboratory.

RICHARD P. FEYNMAN CENTER FOR INNOVATION

www.lanl.gov/feynmancenter | (505) 667-9090 | feynmancenter@lanl.gov