Sandia National Laboratories

Cybersecurity: Decades of experience defending the nation

"The cyber threat to our nation is one of the most serious economic and national security challenges we face." – President Barack Obama, July 2012

Why Sandia?

Sandia was doing cyber before the term cyberspace existed. Today, with cybersecurity a daunting — and rapidly growing — national security problem, Sandia is applying decades of science and engineering expertise to the task. As the most networked nation on Earth, the United States is extremely vulnerable to malicious attacks. To maintain this critical infrastructure and foil attacks, Sandia conducts threat assessments, analyzes government, military, and civilian computer networks, and develops new protective technologies.

Research

Fundamental research helps the nation stay ahead of threats. Sandia's researcha efforts in cybersecurity are focused in three broad areas:

- trusted hardware, software and systems,

- networks and systems architectures and analysis and

- effective cyber defense systems.

Research is conducted in state-of-the-art facilities with extensive computing and information science capabilities, which range from architectures and algorithms to advanced modeling and simulation.

Cyberthreats to daily life

We rely on critical cybernetworks for communication, commerce and the systems that control the electric grid, water distribution and gas and oil pipelines. Attacks on these systems have become more sophisticated and adversaries have become more skilled, increas-

ing the demand on cyberexperts to protect vital national infrastructure. Sandia's multidisciplinary team employs the best and brightest to thwart cyberattacks.

Breakthrough research

Among recent cybersecurity research breakthroughs, Sandia has developed:

- algorithms that separate robotic web crawlers from people using browsers, allowing analysts to look at these groups separately. The goal is to reduce the number of suspicious visitors that cyberanalysts have to check, recognize and warn potential targets of nefarious emails, and, ultimately, spot spear phishing and similar malicious schemes.

- a visualization tool to help network administrators troubleshoot problems with the government's Domain Name System Security during the domain name "lookup" that is a prerequisite for doing almost anything on the Internet, including web browsing, emailing or videoconferencing. The new security feature allows user applications to verify that the domain names and the IP address responses they receive on lookup are authoritative and have not been altered or spoofed.

- a network that links 300,000 virtual hand-held computing devices running the Android operating system so research-

ers can study large smartphone networks and find ways to make them more secure, reliable and free from network disruptions. The goal is a software tool that will allow cyber researchers to model similar environments and help the computing industry better protect hand-held devices from malicious intent.

Careers in Cyber

Addressing sophisticated cyberthreats demands a multidisciplinary team dedicated to protecting the government and infrastructure. A major focus of Sandia's cybersecurity program is delivering the experience and expertise the nation needs by training the next generation of cyberdefenders. A career in cybersecurity research at Sandia offers challenging opportunities for those with a passion to tackle the complexities of protecting critical systems. Sandia's Cyber Defender program creates a pipeline of qualified candidates in cybersecurity by giving undergraduate- and graduate-level computer science students practical internships in computer systems, network operations and information protection.

Cyber Engineering Research Institute (CERI)

CERI focuses on open, exploratory research in cybersecurity that builds partnerships between academia, industry and government collaborators and Sandia's cybersecurity experts. At CERI, visionary, threat-informed research on national cyber challenges pushes the frontiers of science and catalyzes research collaborations, thereby aligning new cyber technologies with national needs. CERI also helps identify, recruit and develop the next generation of cybersecurity experts. CERI supports two facilities: the Cyber Engineering Research Laboratory, in the Sandia Science & Technology Park in Albuquerque, N.M.; and the Cyber Technology Research Laboratory, in the Livermore Valley Open Campus in California. Both lie outside Sandia's classified campus to accommodate academic and industry collaborators.

Sandia
National
Laboratories