BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

CYBER-PHYSICAL SYSTEMS AND AUTONOMY

HIGHLIGHTING RAYTHEON COMPANY'S WORK

Cyber-Physical Systems and Autonomy: Highlighting Raytheon Company's Work

AS COMPUTERS BECOME EVER FASTER AND BANDWIDTH EVER CHEAPER, computing and communication capabilities are being embedded within more and more objects and structures in the physical environment. Engineered systems, which bridge the cyber world of computing and communications with the physical world, are called cyber-physical systems (CPS). Recognizing the need to secure CPS both nationally and statewide, Virginia has developed a world-leading technology ecosystem founded on private industry innovation and public-private partnership. This publication highlights Raytheon Company's (Raytheon) work in Virginia at the intersection of cyber-physical systems and autonomy.

THE CHALLENGE

Currently, it takes security specialists an average of 312 days to identify software vulnerabilities. Once discovered, it can take weeks, months, or even years to completely fix those vulnerabilities across all exposed systems, leaving time for exploitation of those vulnerabilities and damage to occur. At the same time, the cyber talent gap is widening, with more than 1 million cybersecurity job openings in 2016, which is expected to rise to 6 million globally by 2019 according to a 2015 report by Cisco Systems, Inc. This gap has major implications for the Internet of Things, where every device is connected, because the attack surface has grown so large that it has become virtually impossible for people alone to close every gap. To address these concerns, Raytheon is advancing autonomous technologies that can efficiently and effectively diagnose and mitigate against cyber vulnerabilities in the place of human experts.

THE SOLUTION

The automated cybersecurity technologies emerging from Raytheon's cyber centers and the Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge are a significant first step toward developing machines that actively protect themselves. Raytheon has two cyber centers in Virginia: the Cyber Operations, Development and Evaluation Center and the Global Cyber Solutions Center. At these centers, Raytheon engineers sharpen their skills and assess the performance of Raytheon's products using simulated cyber attacks and defenses.

In August 2016, a team of Raytheon engineers from the Virginia and Florida offices competed in the DARPA Cyber Grand Challenge, the world's first all-machine hacking tournament, for a $2 million grand prize. The tournament was held as part of DEF CON, the longest-running offensive/defensive Capture the Flag global competition for hackers, in Las Vegas, Nevada. Following a series of preliminary rounds with an initial field of more than 100 teams, the Raytheon team (DeepRed) was the only large defense contractor to qualify as a finalist alongside six other teams that included academic pioneers in the field and veterans of the Capture the Flag circuit.

Competitors were challenged to reverse engineer unknown software, find hidden weaknesses, and create securely patched replacement code in the live networked competition. The machines used were DARPA-constructed high-performance computers that operated on an open-source operating

system extension called the DARPA Experimental Cybersecurity Research Evaluation Environment. Each team programmed its machine with a cyber reasoning system, which simulates the logic and thought process of a cybersecurity analyst using artificial intelligence. Teams were disconnected from their cyber reasoning system before the grand challenge and watched as their systems competed entirely on their own during the competition.

Over the course of two years, Raytheon worked to develop a system that combined the massive analytical power of supercomputers with the intuition and adaptability of human analysts for the challenge. Raytheon synthesized several different techniques, including static analysis tools and symbolic execution, and incorporated the expertise of another company to develop its technology. To ensure that the code could adapt to evolving threats, Raytheon's cyber reasoning system used advanced analytics, autonomous reverse engineering software, and continuous machine learning. Instead of weeks or months, the team's cyber reasoning system, named Rubeus, automatically found and fixed software vulnerabilities in seconds.

In 2013, no computer with such capabilities existed. After the competition, seven existed. Raytheon continues to dedicate talent and resources to develop self-healing systems based on cyber reasoning technologies. Self-healing systems act as a workforce multiplier, identifying and automatically patching known vulnerabilities autonomously, so that human analysts can focus on the most difficult and unknown problems. Raytheon works closely with its customers to develop self-healing systems that will secure critical infrastructure and improve national security. Since 2013, it has invested more than $3.5 billion in building stronger and more adaptive technologies and analytical services.

RECOMMENDATIONS

Leaders in government, business, and higher education can support cyber-autonomy by continuing to make it a priority and by applying developments in the field as broadly and quickly as possible, thereby protecting critical systems such as financial systems and power grids. By making cyber a state priority, Virginia serves as a prime example of leadership in this regard. In conjunction with such efforts, Raytheon plans to advance its autonomous technologies internally in research and development as well as with its customers. Fully autonomous technology that can defend networks from malicious activity may not exist for at least another decade; however, Raytheon, with the support of other leaders and partners, continues to advance the realm of the possible in cyber-autonomy.

STAFF CONTACT

Mr. Tim Bryant
Principal Cyber Engineer
Raytheon Centers of Innovation
timothy.k.bryant@raytheon.com

ADDITIONAL INFORMATION

http://www.raytheon.com/news/feature/machines-that-think.html

"Our work on the DARPA Cyber Grand Challenge showed it really is possible for a computer to automatically detect and repair its own flaws, and learn from the attacks it sees as they are launched. Our other work in machine-learning enabled hunting gives us machines that automatically correlate the growing masses of threat information, integrate live environmental data in real-time, and most importantly learn from the human analysts. We aren't going to be able to out hire the adversaries. We must have autonomous systems."

MICHAEL K. DALY / CHIEF TECHNOLOGY OFFICER, CYBERSECURITY AND SPECIAL MISSIONS / RAYTHEON COMPANY

ABOUT THE BUSINESS-HIGHER EDUCATION FORUM

The Business-Higher Education Forum (BHEF) is the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the creation of a highly skilled future workforce. BHEF members collaborate and form strategic partnerships to build new undergraduate pathways; improve alignment between higher education and the workforce; and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

ABOUT RAYTHEON COMPANY

Raytheon Company (Raytheon) is a technology and innovation leader specializing in defense, civil government, and cybersecurity solutions. Raytheon tests its automated cybersecurity technologies in cyber centers in Virginia, and a team of Raytheon employees from Virginia and Florida recently competed in the world's first all-machine hacking tournament. Raytheon's work is advancing the realm of possibilities in cyber-autonomy.

ACKNOWLEDGEMENTS

BHEF would like to thank Michael Daly and Matthew Heine for providing detailed information on Raytheon's work in autonomy. BHEF would also like to thank the National Governors Association and the Office of Naval Research for their contributions and support.

This work is funded by the Center for Innovative Technology and the National Science Foundation under Award DUE-1331063.

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

2025 M Street NW, Suite 800, Washington, DC 20036

202.367.1189 / info@bhef.com / www.bhef.com