Time to move beyond 'medieval' cyber security approach, expert says

May 22 2015

Much of the U.S.'s cyber defense is "modeled after medieval perimeter security … and the idea of 'keeping the bad guys out'."

The nation's approach to cyber security has much in common with medieval defense tactics, and that needs to change, says a cyber security expert at Missouri University of Science and Technology.

"Most of our cyber defenses are modeled after medieval perimeter security – a firewall is much like a castle moat – and the idea of 'keeping the bad guys out'," says Dr. Bruce M. McMillin, professor of computer science and associate dean of the College of Engineering and Computing at Missouri S&T. "We live inside modern systems that are both physical and computational, and, in such a smart living environment, attacks can

come from multiple different sources, some even inside what we consider protected."

Earlier this year, the head of U.S. Cyber Command told Congress that the federal government's efforts to deter computer attacks are not working and the U.S. needs to "increase our capacity" to strengthen cyber security. At Missouri S&T, McMillin and other researchers are working to improve cyber security with an emphasis on safeguarding the nation's infrastructure while educating students in this field through its National Center of Academic Excellence in Information Assurance Education.

"We must focus on the information that both flows into and out of every portion of our smart living environment, both hiding what we consider security and private, and disrupting the ability of our adversaries to launch information attacks," McMillin says.

He adds that Missouri S&T provides "a unique contribution to the information assurance field with our focus on developing ways to protect the nation's electric power grid, oil, gas and water distribution systems; and transportation systems from terrorist attacks." Much of that research occurs through Missouri S&T's Center for Critical Infrastructure Protection.

McMillin credits his former Ph.D. student, Gerry Howser, for coming up with the moat analogy to describe contemporary approaches to cyber defense. Howser is a career security expert who returned to Missouri S&T for a Ph.D. in computer science.

McMillin also co-leads Missouri S&T's Smart Living signature area. Smart Living focuses on developing processes and technology to turn home, workplace, transportation and energy systems into "smart" environments.

On March 19, Adm. Michael S. Rogers, the head of the U.S. Cyber Command and the National Security Agency, told the Senate Armed Services Committee that the command's efforts are not working. He pointed out that attackers to U.S. cyber infrastructure want to move beyond disrupting those networks to establish "a persistent presence" on them.

More recently, Dennis Blair, the former director of U.S. national intelligence, said that major sponsors of cyberwarfare forces are reaching a state of deterrence similar to the "mutually assured destruction" of the Cold War era. Blair pointed out that military and civilian systems are often intertwined, and that a cyber attack could have far-reaching consequences. "Should a nation-state take action against the GPS system in another country on a major scale, there's no telling which way the damage would fall," he said.

In their research, McMillin and his fellow Smart Living researchers are also considering the interdependence of computerized systems and their vulnerabilities.

Provided by Missouri University of Science and Technology

Citation: Time to move beyond 'medieval' cyber security approach, expert says (2015, May 22) retrieved 2 May 2024 from https://phys.org/news/2015-05-medieval-cyber-approach-expert.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.