NIST Computer Scientist and Researcher Dr. Ron Ross Discusses Cybersecurity During Latest SGL

Naval Postgraduate School Public Affairs Office

Naval Postgraduate School

NIST Computer Scientist and Researcher Dr. Ron Ross Discusses Cybersecurity During Latest SGL

Article By: Amanda D. Stein

National Institute of Standards and Technology (NIST) senior computer scientist and information security researcher Dr. Ron Ross presented a lecture to students, staff and faculty on the new challenges in cybersecurity, and where the needs will be in the future. Ross received both his Master's and Ph.D. degrees from NPS in Computer Science and leads the Federal Information Security Management Act (FISMA) Implementation Project. He touched on some of the key areas of concern in cybersecurity, and the kinds of partnerships that will be critical to preparing the DoD networks for inevitable attacks.

"It is so critically important today to every one of us, whether in the warfighter side, the intelligence community, the civil part of government or the private sector," said Ross. "Cybersecurity is one of these things that cuts across disciplines. Information technology is at the heart of everything we do. Computer systems are fueling our ability to achieve mission success. And in order for us to be successful and carry out those missions, the technology that we deploy today must be dependable. And in order for that technology to be dependable, we have to make sure that it is properly secure."

Ross spoke about the importance of ensuring government systems are protected from even the most accidental security breaches. He gave the example of an employee of the Department of Veterans Affairs who took a laptop home to get caught up on work. The laptop was stolen from the employee's home, and on it were over 26 million veterans records with personally identifiable information. Setting off a scramble to notify the veterans of the incident, the stolen laptop was later recovered and forensics revealed that the sensitive information had not been compromised. The incident served as a startling reminder of how imperative it is to have the proper security measures on all government computers and devices.

"The ultimate solution to that problem is very simple," explained Ross. "It's called full disk encryption. What happened after this incident is that now our portable and mobile devices such as laptop computers are being outfitted with full disk encryption capability and we have a very low cost solution that makes that problem go away. So a lot of these measures are based on awareness."

Additional security measures have also have been established in response to various other threats and attacks, and have propelled cybersecurity into the spotlight lately within the DoD. Deputy Secretary of Defense William Lynn recently called cyber the 'fourth domain', making it a focus alongside air, sea and land. At a Security Defense Alliance in Belgium on September 15, Lynn expressed the importance of creating a strategy for the future in dealing with cyber threats.

"Cyber is an especially asymmetric technology. The low cost of computing devices means that our adversaries do not have to build expensive weapons, like stealth fighters and aircraft carriers, to pose a significant threat to our military capabilities," explained Lynn. "Cyber is also offense dominant. The Internet was designed to be open and interoperable. Security and identification management were lower priorities in system design. Structurally, our ability to defend networks always lags behind intruders. Defenders must defend everything; adversaries only need a single failure to exploit."

Lynn is just one of the many DoD supporters promoting training, education and awareness within the field of information security. Ross noted that training the future cybersecurity personnel within the DoD will be a critical step to ensuring the future challenges in the field of cybersecurity are being met. On June 23, U.S. Defense Secretary Robert Gates signed a memorandum establishing the U.S. Cyber Command (CYBERCOM) to be lead by General Keith Alexander.

"CYBERCOM is a great example of how we are unifying our forces," explained Ross. "This is a great opportunity now to grow the next generation – the kinds of folks that are going to be critical to keeping our missions operational. Things we didn't consider previously, we now have to consider routinely. We need the cyber warriors to be able to understand what the problems are. We are about 35,000 people short at the federal level with cybersecurity skills. Many of those skills are being developed right here at the Naval Postgraduate School. There are invaluable programs here training and educating the next generation of cyber warriors. And we can't get them to the field fast enough."

As the threats continue to grow, and the adversaries' tactics continue to evolve, there will always be a need for qualified men and women to serve in defending our critical information systems. Ross explained that the enemy is determined and can operate from anywhere in the world, and that requires the DoD to remain vigilant in cyber defense. From amateur hackers working out of their basement to terrorists with a specific target in mind, there is a continuous cyber threat. The important part, Ross noted, is being able to continue to carry out a mission, even when facing an attack.

"The threat is always out there. The adversaries never rest," said Ross. "Therefore we have to make sure that we keep on going every step of the way just like they are. Even deploying the best of everything that we have, we can only hope to stop about 90-95 percent. There will be a small percentage that will get through. We call those the advanced persistent threat. And we have to be able to deal with those."