COMPUTER SCIENCE
DEPARTMENT COLLOQUIUM

Secure Pairing of Constrained Wireless Devices: Challenges and Pitfalls

Dr. Nitesh Saxena, *University of Alabama at Birmingham*

Date and Time: October 25 (Friday), 2013 - 11:00am-12:00pm

Location: 3437 SEC

Abstract:

In this talk, we will focus on one of our projects entailing a fundamental problem of authentication and secure association of wireless devices ("pairing"). Pairing of devices based on auxiliary or out-of-band (OOB) -- audio, visual or tactile -- communication is a well-established research direction. Lack of good quality interfaces on, or physical access to, certain constrained devices (e.g., headsets, access points or medical implants) makes pairing a challenging problem in practice. Prior work shows that pairing of constrained devices based on authenticated OOB (A-OOB) channels can be prone to human errors that eventually translate into man-in-the-middle attacks. An alternative and more usable solution is to employ OOB channel that are authenticated as well as secret (AS-OOB).

Our higher level goal is to analyze the security of AS-OOB pairing. More specifically, we take a closer look at three notable prior AS-OOB pairing proposals and challenge the direct or indirect assumption upon which the security of these proposals relies, i.e., the secrecy of underlying or associated audio channels. The first proposal uses a low frequency audio channel to pair an implanted medical device with an external reader. The second proposal uses an automated vibrational channel to pair a mobile phone with a personal RFID tag. The third proposal uses vibration (or blinking) on one device and manually synchronized button pressing on the other device. In particular, we demonstrate the feasibility of eavesdropping over acoustic emanations associated with these methods. Based on our results, we conclude that all three methods provide a weaker level of security than what was originally assumed for these methods or is desired for the pairing operation.

Biography:

Nitesh Saxena is an Associate Professor in the Department of Computer and Information Sciences at the University of Alabama at Birmingham (UAB), and the founding director of the Security and Privacy in Emerging Systems (SPIES) lab. He works in the broad areas of computer and network security, and applied cryptography, with a strong interest in, and cutting across, device-centered security and user-centered security. Saxena's current research has been externally supported by multiple grants from NSF, and by gifts/awards/donations from the industry, including Google (2 Google Faculty Research awards), Cisco, Intel, Nokia and Research in Motion. He has published over 70 journal, conference and workshop papers, many at top-tier venues in Computer Science. Saxena obtained his Ph.D. in Information and Computer Science from UC Irvine, an M.S. in Computer Science from UC Santa Barbara, and a Bachelor's degree in Mathematics and Computing from the Indian Institute of Technology, Kharagpur, India. Before joining UAB, he was an Assistant Professor in the Department of Computer Science and Engineering at the Polytechnic Institute of New York University (NYU-Poly). He has also previously worked at Nokia Research Center, Finland and at INRIA Rhone-Alpes, France.

On the educational/service front, Saxena is a co-director for UAB's MS program in Computer Forensics and Security Management. He was also the principal architect and a co-director of NYU-Poly's M.S. Program in Cyber-Security. Saxena is serving as an Associate Editor for flagship security journals, IEEE Transactions on Information Forensics and Security (TIFS), and Springer's International Journal of Information Security (IJIS). Saxena's work has also received extensive media coverage, for example, at NBC, MSN, Fox, Discovery, ABC, Bloomberg, ZDNet, ACM TechNews, Yahoo News, Slashdot and Computer World. More information can be found on his lab web site: http://spies.uab.edu/.