Rochester Joint Chapter of the IEEE Computer and Computational Intelligence Societies

Rochester, New York

and

RIT's GCCIS PhD Program

present

Are 4G/5G Networks Vulnerable to Radio Signaling Attacks?

by

Vuk Marojevic

Associate Professor in the Department of Electrical and Computer Engineering at Mississippi State University

Date: Friday, August 30, 2019
Time: 11:30 a.m. to 12:30 p.m. Presentation
Location: RIT Campus, James E. Booth Hall - Bldg 7A, University Gallery (see: https://www.rit.edu/fa/gallery/)
Computer Society announcements and venue information:
http://ewh.ieee.org/r1/rochester/computer
Cost: Free. Open to IEEE members and non-members.
IEEE Event Feed: https://events.vtools.ieee.org/m/202917

Abstract

4G/5G security is an emerging problem, especially with IoT, V2V, UAV and other applications of advanced wireless technology emerging. In order to understand the vulnerabilities of these networks, we built a software radio testbed that models 4G LTE environments and developed a series of different cyber attacks to compromise the LTE radio access network. Motivated by the fact that mobile networks highly rely on control channel signaling, we challenged the system performance and availability by attacking individual LTE control channels and signals. Moreover, since user equipment (UEs) implicitly trust networks before the mutual authentication handshake is completed, we tested the effect that fake base stations and fake signaling, which we coin control channel spoofing, have on the behavior UEs. After running numerous experiments in controlled radio environments with standard compliant and mission critical LTE networks and commercial UEs we found that a number of radio frequency attacks can cause serious damage to the network performance and availability. One of the simplest, yet most severe attacks that can cause denial of service is to transmit the LTE synchronization signals asynchronously to those of legitimate networks. Fortunately, there is a simple solution to this threat that all LTE UEs face. An important lesson learned for 5G development and deployment is that standards need to consider operational edge cases for which simple solutions may exist.

Speaker's Biography

Vuk Marojevic is an associate professor of electrical and computer engineering at Mississippi State University. He graduated from the University of Hannover (M.S.), Germany, and Barcelona Tech-UPC (Ph.D.), both in electrical engineering. Prior to joining Mississippi State, he was with Wireless@Virginia Tech, where he developed various cognitive radio and LTE testbeds and conducted several wireless protocol measurement campaigns. He led Virginia Tech's LTE vulnerability analysis research and proposed several ways to harden LTE. His pioneering work on LTE control channel spoofing was picked up by industry and made it into 3GPP Release 13. His research interests are in software-defined radio, spectrum sharing, 4G/5G cellular technology, wireless network security, and resource management with application to mission-critical networks and unmanned aircraft systems. His website is at: https://www.ece.msstate.edu/people/faculty/vuk-marojevic/