Tutorial T-2: LTE Mobility Security and Virtualization

Presenters: Ashutosh Dutta (AT&T) & Roger Piqueras Jover (Bloomberg LP)

Tutorial overview:

This tutorial will present an introduction to mobile network security, with specific focus on LTE mobile networks. It will also provide an overview of a series of security threats against several of the network layers present in an LTE mobile network including security threats in virtualization.

Starting from the PHYsical and Link layers, the tutorial will provide and overview of the basics of the LTE Radio Access Network (RAN) and Enhanced Packet Core (EPC). Focusing on the RAN, we will cover the threat of advanced protocol-aware radio jamming against Orthogonal Frequency Division Multiple Access (OFDMA), the modulation and multiple-access methods used in LTE. The impact of these threats will be compared to that of known standard radio jamming attacks.

After an overview of the LTE Non-Access Stratum (NAS) protocol, we will discuss the feasibility of rogue base stations in LTE mobile networks as well as other protocol exploits that can potentially lock the device and the SIM card, rapidly exhaust the device battery and allow a passive attacker to follow a victim as it hands off from base station to base station.

Moving onto the EPC, the NAS protocols over the core network will be covered. Based on this, we will introduce the concept of control plane signaling overloads and spikes. We will discuss the potential impact of these threats and a series of known instances of signaling spikes that affected mobile operators all over the world. In this context, we will introduce the control plane scalability issues caused by the rapid spread of the Internet of Things (IoT) over mobile networks.

Finally, we will move onto the paradigm of virtualized mobile networks running on the cloud. While network function virtualization opens up the door for flexible service creation and rapid deployment, it also adds additional security challenges attributed by virtualization and software defined network aspects of the network. Network Function Virtualization introduces additional deployment specific security challenges such as authentication and authorization of VM migration, VM instantiation, hypervisor security, orchestration security, SDN controller security etc.

With the rapid deployment of 4G LTE networks, operators have started the trial deployment of network function virtualization, especially with the components for Evolved Packet Core (EPC), and IP Multimedia Services (IMS). However, very little attention has been given to the security aspects of virtualization by these vendors. While security expert group within ETSI NFV has started looking into many security issues imposed by Network Function Virtualization, additional work is needed with larger security community involvement. This tutorial will provide a comprehensive overview of security virtualization.

Tutorial outline:

I. LTE RAN and Physical layer overview
II. LTE RAN security
  a. Radio jamming
  b. Protocol-aware radio jamming, smart jamming and very-low-power jamming
III. LTE EPC and NAS protocols overview
  a. Rogue base stations, LTE protocol exploits and location leaks
IV. LTE EPC security and scalability
  a. Control plane signaling overloads and spikes
  b. Botnets of mobile devices
  c. IoT scalability and impact on control plane layer
V. Virtualized mobile networks and Network Function Virtualization (NFV) overview
VI. NFV and cloud-based mobile network security
  a. Security for SDN and NFV
  b. Challenges and Opportunities for Security Virtualization
  c. Security Standards Overview (e.g., ETSI/NFV, OPNFV)
  d. Virtualized Network Vulnerabilities and Threats
  e. Secure Virtual Networks
  f. Threat Taxonomy of SDN and NFV
  g. Security Function Virtualization and Security as a Service
  h. Lessons Learnt from Security Virtualization Experiments
  i. NFV security standardization efforts

Presenter Biographies

Ashutosh Dutta, Ph.D. is currently Director Technology Security at AT&T's Security and Mobility Organization within Chief Security Office where he leads the design and architecture of security for next generation mobility networks. His 25 years of career include CTO of Wireless at a Cybersecurity company NIKSUN, Senior Scientist in Telcordia Applied Research, Director of Central Research Facility at Columbia University, and Computer Engineer with TATA Motors. He has more than 80 conference and journal publications, three book chapters, 30 issued patents, and has given tutorials in mobility management at various conferences. Ashutosh's research interests include wireless Internet, multimedia signaling, mobility management, 4G networks, IMS (IP Multimedia Subsystems), VoIP and session control protocols. Ashutosh is co-author of the book, titled, "Mobility Protocols and Handover Optimization: Design, Evaluation and Application," published by John & Wiley. He serves as the editor-in-chief for the Journal of Cybersecurity and Mobility published by River Publishers. As a senior member of IEEE and ACM, Ashutosh served as the chair for IEEE Princeton / Central Jersey Section, Industry Relation Chair for Region 1 and MGA, Pre-University Coordinator for IEEE MGA and chair for Ad Hoc Committee for Public Visibility for ComSoc. As the vice chair of Education Society Chapter of PCJS, he co-founded the IEEE STEM conference (ISEC) in 2011 and helped to implement EPICS (Engineering Projects in Community Service) in the high schools within PCJS. Ashutosh currently serves as the director of Marketing and Industry Relations for IEEE ComSoc. He was recipient of the prestigious 2009 IEEE MGA Leadership award and 2010 IEEE-USA professional leadership award. Ashutosh obtained his BS in EE from NIT Rourkela, India, MS in Computer Science from NJIT and earned his M. Phil. and Ph.D. in Electrical Engineering from Columbia University, under the supervision of Prof. Henning Schulzrinne.

http://www.cs.columbia.edu/~dutta/

Roger Piqueras Jover is a Wireless Security Research Scientist at Bloomberg LP, where he leads the projects on mobile and wireless security. Previously, he spent 5 years at the AT&T Security Research Center (AT&T SRC) with the role of Member, Senior Member and Principal Member of Technical Staff. He led the projects on LTE mobile network security, investigating PHY layer threats and LTE protocol exploits, as well as control plane signaling scalability issues.

He holds an MPhil in Electrical Engineering from Columbia University, an MSc in Electrical and Computer Engineering from University of California Irvine and a Dipl.-Ing. in Telecommunications Engineering from Universitat Politècnica de Catalunya, in Barcelona.

Roger holds over a dozen issued and published patent applications. He has co-authored manuscripts in numerous top communications and security conference and has been in the TPC Committee for numerous conferences and workshops. He is the TPC Co-Chair for the ongoing IEEE 5G Summit series and a member of the IEEE ComSoc Marketing and Industry Relations taskforce. He is also the author of a book chapter on the security and impact of the IoT on LTE mobile networks. He holds numerous awards, including the AT&T Chief Technology Award, the AT&T CSO Award and the Distinguished Reviewer award from IEEE Transactions on Mobile Computing.

His research interests are in the area of mobile and wireless communications, resource allocation, new network architectures and technologies for 5G and security for wireless networks. In his spare time, he actively works in identifying, implementing on software-radio and proposing solutions to PHY layer threats, rogue base stations and protocol exploits against LTE cellular networks.

http://www.ee.columbia.edu/~roger/
http://www.bloomberg.com/company/announcements/mobile-security-a-conversation-with-roger-piqueras-jover/