UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

"Practical Cellular Network (3G/4G/5G) Security and Attacks"

Prof. Dr. Ravishankar Borgaonkar

SINTEF AS & University of Stavanger, Norway

e-mail: Ravi.Borgaonkar@sintef.no

Short Abstract: The cellular networks such as 2G, 3G, 4G and 5G are already becoming a part of national critical communication infrastructure. In addition, the threat landscape of new network generations (for example, 5G) is changing rapidly, indicating a need of understanding the implication to national critical assets (focusing on telecommunication networks) and prepare security strategy accordingly. In this regard, this advanced course module provides a brief overview of cellular networks including 5G and demonstrate practical risks associated in every generations to mobile endpoints.

Course Contents in brief:

Topic 1:

- Abstract view of cellular network architecture
- 2G/3G network security and weaknesses

Lab 1 - Get familiar with software and hardware tools to investigate mobile networks and their security configurations. We will be providing extensive knowledge on such low-cost security testing tools and their limitations. We will do a few exercises in understanding practical implications of 2G vulnerabilities.

Topic 2:

- 4G network architecture and security
- Authentication in 4G networks
- Security attacks in 4G networks

Lab 2 – This lab will focus on 4G network related hardware and software tools for performing security analysis of live networks. The candidates will get an opportunity to play with commercial hardware tools which is used for network diagnostic purpose as well.

Topic 3:

- Abstract view of 5G NSA and SA network
- Authentication in 5G networks
- 5G NSA and SA radio/core network issues (covers both vendors and standard specific issues)
- Hardware and software tools for security investigations

Lab 3 – This lab will focus on 5G related tools for debugging and identification of network threats.

Total # of hours of lecture: 20

References:

1. Bour, Guillaume, Anniken Wium Lie, Jakob Stenersen Kok, Bendik Markussen, Marie Elisabeth Gaup Moe, and Ravishankar Borgaonkar. "Security Analysis of the Internet of Medical Things (IoMT): Case Study of the Pacemaker Ecosystem." In *International Joint Conference on Biomedical Engineering Systems and Technologies*, pp. 73-96. Cham: Springer Nature Switzerland, 2022.
2. Borgaonkar, Ravishankar, Inger Anne Tøndel, Merkebu Zenebe Degefa, and Martin Gilje Jaatun. "Improving smart grid security through 5G enabled IoT and edge computing." *Concurrency and Computation: Practice and Experience* 33, no. 18 (2021)
3. Park, Shinjo, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. "Anatomy of commercial IMSI catchers and detectors." In *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, pp. 74-86. 2019.
4. Shaik, Altaf, and Ravishankar Borgaonkar. "New vulnerabilities in 5G networks." In *Black Hat USA Conference*. 2019
5. Shaik, Altaf, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities." In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221-231. 2019.
6. Arfaoui, Ghada, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix Klaedtke et al. "A security architecture for 5G networks." *IEEE access* 6 (2018): 22466-22479.

CV of the Teacher

Ravishankar Borgaonkar works as a senior research scientist at SINTEF Digital and Associate Professor II at the University of Stavanger in Norway. In 2007, he received an Erasmus Mundus award from the European Union and completed a dual master's degree from the Royal Institute of Technology (Sweden) and Aalto University (Finland, previously TKK) in 2009. While working in Germany, he holds a PhD in telecommunication security area from Technischen Universität Berlin (TU Berlin, 2013). His primary research themes are related to mobile telecommunication networks and security threats for the next generation of digital communication, ranging from 2G/3G/4G/5G network security to end-user device security. As a research fellow in 5G security area at University of Oxford, he led the EU project “5G-ENSURE” together with 14 companies including Nokia and Ericsson. He has extensive experience in a cellular network and information security domain at Deutsche Telekom's lab (Germany), TU Berlin (Germany), Intel Collaborative Research Institute for Secure Computing at Aalto University (Finland), and University of Oxford (United Kingdom). He has found several protocol flaws in 3G/4G/5G technologies (affecting billions of devices) and assisted in improving 4G/5G security standards. Also, he is a frequent speaker at several leading security (hacking/academic/industry) conferences and is listed in the Hall of Fame of Google, Qualcomm, Huawei, and GSMA.

Final Exam: Yes

Final Test

Room and Schedule

Room: *Aula Riunioni del Dipartimento di Ingegneria dell'Informazione, Via G. Caruso 16, Pisa – Ground Floor*

Schedule:

07/10/2024 – 9:30 – 13:30

08/10/2024 – 9:30 – 13:30

09/10/2024 – 9:30 – 13:30

10/10/2024 – 9:30 – 13:30

11/10/2024 – 9:30 – 13:30