Università degli Studi di Napoli Federico II

PhD Student: Giovanni Stanco

Year end presentation

Tutor: prof. Giorgio Ventre

Cycle: XXXV

Year: First (2019/2020)

My background

- MSc degree: Telecommunications Engineering
- Research group/laboratory: ARCLAB
- PhD start date: November 2019
- Scholarship type: company funded scholarship
- Partner company: Rislab SRL
- Company tutor: Ing. Flavio Frattini

Research field of interest

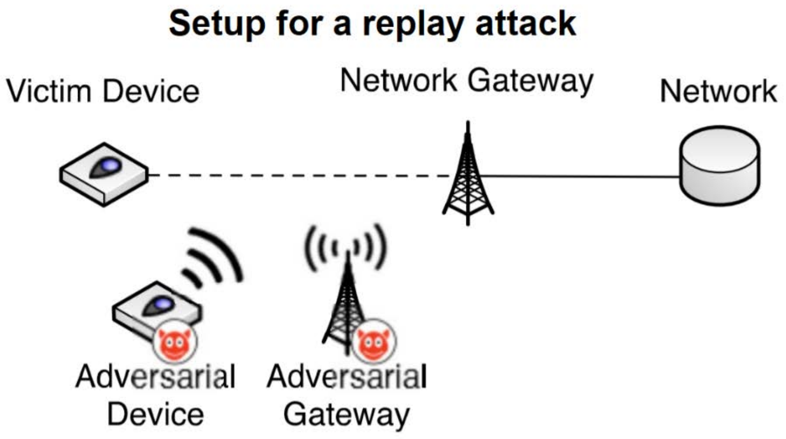
- My research topic is: “Networking in IoT and Cyber-Physical Systems: Performance and Security Issues”.
- IoT: networking infrastructure to connect a massive number of devices
- CPS: system that leverages cyber components to monitor physical components
- Some of the previous works on security:
  - Abomhara, Køien: ‘Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks’
  - Butun, Osterberg, Song, ‘Security of the Internet of Things: vulnerabilities, attacks, and countermeasures’
  - Meneghello, Calore, Zucchetto, Polese, Zanella, ‘IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices’
- Our focus is network security in wireless communications for IoT and CPS services, especially for long range technologies.

Summary of study activities

- Ad hoc PhD courses:
  - Intelligenza artificiale ed etica
  - Scientific programming and visualization with Python
  - Innovation management, entrepreneurship and intellectual property
  - Machine learning
  - Strategic orientation for STEM Research and Writing
- Courses attended borrowed from MSc curricula
  - Protocolli per reti mobili (prof. Avallone)
  - Network security (prof. Romano)
  - Software security per sistemi industriali (proff. Cotroneo, Natella)
- Conferences / events attended
  - 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud)
  - DSN2020: 50th IEEE/IFIP International Conference on Dependable Systems and Networks

Research activity: Overview

- Problem
  - Wireless communications are important in several scenarios
  - But they are insecure and subject to several attacks:
    - Jamming
    - Packet forging
    - Replay attack
    - DoS
    - Spoofing
    - Man in the middle



Research activity: Overview

- Objective
  - Assess the current security level of IoT devices and networks and assess the performance of IoT devices in terms of security
  - Discover vulnerabilities
  - Understand if it is safe to use wireless communications in IoT
- Intended contribution (in perspective)
  - Mitigate vulnerabilities of IoT communication technologies
  - Evaluation of the most secure communication technology for safety critical applications
  - Final goal: use of wireless communications in IoT in a safe way

Products

[P1]	**Conference paper** Title: ‘DewROS: a platform for informed Dew Robotics in ROS’ Authors: Giovanni Stanco, Alessio Botta, Giorgio Ventre Presented at the 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud)
[P2]	**Journal article** Title: ‘DewROS: a platform for informed Dew Robotics in ROS’ Authors: Giovanni Stanco, Gennaro Esposito Mocerino, Alessio Botta, Giorgio Ventre Not submitted yet

References

[R1]	J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.
[R2]	A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.
[R3]	T. Salman and R. Jain, Networking protocols and standards for internet of things, 02 2017, pp. 215–238.
[R4]	M. Abomhara and G. M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” J. Cyber Secur. Mobil., vol. 4, pp. 65–88, 2015.
[R5]	I. Butun, P. Osterberg, and H. Song, “Security of the internet of things: Vulnerabilities, ¨ attacks, and countermeasures,” IEEE Communications Surveys Tutorials, vol. 22, no. 1, pp. 616–644, 2020.
[R6]	F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of threats? a survey of practical security vulnerabilities in real IoT devices,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182–8201, 2019.
[R7]	F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, “Security issues in internet of things:Vulnerability analysis of lorawan, sigfox and nb-iot,” in2019 Global IoT Summit (GIoTS), 2019,pp. 1–6