Research Project (PhD) on Wireless Sensing Security

Supervision: Thomas Clausen, LIX, École Polytechnique (thomas.clausen@polytechnique.edu)
Kevin Jiokeng, LIX, École Polytechnique (kevin.jiokeng@polytechnique.edu)

Wireless networks are more and more pervasive and ubiquitous in our society where they enable a large variety of applications for our daily lives. At the same time, if they are primarily designed for communication, their spectrum of services is increasingly expanding to include related uses to which they are particularly well suited. Ongoing research around *wireless sensing* has shown that these networks can be used, among other things, to track the position of users [1], monitor their health (heart rate, breathing rate, sleep quality, etc.) [2], authenticate them in a biometric way (recognize their walking, breathing, etc.) [3], or to recognize what they are doing (gesture and activity recognition [4]), and this is already being adopted by the market [5, 6]. The list is far from being exhaustive. As an emerging multidisciplinary research field, wireless sensing takes advantage of the physical properties of electromagnetic waves when they encounter or travel through obstacles (reflection, absorption, diffraction, etc.) and builds on top of knowledge from different scientific fields – including Networking, Signal Processing and Machine Learning/Artificial Intelligence – to enable a wide variety of applications and therefore speed up the entrance in a more connected and smarter world.

However, existing research works in this field have focused mostly on expanding capabilities and enabling new applications, thereby neglecting the security of developed systems. Recent research works have shown that an attacker with a single off-the-shelf wifi device can strongly disturb wireless sensing systems performance and even make them behave as they want [7, 8]. Moreover, the inherent nature of wireless waves, which can travel through objects and walls, naturally raises privacy concerns, as an attacker could "listen", from outside, to what is happening in the targeted room.

The aim of this research project is to tackle these challenges and advance the field on the security aspect by:

- Studying, both theoretically and practically, security issues that are inherent to wireless sensing applications
- Exploiting the identified breaches to develop "exploiting systems" that will act as demonstrators of these vulnerabilities
- Developing security primitives, counter-measures, methodologies and tools that could help in the design of secure wireless sensing systems
- Applying these concepts and tools to chosen applications to evaluate their performance and showcase their benefits

Effectively addressing these challenges requires a rigorous scientific approach, involving both theoretical and practical skills. We intend to apply a methodology strongly driven and supported by experiments, whether for the validation of initial hypotheses, the design of solutions and the evaluation of these solutions that will always be deployed on real hardware.

Expected candidate skills:

The most important skill for this PhD is **to be eager to learn while trying new solutions.** On top of that, the following skills would be strongly appreciated.

- Hands-on experience and strong skills in Machine and Deep Learning. Knowledge of modern learning schemes such as Multi-task Learning, Autoencoders and Transfer Learning would be appreciated.
- Strong programming skills in any common language such as C++, Python, Java, etc.
- Knowledge of network protocols functioning would be appreciated

References

[1] J. Wang, X. Zhang, et al., “Device-free wireless localization and activity recognition: A deep learning approach,” IEEE Transactions on Vehicular Technology, vol. 66, no. 7, pp. 6258–6267, 2017. doi: 10.1109/TVT.2016.2635161.

[2] S. Yue, H. He, et al. “Extracting multi-person respiration from entangled rf signals,” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 2, no. 2, pp. 1–22, Jul. 2018. doi: 10.1145/3214289.

[3] F. Lin, C. Song, et al., “Cardiac scan: A non-contact and continuous heart-based user authentication system,” in International Conference on Mobile Computing and Networking (MobiCom), ACM, 2017, pp. 315–328. doi: 10.1145/3117811.3117839.

[4] E. Kim, S. Helal, et al., “Human activity recognition and pattern discovery,” IEEE Pervasive Computing, vol. 9, no. 1, pp. 48–53, 2010. doi: 10.1109/MPRV.2010.7.

[5] https://www.originwirelessai.com/

[6]https://www.01net.com/actualites/wi-fi-sensing-lastucieuse-technologie-dorange-pour-securiser-votre-maison-avec-une-simple-livebox.html.

[7] J. Liu, Y. He, C. Xiao, J. Han, L. Cheng and K. Ren, "Physical-World Attack towards WiFi-based Behavior Recognition," *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, London, United Kingdom, 2022, pp. 400-409, doi: 10.1109/INFOCOM48880.2022.9796920.

[8] Y. Xie, R. Jiang, X. Guo, Y. Wang, J. Cheng and Y. Chen, "Universal Targeted Adversarial Attacks Against mmWave-based Human Activity Recognition," *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, New York City, NY, USA, 2023, pp. 1-10, doi: 10.1109/INFOCOM53939.2023.10228887.