Ph.D position on Physical layer authentication for IoT

University of Bordeaux - France, KU Leuven - Belgium

We invite applications for a fully funded PhD research position in computer science co-supervised between University of Bordeaux, France, and KULeuven, Belgium.

The French part of the Ph.D. thesis will take place within the Progress[1] research group of LaBRI at the University of Bordeaux, France. The Belgian part of the Ph.D. thesis will take place within the Computer Security and Industrial Cryptography (COSIC) group[2] research group of KU Leuven, Belgium. The position is funded for 3 years and will address research challenges in the fields of physical layer authentication in distributed systems. When successful, the Ph.D. candidate will obtain a dual Ph.D. degree from both the University of Bordeaux and KU Leuven. The research work will be conducted under the supervision of Dr. Dave Singelée (KU Leuven) and Dr. Stéphane Delbruel (University of Bordeaux), in the context of a collaboration between the two universities. Applicants must have an MSc degree in either Computer Science or Electrical Engineering (or equivalent), be fluent in English, and demonstrate strong team-working abilities. Candidates with proven programming skills who are knowledgeable in wireless communications, embedded architectures, signal processing and security are particularly encouraged to apply.

Key-words: wireless sensor networks, IoT, signal processing, security.

Scientific Context and Objectives

Mass adoption, among others within critical use cases, led to a strong need to provide security in wireless sensor networks (WSNs). In today's infrastructures, this role tends to be handled by a core entity, using authentication and encryption provided by application layer-based secure mechanisms. This approach inherited from decades of wired network infrastructures as the environment to secure, showed its limits and inadequacy when applied to WSNs.

Due to energy constrained environments, limited computing power and connectivity as well as heterogeneity within the used radio technologies, this top-down approach fails to provide full security coverage at a satisfactory energy demand [1, 2]. Moreover, being usually orchestrated by a central server when applied to WSNs, it led to the impossibility of preserving security and privacy features between end-devices and gateways suffering a

[1] https://www.labri.fr/en/programming-networks-and-systems
[2] https://www.esat.kuleuven.be/cosic

disconnection from the rest of the infrastructure. This state of the art approach led to industrial actors removing some security features for the sake of simplicity and malicious attacks targeting surfaces left unprotected [3].

Facing these difficulties, it becomes of prime importance to investigate novel security mechanisms able to operate in a more pervasive fashion within the end- devices. Physical (PHY) layer-based security is a novel and promising approach based on information-theoretic security, operating at the lowest level and providing secure mechanisms relying on physical phenomena of the radio link itself [4, 5]. Such mechanisms for constrained environments hold the promises of overcoming the previously cited limitations while potentially offering substantial energy savings [6, 7].

Leveraging this emerging field of PHY-based security, we propose to investigate a novel network and system security paradigm, able to strengthen the authentication guarantees offered by any infrastructure operator while simplifying their implementation.

In this context, the goal of this Ph.D research project is twofold: First, we wish to propose new approaches to use PHY-based authentication in LPWANs, by overcoming some of the current practical limitations of PHY-based authentication. Second, to rely on the mobile edge for abstraction and resilience, we will research how secure authentication mechanisms traditionally managed by the upper layers can be delegated to lower layers through system abstraction.

Requirements

The working languages at the University of Bordeaux are French and English. The working languages at the KU Leuven is English. The candidate is expected to use state-of-the-art tools for software development and collaboration, such as git, Docker, and such.

Location

The University of Bordeaux welcomes 56,000 students and is ranked among the top French universities. The city of Bordeaux is located at the very heart of Southern Europe, only one hour from the Atlantic Ocean and two hours from Paris by train, thus enjoying a mild oceanic climate and rich natural surroundings.

The KU Leuven welcomes 66,000 students and is ranked among the top universities in the world. The city of Leuven is located in Flanders, the northern region of Belgium, only thirty minutes to Brussels, and less than two hours from the North sea by train, thus enjoying an oceanic climate and historical surroundings.

The Ph.D. candidate is expected to work 1.5 years of his/her Ph.D. in Bordeaux and 1.5 years in Leuven.

Application

Applications should be submitted by e-mail to Dave Singelée (dave.singelee@esat.kuleuven.be) and Stéphane Delbruel (stephane.delbruel@u-bordeaux.fr) with the title “Ph.D Application

2023", including

- Curriculum vitae;
- List of 2-3 reference persons and their e-mail addresses (we ask for recommendation letters ourselves and we will ignore any recommendation letter sent by the candidate her/himself);
- Transcripts of undergraduate and graduate studies;
- Links to MSc and internship thesis/reports, and any publications, if applicable;
- Links to examples of personal software contributions (on GitHub or similar), if applicable.

All documents must be sent as a single pdf. The expected starting date is as soon as possible and at the latest before the end of 2023. Applications will be screened as they arrive and until an appropriate candidate is selected.

References

[1] L. Wang, *Physical Layer Security in Wireless Cooperative Networks*. Wireless Networks, Cham: Springer International Publishing, 2018.

[2] P. Kietzmann *et al.*, "A performance study of crypto-hardware in the low-end iot," in *Cryptology ePrint Archive*, 2021.

[3] K. S. team, "Kaspersky iot security report," 2022. https://www.kaspersky.com/blog/iot-report-2022/.

[4] H. Zhou and A. El Gamal, "Network information theoretic security," in *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 978–983, IEEE, 2020.

[5] Hongbo Liu *et al.*, "Collaborative secret key extraction leveraging Received Signal Strength in mobile wireless networks," in *IEEE INFOCOM*, 2012.

[6] D. Altolini *et al.*, "Low power link layer security IoT: Implementation and performance analysis," in *IEEE IWCMC*, 2013.

[7] Z. Wei *et al.*, "Energy- and Cost-Efficient Physical Layer Security in the Era of IoT: The Role of Interference," in *IEEE Communications Magazine*, 2020.