Ten Years of Studies on the Security of Connected Objects: a Wrap-up (Keynote Abstract)

Vincent Nicomette¹, Romain Cayre²

Keywords

Cybersecurity, IoT, Offense and Defense, Vulnerability analysis, Communication protocols, Intrusion detection, Identification

Topic

Connected objects are invading our professional and personal daily lives. These objects are more and more efficient and provide more and more varied services, but are they sufficiently secure? This keynote will try to answer this question by taking stock of ten years of research in the context of the security of connected objects. This work was carried out within the LAAS-CNRS's TSF team (Fault Tolerance and Computer Operating Safety), within the framework of 4 theses. This work brought contributions on both offensive and defensive aspects. On the offensive side, the presentation will address in particular the analysis of vulnerabilities targeting various objects and protocols (ADSL Box, connected TVs, BLE objects, wireless keyboard/mouse, specification of the BLE protocol). On the defensive side, the presentation will address intrusion detection and identification of connected objects. This keynote will be illustrated with several demonstrations.

Biography

Vincent Nicomette is an engineer from ENSEEIHT Toulouse (1992), doctor of INPT (1996) and holder of an HDR from the INPT (2009). After having worked as an engineer in Matra Marconi Space (today Airbus Defense and Space), from 1997 to 2000, he is now a teacher at INSA Toulouse and a researcher at LAAS-CNRS since October 2000. His main research work covers 3 main aspects: 1) network security, and in particular lately the security of IoT communication protocols, 2) the security of the lower layers of operating systems, and 3) the security of critical embedded systems. He is also co-manager of the

 $\label{eq:constraint} \textit{C&ESAR'23: Computer & Electronics Security Application Rendezvous, Nov.~21-22,~2023,~Rennes, France$

https://dblp.org/pid/230/3815.html (R. Cayre)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

¹ INSA Toulouse / LAAS-CNRS

² Eurecom

TLS-SEC course in Toulouse, a course dedicated to computer security and provided at three different schools: INSA, ENAC and N7.

Romain Cayre is currently a post-doctoral researcher in the S3 (Software and System Security) team at the EURECOM Institute in Biot. His research work is devoted to the security of wireless communication protocols and the security of embedded systems, with a particular interest in the analysis of interactions at the boundary between software and hardware. He received an engineering degree in computer science from the Institut National des Sciences Appliquées de Toulouse in 2018, and carried out his doctoral thesis from 2019 to 2022 within the TSF team (Tolerance to faults and Dependability) from LAAS-CNRS. During his PhD thesis, his work focused on the security of wireless communication protocols in the context of the Internet of Things. As part of this work, he has produced several software tools published under a free license, in particular the Mirage wireless protocol vulnerability analysis tool.