

Embedded Systems Security

Andrei-Lucian MAZILU

Faculty of Electronics, Telecommunications, and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest,
Romania

andrei.mazilu2410@stud.etti.upb.ro

Abstract

Embedded systems have been increasingly integrated into various aspects of our modern life, from smart appliances to industrial control systems, creating a pressing need for security measures to mitigate potential risks which may arise. This article aims to provide an overview of the challenges and opportunities associated with securing embedded systems, highlighting their vulnerabilities due to limited resources and interdependence. The industry standards and regulations have been playing a crucial role in bolstering the security posture of embedded systems, while also exploring the latest advancements in protection mechanisms.

Index terms: embedded systems, security, risks, vulnerabilities

References

- [1]. Philip Koopman, "Embedded System Security", Carnegie Mellon University, 37(7), 95-97, 2004.
- [2]. S. Ravi A. Raghunathan, P. Kocher, S. Hattangady, Security in embedded systems: design challenges. *Trans Embed Comput Syst* 3(3):461-491, 2004.
- [3]. R. Muresan, C. Gebotys, Current flattening in software and hardware for security applications. In: *CODES+ISSS*, pp 218-223, 2004.
- [4]. F. Vahid and T. Givargis, "Embedded system design: A unified hardware/software approach," Department of Computer Science and Engineering University of California, 1999.
- [5]. D. Lake, R. Milito, M. Morrow, and R. Vangheese, "Internet of things: Architectural framework for ehealth security," *Journal of ICT*, vol. 3, pp. 301-330, 2014.
- [6]. D. Kleidermacher and M. Kleidermacher, *Embedded systems security: practical methods for safe and secure software and systems development*. Elsevier, 2012.
- [7]. R. Islam, S. Choudhury, A. Anwar, T. Rahman, *Embedded Systems and Network Security*.