SUIT: Security of Update-related IoT Traffic

Ahmad B. Usman[1], Emre Süren[2], and Mikael Asplund[1]

[1] Dept. of Computer and Information Science, Linköping University, Sweden
{ahmad.usman,mikael.asplund}@liu.se
[2] KTH Royal Institute of Technology, Stockholm, Sweden
emsuren@kth.se

Abstract. Software updates are essential for maintaining the security of smart home IoT devices, yet the network-level behavior and the security of update delivery remain largely underexplored in this domain. We present a multidimensional analysis of IoT update traffic, identifying characteristics of the update process, and combining entropy-based encryption characterization, cipher-suite evaluation, and certificate security assessment. Our study covers controlled experiments on ten heterogeneous devices in a laboratory environment and retrospective analysis of a large-scale real-world dataset to assess generalizability. Results reveal three classes of weakness: a substantial share of update traffic is carried over plaintext channels; weak cipher-suites dominate TLS configurations; and a portion of certificates fall below the NIST 128-bit security minimum recommended for protection from 2031 onward, highlighting concrete long-term risks. By mapping weak and insecure cryptographic configurations to public vulnerability records, we demonstrate that the observed weaknesses correspond to known, actively tracked security risks, underscoring the concrete threats to update delivery confidentiality, integrity, and authenticity.

Keywords: Software Update · Firmware Update · Traffic Analysis · IoT Security