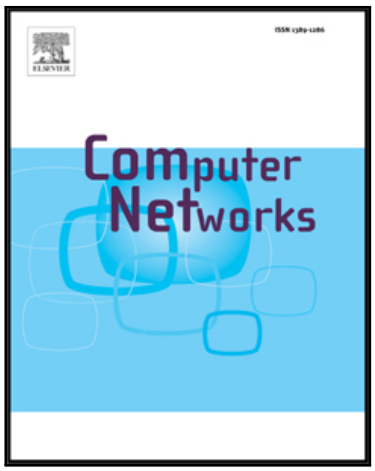

AAoT: Lightweight Attestation and Authentication of low-resource Things in IoT and CPS

Wei Feng, Yu Qin, Shijun Zhao, Dengguo Feng

PII: S1389-1286(18)30047-1
DOI: 10.1016/j.comnet.2018.01.039
Reference: COMPNW 6387

To appear in: *Computer Networks*

Received date: 24 July 2017
Revised date: 4 December 2017
Accepted date: 18 January 2018

Please cite this article as: Wei Feng, Yu Qin, Shijun Zhao, Dengguo Feng, AAoT: Lightweight Attestation and Authentication of low-resource Things in IoT and CPS, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.01.039

AAoT: Lightweight Attestation and Authentication of low-resource Things in IoT and CPS

Wei Feng[a,*], Yu Qin[a], Shijun Zhao[a], Dengguo Feng[a,b]

[a] *TCA Laboratory, ISCAS, Beijing*
[b] *State Key Laboratory of Computer Science, ISCAS, Beijing*

Abstract

With the rise of Internet of Things (IoT) and Cyber-Physical Systems (CPS), the need for smart embedded devices is rapidly increasing, and so does the security and privacy risk. This paper focuses on enabling both remote attestation and authentication of current commodity low-resource embedded devices to enhance security in the IoT and CPS contexts. We demonstrate a detailed design and prototype implementation of AAoT, a lightweight and practical mechanism for Attestation and Authentication of Things, that can provide software integrity, mutual authentication and tamper-proof feature for smart embedded devices. AAoT is based on physical unclonable functions (PUFs), random memory filling and software attestation without requiring any changes in existing micro-controller units (MCUs). We show how to obtain efficient implementations and optimizations for each of the building blocks of AAoT, including a PUF-based memory filling, a checksum function with block-based traversal, a pseudorandom function, a reverse fuzzy extractor and a random number generator. The prototype is implemented on a low-end MCU platform (TI MSP430) by using onboard SRAM, registers and Flash resources.

Keywords: IoT Security, CPS Security, Remote Attestation, Authentication, Embedded Security, Physically Unclonable Function (PUF)

1. Introduction

Smart embedded devices are the core components of Internet of Things (IoT) and Cyber-Physical Systems (CPS). Security and privacy problems of these devices have become one of the main challenges in IoT and CPS contexts. Firstly, these devices are resource-constrained and often lack the security capabilities or mechanisms of general purpose computing platforms. Secondly, more and more devices are beginning to be exposed to the public network (e.g., Internet and cloud platforms), and malicious attackers are easy to access them. Thirdly, these devices usually interact directly with the physical world to collect privacy data or control physical environment variable, which makes them an attractive target of attackers. A successful attack on these devices could bring serious damages to our modern life. For example, as recently reported,

*Corresponding author
Email addresses: vonwaist@gmail.com (Wei Feng), qin_yu@tca.iscas.ac.cn (Yu Qin), zhaosj@tca.iscas.ac.cn (Shijun Zhao), feng@tca.iscas.ac.cn (Dengguo Feng)