Securing Embedded Networks through Secure Collective Attestation

Ahmad Ibrahim
Technische Universität Darmstadt, Germany
ahmad.ibrahim@trust.tu-darmstadt.de

ABSTRACT

Embedded devices are increasingly permeating our environment to collect data and act on the insight derived. Examples of such devices include smart environments and autonomous systems. The increasing ability to connect, communicate with, and remotely control such devices via the legacy internet has raised considerable security and privacy concerns. One key mechanism to protect the software integrity of these devices is attestation.

In this dissertation, we devise attestation schemes that are scalable and applicable for large networks of embedded devices. In particular, we present attestation schemes that are capable of detecting remote malware infestation, physical, and run-time attacks in different settings including smart environments and autonomous systems.

CCS CONCEPTS

• Security and privacy → Security protocols;

ACM Reference Format:
Ahmad Ibrahim. 2018. Securing Embedded Networks through Secure Collective Attestation. In MobiSys PhD Forum ’18, June 10, 2018, Munich, Germany. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3212711.3212712

1 INTRODUCTION

Embedded devices are rapidly proliferating into every domain of our life. Current industrial trends envision systems consisting of large numbers of heterogeneous embedded devices. Billions of devices will be connected to enable many new services and experiences. Examples include: (1) attended control systems, where large numbers of heterogeneous devices monitor and control safety-critical processes; and (2) unattended autonomous networks where a multitude of devices collaborate to achieve a certain task.

Unlike traditional computers, embedded devices lack the necessary security capabilities which protect them against attacks. Today, an adversary can easily attack such devices compromising both privacy and safety. A key mechanism for detecting such attacks and ensuring the safe and secure operation of a device, is remote attestation [3, 5]. However, remote attestation solutions do not scale to very large embedded networks, are not applicable in the autonomous settings, and are incapable of detecting advanced attacks such as physical and run-time attacks.

In this dissertation, we devise collective attestation schemes for embedded devices that are capable of detecting remote malware infestation, physical, and run-time attacks on devices of both attended and autonomous embedded networks.

2 FINDINGS

The dissertation is composed of three core components, the current and planned progress of which is outlined below.

2.1 Detection of Malware

Traditional attestation schemes consider only a single prover and verifier and are not scalable to very large embedded networks. In this part of the dissertation we develop solutions that scale existing attestation schemes to verify networks of embedded devices by leveraging in-network attestation and novel cryptographic primitives.

SEDA. In this work [2] we investigate the security of networks of embedded devices and present the first efficient attestation protocol for large networks, which allows a central verifier to assess the trustworthiness of million-device networks in order of seconds. To achieve this goal, the attestation burden is distributed across the network, allowing neighbors to attest each other and to aggregate the attestation results. In SEDA, each device in the network is initialized with its own software configuration and secret key. When two devices meet, they exchange software configuration and generate a shared key. To attest a network, the verifier chooses a device as initiator and sends it a random challenge. The challenge is then flooded in the network forming a spanning tree rooted at the initiator. Starting at leaf nodes, each device generates an attestation report and sends it to its parent for verification. This process ends when the initiator forwards the aggregated attestation report of the entire network to the verifier. Using the information included in the report, the verifier determines the number of the trusted devices in the network. As shown in Figure 1, attestation in SEDA imposes a run-time overhead which is logarithmic in the network size.

SANA. In this work [1] we present a novel cryptographic primitive, called Optimistic Aggregate Signatures (OAS), which is a generalization of aggregate and multisignatures. OAS provides a short
signature size and verification time which is independent of the number of signers. Based on OAS, SANA presents an attestation protocol for embedded networks, which is more resilient to physical and Denial of Service (DoS) attacks than SEDA. In comparison with SEDA, the attestation responses in SANA are not verified by parents in the spanning tree but by the verifier at the end of the protocol. Moreover, after executing SANA, the verifier is able to determine the IDs of the untrustworthy devices rather than their mere number. Authentication of device IDs in an end-to-end manner provides more resiliency to physical attacks. Finally, in order to mitigate DoS attacks on the network, SANA requires the verifier to possess a secure token. This token is issued by a trusted third party and is verified by the network devices during the protocol execution. Figure 2 shows comparison between SANA and SEDA in terms of run-time.

Systematic Collective Attestation. We plan to make the effort towards establishing collective attestation on solid ground, by presenting a careful analysis of its requirements, and a systematic identification of its protocol, software, as well as hardware components. In particular, we are working on extracting the properties that are needed for securing collective attestation, deriving necessary features that allow satisfying these properties, and presenting practical implementation that provide these features.

2.2 Detection of Physical Attacks

In the single-prover setting, it is reasonable to assume that physical attacks on the prover are either impossible or very unlikely, especially, if the device is physically protected or unreachable, e.g., located on secure premises. However, in current and emerging scenarios that involve multiple inter-connected devices, e.g., automotive, building, office, and factory automation environments, provers might be heterogeneous and distributed over a large physical area, e.g., a factory floor. Consequently, some provers might be within adversary’s grasp. In this part of the dissertation we devise attestation schemes that fulfill the security requirements in such scenarios by enabling the detection of physical attacks.

DARPA. In this work [4] we aim at detecting software manipulations and physical attacks in embedded networks. To achieve this, we extend collective attestation with an absence detection protocol based on periodic network-wide heartbeats. Assuming that physically attacking a device causes it to be offline for a non-negligible amount of time, devices in a network are able to detect physical attacks on their peers and report it to a central verifier. The proposed absence detection protocol states that each device periodically sends a heartbeat, containing a timestamp, to all other devices in the network. If a device’s heartbeat is not received by its peers at the expected time, it is marked as physically attacked. At attestation time, the list of the devices marked as physically attacked is sent to the verifier along with attestation reports. Figure 3 shows the run-time of DARPA.

DARPA++. We are currently working on a collective attestation protocol for large, unattended and dynamic-topology networks of embedded devices, that is capable of detecting physical attacks. We plan to combine continuous attestation of neighbors and periodic local heartbeats with a key exchange mechanism to detect both software and physical attacks with minimal cost. We further handle dynamic topology using a dedicated roaming protocol, which allows devices to move around and connect to their benign peers.

2.3 Detection of Run-time Attacks

Conventional remote attestation solutions are static, i.e., they provide a proof that the software initially loaded by the prover is unmodified, but cannot detect run-time attacks that exploit code-reuse techniques. In this part of the dissertation we develop efficient and secure collective run-time attestation scheme for autonomous collaborative systems of embedded devices.

Autonomous Attestation. We are currently working on collective run-time attestation for autonomous collaborative systems, that is capable of ensuring integrity of data exchanged between devices against any malicious manipulation. We plan to achieve efficiency by decomposing the underlying embedded software into small interacting software modules, and attest the control-flow of those modules that are relevant for a given data exchange.

3 CONCLUSIONS

Collective attestation is a building block for securing networks of embedded devices. In this dissertation, we have proposed practical and secure collective attestation schemes that allow the detection of remote malware infestation, physical, and run-time attacks on embedded networks. The presented schemes are secure, efficient, scalable, and applicable to a wide range of emerging embedded networks.

REFERENCES

[1] M. Ambrosin et al. SANA: Secure and Scalable Aggregate Network Attestation. In ACM CCS, 2016.
[2] N. Asokan et al. Seda: Scalable embedded device attestation. In ACM CCS, 2015.
[3] K. Eldefrawy et al. SMART: Secure and minimal architecture for (establishing a dynamic) root of trust. In NDSS, 2012.
[4] A. Ibrahim et al. DARPA: Device Attestation Resilient against Physical Attacks. In WSec, 2016.
[5] J. McCune et al. TrustVisor: Efficient TCB reduction and attestation. In IEEE S&P, 2010.