1 SEDA: Scalable Embedded Device Attestation

1.1 Introduction

1.1.1 Overview

We design SEDA, Scalable Em- bedded Device Attestation, which is, to the best of our knowledge, the first attestation scheme for large-scale swarms. SEDA repre- sents the first step in a new line of research on multi-device attesta- tion. Although SEDA adheres to the common assumption – made in most (single-prover) attestation techniques – of ruling out phys- ical attacks on devices, we discuss mitigation techniques for such attacks in Section 9.

1.1.2 Contributions

- First Swarm Attestation Scheme
- Security Model & Analysis
- Two Working Prototypes
- Performance Analysis

1.2 Swarm Attestation

1.2.1 Requirements

- Support the ability to remotely verify integrity of the swarm (S) as a whole.
- Be more efficient than individually attesting each device (D) in S.
- Not require the verifier (VRF) to know the detailed configuration of S.
- Support multiple parallel or overlapping attestation protocol instances.
- Be independent of the underlying integrity measurement mechanism used by devices in S.

1.2.2 Adversary Model

As common in the attestation literature [16, 24, 47, 48] we consider software-only attacks. This means that, although the adversary, denoted as ADV, can manipulate the soft- ware of (i.e., compromise) any device D in S, it cannot physically tamper with any device. However, ADV can eavesdrop on, and ma- nipulate, all messages between devices, as well as between devices and VRF. Furthermore, we rule out denial-of-service (DoS) at- tacks since ADV typically aims to remain stealthy and undetected while falsifying the attestation result for VRF.

1.2.3 Protocol Description

SEDA has two phases: (1) an off-line phase whereby devices are introduced into the swarm, and (2) an on-line phase performing actual attestation. The off-line phase is executed only once and consists of device initialization and device registration. The on-line phase is executed repeatedly for every attestation request from a verifier VRF.

1.2.4 Swarm Attestation

VRF starts attestation of S by sending an attestation request attest (containing a random challenge) to D 1 . VRF can randomly chose any device in S as D 1 or depending on its location or preference. Recall that VRF might be remote, or within direct communication range of one or more swarm devices. Eventually, VRF receives an attestation report from D 1 . VRF outputs a bit b = 1 indicating that attestation of S was successful, or b = 0 otherwise. VRF starts the protocol by sending a nonce N to D 1 . It, in turn, generates a new q and runs attdev with all its neighbors, which recursively run attdev with their neighbors. Note that N prevents replay attacks on communication between VRF and D 1 while the purpose of q is to identify the protocol instance and to build the spanning tree. Even- tually, D 1 receives the accumulated attestation reports of all other devices in S.