Towards Remote Attestation as a Service for IoT

Edlira Dushku
dushku@di.uniroma1.it
Dipartimento di Informatica, Sapienza University of Rome
Rome, Italy

ABSTRACT

The Internet of Things (IoT) systems are increasingly becoming an attractive target for cyber attacks due to the importance of the data that IoT devices collect and the limited capabilities of IoT devices to implement complex security techniques. To improve the security level of IoT devices, one promising security mechanism is remote attestation. Considerable research works have proposed various attestation approaches to attest devices in an efficient way. In this poster, we use cloud computing to push the remote attestation protocol to a further level. We propose to develop a cloud service called Remote Attestation as a Service (RAaS) that is able to securely perform the remote attestation on behalf of a low-end IoT device.

CCS CONCEPTS

• **Computer systems organization** → **IoT systems**; *Remote attestation*; • **Networks** → Security & Privacy; Network reliability.

KEYWORDS

Internet of Things Security, Remote attestation, Cloud service

1 INTRODUCTION

Remote attestation can be seen as a suitable malware detection technique that is able to check remotely the adversarial presence on IoT devices. Remote attestation is a two-party security protocol that allows a trusted party called Verifier to verify the trustworthiness of a remote untrusted party called Prover.

In a typical remote attestation protocol, the Verifier initiates the attestation by sending a challenge to the Prover. Upon the attestation request, the Prover stops the normal operation to perform the attestation immediately. Thus, from the Prover 's perspective, remote attestation is an overhead operation that consumes computational power and battery life. In addition, the complexity of the attestation protocol may cause a long suspension of the usual work of the Prover while performing attestation. These drawbacks can cause intolerable disruptions especially in time-critical infrastructures (e.g., medical facilities, nuclear plants).

In order to run the attestation efficiently for low-end IoT devices, many research works have made different assumptions about the device 's hardware, the adversary capabilities and have proposed various attestation algorithms [2–4]. In this work, we aim to optimize the attestation protocol for low-end devices by following a different approach: we propose to securely offload the attestation computation to the cloud.

2 OUR APPROACH

Nowadays, the data sensed from IoT devices are stored and processed in cloud systems, either directly or through an intermediary device, such as a base station, a smartphone, a fog node. The basic idea of our approach is to extend the existing ability of low-end devices to upload data on cloud by enabling devices to upload also the content of their memory blocks. A cloud service (i.e., RAaS) will be able to get the content of the memory blocks from a low-end device and then run independently the attestation protocol on the cloud.

In our system, we consider three main entities as follows: (1) Prover (Pvr): it is a potentially untrusted low-end IoT device that should be attested, (2) RAaS: it is a cloud-service that will perform the attestation on behalf of the Prv, and (3) Verifier (Vrf): it is an external trusted entity that knows in advance the legitimate state of the Prv. At the attestation time, Vrf sends a challenge to RAaS, and RAaS initiates the interaction with Prv. Prv will offload its memory blocks to RAaS. Once the content of the memory blocks is copied to RAaS, Prv continues the usual work, while RAaS performs the necessary computation to run the attestation. At the end, RAaS sends the attestation result to the Verifier, which can afterwards check whether Prv is compromised or trustworthy.

Secure Memory offload. We consider an adversary that may destroy or relocate itself on other memory blocks to avoid uploading the infected memory part on the cloud service, and consequently remain undetected by the attestation protocol executed on the cloud. In particular, we apply a *data-memory lock* mechanism which prevents other tasks from accessing the memory blocks while the content of the memory is getting copied to the cloud application and prevents the adversary from evading detection.

Communication latency. The problem of communication delays between IoT devices and cloud systems has already been considered in the fog computing paradigm [1]. Fog computing distributes the computation power close to the low-end devices to enable real-time decision making with low latency. In this context, in order to reduce the latency, RAaS can be offered as a service by a fog node.

3 CONCLUSION

This work is an ongoing effort which requires extensive experiments to evaluate the benefits of the proposed approach in terms of reducing attestation operations running on real-devices, saving energy consumption, and reducing the interruption time of the usual work on low-end devices. We believe that this research direction opens up new perspectives in developing lightweight remote attestation protocols for low-end devices that rely on the cloud.

REFERENCES

[1] 2019. Open Fog consortium. https://www.openfogconsortium.org/.
[2] Conti et al. 2018. Distributed Services Attestation in IoT. In *From Database to Cyber Security. Springer, 2018.*
[3] Conti et al. 2019. RADIS: Remote Attestation of Distributed IoT Services. In *Proceedings of the 6th IEEE International Conference on Software Defined Systems (SDS-2019).*
[4] Rodrigo Vieira Steiner and Emil Lupu. 2016. Attestation in Wireless Sensor Networks: A Survey. *ACM Comput. Surv.* (2016).