Remote Attestation based Software Integrity of IoT devices

Submitted by aekwall on Mon, 12/07/2020 - 12:24pm

Title	Remote Attestation based Software Integrity of IoT devices
Publication Type	Conference Paper
Year of Publication	2019
Authors	Sundar, S., Yellai, P., Sanagapati, S. S. S., Pradhan, P. C., Y, S. K. K. R.
Conference Name	2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)
Date Published	dec
Keywords	antivirus, composability, cryptographic operations, cryptographic protocols, cryptography, cyber-physical system security, hashed message authentication code, HMAC, HMAC values, Internet of Things, IoT, IoT devices, message authentication, neural style transfer, Predictive Metrics, pubcrawl, reasonable computational power, Resiliency, Scalability, security issues, software integrity, software trusted platform module, telecommunication security, TPM, Trusted Computing, trusted platform modules, trusted solution
Abstract	Internet of Things is the new paradigm towards which the world is moving today. As these devices proliferate, security issues at these scales become more and more intimidating. Traditional approach like an antivirus does not work well with these devices and there is a need to look for a more trusted solution. For a device with reasonable computational power, we use a software trusted platform module for the cryptographic operations. In this paper, we have developed a model to remotely attest to the integrity of the processes running in the device. We have also explored the various features of the TPM (Trusted Platform Module) to gain insight into its working and also to ascertain those which can make this process better. This model depends on the server and the TPM to behave as roots of trust for this model. The client computes the HMAC (Hashed Message Authentication Code) values and appends a nonce and sends these values periodically to the server via asymmetric encryption. The HMAC values are verified by the server by comparing with its known good values (KGV) and the trustworthiness of the process is determined and accordingly an authorization response is sent.
DOI	10.1109/ANTS47819.2019.9117946
Citation Key	sundar_remote_2019

antivirus composability cryptographic operations Cryptographic Protocols Cryptography cyber-physical system security hashed message authentication code HMAC HMAC values Internet of Things IoT IoT devices message authentication neural style transfer Predictive Metrics pubcrawl reasonable computational power Resiliency Scalability security issues software integrity software trusted platform module

telecommunication security tpm Trusted Computing trusted platform modules trusted solution