International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

LIGHTWEIGHT ATTESTATION, AUTHENTICATION AND RUNTIME SECURITY OF IOT DEVICES

Avani Dave
daveavani@gmail.com

Krunal Dave
krunaldave10@gmail.com

Abstract

With the increase utilization of resource constrained small embedded and IOT devices for applications ranging in automotives, home security, cameras, smart home, smart farming, the security and data protection of this devices has emerged as hot research topic. By design this device do not have on board security primitives such as TPM2.0, SGx, secure boot, PMP etc. These devices often share and process security critical user data and information and security of it become highly important. To this end, this work present lightweight attestation, authentication and run time security mechanism for resource constrained embedded and IOT devices.

Keywords: Secure boot, attestation, authentication, TPM2.0, IOT device security, embedded security

I. INTRODUCTION

Enhancing security of IOT devices is challenging problem in current time, as the number of connected IOT devices will be increased in coming years security of IOT device and communicated data will be biggest challenge. Our research work focusing on providing lightweight attestation, authentication and run time security to resource constrained small IOT devices. For resource reach platform TPM2.0 or trust zone-based TEE or OPTEE implementation is viable option to secure platforms, Trusted computing Group (TCG) has created standards for small resource constrained platform security called DICE., but it is not available as current solution as its under proof of concepts stage. Also Dice and TPM2.0 based implementation can provide boot measurements and root of trust but not runtime security.

II. BACKGROUND AND RELATED WORK

With the advance it industrial 4.0 the utilization of embedded IOT devices has increased significantly with wire range of applications such as security cameras, portable devices, smart farming, vehicular ECUs, sensors for temperatures, different sensors for cars, smart homes, appliances etc. This device often transfers and share security critical user data and information. Thus, security of this device becomes significant important. Furthermore, these devices oftentimes do not have TPM, secure boot, SGX or TEE like security primitives. As embedded and IOT devices are resource constrained the security focused product development gets back stagged. Fig-1 indicates the US IOT security market size and projects the trend till 2025 [1].

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

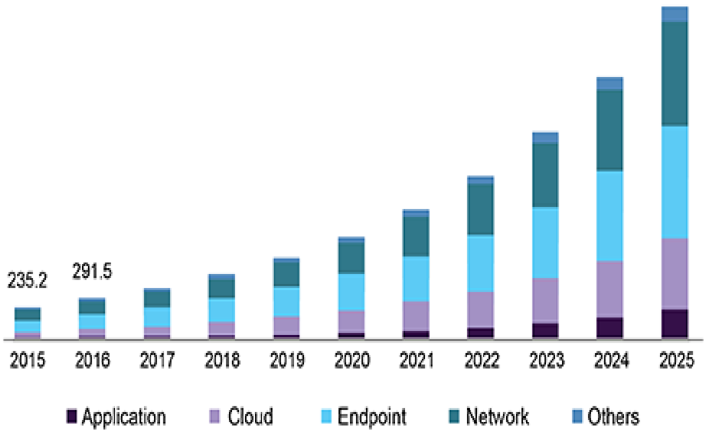

Fig-1 U.S. IoT security market size, by security type, 2015 -2025 (USD Million) [1]

III. PROPOSED TECHNIQUE

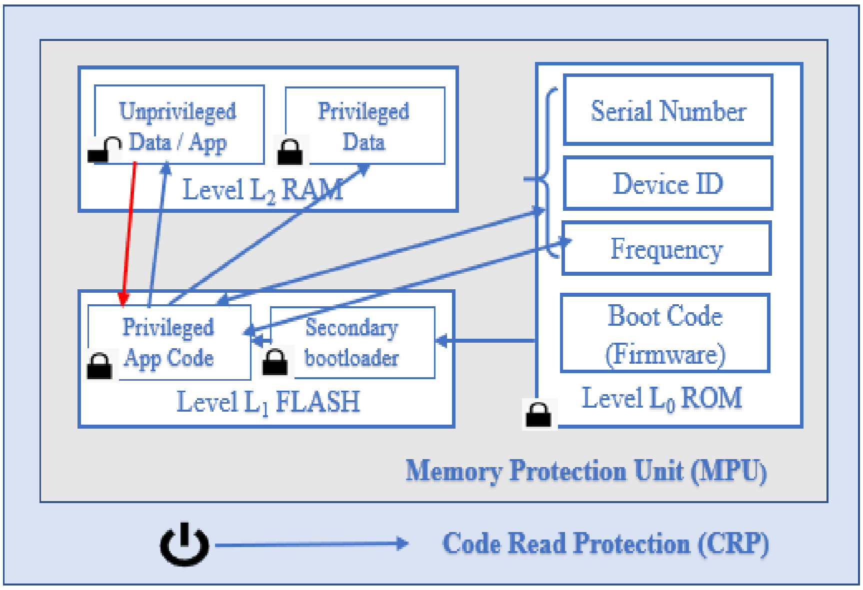

Fig-2 Architecture of IOT Security

Fig -2 shows the high-level architecture of the proposed IOT device attestation and secure boot flow.

Our approach is to secure small IOT devices at platform and during transport on wire using on-chip resources. We have leveraged mbed microcontrollers' Memory protection Unit and Code Read Protection mechanism to achieve our goal, and for on wire security, we have used Single Packet Authentication protocol for securing communication channel from man in the middle, DOS and replay types of attack. Chain of boot code measurements and segmentation of memory is done

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

with MPU, and secondary boot loader and Code Read Protection feature of microcontroller are used to protect memory read from unauthorized user (attacker) access.

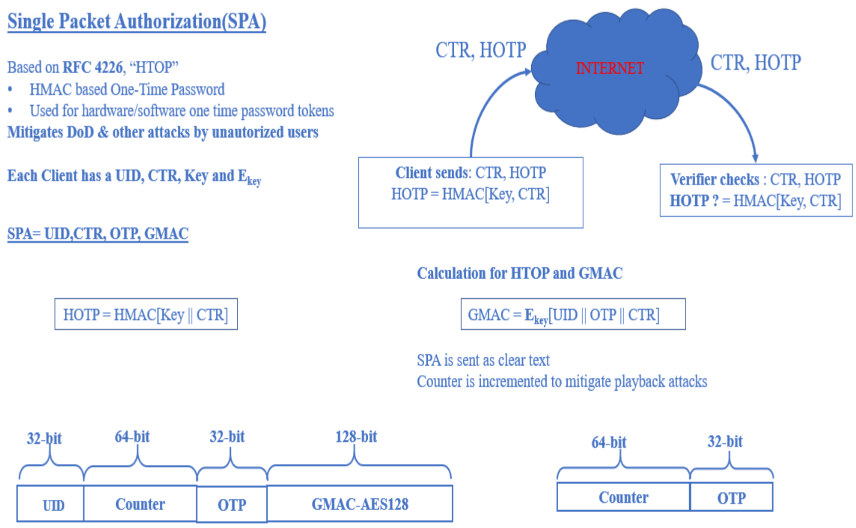

Fig-3Single Packet Authorization (SPA)

Fig 3 depicts the single packet authorization flow for resource constrained small embedded IOT devices. Single packet authorization is used to secure communication channel in which key or secret (seed) is never send on wire so that even wire tapping cannot help attacker to get device credentials. In this method, prover sends first packet with four parameters namely - user ID, counter, One-Time Password (OTP), GMAC-AES256.

In our implementation, we have used three parameters for user ID creation - which is combination of serial number, device ID and operating frequency of the microcontroller. Counter is a random number - first time generated by devices analog entropy and it will be incremented by specific number for every iteration it follows.

OTP will be generated by shared key and counter value hashing at both prover and verifiers end. GMAC-AES256 is calculated at prover side by using pre-shared encryption key and all of other three parameters. For authentication only counter value and HOTP are sending through wire so even if it is tapped hacker cannot get secret key or OPT value and can't access the system. Then after, even if attacker manages to get device access, we have CRP so, that memory regions are read protected from unauthorized users, so they will read NULL.

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

IV. RESULT EVALUATION

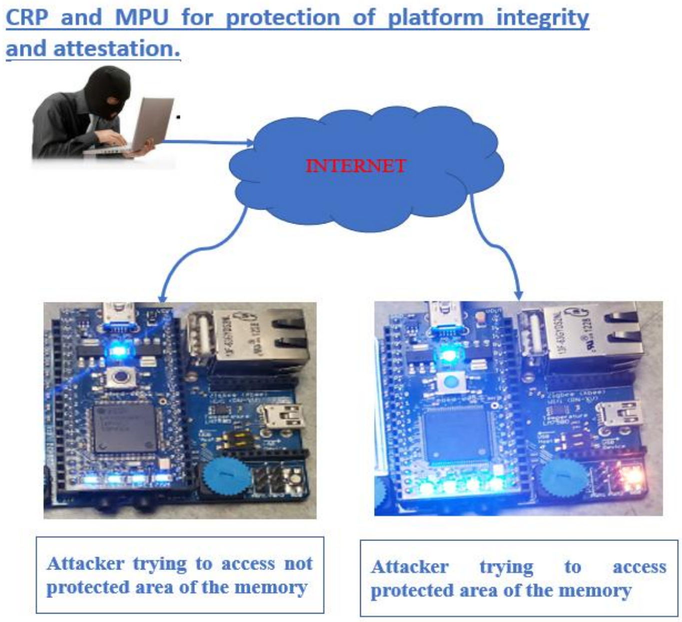

Fig-4. Result of the proposed technique

Fig 4 indicates that when an adversary tries to read the CRP and MPU protected memory region the platform indicates the red LED light and all memory access results in encrypted data.

Security features	State of the Art	Our Solution
Root of Trust measurements	TPM2.0 , trustzone, TEE ,Dice (POC)	By leveraging MPU and Dice like implementation
Boot security	TPM2.0 , Trustzone or Arm v8 ,TEE	Writing secondary boot loader with customized
Platform Identity	UID, UUID	Serial Number, Device ID, Clock frequency combination
Platform Authenticity	Boot level only	Boot level and Run time by
Platform Integrity and read protection	Only boot time	Boot and runtime with CRP
Replay Protection	Generally No	Yes with SPA
Man-in the middle	Generally No	Yes with SPA

Fig-5 Comparison with state-of-the-art techniques

Fig 5 compares the proposed technique with state-of-the-art techniques for different security features analysis such as secure boot, platform integrity, authenticity, attestation, replay protection, men in the middle prevention etc.

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

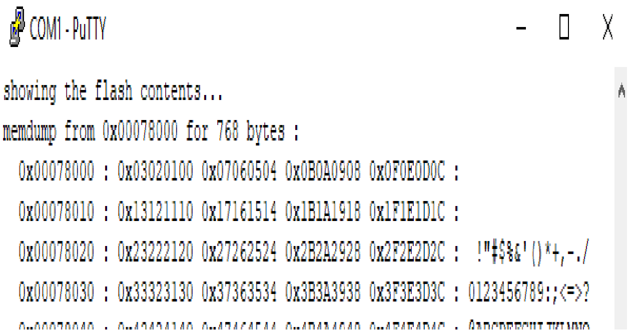

Fig-6 Plain text memory content

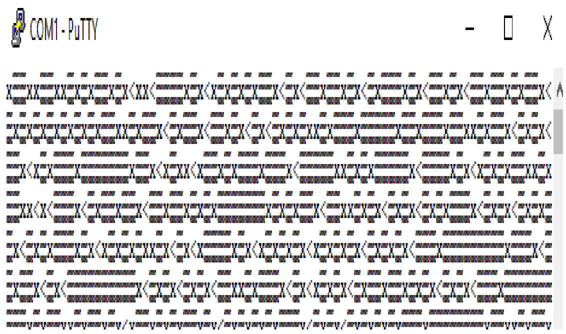

Fig-7 Encrypted text memory content

V. CONCLUSION

This work presents the lightweight runtime and boot time security with attestation prototype for over the shelf IOT devices without requiring TPM2.0 or any resource heavy mechanism. The evaluation results show the memory contents cannot be read by external user when it has memory read protection and encrypted data from the memory will be available. This prevents the memory read attacks.

REFERENCES

1. Internet of Things (IoT) Security Market Analysis Report By Component, By Solution, By Services, By Application, By Security Type (Endpoint, Cloud, Network, Application), And Segment Forecasts, 2018 – 2025https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market
2. Practical Runtime Attestation for Tiny IoT Devices: https://www.ndss-symposium.org/wp-content/uploads/2018/07/diss2018_11_Hristozov_paper.pdf
3. TPM 2.0 https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c
4. Secure boot RISCV architecture for secure boot OpenTitanhttps://opentitan.org/book/doc/security/specs/secure_boot/