doi:10.3233/APC210201

A Session Key Based Security Mechanism for Cyber Physical System

Sandip Thite [a,1] and J. Naveenkumar [a]
[a] *Bharati Vidyapeeth University Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India*

Abstract. In recent years extensive research is going on for the development of applications which convert physical devices into smart devices. Industry 4.0 adopt the technologies under Cyber Physical Systems (CPS) for the development of such types of smart devices. Increase in the use of such type of smart devices without any security mechanism causes an open invitation for cyber attackers to perform cyber-attacks on such devices. Even current security algorithms are not efficiently work due to some constraints of smart devices. The goal of this research paper is to provide effective solution against different cyber-attacks on CPS applications. This paper proposed session key-based security mechanism which is used for the prevention of cyber-attacks and authentication of cyber devices.

Keywords. Security, Cyber Physical System, Replay attack, Internet of things, Session key, Cyber-attacks, man-in-the middle attack

1. Introduction

Cyber Physical system (CPS) is defined as a new generation of electronics system which works with integration of physical system and computational algorithm. It is broadly used in the development and deployment of smart devices.[1] A basic architecture of the CPS represent four different components, which include physical system, computation, communication and information system. Physical system is represented by the basic static system that work manually. A next component of CPS is Computation system. It is used to convert physical system into automated system. To convert into automated system it uses set of instructions into coded form. This code will be executed to perform automated operations of physical device. The next important component of CPS is communication. To establish communication in between devices it uses communication protocols under wireless (IEEE 802.11) and wired (IEEE 802.3) environment. Even now a days for short range devices Zigbee (IEEE 802.15.4) protocols also used. Communicating devices establish ad hoc network in between them. Information exchange for execution of task is also performed by communicating devices.

The use of cyber physical system in different application is increased rapidly but at the same time negligence of security of such type of devices also happened. Due to this it is open invitation for attacker to perform attacks on these devices [2][7]. From last two years if we going through different security reports, we found that cyber-attacks increase significantly on CPS [4].

[1] Sandip Thite,Bharati Vidyapeeth University Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune ,Email: sandipthite83@gmail.com.

The main reason behind that people taking more care of their devices like desktop computer or laptop by installing antiviruses, firewall or they implement current security mechanism in it.

2. Background

Basic Architecture of CPS represent four different components which include Physical system, computation system, communication system and Information system. These four components are used for development of CPS. At the same time these components having some loophole to perform cyber-attacks. These attacks have two parts Physical attack and Cyber-attack. Attacker founds different attack points in CPS which includes Fake devices, Weak protocol of communication, Fake access point, Spoof user interaction and manufacturer infrastructure, weak application programming interfaces etc.

One of the most important parameters for securing CPS infrastructure is device identity and mechanisms for authentication. But many CPS devices do not have the required computation power, memory or storage to support and implement current security algorithm [8]. Today's strong encryption and schemes of authentication are based on cryptographic suites such as Advanced Encryption Suite (AES) for confidentiality, Rivest- Shamir-Adleman (RSA) for digital signatures and key exchange and Diffie-Hellman (DH) for key negotiations and management [3]. While these algorithms are robust. They require high computation resource that may not exist in all CPS based devices. Consequently, authentication and authorization will require systematic study and reengineering to accommodate security needs of new CPS connected networks [9].

Secondly, existing authentication and authorization protocols also require a degree of user intervention in terms of configuration and provisioning [5]. However, many CPS devices will have limited access, thus requiring re-designing of the new techniques and protocols that can support tiny, low memory and low computational power CPS devices. Furthermore, preservation of privacy has been a concern since the dawn of the Internet. Identity management in the CPS is important characteristics required in the security framework [6]. The main aim of this research paper is to present a general and flexible security framework that provides robust security for CPS-based applications in diverse and user-centric environments. We also proposed Session key-based security mechanism which prevent attacker to perform cyber-attacks on the system.

3. Secure CPS Flexible Framework

Figure 1 shows secure CPS flexible framework. Bottom layer of the CPS framework is physical layer which describes hardware used for the development of security mechanism for cyber physical systems. Microcontroller interface includes Raspberry pi or Arduino. Both the interfaces are small in size but capable to handle heavy tasks. These interfaces acts as a Gateway server. While at the client side we can choose communication, interface depends on environment. Where we can use IEEE 802.11, 802.15 or 802.15.4. It is totally depends on wireless environment which we used. Whether it is short range or long range. Depends on physical distance between

Gateway controller and client node we can choose suitable hardware interface like ESP8266, ESP32, XBEES2C or BLE4.0.

Second layer is provides device drivers for hardware interfaces which is used for security mechanism. These device drivers are used to activate all hardware which we used to implement security mechanism in cyber physical system. It also work for power management of all the hardware. Handling of Input/Output devices also done in this layer.

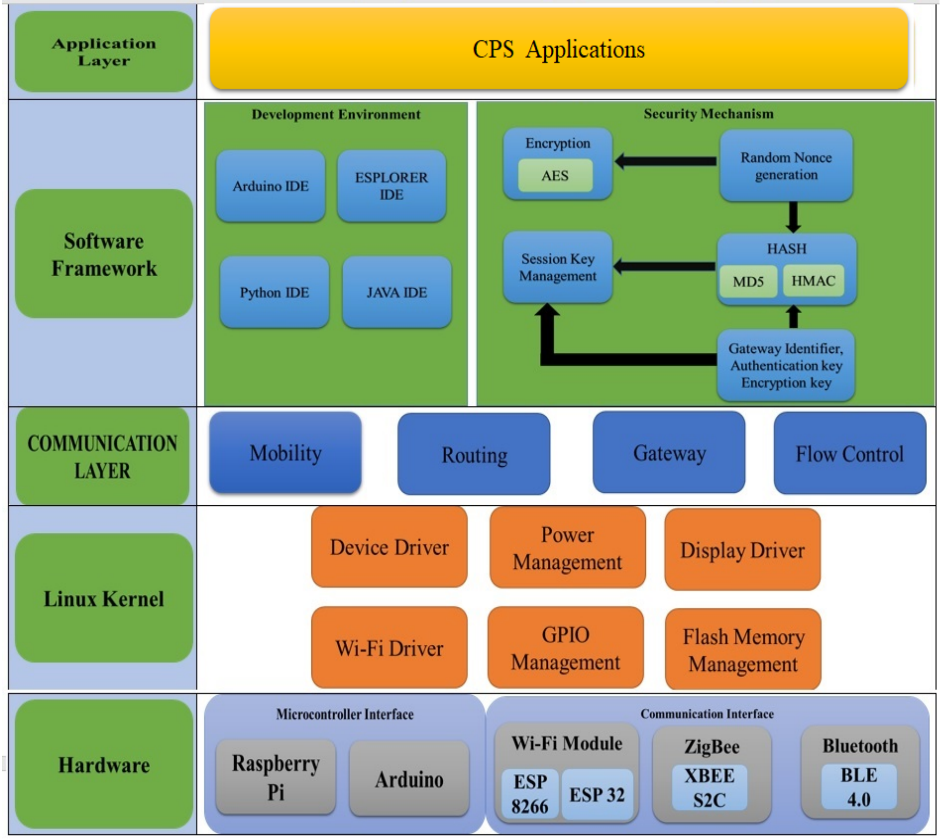

Figure 1. Secure CPS flexible framework.

Communication layer is a bridge in between Application user, application software and hardware. Which works for the mobility of the application. It provides connection establishment between gateway server and client node. It also used to exchange messages in between the nodes for authentication and authorization purpose.

Software framework layer contain two modules. First module works for development environment for security mechanism. It is used for execution of code building procedure. While second module is actually used to code development for security mechanism.

The top most layer is Application layer, which includes applications that we used in cyber physical system. Security mechanism is specially developed in a way that where it support client server environment.

4. A Session key based Security Mechanism

The CPS consists of various small capacity devices which include microcontroller sensors etc. which works under wireless environment.

We proposed a new security mechanism for CPS. It is a session key-based mechanism. It is a lightweight mechanism developed for constraint-based devices which has a issues like low computational power, less energy, less memory etc. Where following mentioned parameters are used for successful execution of mechanism

MK = Microcontroller key
PK1 = Public key for authentication
PK2= Public Key for Encryption
S1, S2 =Random nonce for Session key generation
AT_D= Authentication token at smart device
ST_D= Session token at smart device
AT_M = Authentication token at Microcontroller
ST_M = Session Token at Microcontroller
SK_D = Session key at smart device
SK_M = Session key at Microcontroller

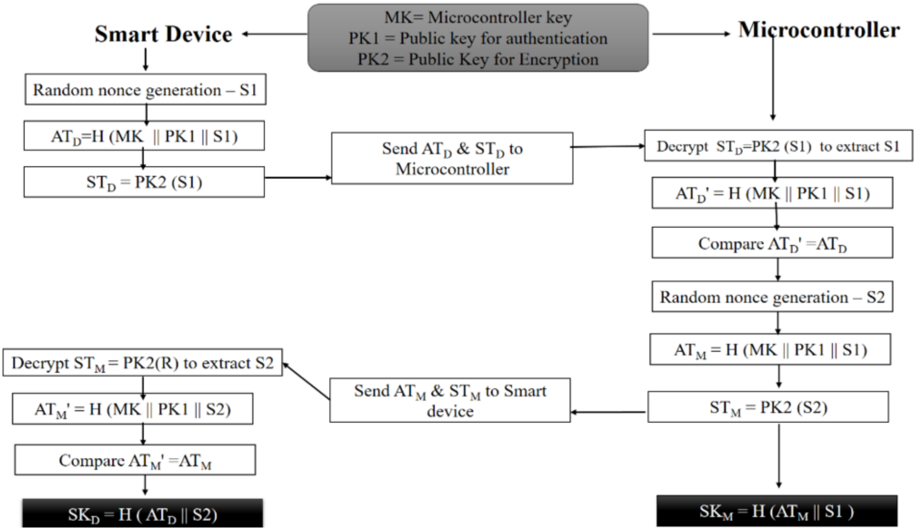
Smart Device
MK= Microcontroller key
PK1 = Public key for authentication
PK2 = Public Key for Encryption
Microcontroller
Random nonce generation – S1
AT_D=H (MK || PK1 || S1)
ST_D = PK2 (S1)
Send AT_D & ST_D to Microcontroller
Decrypt ST_D=PK2 (S1) to extract S1
AT_D' = H (MK || PK1 || S1)
Compare AT_D' =AT_D
Random nonce generation – S2
AT_M = H (MK || PK1 || S1)
ST_M = PK2 (S2)
Send AT_M & ST_M to Smart device
Decrypt ST_M = PK2(R) to extract S2
AT_M' = H (MK || PK1 || S2)
Compare AT_M' =AT_M
SK_D = H (AT_D || S2)
SK_M = H (AT_M || S1)

Figure 2. Session key based Security Mechanism

The figure 2 shows key generation algorithm in between smart device and microcontroller device which controls all smart devices. As shown in figure MK, PK1 and PK2 are common parameters used in between smart device and microcontroller for the implementation of security mechanism for generation of session key.

Stepwise execution of Security mechanism is divided into two parts where part 1 execute at smart device and part 2 execute at microcontroller for the generation of session key.

Step 1: S1 is a random number generated by using random nonce generation function at smart device.

Step 2: Authentication token (AT_D) is generated by implementing Hash function(H) at smart device by using three parameters MK, PK1 and S1.
Step 3: Session token (ST_D) is generated at smart device by using Public key for encryption and random nonce S1.
Step 4: Authentication token (AT_D) and session token (ST_D) sent to microcontroller from smart device through communication channel.
Step 5: At microcontroller random nonce S1 is extracted by decrypting Session token (ST_D) and by using common parameter PK2.
Step 6: Authentication token (AT_D') is regenerate again at microcontroller by implementing hash function on MK, PK1 and S1.
Step 7: Newly generated Authentication token (AT_D') compare with Authentication token (AT_D) sent by smart device. If both are same then execute step 8 else authentication not done with smart device so discard smart device.
Step 8: S2 is a random number generated by using random nonce generation function at Microcontroller.
Step 9: Authentication token (AT_M) is generated by implementing Hash function(H) at microcontroller by using three parameters MK, PK1 and S1.
Step 10: Session token (ST_M) is generated at microcontroller by using Public key (PK2) and random nonce S2.
Step 11: Authentication token (AT_M) and session token (ST_M) sent to Smart device from microcontroller through communication channel.
Step 12: At smart device random nonce S2 is extracted by decrypting Session token (ST_M) and by using common parameter PK1.
Step 13: Authentication token (AT_M') is regenerate again at smart device by implementing hash function on MK, PK1 and S2.
Step 14: Newly generated Authentication token (AT_M') compare with Authentication token (AT_M) sent by Microcontroller. If both are same then execute step 11 else authentication not done with microcontroller so communication will not be established with Microcontroller.
Step 15: Session Key (SK_D) is generated at smart device by implementing Hash function on Authentication token (AT_D) and S2.
Step 16: Session key (ST_M) is generated at microcontroller by implementing Hash function on Authentication token (AT_M) and S1.
Step 17: Session key (ST_D) at smart device and session key (SK_M) at microcontroller authenticate both the devices.

5. Experimental Setup

Experimental setup implemented on home automation system where for microcontroller we used Raspberry Pi Model B 4. Home devices like FAN, Bulb, TV connected with ON / OFF switch where we used Wi-Fi module ESP32 for connectivity with microcontroller. In between microcontroller and smart device, we used Access point (IEEE 802.11) to establish communication in between these devices.

6. Results

A new session key is generated at every communication session in between microcontroller and smart devices. New session key at every session causes difficulty for attacker to capture authentication information. To test the system, we performed Man in the Middle attack on system. To perform this attack we used Ettercap tool. Which is open source and free security tool to perform man-in-the-middle attacks on network. We also developed other unsecure infrastructure of home automation system. After execution of the system, it was found that unsecure system easily breakable under Man In the Middle attack while the secure system developed with Session key based security mechanism not breakable under Man In the Middle attack by using Ettercap.

7. Conclusion

Increase in the use of Cyber physical system with less focus on security causes attacks on such system. So better security mechanism is basic requirement for the development of Cyber physical system. In this paper we proposed Secure Cyber Physical System Framework which shows that we can implement independent security mechanism on CPS. Hardware compatibility issues removed with secure CPS Framework. We also proposed a security mechanism which generate a new session key at every communication session causes difficulty for cyber attacker to get authentication information which will be used to perform attacks on the system.

References

[1] Thite S., Thakore D. (2020) A Survey on the Internet of Things: Applications, Challenges and Opportunities with India Perspective. In: Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, vol 601. Springer, Singapore. https://doi.org/10.1007/978-981-15-1420-3_138

[2] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, thirdquarter 2015, doi: 10.1109/COMST.2015.2388550.

[3] Q. Jawadwala and K. Patil, "Design of a novel lightweight key establishment mechanism for smart home systems," 2016 11th International Conference on Industrial and Information Systems (ICIIS), Roorkee, 2016, pp. 469-473.

[4] Banerjee, A., Venkatasubramanian, K.K., Mukherjee, T., Gupta, S.K.S.: Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems. Proceedings of the IEEE 100(1), 283–299 (2012).

[5] S. Thite, D. Thakore, “Key Establishment Algorithm for Secure Cyber Physical System to Prevent Cyber-attacks ”, International Journal of Innovative Technology and Exploring Engineering Volume-9 Issue-2, December 2019.

[6] Mehmet Hazar Cintuglu , Osama A. Mohammed , Kemal Akkaya , A. Selcuk Uluagac “A Survey on Smart Grid Cyber Physical System Testbeds” in IEEE Communications Surveys & Tutorials, Vol-19, Issue-1, 2017 DOI 10.1109/COMST.2016.2627399

[7] Sandip Thite, J. Naveenkumar. (2021). FASSSTeR: A Novel Framework Aligned with ISA and ISO Standards for Cyber Physical System Safety, Security, Sustainability and Resiliency. Design Engineering, 2021(02), 399 – 411

[8] Y. Chen, S. Kar, and J. M. Moura, “Dynamic attack detection in cyber physical systems with side initial state information,” IEEE Transactions on Automatic Control, vol. 62, no. 9, pp. 4618–4624, 2017.

[9] A. Y. Nur and M. E. Tozal, “Defending cyber-physical systems against dos attacks,” in 2016 IEEE International Conference on Smart Computing (SMARTCOMP), May 2016, pp. 1–3