INFOGAIN PUBLICATION

International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-8, Issue-5; May, 2022
Journal Home Page: https://ijaems.com/
Article DOI: https://dx.doi.org/10.22161/ijaems.85.2

Information Security Technology for IPv6-based IoT (Internet-of-Things)

In-Yeup Kong

Department of Electronics Engineering, Kumoh National Institute of Technology, Republic of Korea
Email: iykong@kumoh.ac.kr

Received: 11 Apr 2022; Received in revised form: 03 May 2022; Accepted: 07 May 2022; Available online: 14 May 2022

Abstract**—***Various security threats may occur in the Internet-of-Things (IoT) environment. In this paper, we look at the threat factors for each layer that can occur in IoT, and especially recent studies related to authentication in the 6LoWPAN environment using IPv6 at the network layer. Based on this, in the future, we plan to configure the authentication protocol in the form of using a session key so that the other party can be verified before communication begins, and the session key is used so that they can trust each other and protect information during communication.*

Keywords**—*IoT security, IPv6 security, IPv6, 6LoWPAN, Authentication.***

I. INTRODUCTION

Although IoT devices and services have provided convenience to humans through smart control, recent incidents such as hacking and DDoS attacks are occurring because their security is weak. Personal information can be hacked through security loopholes, and furthermore, hacked IoT devices can be used for DDoS attacks or crimes.

IoT devices are being designed and manufactured to maintain minimum performance according to the lightweight and low-cost characteristics that try to keep the size and cost to the minimum possible. Therefore, it is necessary to internalize security from the initial design stage because it is often impossible or expensive to update security patches after being manufactured, distributed, or installed.

IoT device security requirements are common to all IoT devices. However, since IoT devices have different resources and processing capabilities, TTAclassifies them into several classes, and defines the security requirements according to this classification as shown in Table 1 [1].

- Class 0 devices: Devices such as ultra-small/ultralight/ultra-power-saving sensors with very high restrictions. Due to limitations in memory and processing power, direct Internet communication cannot be performed in a secure manner.

- Class 1 device has limitations in resources and processing capabilities, so it cannot easily communicate with other Internet devices to which protocol stacks such as HTTP or TLS, which are existing communication protocols, are fully applied. (Example: Medical health devices such as blood glucose meters based on 8/16 bit processors, smart home devices such as thermostats)

- Class 2 device: Basically, it is a device that can support the existing communication protocol stack or has almost no resource restrictions. (Example: IP cameras or smart meters based on 32-bit processors)

- Class 3 device: A device such as a smartphone or tablet with a class 2 or higher capability. Existing protocols are used, but most of the existing protocols can be used without changes or modifications.

In Table.1, SR-C, SR-I, SR-A and SR-AU means security requirement related on confidentiality, integrity, availability, and authentication/authorization, respectively.

Table. 1: Security Requirements by IoT Device Classification

	Security Requirements
Grade 0	2 security requirements applied [SR-C5] Management of identification information [SR-A2] Status information transmission
Grade 1	11 security requirements applied [SR-C1] Transmission message encryption, [SR-C3] Data encryption, [SR-C5] Management of identification information [SR-I1]Data Integrity [SR-A2] Status information transmission, [SR-A7] Software safety [SR-AU1] User authentication, [SR-AU2] Device authentication, [SR-AU3] password management, [SR-AU5] permission control, [SR-AU6]Access Control
Grade 2	Application of 20 security requirements other than the two below [SR-C2] Malware Response [SR-A3] Response to external attacks
Grade 3	All 22 security requirements applied

In this paper, we look at various security threats of IoT devices by layer, and then, with interest in the process of authenticating the communication target in 6LoWPAN communication based on IPv6, we looked at recent papers related to this.

II. IOT SECURITY ISSUES

First, we looked at studies that summarized IoT security issues. Among them, the IoT security issues discussed in [2] are summarized in Table2 so that you can see them at a glance.

Table. 2: IoT security issues

High-level security issues (Application layer)	CoAP security with Internet	It requires adequate key management and authentication mechanisms
	Insecure interfaces	The interfaces are vulnerable to different attacks which may severely affect the data privacy
	Insecure software/firmware	The software/firmware updates need to be carried out in a secure manner
	Middleware security	Different interfaces and environments using middleware need to be incorporated to provide secure communication
Intermediate-level security issues (Network Layer)	Replay or duplication attacks due to fragmentation	- Reconstruction of the packet fragment fields: depletion of resources, buffer overflows and rebooting of the device - Duplicate fragments sent by malicious nodes: hindering the processing of other legitimate packets
	Insecure neighbor discovery	Neighbor discovery packets without proper verification may have severe implications along with denial-of-service.
	Buffer reservation attack	sending incomplete packets results in denial-of-service
	RPL routing attacks	It results in depletion of resources and eavesdropping.
	Sinkhole and Wormhole attacks	These attacks have severe implications including eavesdropping, privacy violation and denial-of-service.
	Sybil attacks on intermediate layers	Sybil nodes using fake identities may result in spamming, disseminating malware or launching phishing attacks
	Authentication and secure communication	Any loophole in security at network layer or large overhead of securing communication may expose the network to a large number of vulnerabilities

	Transport level end-to-end security	It requires comprehensive authentication mechanisms which ensure secure message communication in encrypted form without violating privacy.
	Session establishment and resumption	The session hijacking with forged messages can result in denial-of-service
	Privacy violation on loud based IoT	This violates identity and location privacy may be launched on cloud or delay tolerant network
Low-level security issues (Physical and data link layer)	Jamming adversaries	IoT target deterioration of the networks by emitting radio frequency signals without following a specific protocol
	Insecure initialization	Physical layer ensures a proper functionality of the system without violating privacy and disruption of network services
	Low-level Sybil and spoofing attacks	random forged MAC values for masquerading as a different device while aiming at depletion of network resources
	Insecure physical interface	The poor physical security, software access through physical interfaces, and tools for testing/debugging may be exploited to compromise nodes in the network
	Sleep deprivation attacks	"sleep deprivation" attacks by causing the sensor nodes to stay awake, and it result indepletion of battery

As we have seen, security threats can occur in various ways at various layers, and our interest was in security attacks that can occur in an environment using IPv6 and their solutions. In particular, the idea of authentication to be considered in the IPv6-based network layer was further explored. Therefore in next section, we summarize several authentication methods for 6LoWPAN (IPv6 over WPAN) environments.

III. 6LOWPAN AUTHENTICATION

6LoWPAN provides the connectivity between IPv6 network and resource constrained devices. 6LoWPAN does not support any kind of authentication mechanism, and then any node can join the networks. Therefore, various studies have been conducted to solve this problem, and in this paper, we mainly look at recent papers.

3.1 ASCON [3]

Before looking at recent research, let's take a look at ASCON, which is widely used in various papers.

ASCON is a family of authenticated encryption designs $ASCON_{a,b}^{-k-r}$. The family members are parametrized by the key length $k \leq 128$ bits, the rate r and internal round numbers a and b. Each design specifies an authenticated encryption algorithm $E_{a,b,k,r}$ and a decryption algorithm $D_{a,b,k,r}$.

The inputs for the authenticated encryption procedure $E_{a,b,k,r}$ are the plaintext P, associated data A, a secret key K with k bits and a public message number (nonce) N with k bits. No secret message number is used, i.e., its length is 0 bits. The output of the authenticated encryption procedure is an authenticated ciphertext C of exactly the same length as the plaintext P, and an authentication tag T of size k bits, which authenticates both A and P:

$$E_{a,b,k,r}(K, N, A, P) = (C, T)$$

The decryption and verification procedure $D_{a,b,k,r}$ takes as input the key K, nonce N, associated data A, ciphertext C and tag T, and outputs the plaintext P if the verification of the tag is correct or $\perp$ if the verification of the tag fails:

$$D_{a,b,k,r}(K, N, A, C, T) \in \{P, \perp\}$$

3.2 S6AE [4]

S6AE verifies the legitimacy of SN(Sensor Node)s at the CS(Central Server), and validates the integrity and authenticity of messages exchanged between SNs and the CS in 6LoWPANs. In S6AE, after verifying the authenticity of SNs, CS and SNs establish secret keys using ASCON as the encryption scheme. SHA-256 is used to generate unique output strings by using the S6AE secret parameters, and bit-wise XOR operations are used to reduce the computational and storage costs.

In the performance evaluation, it includes very variable point-of-view analysis including security functionality, computational overhead, communication overhead, energy consumption, storage overhead, and handover phase overhead.

3.3 LAS-6LE [5]

LAS-6LE is divided into two phases, namely, (i) SN deployment phase, and (ii) AKE phase. LAS-6LE employs HF, XOR and ASCON. ASCON is an AE and LWC

mechanism, which ensures the authenticity and confidentiality of plaintext simultaneously.

They express the logical cryptographic operation of the ASCON encryption and decryption algorithm by *(CT, TAG)* = E_{Si} *{AD, PT}*, where S^i is the initialization sate of ASCON, which acts as a shared secret between SN and SR, and *(PT, TAG1)* =$D_S{}^i${AD, CT}. And they evaluate the efficiency of the proposed LAS-6LE in terms of communication cost, compared with other ideas.

3.4 LC-DEX [6]

HIP DEX was standardized to be suitable with low power and resources constrained devices in IEEE 802.15 networks and used as a keying material in the MAC layer. Compared with the previous HIP-based solutions, it proposed an efficient compression header of HIP DEX protocol over 6LoWPAN in a T2T architecture. Evaluation results in terms of transmission delays during the handshake minimize considerably the communication overhead between the communicating peers (the initiator and the responder).

3.5 SLAP [7]

SLAP is a lightweight authentication protocol to enhance the security functionality of M2M communication in Industry 4.0. This minimizes the computational and communication overhead. It generates a shared secret key only after two rounds of communication and without any human intervention. Although SLAP uses only symmetric cryptographic operations, it ensures anonymity and untraceability in the secret key generation process.

It comprises two phases: Initialization phase, and Authentication phase.The initialization phase, the AS (Authentication Server) provides a secret key *PSK* to the controller via a secure channel and the controller securely stores the received *PSK*. Before a sensor is deployed, AS assigns a unique identity *IDs* to it. In authentication phase, the sensor and controller authenticate each other in 3-step handshaking, and share a *SK(session key)*between them for future communication.

The correctness of the proposed SLAP is verified using the BAN logic and using the AVISPA tool.

3.6 CATComp [8]

CATComp is a compression-aware authorization protocol for constrained application protocol (CoAP) and datagram transport layer security (DTLS) that enables IoT devices to exchange small-sized certificates and capability tokens over the IEEE 802.15.4 media. This proposes handshakes at the DTLS and CoAP layers that enable IoT devices to apply compression and decompression at the application and transport layers.And they design various messages that allow a sender device to negotiate a particular compression method with a receiver device while establishing a DTLS session.

IV. CONCLUSION

IoT devices conveniently provide various functions for a smart life, but there are many loopholes in security. In this paper, we looked at the security loopholes of IoT itself and looked at recent research on various authentication protocols in 6LoWPAN using IPv6. According to the result of the analysis of the thesis, it is possible to go through the authentication process for the communication target before starting communication, and to selectively apply an algorithm for data protection during communication. However, since IoT devices have hardware limitations, security design should be applied in consideration of device specifications and future maintenance. As the next study, we intend to design a protocol that is light enough to be used casually in IoT devices of various specifications and has good security effect.

ACKNOWLEDGEMENTS

This study is the result of research conducted by the professor's research year of Kumoh National Institute of Technology.

REFERENCES

[1] Korea Information and Communication Technology Association, “Internet of Things Device Classification and Security Requirements”, 2016

[2] Minhaj Ahmad Khan, Khaled Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018.

[3] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schl¨affer, ASCON V1.2: Submission to the CAESAR Competition, 2016, [online] Available: https://competitions.cr.yp.to/round3/asconv12.pdf.

[4] Muhammad Tanveer,Ghulam Abbas,Ziaul Haq Abbas,Muhammad Waqas,Fazal Muhammad, and Sunghwan Kim, "S6AE: Securing 6LoWPAN Using Authenticated Encryption Scheme", Sensors, vol. 20, no. 9, May 2020.

[5] Muhammad Tanveer, Ghulam Abbas, Ziaul Haq Abbas, "LAS-6LE: A Lightweight Authentication Scheme for 6LoWPAN Environments", Journal of International Conference on Open Source Systems and Technologies (ICOSST), pp. 1-6, Dec. 2020.

[6] Balkis Bettoumi and RidhaBouallegue, "LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop

6LoWPAN Wireless Sensor Networks in HIP-Based Internet of Things", Sensors, pp. 1-36, 2021.

[7] Suryakanta Panda, Samrat Mondal, Neeraj Kumar, "SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0", Computers and Electrical Engineering, vol. 98, pp. 1-13, March 2022.

[8] Mahmud Hossain, Golam Kayas, Yasser Karim, Ragib Hasan, Jamie Payton, S. M. Riazul Islam, "CATComp: A Compression-aware Authorization Protocol for Resource-efficient Communications in IoT Networks", IEEE Internet of Things Journal, vol. 9 Issue: 3, pp. 1667-1682, February 2022.