Received: 24 October 2023 | Revised: 14 November 2023 | Accepted: 1 December 2023 | Published online: 5 December 2023

RESEARCH ARTICLE

Archives of Advanced Engineering Science

yyyy, Vol. XX(XX) 1–7

DOI: 10.47852/bonviewAAES32021937

Forward Secrecy Attack on Privacy Preserving Machine Authenticated Key Agreement for Internet of Things

Batamu Anderson Chiphiko[1], Hyunsung Kim[1,2,*], Patrick Ali[1], and Levis Eneya[1]

1 Mathematical Science Department, University of Malawi, Malawi

2 Department Smart Security, Kyungil University, Republic of Korea

***Corresponding author:** Hyunsung Kim, Department of Smart Security, Kyungil Univesity, Korea. Email: kim@kiu.ac.kr ORCID: 0000-0002-7814-7454

Abstract: Internet of things (IoT) is to connect billions of devices and machines via Internet and to have a smart system. Sensors and devices in IoT environment are connected and communicated together. Connecting such a huge number of devices requires high level of security and privacy. A crucial characteristic of ubiquitous IoT devices is their limited resources. In recent times, a scheme for privacy-preserving machine authenticated key agreement scheme (PPMAKA) has been introduced for the IoT environment. It was argued that PPMAKA provides security and privacy at the same time including forward secrecy. Nevertheless, this paper will demonstrate that PPMAKA lacks forward secrecy, a crucial security and privacy feature in the IoT environment. We use Cannetti and Krawzyck threat model for the detailed analysis of PPMAKA. Furthermore, we provide remarks for the future research as it is recommendable to design any security and privacy schemes over IoT environments with lightweight operation and communication property, authenticated key agreement with forward secrecy, anonymity and unlinkability.

Keywords: Internet of Things, authenticated key agreement, forward secrecy, privacy, security, cryptography

1. Introduction

The substantial expansion of the Internet of things (IoT) enables smart devices to communicate and engage with individuals, devices, and the surrounding environment, facilitating a wide range of tasks (Zhou et al., 2023; Tao et al., 2021; Aryavalli, S. N. G & Kumar, G. H., 2023). IoT has gained huge popularity with potential applications ranging from basic household electronics to large-scale industrial facilities (Tao et al., 2021). Ensuring the privacy and security of users, resources, devices, and data is imperative in the collection and transmission of information (Tao et al., 2021; Tao et al., 2021; Wang et al., 2023; Kim & Kapito, 2021). By focusing on IoT devices, attackers can harvest sensitive personal information from various devices or extract confidential details from device encryption and decryption keys. Since IoT devices have limited resources, traditional security measures cannot be applied in IoT-based networks (Wang et al., 2023). Furthermore, the functionalities of IoT devices pose new challenges to security design, encompassing heightened privacy apprehensions, scalability issues, a preference for services over security, cost-effective architectural considerations, device heterogeneity, resource constraints, and stringent trust management (Kim & Kapito, 2021; Celdran et al., 2023; Strahl & Gounaris, 2023; Ding et al., 2023; Khan & Alghathbar, 2010).

Since the initial authentication scheme in IoT was introduced by Wong et al. (2006), there are various efforts to design authentication scheme for wireless sensor networks (Das, 2009; Chen & Shih, 2010; Wang & Wang, 2014; Das et al., 2012; Li et al., 2018; Fan et al., 2011; Amin et al., 2018; Chang & Le, 2016). Das (2009) discovered security vulnerabilities in Wong et al.'s scheme, including susceptibility to logged-in users attacks, stolen verifier attacks, and other weaknesses. Subsequently, Das (2006) introduced an authentication protocol employing smart card technology (Chen & Shih, 2010). Das's scheme has been identified as susceptible to offline password guessing attacks, insider attacks, and impersonation attacks, as uncovered by certain researchers (Wang & Wang, 2014; Das et al., 2012; Li et al., 2018; Fan et al., 2011). Fan et al. introduced an enhanced scheme designed to address the identified weaknesses in Das's approach, employing one-way hash functions (Fan et al., 2011). Wang and Wang discovered that the scheme proposed by Fan et al. lacks the provision of user anonymity (Wang & Wang, 2014). Amin et al. devised an enhanced scheme by introducing a biometric factor, revealing certain security weaknesses in Chang and Le's scheme (Amin et al., 2018; Chang & Le, 2016). Li et al. highlighted that the scheme proposed by

Jiang et al. (2016) is incapable of detecting unauthorized logins and is not suitable for IoT environments. Subsequently, Li After that, Li et al. (2018) introduced an enhanced scheme featuring a biometric factor and asserted that their approach is resilient against a range of attacks. Nonetheless, Kapito et al., (2021) reveled vulnerabilities in Li et al.'s scheme, including susceptibility to sensor node masquerading attacks, known session-specific temporary information attack and the absence of forward secrecy (Kapito et al., 2021). Kapito et al. (2021) proposed a privacy preserving machine authenticated key agreement scheme (PPMAKA) for IoT environments. They provided Burrows-Abadi-Needham (BAN) logic validation with security and privacy analysis and insisted that their scheme provides IoT device privacy, is secure against IoT device impersonation attack, resists session-specific temporary information attack and resists replay attack and various other attacks.

However, this paper shows an important security flaw that PPMAKA fails to provide forward secrecy. Privacy issue based on the forward secrecy is an important feature in IoT environment especially. Cannetti and Krawzyck threat model is used for the detailed analysis of PPMAKA. Finally, we will provide security and privacy goals in IoT environment for the future cryptographic algorithm design.

The remaining parts of this paper are as follows. Section 3 provides literature review. Section 3 reviews PPMAKA. Section 4 describes the security considerations on PPMAKA. Finally, Section 5 concludes the paper.

2. Literature Review

Following Wong et al.'s introduction of user authentication in IoT, numerous subsequent studies have explored authentication schemes within the realm of IoT (Wong et al., 2006; Das, 2009; Chen & Shih, 2010; Wang & Wang, 2014; Das et al., 2012; Li et al., 2018; Fan et al., 2011; Amin et al., 2018; Chang & Le, 2016). Das (2009) proposed an authentication scheme for wireless sensor networks based on smart care, which is two-factor authentication after providing cryptanalysis on Wong et al. (2006)'s scheme. Some researchers were shown the vulnerability and proposed improvement of Das's scheme, which are prone to sensor node capture, password guessing, gateway bypassing and denial of service attacks (He et al., 2015; Khan & Alghathbar, 2010). Vaidya et al. (2010) introduced an enhanced scheme as a countermeasure to the one proposed by Khan & Alghathbar (2010). This improved scheme offers features such as authenticated key agreement and resilience against various attacks.

Yeh et al. (2011) suggested a two-factor authentication scheme utilizing elliptic curve cryptography (ECC) in wireless sensor networks. They asserted that their scheme offers enhanced security features with greater efficiency in terms of computational overhead. Shi & Gong (2013) showed that Yeh et al. (2011) failed to achieve mutual authentication and support the key agreement and user anonymity in their scheme. Shi & Gong (2013) proposed an improved ECC-based authentication scheme and claimed the efficiency and more functionality than Yeh et al.'s scheme. However, Choi et al. (2014) found the stolen smart card attack and unknown key share attack in Shi & Gong's scheme. They also proposed an enhanced scheme for wireless sensor networks using temporal credentials (Choi et al., 2014). Even if ECC is implementable over IoT environment, it requires a heavy weight operation.

In order to address the lightweight operation requirement over IoT, Li et al. (2018) introduced a three-factor anonymity authentication protocol IoT environments. To adopt biometrics to the scheme, Li et al. (2018) used error correction codes with fuzzy commitment scheme. To be independent from human involvement, Kapito et al. (2021) proposed a privacy preserving machine authenticated key agreement scheme (PPMAKA) with machine authentication factor. PPMAKA has a lightweight scheme and adjusted well to IoT environment. However, it has lack of discipline on the key agreement aspect even if they provided BAN logic validation with various security and privacy analysis on PPMAKA.

Following the examination of authentication schemes in IoT through a literature review, we found that forward secrecy is one of important feature for the security and privacy, which does not provide by many schemes. Thereby, we will examine PPMAKA proposed by Kapito et al. (2021) in detail to emphasize the forward secrecy.

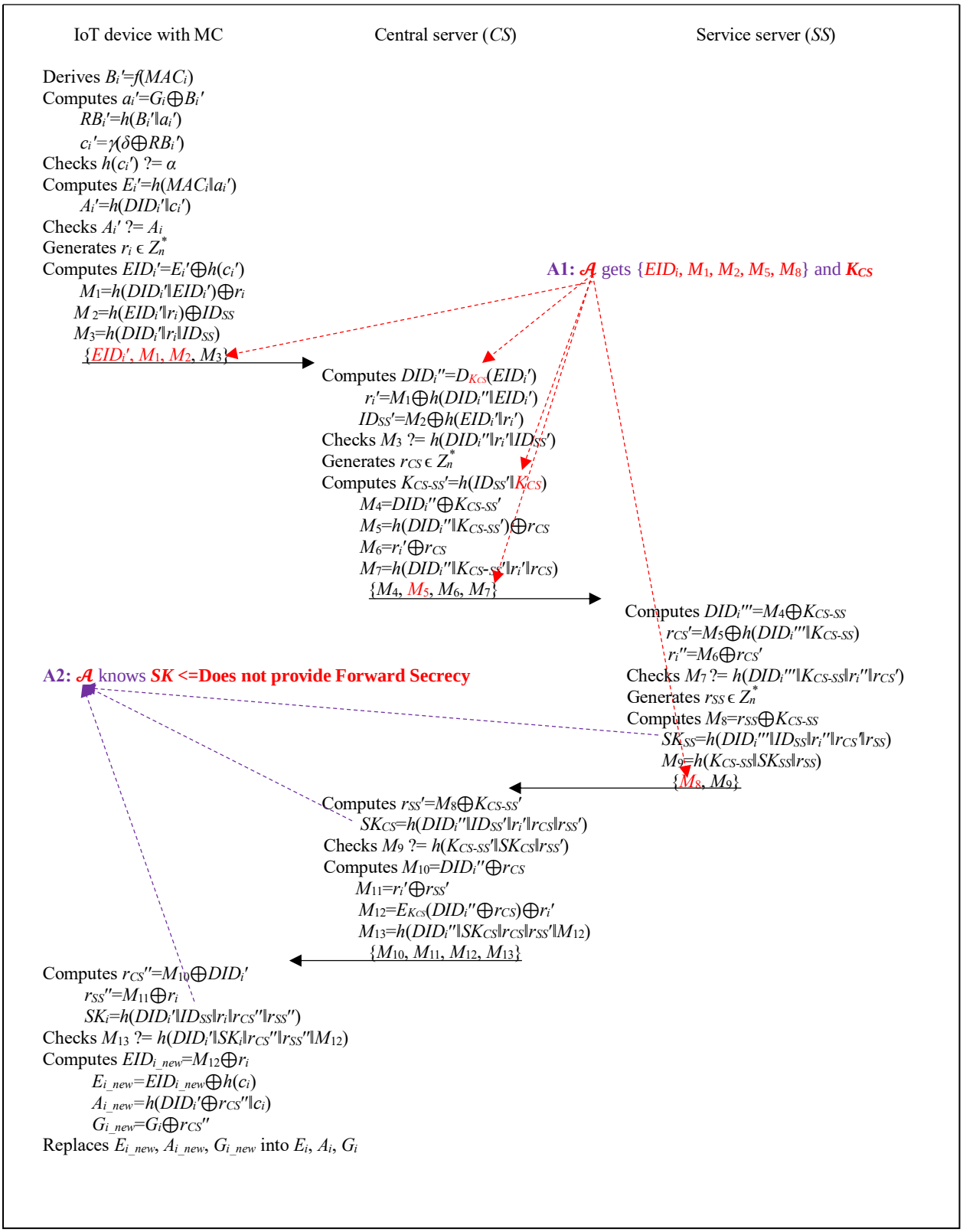
Table 1
Notations

Notation	Definition
ID_{CS}, ID_{SS}	Identities of CS and SS
DID_i	The dynamic identity of the ith IoT device
$h(.)$	An one-way secure hash function
$F(.)$	A fuzzy commitment scheme
$f(.)$	A decoding function for the fuzzy commitment
K_{CS}, K_{SS}	Keys generated by *CS* and *SS*
SK	A session key
$C \subseteq \{0, 1\}^n$	A set of code words of length n
r_i, r_{cs}, r_{ss}	Random numbers generated by IoT device, CS and SS
$\|$	A concatenation operation
$\oplus$	XOR operation
$E(.)$	A symmetric key cryptography encryption function
$D(.)$	A symmetric key cryptography decryption function
G	A generator in Z_P
$\Rightarrow$	A message transmission

3. Review of Privacy Preserving Authenticated Key Agreement

Kapito et al. (2021) proposed a privacy preserving authenticated key agreement scheme (PPAKA) based on machine fingerprinting identification in IoT environments. Their scheme consists of three entities, IoT device, central server (CS) and service server (SS). CS is assumed to be a trusted entity and performs regular communication between IoT device and SS. Before the execution of PPAKA, *CS* performs system initialization as follows; *CS* selects a group Z_p where p is a very large number to be secure enough, and a code set $C \in \{0, 1\}^n$. After that, *CS* generates a long-term

Figure 1
Forward secrecy attack in PPAKA



and random private key $K_{CS} \in Z_n$ and specifies a set of functions, including a hash functions $h(.)$, two fuzzy commitment functions $f(.)$ and $F(.)$ and two asymmetric key functions $E(.)$ and $D(.)$, responsible for encryption and decryption operations, based on the symmetric key cryptosystem. Finally, *CS* publishes **{**Z_n, $h(.)$, $f(.)$, $F(.)$, $E(.)$, $D(.)$} to the target IoT network. PPAKA includes three phases, which are IoT device registration phase, SS registration phase and login and authenticated key agreement phase. Table 1 shows the notations used in this paper.

3.1 Registration phase

PPAKA has two registration phases, IoT device registration and SS registration. For the IoT device registration, an IoT device performs the following steps:

Step 1. IoT device ⇒ *CS*: {DID_i, RB_i} where DID_i is computed as $h(MAC_i \| a_i)$, RB_i is expressed as $h(B_i \| a_i)$ and B_i is represented as $f(MAC_i)$. MAC_i is IoT device's unique radio frequency (RF) signal and a_i represents a randomly generated number.

Step 2. *CS*⇒IoT device: *MC* with {α, δ, A_i, E_i, X, $F(.)$, $f(.)$, $h(.)$}. Here α is defined as $h(c_i)$, δ is expressed as $c_i \oplus RB_i$, A_i is given by $h(DID_i \| c_i)$, E_i is equals $EID_i \oplus h(c_i)$, and EID_i is represented as $E_{Kcs}(DID_i)$. c_i is a random code word ϵ *C*. *CS* keeps DID_i in its database.

Step 3. IoT device with *MC* computes G_i by computing $a_i \oplus B_i$ and stores G_i into *MC*.

To register *SS*, it chooses an identifier ID_{SS} and transmits it to *CS*. *CS* then calculates a confidential master key $K_{CS\text{-}SS}$ as the result of $h(ID_{SS} \| K_{CS})$ for *SS*. Subsequently, *CS* securely communicates {ID_{SS}, $K_{CS\text{-}SS}$} to *SS*.

3.2 Login and authenticated key agreement phase

Login involves accessing the system to avail certain services. The IoT device initiates a service request from *SS* and *CS* authenticates the IoT device's legitimacy before authorizing access to *SS*. This phase works as follows:

Step 1. IoT device⇒*CS*: {EID_i', M_1, M_2, M_3}. Following the input of MAC_i by the IoT device, *MC* performs the calculations B_i' by applying $f(MAC_i)$, a_i' as the result of $G_i \oplus B_i'$, RB_i' as the outcome of $h(B_i' \| a_i'')$ and c_i' as the XOR operation result of δ and RB_i', then validates $h(c_i')$?= α, where ?= signifies the equality check. If they are identical, *MC* proceeds to calculate E_i' by applying $h(MAC_i \| a_i')$ and A_i' as the result of $h(DID_i' \| c_i')$, and verifies whether A_i' ?= A_i. If they are equal, *MC* calculates EID_i' as the computation result of $E_i \oplus h(c_i')$, M_1 as the outcome of XOR operation of $h(DID_i' \| EID_i')$ and r_i, M_2 as XOR computation of $h(EID_i' \| r_i)$ and ID_{SS}, and M_3 by deriving the hash operation $h(DID_i' \| r_i \| ID_{SS})$.

Step 2. *CS*⇒*SS*: {M_4, M_5, M_6, M_7}. *CS* calculates DID_i'' as $D_{Kcs}(EID_i')$, r_i' as the result of $M_1 \oplus h(DID_i'' \| EID_i')$ and ID_{SS}' as the outcome of $M_2 \oplus h(EID_i' \| r_i')$. *CS* then verifies the equality of M_3 with $h(DID_i'' \| r_i' \| ID_{SS}')$. *CS* proceeds to calculate $K_{CS\text{-}SS}'$ as $h(ID_{SS}' \| K_{CS})$ and performs additional computations only if they are equal. In that case, *CS* determines M_4 as XOR operation of DID_i'' and $K_{CS\text{-}SS}'$, M_5 as XOR computation of $h(DID_i'' \| K_{CS\text{-}SS}')$ and r_{cs}, M_6 as XOR operation of r_i' and r_{cs} and M_7 as the result of hash operation $h(DID_i'' \| K_{CS\text{-}SS}' \| r_i' \| r_{cs})$.

Step 3. *SS* ⇒*CS*: {M_8, M_9}. *SS* calculates DID_i''' as the result of XOR operation of M_4 and $K_{CS\text{-}SS}$, r_{cs}' as XOR result of M_5 and $h(DID_i''' \| K_{CS\text{-}SS})$ and r_i'' as applying XOR operation of M_6 and r_{CS}', then verifies the equality of M_7 with $h(DID_i''' \| K_{CS\text{-}SS} \| r_i'' \| r_{CS}')$. If they are equal, *SS* proceeds to compute M_8 by applying XOR operation of $K_{CS\text{-}SS}$ and r_{ss}, SK_{SS} as applying hash operation $h(DID_i''' \| ID_{SS} \| r_i'' \| r_{CS}' \| r_{SS})$ and M_9 as the result of hash function $h(K_{CS\text{-}SS} \| SK_{SS} \| r_{SS})$.

Step 4. *CS*⇒IoT device: {M_{10}, M_{11}, M_{12}, M_{13}}. *CS* calculates r_{ss}' as the result of XOR operation of M_8 and $K_{CS\text{-}SS}'$ and SK_{CS} as the result of hash operation $h(DID_i'' \| ID_{SS}' \| r_i' \| r_{CS} \| r_{SS}')$, then checks the equality of M_9 with $h(K_{CS\text{-}SS}' \| SK_{CS} \| r_{SS}')$. If they are equal, *CS* proceeds to compute M_{10} as the result of XOR operation of DID_i'' and r_{CS}, M_{11} as XOR operation result of r_i' and r_{SS}', M_{12} as the result of XOR computation of $E_{Kcs}(DID_i'' \oplus r_{CS})$ and r_i' and M_{13} as the hash function result of $h(DID_i'' \| SK_{CS} \| r_{CS} \| r_{SS}' \| M_{12})$.

Step 5. The IoT device, in collaboration with *MC*, determines r_{cs}'' as the result of XOR calculation of M_{10} and DID_i', r_{ss}'' as XOR result of M_{11} and r_i and SK_i as the hash function result of $h(DID_i' \| ID_{SS} \| r_i \| r_{CS}'' \| r_{SS}'')$. It then verifies the equality of M_{13} with $h(DID_i' \| SK_i \| r_{CS}'' \| r_{SS}'' \| M_{12})$. Authentication is deemed successful only if they are equal. The IoT device and *SS* subsequently share the same session key *SK*, calculated as $h(DID_i \| ID_{SS} \| r_i \| r_{CS} \| r_{SS})$.

4. Lack of Forward Secrecy

This section provides the lack of forward secrecy in PPAKA as shown in Figure 1. To show the flaw, we first review Cannetti and Krawzyck (CK) threat model (Sarr et al., 2010).

4.1 CK threat model

In an IoT environment, smart devices are connected to the Internet, so they often transmit data through insecure communication channels. Because of this environment feature, when designing any security protocol, we need to

consider how to counter security attacks. The threat model involves categorizing vulnerabilities and targets, followed by establishing preventive measures to enhance the security of a system. In this work, we adopt the CK threat model (Sarr et al., 2010). In this framework, a threat refers to a possible malicious attack initiated by an adversary, capable of causing harm to assets. Under the CK-adversary model, we define the power of an adversary $\mathcal{A}$ as follows:

- $\mathcal{A}$ has complete control over the communication channel for IoT between network entities including inserting, deleting, modifying, intercepting and eavesdropping any messages over the IoT channel.
- $\mathcal{A}$ might also have permission to compromise the CS to acquire long-term keys for the purpose of establishing forward secrecy.
- $\mathcal{A}$ has the capability to extract secret parameters stored in the MC of the IoT device through side-channel attacks in the event of the device being stolen or acquired by $\mathcal{A}$.
- $\mathcal{A}$ could be a valid but malicious IoT device.
- $\mathcal{A}$ can execute various forms of replay attacks, impersonation attacks, and attacks targeting known session-specific temporary information.

In addition to this, we make the following assumptions:

- We presuppose that the security and privacy scheme employed is familiar to the attacker.
- We posit that the cryptographic system should maintain security even when everything about the system, except the session key, is publicly known.

4.2. Lack of forward secrecy

Forward secrecy guarantees the security of established session keys, even in the event of the disclosure of one participant's long-term key (Cerrudo, 2023; Rescorla, 2023; Xue et al., 2013). These security features are becoming increasingly important as information systems become increasingly complex and ensuring that systems remain impervious to breaches and that long-term keys remain confidential is an exceedingly challenging task. This holds especially true for security-sensitive IoT applications, particularly in light of prevalent zero-day attacks (Wang, 2023; Cerrudo, 2023). Indeed, emerging security standards like WiFi protected access (WPA3) and transport layer security (TLS) 1.3 have incorporated forward secrecy as a key feature within their key exchange protocols (Rescorla, 2023; Kastrenakes, 2023).

If $\mathcal{A}$ knows the long-term key K_{CS} in PPAKA, $\mathcal{A}$ has the capability to calculate all session keys between IoT device, *SC* and *SS* as shown in Figure 2. The previously mentioned attack by $\mathcal{A}$ is feasible because of a breach of the "forward secrecy principle" in PPAKA. Following $\mathcal{A}$'s attack, in addition to obtaining the previously agreed-upon session key, $\mathcal{A}$ with K_{CS} can also compute the IoT device identity by computing $DID_i'=D_{K_{CS}}(EID_i)$ with computing overhead of $5T_H+1T_{E/D}$, which is not advisable for preserving user privacy. Since the purpose of PPAKA was to provide privacy in authenticated kay agreement protocol, we observe that with the deficiency of forward secrecy, the intended privacy is not achieved. Furthermore, the lack of forward secrecy renders PPAKA susceptible to known session-specific temporary attacks since in $SK=h(DID_i||ID_{SS}||r_i||r_{cs}||r_{ss})$, DID_i has been exposed.

Figure 2
Attack flow for the forward secrecy in PPAKA

- *$\mathcal{A}$'s capability*:
  (1) Eavesdropping $\{EID_i, M_1, M_2\}$, $\{M_5\}$ and $\{M_8\}$
  (2) Acquiring the long-term secret key K_{CS}.
- *The attack result*: Obtaining all previous session keys. In this attack, we illustrate the session key between IoT device and *SS* as an example.
- *The attack steps of $\mathcal{A}$*:
  Step 1. Computes $DID_i=D_{K_{CS}}(EID_i)$
  Step 2. Computes $r_i'=M_1 \oplus h(DID_i'' \,||\, EID_i')$
  Step 3. Computes $ID_{SS}'=M_2 \oplus h(EID_i' \,||\, r_i')$
  Step 4. Computes $K_{CS\text{-}SS}=h(ID_{SS}||K_{CS})$
  Step 5. Computes $r_{cs}'=M_5 \oplus h(DID_i''' \,||\, K_{CS\text{-}SS})$
  Step 6. Computes $r_{ss}'=M_8 \oplus K_{CS\text{-}SS}'$
  Step 7. Computes $SK=h(DID_i||ID_{SS}||r_i||r_{cs}||r_{ss})$
- *The time overhead of $\mathcal{A}$*: $5T_H+1T_{E/D}$, where T_H represents the time for the hash function, and $T_{E/D}$ denotes the time for encryption and decryption

Figure 1 shows the conceptual flow for $\mathcal{A}$'s attack with two steps, A1 and A2. A1 is the same as $\mathcal{A}$'s capability in Figure 2, which means that $\mathcal{A}$ has the power to get $\{EID_i, M_1, M_2, M_5, M_8\}$ and K_{CS}. A2 is the steps for $\mathcal{A}$ to get *SK*. This means that PPAKA has lack of forward secrecy.

5. Conclusion

This paper has demonstrated that the privacy-preserving machine authenticated key agreement proposed by Kapito et al. (2021) for IoT environments lacks forward secrecy, a critical feature for the scheme. An adversary processing knowledge of the long-term secret key could calculate all session keys, both past and future. We have also shown that privacy of IoT devices is compromised in PPAKA due to the failure to provide forward secrecy. The foremost challenges crucial for the success of IoT are Security and privacy. With the growing technology, attackers learn new means of compromising the system. Therefore, authenticated key agreement schemes for IoT should incorporate protective measures, even in scenarios where the long-term secret key is compromised. Researchers should keep in mind to consider the forward secrecy importantly to devise any security and privacy schemes in IoT environment.

IoT provides users with various benefits and services. A crucial aspect of pervasive IoT devices lies in their limited resources. Therefore, it is crucial to design energy-efficient and lightweight security and privacy-preserving algorithms and schemes that cater to the storage, processing, and transmission of data in accordance with application requirements, employing optimized resource management.

It is recommendable to design any security and privacy schemes over IoT environments with lightweight operation and communication properties, authenticated key agreement with forward secrecy, anonymity, and unlinkability.

Acknowledgement

The findings presented in this paper are a component of Mr. Batamu Anderson Chiphiko's Master degree thesis.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

References

Amin, R., Islam, S. K. H., Kumar, N. & Choo, K. K. R. (2018). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. *Journal of Network and Computer Applications*, 104, 133-144.

Aryavalli, S. N. G. & Kumar, G. H. (2023). Futuristic Vigilance: Empowering Chipko Movement with Cyber-Savvy IoT to Safeguard Forests. *Archives of Advanced Engineering Science*, Online First, https://doi.org/10.47852/bonviewAAES32021480.

Celdran, A. H., Sanchez, P. M. S., Assen, J., Shushack, D., Gomez, A. L. P., Bovet, G., Perez, G. M. & Stiller, B. (2023). Behavioral fingerprinting to detect ransomware in resource-constrained devices. *Computers & Security*, 135, 103510.

Cerrudo, C. (2023). Why the Shellshock Bug Is Worse Than Heartbleed, Retrieved August 18, https://www.technologyreview.com/s/531286/why-the-shellshock-bug-is-worse-than-heartbleed/.

Chang, C. C., & Le, H. D. (2016). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on Wireless Communications*, 15(1), 357-366.

Chen, T. H. & Shih, W. K. (2010). A robust mutual authentication protocol for wireless sensor networks. *ETRI Journal*, 36(1), 316-323.

Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J. & Won, D. (2014). Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 14, 10081-10106.

Das, A. K., Sharma, S., Chatterjee, P. & Sing, J. K. (2012). A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, 35(5), 1646-1656.

Das, M. (2009). Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 8, 1086-1090.

Ding, H., Zhuang, C. & Liu, J. (2023). Extensions of the resource-constrained project scheduling problem. *Automation in Construction*, 153, 104958.

Fan, R., He, D., Pan, X. & Ping, L. (2011). An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks. *Journal of Zhejiang University SCIENCE C*, 12(7), 550-560.

He, D., Kumar, N. & Chilamkurti, N. (2015). A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Science*, 321, 263-277.

Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J. & Yang, Y. (2016). An untraceable temporal-credential-based two factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*, 76, 37-48.

Kapito, B., Nyirenda, M. & Kim, H. (2021). Privacy-Preserving Machine Authenticated Key Agreement for Internet of Things. *International Journal of Computer Networks & Communications*, 13(2), 99-120.

Kastrenakes, J. (2023). Wi-Fi Security Is Starting to Get Its Biggest Upgrade in Over a Decade, Retrieved August 18, https://www.theverge.com/circuitbreaker/2018/6/26/17501594/wpa3-wifi-security-certification.

Khan, M. K. & Alghathbar, K. (2010). Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. *Sensors*, 10(3), 2450-2459.

Kim, H. & Kapito, B. (2021). Security Considerations on Three-Factor Anonymous Authentication Scheme for WSNs. *Journal of Computer and Communications*, 9(3) 1-9.

Li, X., Niu,, J., Kumari, S., Wu, F., Sangaiah, A. K. & Choo, K. K. R. (2018). A three factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments. *Journal of Network and Computer Applications*, 103, 194-204.

Li, X., Niu, J., Bhuiyan, Z. A., Wu, F., Karuppiah, M. & Kumari, S. (2018). A robust ECC based provable secure authentication protocol with privacy protection for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(8), 3599-3609.

Rescorla, E. (2023). The Transport Layer Security (TLS) Protocol Version 1.3, Retrieved August 18, https://datatracker.ietf.org/doc/rfc8446/?include_text=1.

Sarr, A. P., Elbaz-Vincent, P. & Bajard, J.-C. (2010). A new security model for authenticated key agreement. *Cryptology ePrint Archive*, 237, 1-23.

Shi, W. & Gong, P., (2013). A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. *International Journal Distributive Sensor Network*, 12(3), 42-49.

Srinivas, J., Das, A. K., Wazid, M. & Kumar, N. (2020). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 17(6), 1133-1146.

Strahl, W. R. & Gounaris, C. E. (2023). A priority rule for scheduling shared due dates in the resource-constrained project scheduling problem. *Computers & Industrial Engineering*, 183, 109442.

Tao, W., Zhao, L., Wang, G. & Liang, R. (2021). Review of the internet of things communication technologies in smart agriculture and challenges. *Computers and Electronics in Agriculture*, 189, 106352.

Vaidya, B., Makrakis, D. & Mouftah, H. (2010). Improved two-factor user authentication in wireless sensor networks. IN: *Proc. of IEEE 6th Wireless and Mobile Computing, Networking and Communications conference*, 600-606.

Wang, D. & Wang, P. (2014). Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, 20(2), 1-15.

Wang, D., Wang, P. & Wang, C. (2020). Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. *ACM Transactions on Cyber-Physical Systems*, 4(3), 1-26.

Wang, W. (2023). Heartbleed—OpenSSL Zero-Day Bug Leaves Millions of Websites Vulnerable, Retrieved August 18, https://thehackernews.com/2014/04/heartbleed-openssl-zero-day-bug-leaves.html?utm_source=tuicool&utm_medium=referral.

Wang, Z., Huang, J., Miao, K., Lv, X., Chen, Y., Su, B., Liu, L. & Han, M. (2023). Lightweight zero-knowledge authentication scheme for IoT embedded devices. *Computer Networks*, 236, 110021.

Wong, K. H., Zheng, Y., Cao, J. & Wang, S. (2006). A dynamic user authentication scheme for wireless sensor networks. IN: *Proc. of IEEE SUTC 2006*, 1, 8.

Xue, K., Ma, C., Hong, P. & Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, 36(1), 316-323.

Yeh, H., Chen, T., Liu, P., Kim, T.-H. & Wei, H. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 11, 4767–4779.

Zhou, J., Hai, T., Jawawi, D. N. A., Wang, D., Lakshmanna, K., Maddikunta, P. K. R. & Iwendi, M. (2023). A lightweight energy consumption ensemble-based botnet detection model for IoT/6G networks. *Sustainable Energy Technologies and Assessments*, 60, 103454.

How to Cite: Chiphiko, B., Kim, H., Ali, P., & Eneya, L. (2023). Forward Secrecy Attack on Privacy Preserving Machine Authenticated Key Agreement for Internet of Things. Archives of Advanced Engineering Science. https://doi.org/10.47852/AAES32021937