A Note on "a two-factor security authentication scheme for wireless sensor networks in IoT environments"

Zhengjun Cao[1], Lihua Liu[2]

Abstract. We show that the scheme [Neurocomputing, 2022 (500), 741-749] fails to keep anonymity, not as claimed. The scheme neglects the basic requirement for bit-wise XOR, and tries to encrypt data by the operator. The negligence results in some trivial equalities. An adversary can retrieve the user's identity from one captured string via the open channel.
Keywords: Authentication, Anonymity, Key agreement, Gateway node, Sensor node

1 Introduction

Wireless sensor networks have attracted great attention. In 2021, Azrour et al. [1] presented an authentication protocol for remote healthcare systems. Alanazi and Nashwan [2] designed an anonymous three-factor authentication scheme for remote healthcare systems. Dewan et al. [3] discussed the flaws in some authentication schemes in telemedical healthcare systems. Kumar et al. [4] designed a reliable RFID authentication scheme for healthcare systems. Servati and Safkhani [5] proposed an ECC based authentication scheme for healthcare IoT systems.

Recently, Hu et al. [6] have presented a two-factor authentication scheme for wireless sensor networks in IoT environments. In the considered scenario, there are three kinds of entities: users, sensor nodes and a trusted gateway node (GWN). Each user or sensor node registers with GWN, but only once. Besides, a smart card will be issued by GWN to each user.

The scheme is designed to meet many security requirements, including user authentication, session-key establishment, user anonymity and unlinkability, resistance to impersonation attack, reply attack, known session key attack, etc. In this note, we show that the scheme fails to keep user anonymity, not as claimed.

2 Review of the scheme

Let E be an elliptic curve, and P be a base point of the elliptic curve group G_q with the prime order q. Let $h(\cdot)$ be a secure hash function. The GWN picks $K_{GU}, K_{GS} \in Z_q^*$ as its private keys, and computes $P_{pub} = K_{GU}P$ as a public key. The scheme can be depicted as follows (see Table 1).

[1]Department of Mathematics, Shanghai University, Shanghai, 200444, China
[2]Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

Table 1: The Hu-Tang-Xie authentication scheme

User: U_i	Trusted gateway node: GWN	Sensor node: S_j
	Registration	
Choose identity ID_i and password PW_i.		
Pick a nonce r_i to compute	Select the expiration time TE_i.	
$A_i = h(ID_i \| PW_i \| r_i)$.	Compute $P_{pub} = K_{GU} \cdot P$,	
$\xrightarrow[\text{[secure channel]}]{ID_i, A_i}$	$TC_i = h(ID_i \| ID_{GWN} \| K_{GU} \| TE_i)$,	
	$PTC_i = TC_i \oplus A_i$. Store	
	$\{ID_{GWN}, TE_i, P_{pub}, h(\cdot), PTC_i\}$	
Compute $TC_i = PTC_i \oplus A_i$,	into the user's smart card SC.	
$B_i = TC_i \oplus h(ID_i \| PW_i)$.	$\xleftarrow{SC}$	
Store B_i into SC and delete PTC_i.	Select an identity SID_j.	
SC contains $\{ID_{GWN}, B_i, TE_i, P_{pub}, h(\cdot)\}$.	Compute $TC_j = h(K_{GS} \| SID_j)$.	
	$\xrightarrow{TC_j, SID_j}$	Store $\{TC_j, SID_j\}$.
	Login & key agreement	
Input ID_i, PW_i. Pick N_1, x_1. Compute		
$TC_i = B_i \oplus h(ID_i \| PW_i), T_1 = x_1 P$,		
$T_2 = (ID_i \| TE_i \| SID_j \| N_1) \oplus h(x_1 P_{pub})$,	$ID_i \| TE_i \| SID_j \| N_1 = T_2 \oplus h(K_{GU} T_1)$	
$T_3 = h(T_1 \| ID_i \| ID_{GWN} \| TC_i \| N_1 \| TE_i \| SID_j)$.	Check TE_i. If true, compute	
$\xrightarrow[\text{[open channel]}]{M_1 = \{T_1, T_2, T_3\}}$	$TC_i = h(ID_i \| ID_{GWN} \| K_{GU} \| TE_i)$. Check	
	$T_3 = h(T_1 \| ID_i \| ID_{GWN} \| TC_i \| N_1 \| TE_i \| SID_j)$.	
	If so, pick N_2, x, x_2.	$x_2 = T_4 \oplus h(TC_j \| N_2 \| ID_{GWN})$,
	Compute $TC_j = h(K_{GS} \| SID_j)$,	$h(ID_i \| TE_i \| x) = T_5 \oplus h(N_2 \| TC_j)$.
	$T_4 = x_2 \oplus h(TC_j \| N_2 \| ID_{GWN})$,	Check $T_6 = h(T_1 \| h(ID_i \| TE_i \| x) \| x_2 \| N_2)$.
	$T_5 = h(ID_i \| TE_i \| x) \oplus h(N_2 \| TC_j)$,	If so, pick N_3, x_3, compute $T_7 = x_3 P$,
	$T_6 = h(T_1 \| h(ID_i \| TE_i \| x) \| x_2 \| N_2)$.	$SK = h(h(ID_i \| TE_i \| x) \| SID_j \| x_3 T_1 \| T_1 \| T_7)$,
	$\xrightarrow{M_2 = \{T_1, T_4, T_5, T_6, N_2\}}$	$T_8 = h(SK \| N_3)$, $T_{10} = h(TC_j \| T_7 \| N_2 \| T_8)$,
		$T_9 = (T_8 \| T_7 \| N_3) \oplus h(TC_j \| N_2)$.
	$T_8 \| T_7 \| N_3 = T_9 \oplus h(TC_j \| N_2)$.	$\xleftarrow{M_3 = \{T_9, T_{10}\}}$
	Check $T_{10} = h(TC_j \| T_7 \| N_2 \| T_8)$.	
$T_8 \| N_1 \| T_7 \| N_3 \| x = T_{11} \oplus h(N_1 \| TC_i)$,	If so, compute	
$SK = h(h(ID_i \| TE_i \| x) \| SID_j \| x_1 T_7 \| T_1 \| T_7)$.	$T_{11} = (T_8 \| N_1 \| T_7 \| N_3 \| x) \oplus h(N_1 \| TC_i)$.	
Check $T_8 = h(SK \| N_3)$. If so, OK.	$\xleftarrow{M_4 = \{T_{11}\}}$	

3 The loss of anonymity

As we know, a hash function converts any digital data into an output string with a fixed number of characters, Hashing is the one-way act of converting the data (called a message) into the output (called the hash). It is useful to ensure the authenticity of a piece of data and that it has not been tampered with, since even a small change in the message will create an entirely different hash. Hash functions can ensure data integrity. One can identify whether digital data has been tampered with after it's been created. Keyed hash functions can ensure data authenticity. Only the shared key owners can generate and verify the hash values.

The Boolean logic operation XOR, denoted by $\oplus$, is widely used in cryptography which compares two input bits and generates one output bit. When the operator is performed on two strings, they must be of a same bit-length. Otherwise, the shorter string should be stretched by padding some

0s to its left side. In this case, the partial string corresponding to the padding bits is eventually exposed.

In the scheme the transfer of string $ID_i\|TE_i\|SID_j\|N_1$ from U_i to GWN depends on the transformations

$$\begin{aligned}&\text{Encryption: } T_2 = (ID_i\|TE_i\|SID_j\|N_1) \oplus h(x_1 P_{pub}),\\ &\text{Decryption: } ID_i\|TE_i\|SID_j\|N_1 = T_2 \oplus h(K_{GU} T_1),\end{aligned}$$

due to that

$$K_{GU} T_1 = K_{GU} x_1 P = x_1 K_{GU} P = x_1 P_{pub}.$$

In practice, the string $h(x_1 P_{pub})$ is generally of 256 bits (SHA-256). So, we find the effective string length of operand $ID_i\|TE_i\|SID_j\|N_1$ is also of 256 bits. Though the scheme has not specified the bit length of nonce N_1, it is usual to require that $N_1 \in Z_q^*$ where q is a 256-bit prime number [7]. Hence, we have

$$T_2 = (ID_i\|TE_i\|SID_j\| \underbrace{N_1}_{256-\text{bit}})\oplus(00\cdots0\| \underbrace{h(x_1 P_{pub})}_{256-\text{bit}})$$

That means the substring $ID_i\|TE_i\|SID_j$ is almost copied into the string of T_2. Therefore, an adversary can retrieve the user's identity ID_i by capturing T_2 via the open channel.

Likewise, the following transformations

$$\begin{aligned}&\text{Encryption: } T_9 = (T_8\|T_7\|N_3) \oplus h(TC_j\|N_2),\\ &\text{Decryption: } T_8\|T_7\|N_3 = T_9 \oplus h(TC_j\|N_2),\\ &\text{Encryption: } T_{11} = (T_8\|N_1\|T_7\|N_3\|x) \oplus h(N_1\|TC_i),\\ &\text{Decryption: } T_8\|N_1\|T_7\|N_3\|x = T_{11} \oplus h(N_1\|TC_i),\end{aligned}$$

are not secure to transfer the messages

$$T_8\|T_7\|N_3 \quad \text{and} \quad T_8\|N_1\|T_7\|N_3\|x$$

because the blinding strings $h(TC_j\|N_2)$ and $h(N_1\|TC_i)$ are too short to mask the target strings. We want to stress that one needs to use other encryption mechanics (block cipher, stream cipher, etc.) to securely transfer such long target strings.

4 Conclusion

We show that the Hu-Tang-Xie authentication scheme is flawed. It seems difficult to revise the scheme because the underlying encryption is misused. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] M. Azrour, J. Mabrouki, R. Chaganti, New efficient and secured authentication protocol for remote healthcare systems in cloud-IoT, *Secur. Commun. Networks* (2021), 5546334.

[2] M. Alanazi, S. Nashwan, Secure and anonymous three-factor authentication scheme for remote healthcare systems, *Comput. Syst. Sci. Eng.* (2022), 42(2), 703-725.

[3] C. Dewan, T. G. Kumar, S. Gupta, A comparative analysis on remote user authentication schemes in telemedical healthcare systems, *Int. J. Syst. Eng.* (2022), 12(2).

[4] A. Kumar, K. Singh, M. Shariq, C. Lal, M. Conti, R. Amin, S. A. Chaudhry, An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems, *Comput. Commun.* (2023), 205, 147-157.

[5] M. R. Servati, M. Safkhani, ECCbAS: an ECC based authentication scheme for healthcare IoT systems, *Pervasive Mob. Comput.* (2023), 90, 101753.

[6] B. Hu, W. Tang, Q. Xie, A two-factor security authentication scheme for wireless sensor networks in IoT environments, *Neurocomputing* (2022) 500, 741-749.

[7] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, New York, USA (2006)