Cryptanalysis of A Dynamic Password Based User Authentication Scheme for HWSNs

Chun-Ta Li*, Chin-Wen Lee, Yi-Rui Zhu, Jian-Jhong Jheng and Xiao-Qian Zhang

Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.)
*Corresponding author: th0040@mail.tut.edu.tw

Abstract. Recently, Das, Sharma, Chatterjee and Sing proposed a dynamic password-based user authentication scheme for hierarchical wireless sensor networks (HWSNs). Authors claimed that their authentication scheme can achieve better security and efficiency as compared to those for other related password-based authentication methods. However, in this paper, we found their scheme is insecure and any dishonest cluster head in HWSNs can easily reveal the base station's secret key by adopting power analysis attack.

Keywords: Cryptanalysis, Hierarchical wireless sensor networks, Network security, Power analysis attack, User authentication.

1 Introduction

Hierarchical wireless sensor networks (HWSNs) composing of a large number of sensors can be quickly deployed in a target environment, such as forest monitor, ocean observation, and military battlefield. There are three kinds of participants, namely: base station (*BS*), cluster heads (*CH*) and sensor nodes. In general, sensor nodes have limited computation and communication capabilities and they are randomly deployed in their corresponding cluster heads. The basic function of a cluster head is to gather sense data for authorized users and it is more resource rich than normal sensor nodes.

To prevent abusively, login users and sensor nodes should be authenticated by the base station. On the other hand, malicious intruders may launch various security attacks or insert compromised sensor nodes into networks for damaging the security of HWSNs. Therefore, mutual authentication among the user, the base station and the sensor node in HWSNs is an important research issue and it prevents unauthorized participants from accessing services provided by HWSNs.

In 2009, Das first proposed an efficient two-factor user authentication scheme [4] based on easy-to-remember passwords and smart cards in HWSNs. However, Khan and Alghathbar showed that Das's scheme is insecure and presented several improvements. Moreover, Das's scheme has attracted a lot of attention and several two-factor based schemes with mutual authentication and key agreement have been proposed in Chen and Shih (2010) [2], He et al. (2010) [5], Li et al. (2011) [6] and Das et al. (2012) [3].

In this paper, we analyze the security weaknesses of one most recent dynamic password-based user authentication scheme with smart cards for HWSNs proposed by Das et al. [3]. Das et al. claimed that their authentication scheme is secure against various known attacks with dynamic nodes addition and is suitable for some practical scenarios. However, we find that Das et al.'s scheme still has other security weaknesses such as disclosing of the base station's secret key.

2 Review of Das et al.'s Authentication Scheme

Das et al.'s password-based user authentication scheme contains five phases, pre-deployment, registration, login, authentication and password change. Their scheme consists of one base station (BS), sensor nodes (S_i), cluster head in the *j*-th cluster (CH_j) and users (U_i). To shorten the length of this paper, in this section, we only introduce pre-deployment and registration phases of Das et al.'s authentication scheme. We omit the detailed reviews of login, authentication and password change phases. Please refer to [3].

2.1 Pre-deployment Phase

Before deployment of sensor nodes and cluster heads, BS assigns ID_{CH_j} for each cluster head CH_j and ID_{S_i} for each sensor node S_i. Then, BS assigns a unique master key MK_{CH_j} for each CH_j and it is kept secret between BS and CH_j. Moreover, BS assigns a master key MK_{S_i} for each S_i and it is kept secret between BS and S_i.

2.2 Registration Phase

In this phase, a login user U_i computes $RPW_i = h(y \| PW_i)$ and sends his/her identity ID_i and RPW_i to BS through a secure channel, where $h(.)$ is a secure one-way hashing function, y is a random number and PW_i is the password of U_i. Then, BS computes $f_i = h(ID_i \| X_s)$, $x_i = h(RPW_i \| X_A)$, $r_i = h(y \| x)$ and $e_i = f_i \oplus x$, where X_s is a secret key maintained by BS and X_A is shared between BS and U_i. In addition, BS computes m key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m\}$ for m

deployed cluster heads, where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s)$. For replacing some compromised cluster heads after the initial deployment in the networks, BS computes another m' key-plus-id combinations $\{(K_{m+j}, ID_{CH_{m+j}}) | 1 \le j \le m'\}$ for dynamic node addition, where $K_{m+j} = E_{MK_{CH_{m+j}}}(ID_i \| ID_{CH_{m+j}} \| X_s)$. Finally, BS stores $\{ID_i, y, X_A, r_i, e_i, h(.)\}$ and $m+m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m+m'\}$ into U_i's smart card and issues it to U_i through a secure channel.

3 Cryptanalysis of Das et al.'s Authentication Scheme

Das et al.'s authentication scheme could be better convinced after resolving the following security vulnerability. In this section, we describe the details of this security weakness in the following.

In Das et al.'s authentication scheme, any dishonest cluster head CH_j can derive BS's secret key X_s and use it to reproduce many accounts for multiple non-registered users by performing the following two steps:

Step 1: We assume that a legal user U_i's smart card is stolen by CH_j and the $m+m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m+m'\}$ which are stored in U_i's smart card can be extracted by launching power analysis attack [7], where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s)$, MK_{CH_j} is a unique master key for each CH_j, $E_{MK_{CH_j}}(M)$ is encryption of data M using key MK_{CH_j} based on advanced encryption standard (AES) [1], ID_i is the identity of U_i, ID_{CH_j} is the identity of CH_j and X_s is a secret key maintained by BS.

Step 2: By using CH_j's master key MK_{CH_j}, CH_j can easily reveal $(ID_i \| ID_{CH_j} \| X_s)$ by computing $D_{MK_{CH_j}}(E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s))$. As a result, the system secret key X_s is successfully derived by a compromised cluster head CH_j and Das et al.'s authentication scheme still has serious deficiency.

4 Conclusion

In this paper, we found that Das et al.'s authentication scheme is insecure. By adopting power analysis attack, $m + m'$ key-plus-id combinations which are stored in user's smart card can be extracted. Then, their scheme may suffer from secret key disclosure attack and any dishonest cluster head who possesses the master key MK_{CH_j} can easily obtain the base station's secret key X_s. In future work, we plan to propose an improved version of Das et al.'s authentication scheme and we also encourage readers can propose their improvement to remedy security problem of Das et al.'s authentication scheme.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 101-2221-E-165-002.

References

1. National Institute of Standards and Technology: US department of commerce, advanced encryption standard. US Federal Information Processing Standard Publication, 2001.
2. Chen, T.H., Shih, W.K.: A robust mutual authentication protocol for wireless sensor networks. ETRI Journal 32, 704--712 (2010)
3. Das, A.K., Sharma, P., Chatterjee, S., Sing, J.K.: A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Journal of Network and Computer Applications 35, 1646--1656 (2012)
4. Das, M.L.: Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications 8, 1086--1090 (2009)
5. He, D., Gao, Y., Chan, S., Chen, C., Bu, J.: An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Sensor Wireless Network 10, 361--371 (2010)
6. Li, C.T., Lee, C.C., Wang, L.J., Liu, C.J.: A secure billing service with two-factor user authentication in wireless sensor networks. International Journal of Innovative Computing, Information and Control 7, 4821--4831 (2011)
7. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attack. IEEE Transactions on Computers 51, 541--552 (2002)