Security Enhancement to a Group Key Transfer Protocol Against Insider Attack

Juan Huang, Yajun Li, Yining Liu

School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin, 541004 China

Summary
Group key transfer protocol distributes a session key to authorized members with a trusted key generation center. Nam et al. claim that they achieve security, efficiency and correctness based on Shamir's secret sharing, which is the improved version of Harn-Lin's protocol. Our main contribution is to show the security flaws of Nam-protocol and Harn-Lin's protocol that malicious authorized group member can compromise other member's long-term secret. An improved protocol against insider attack and outsider attack is proposed which is secure and efficient.

Key words:
group transfer protocol, session key, insider attack

1. Introduction

In order to ensure the message confidentiality and authentication in a communication group, one-time session key need to be shared among communicating parties. Key establishment is a fundamental cryptographic protocol to build a secure channel over public networks, which are often classified into two types: key agreement protocols and key transfer protocols. In key agreement protocol, all communication entities are involved to the generation of session key, while key transfer protocols rely on a trusted key generation center (KGC) to select session key and transfer it to all authorized members.

In 2011, Nam, et al. [1] proposed a session key transfer protocol which is the improved version of Harn-Lin's protocol [2]. Nam, et al. claimed that their protocol achieves implicit key authentication, efficiency and correctness contrasting with Harn-Lin's protocol. But, we found it is really not true. In fact, neither Nam-protocol nor Harn-Lin's protocol can resist against the insider attack, i.e., the target member's long-term secret shared with KGC can be easily compromised by insider adversary. In this article, we analyze their security weakness and show how to address it.

2. Review of Nam-protocol and the security analysis

2.1 Review of Harn-Lin protocol

Harn-Lin group key transfer protocol consists of pre-distribution phase and key distribution phase. In the former phase, KGC chooses secure prime p, q, publishes $n = pq$. Each user U_i shares a long-term secret (x_i, y_i) $(x_i, y_i \in Z_n^*)$ with KGC in a secure manner.

Key distribution phase is in broadcast channel, all computations are performed modulo n, the steps are as follows:

1. Initiator sends a key distribution request to KGC with the list of $\{U_1, \cdots, U_t\}$;
2. KGC responses with broadcasting $\{U_1, \cdots, U_t\}$;
3. U_i $(1 \le i \le t)$ broadcasts a random challenge $R_i \in Z_n^*$;
4. KGC randomly selects session key k and generates an interpolation polynomial $f(x)$ passing through $(0, k)$, $(x_1, y_1 + R_1)$, $\cdots, (x_t, y_t + R_t)$. KGC computes t additional points $P_i = f(i)$, $(1 \le i \le t)$, and $\beta = h(k, U_1, \cdots, U_t, R_1, \cdots, R_t, P_1, \cdots, P_t)$, where h is a secure hash function. KGC broadcasts $\{\beta, P_1, \cdots, P_t\}$;
5. U_i reconstructs $f(x)$ with his $(x_i, y_i + R_i)$ and public point $P_1, \cdots, P_t$. Then U_i recovers $k = f(0)$, authenticates k with β.

2.1 2.2 Review of Nam-protocol

Nam-protocol is the improved version to achieve

Manuscript received November 5, 2012
Manuscript revised November 20, 2012

implicit authentication, efficient, and correctness. First, composite number n is replaced with a prime p to assure the existence of interpolation polynomial $f(x)$. Secondly, the challenge R_i of U_i is abolished to shorten the length of broadcast message. Thirdly, a fresh random r_0 is simultaneously broadcasted when KGC responses the request of initiator to resist the replay attack. Nam-protocol can also be classified to the pre-distribution phase and key distribution phase.

Pre-distribution. KGC chooses and publishes a random prime p, KGC shares a secret (x_i, y_i), $(x_i, y_i \in Z_p^*)$ with each user U_i in a secure manner.

Key distribution. KGC randomly selects a session key and distributes it upon receiving a request from any user. All communications in this phase are in broadcast channel. The detailed steps are as follows:

1. Initiator sends a key distribution request to KGC with the list of $\{U_1, \cdots, U_t\}$;
2. KGC responses with broadcasting r_0, and $\{U_1, \cdots, U_t\}$ where $r_0 \in Z_p^*$ is randomly chosen;
3. U_i $(1 \le i \le t)$ computes $\alpha_i = h(x_i, y_i, r_0, U_1, \cdots, U_t)$ and sends $\{U_i, \alpha_i\}$ to KGC;
4. If α_i is authenticated, KGC randomly selects session key k and generates an interpolation polynomial $f(x)$ passing through $(0, k)$, $(x_1, y_1 r_0)$, $\cdots, (x_t, y_t r_0)$. KGC computes t additional points $P_i = f(i)$, $(1 \le i \le t)$, and $\beta = h(k, U_1, \cdots, U_t, r_0, P_1, \cdots, P_t)$, where h is a secure hash function. KGC broadcasts $\{\beta, P_1, \cdots, P_t\}$
5. U_i reconstructs $f(x)$ with his $(x_i, y_i r_0)$ and public point $P_1, \cdots, P_t$. Then U_i recovers $k = f(0)$, authenticates k with β.

2.3 The security analysis of Nam-protocol

Nam et al. claim their protocol is secure, efficient and correct. In fact, the long-term secret (x_i, y_i) between KGC and U_i can be compromised by inside adversary, i.e., Nam-protocol fails to achieve the security requirement. We prove this by giving an attack to show how inside adversary to obtain the target member's long-term secret. We denote inside adversary by U_A, the target member by U_T, the corresponding long-term secret by (x_A, y_A) and (x_T, y_T). All computations are performed over Z_p. The attack proceeds as follows:

1. U_A sends key distribution request along with the list $\{U_A, U_T\}$ three times $(i = 1,2,3)$;
2. Each time, KGC selects a random $r_{0,i} \in Z_p^*$, and broadcasts $\{r_{0,i}, U_A, U_T\}$;
3. U_T computes $\alpha_{T,i} = h(x_T, y_T, r_{0,i}, U_A, U_T)$, broadcasts $\{U_T, \alpha_{T,i}\}$; U_A computes $\alpha_{A,i} = h(x_A, y_A, r_{0,i}, U_A, U_T)$ and broadcasts $\{U_A, \alpha_{A,i}\}$;
4. If $\alpha_{T,i}$ and $\alpha_{A,i}$ are all authenticated, KGC constructs $f_i(x) = c_{i,2}x^2 + c_{i,1}x + k_i$ passing through $(0, k_i)$, $(x_A, y_A r_{0,i})$, $(x_T, y_T r_{0,i})$, and computes $P_{1,i} = f_i(1)$, $P_{2,i} = f_i(2)$, $\beta_i = h(k_i, U_A, U_T, r_{0,i}, P_{1,i}, P_{2,i})$, then broadcasts $\{\beta_i, P_{1,i}, P_{2,i}\}$;
5. U_A recovers $f_i(x)$ with his $(x_A, y_A r_{0,i})$ and public points $P_{1,i}, P_{2,i}$;
6. Obviously, $f_i(x)$ also passes through $(x_T, y_T r_{0,i})$, U_A obtains three equations $\begin{cases} c_{1,2}x_T^2 + c_{1,1}x_T + k_1 = y_T r_{0,1} \\ c_{2,2}x_T^2 + c_{2,1}x_T + k_2 = y_T r_{0,2} \\ c_{3,2}x_T^2 + c_{3,1}x_T + k_3 = y_T r_{0,3} \end{cases}$, which can be translated to $\begin{cases} (c_{1,2}/r_{0,1})x_T^2 + (c_{1,1}/r_{0,1})x_T - y_T = -k_1/r_{0,1} \\ (c_{2,2}/r_{0,2})x_T^2 + (c_{2,1}/r_{0,2})x_T - y_T = -k_2/r_{0,2} \\ (c_{3,2}/r_{0,3})x_T^2 + (c_{3,1}/r_{0,3})x_T - y_T = -k_3/r_{0,3} \end{cases}$, where x_T^2, x_T and y_T are indeterminate, others are known by U_A.

Assuming $x_T^2 = u_2$, $x_T = u_1$, $-y_T = u_0$, U_A obtains $u_2 = \frac{A_2}{A}$, $u_1 = \frac{A_1}{A}$, and $u_0 = \frac{A_0}{A}$ if $A \neq 0$, where $A = \begin{vmatrix} c_{1,2}/r_{0,1} & c_{1,1}/r_{0,1} & 1 \\ c_{2,2}/r_{0,2} & c_{2,1}/r_{0,2} & 1 \\ c_{3,2}/r_{0,3} & c_{3,1}/r_{0,3} & 1 \end{vmatrix}$,

$A_2 = \begin{vmatrix} -k_1/r_{0,1} & c_{1,1}/r_{0,1} & 1 \\ -k_2/r_{0,2} & c_{2,1}/r_{0,2} & 1 \\ -k_3/r_{0,3} & c_{3,1}/r_{0,3} & 1 \end{vmatrix}$,

$A_1 = \begin{vmatrix} c_{1,2}/r_{0,1} & -k_1/r_{0,1} & 1 \\ c_{2,2}/r_{0,2} & -k_2/r_{0,2} & 1 \\ c_{3,2}/r_{0,3} & -k_3/r_{0,3} & 1 \end{vmatrix}$, and

$A_0 = \begin{vmatrix} c_{1,2}/r_{0,1} & c_{1,1}/r_{0,1} & -k_1/r_{0,1} \\ c_{2,2}/r_{0,2} & c_{2,1}/r_{0,2} & -k_2/r_{0,2} \\ c_{3,2}/r_{0,3} & c_{3,1}/r_{0,3} & -k_3/r_{0,3} \end{vmatrix}$.

So the long-term secret (x_T, y_T) between U_T and KGC can be easily compromised by malicious authorized member.

Remark: If $A = 0$, U_A initiates a request of key establishment again to get another series of equation until $A \neq 0$.

2.4 Security Analysis of Harn-Lin protocol

With the above method, Harn-Lin's group key transfer protocol is also vulnerable against insider attack, the attack proceeds as follows:

1. U_A sends key distribution request along with the list $\{U_A, U_T\}$ three times $(i = 1,2,3)$; KGC responses with $\{U_A, U_T\}$;
2. Each time $(i = 1,2,3)$, U_A broadcasts a random challenge $R_{A,i}$, and U_T broadcasts a random challenge $R_{T,i}$;
3. KGC selects k_i and generates an interpolation polynomial $f_i(x) = c_{i,2}x^2 + c_{i,1}x + k_i$ passing through $(0, k_i)$, $(x_A, y_A + R_{A,i})$, $(x_T, y_T + R_{T,i})$. KGC computes $P_{1,i} = f_i(1)$, $P_{2,i} = f_i(2)$, and $\beta = h(k_i, U_{A,i}, U_{T,i}, R_{A,i}, R_{T,i}, P_{1,i}, P_{T,i})$, and broadcasts $\{\beta, P_{1,i}, P_{2,i}\}$;
4. U_A reconstructs $f_i(x)$, and obtains $\begin{cases} c_{1,2}x_T^2 + c_{1,1}x_T + k_1 = y_T + R_{T,i} \\ c_{2,2}x_T^2 + c_{2,1}x_T + k_2 = y_T + R_{T,i} \\ c_{3,2}x_T^2 + c_{3,1}x_T + k_3 = y_T + R_{T,i} \end{cases}$, which can be translated to $\begin{cases} c_{1,2}x_T^2 + c_{1,1}x_T - y_T = -k_1 + R_{T,i} \\ c_{2,2}x_T^2 + c_{2,1}x_T - y_T = -k_2 + R_{T,i} \\ c_{3,2}x_T^2 + c_{3,1}x_T - y_T = -k_3 + R_{T,i} \end{cases}$, where x_T^2, x_T and y_T are indeterminate, others are known by U_A. So the long-secret (x_T, y_T) can be compromised by U_A.

Remark: All computations are over modulo n.

3. The improved group key transfer protocol against inside adversary

3.1 The proposed protocol

In Nam-protocol, all members $\{U_1, \cdots, U_t\}$ share a common t-th degree interpolation polynomial in each group. Certainly, an inside adversary can obtain an equation on the target member's long-term secret (x_T, y_T), $y_T r_0 = c_t x_T^t + \cdots + c_1 x_T + k$ in which $x_T, \cdots, x_T^t, y_T$ are indeterminate. In order to get $x_T, \cdots, x_T^t, y_T$, $t+1$ linearly independent equations are necessary. If there are no fewer than $t+1$ times for an inside adversary and the target member belonging to a group, the adversary can obtain the target member's long-term secret. The reason of security flaws is suitable for Harn-Lin's protocol.

In order to overcome this security weakness, an improved key transfer protocol is proposed as follows:

Pre-distribution. KGC publishes a prime p, shares a secret (x_i, y_i), ($x_i, y_i \in Z_p^*$) with each registered user U_i in a secure manner.

Key distribution. All communications in this phase are in broadcast channel. After receiving the request from initiator, KGC randomly selects a session key and transfers

it to authorized members securely. Authorized user can recover the session key, knows nothing about other user's long-term secret. Unauthorized member can not get any useful knowledge even if he has recorded all broadcasted messages. The steps are as follows:

1. Initiator sends a key establishment request to KGC with $\{U_1,\cdots,U_t\}$;
2. KGC selects an unused random $r_0 \in Z_p^*$, broadcasts r_0 and $\{U_1,\cdots,U_t\}$;
3. U_i $(1 \le i \le t)$ computes $\alpha_i = h(x_i, y_i, r_0, U_1,\cdots,U_t)$ and broadcasts $\{U_i, \alpha_i\}$;
4. If α_i is authenticated, KGC constructs an interpolation polynomial $f(x)$ passing through $(0,k)$, $(x_1, h(y_1 \| r_0)),\cdots,(x_t, h(y_t \| r_0))$, where k is session key for communication group. KGC computes t additional points $P_i = f(i)$ $(1 \le i \le t)$, and authentication message $\beta = h(k, U_1,\cdots,U_t, r_0, P_1,\cdots,P_t)$, where h is a secure hash function. KGC broadcasts $\{\beta, P_1,\cdots,P_t\}$.
5. U_i reconstructs $f(x)$ from $P_1,\cdots,P_t$ and $(x_i |, h(y_i \| r_0))$, recovers $k = f(0)$, and verify if it is correct with β.

3.2 Security analysis of the proposed protocol

The proposed key establishment protocol not only inherits the merits of Nam-protocol such as efficiency and correctness but also eliminates the security weakness. In this section, we analyze the improved protocol is secure against two types of attack, insider attack and outsider attack.

Scenario 1. Assuming that the protocol runs successfully, inside adversary can not know other member's secret (x_i, y_i).

Proof. First, we assume the KGC is a trusted entity who assures r_0 freshness. Next, KGC constructs $f(x) = c_t x^t + \cdots + c_1 x + k$ with $t+1$ points $(0,k)$, $(x_1, h(y_1 \| r_0))$, $\cdots,(x_t, h(y_t \| r_0))$. An authorized member U_i can reconstruct $f(x)$ with t public points and his $(x_i, h(y_i \| r_0))$ where (x_i, y_i) is long-term secret shared with KGC, r_0 is random to resist the replay attack. Obviously, U_i obtain $h(y_T \| r_0) = f(x_T) = c_t {x_T}^t + \cdots + c_1 x_T + k$ where (x_T, y_T) is the target member's long-term secret. If only KGC is trusted, $(x_T, h(y_T \| r_0))$ is different for each communication group. With a single equation, U_i can not obtain $(x_T, h(y_T \| r_0))$. Of course, (x_T, y_T) is secure against insider attack.

Scenario 2. Assuming that an outside adversary impersonates all broadcasted messages, he can neither share the session key nor obtain other user's long-term secret.

Proof. Assuming U_A is an adversary not belonging to a communication group, he obtains nothing about $f(x)$ even if he has eavesdropped all broadcasted messages $\{U_i, \alpha_i\}$ and $\{\beta, P_1,\cdots,P_t\}$. The restriction of t-th degree polynomial $f(x)$ need no fewer than $t+1$ points.

If U_A impersonates an authorized member to initiate a communication group, he must send the authentication message $\{U_i, \alpha_i\}$ to KGC, which will terminate the attack. Moreover, U_A can not initiate replay attack for one-time random r_0. So the improved protocol is against outsider attack.

4. Conclusion

In this article, we present an improved group key transfer protocol which can resist against insider attack and outsider attack based on secret sharing.

References

[1] Junghyun Nam, Juryon Paik, Byunghee Lee, et al. An improved protocol for server-aided authenticated group key establishment. In ICCSA2011, LNCS 6786, pp.437-446, 2011.

[2] L. Harn, C. Lin. Authenticated group key transfer protocol based on secret sharing. IEEE Transactions on Computers, 2010, 59 (6): 842-846.

Juan Huang received the M.E. degrees, from University of Electronic Science and Technology of China in 2011. Her research interest includes information system security, protocol analysis.

Yajun Li received the B.S., from Henan Normal University. in 2001, now she is a graduate in Guilin University of Electronic Technology. Her research interest includes information security and e-voting.

Yining Liu received the B.S. degree in Applied Mathematics from Information Engineering University, Zhengzhou, P. R. China, in 1995, the M.S. in Computer Software and Theory from Huazhong University of Science and Technology, Wuhan, P. R. China, in 2003, and the Ph.D. degree in Mathematics from Hubei University, Wuhan, P.R. China, in 2007. He is currently an Associate Professor in Guilin University of Electronic Technology, Guilin, China. His research interests focus on the analysis of security protocols and secure e-voting.