Yet another attack on a password authentication scheme based on quadratic residues with parameters unknown[1]

Lizhen Yang, Xiaoyun Wang, Dong Zheng, Kefei Chen

Abstract: In 1988, Harn, Laih and Huang proposed a password authentication scheme based on quadratic residues. However, in 1995, Chang, Wu and Laih pointed out that if the parameters α, β, δ and λ are known by the intruder, this scheme can be broken. In this paper, we presented another attack on the Harn-Laih-Huang scheme. In our attack, it doesn't need to know the parameters and it is more efficient than the Chang-Wu-Laih attack.

Key words: cryptanalysis, authentication, password

1. Introduction

Password authentication is the most widely used mechanism for authenticating legitimate users in multiuser computing systems, and many papers are dedicate to solve this problem, such as [2-5]. In 1988, Harn, Laih and Huang [2] proposed a password authentication scheme based on quadratic residues. They claimed that their password authentication scheme can prevent the password from being revealed since the system only maintains a verification table to indicate the corresponding parameters of the users password. However, in 1995, Chang, Wu and Laih pointed out that if the parameters α, β, δ and λ are known by the intruder, this scheme can be broken by registering four valid accounts and applying to the system for these four valid accounts at most three times to obtain the password of a legitimate user. In this paper, we proposed another attack in which an intruder only need a valid account to discover the password of a legitimate user without

[1] This work has been supported by NFSE under grants 90104005 and Nation 863 program of China under grants 2001AA144060.

knowledge of the system parameters α, β, δ and λ. Furthermore, our attack is more efficient than the previous attack presented by Chang, Wu and Laih [1] even though our attack doesn't need any knowledge of the four parameters. Moreover, it is impossible for the system to notice our attack.

2. Review of Lain et al.'s scheme

Before introducing Laih et al.'s scheme, we first review some characteristics of quadratic residues. A number y is said to be quadratic residue (QR) modulo n if $\gcd(y, n) = 1$, and there exists a x satisfying $x^2 = y (\mathrm{mod}\, n)$. Otherwise y is said to be a quadratic nonresidue (NQR) modulo p. Let S_{QR-n} denote the set of quadratic residues modulo n, and S_{NQR-n} denote the set of quadratic nonresidues modulo n. The properties of quadratic residue [2] are as follows:

1. $x^{(n-1)/2} \bmod n = \begin{cases} 1, & x \in S_{QR-n} \\ -1 & x \notin S_{NQR-n} \end{cases}$
2. Suppose p, q are primes. Then integer x must belong to one of the following four cases: (1) $x \in S_{QR-p} \cap S_{QR-q}$; (2) $x \in S_{QR-p} \cap S_{NQR-q}$; (3) $x \in S_{NQR-p} \cap S_{QR-q}$; (4) $x \in S_{NQR-p} \cap S_{NQR-q}$.
3. If $x \in S_{QR-n}, y \in S_{QR-n}$ then $xy \in S_{QR-n}$. If $x \in S_{QR-n}, y \in S_{NQR-n}$ then $xy \in S_{NQR-n}$. If $x \in S_{NQR-n}, y \in S_{NQR-n}$ then $xy \in S_{NQR-n}$.

Base on the properties of quadratic residue stated above, Laih et al.'s scheme is described in the following. Initially, the system selects two large primes p and q satisfying $(p+1) \mid 4$ and $(q+1) \mid 4$ respectively, and computes $n = pq$. The value of n is made public, while p and q are kept secret. Let the parameters α, β, δ and λ be defined as:

$$\alpha \in S_{QR-p} \cap S_{QR-q}$$
$$\beta \in S_{QR-p} \cap S_{NQR-q}$$
$$\delta \in S_{NQR-p} \cap S_{QR-q}$$
$$\lambda \in S_{NQR-p} \cap S_{NQR-q}$$

In the registration phase, each user submits his identity ID to the system. Then system chooses a proper parameter $r \in \{\alpha, \beta, \delta, \lambda\}$ such that $ID' = r \cdot ID \in S_{QR-p} \cap S_{QR-q}$. By the properties 2 and 3 of quadratic residue, we know for any ID there exists only one parameter $r \in \{\alpha, \beta, \delta, \lambda\}$ satisfying $r \cdot ID \in S_{QR-p} \cap S_{QR-q}$. Next system computes the corresponding password *PW* such that $PW^2 = ID' \bmod n$ from the following procedure:

Procedure Compute Password(ID:PW)

Begin

$x_1 = ID'^{(p+1)/4} \bmod p;$
$x_2 = ID'^{(q+1)/4} \bmod q;$

$y_1 = q^{-1} \bmod p;$
$y_2 = p^{-1} \bmod q;$
$PW = (qx_1y_1 + px_2y_2) \bmod n;$

End

Finally the system saves the pair (ID, r) into the verification table, and sends the password *PW* to the registered user via a secure channel or by hand.

In the login phase, user U_i submits his ID_i and PW_i to the system. The system performs the following tasks:

1. Check if the format of ID_i is valid. If it is invalid, then reject the login request.
2. Get the value of r_i with respect to ID_i from the verification table. Compute $ID_i' = r_i \cdot ID_i$.
3. Compute $ID_i'' = PW_i^2 \bmod n$.

4. Check if $ID_i' = ID_i''$. If it is false, then reject the login; otherwise accept the login request.

3. Attack without knowledge of parameters

Now we show how to compute the corresponding PW_i for ID_i without knowing parameters α, β, δ and λ. An intruder chooses a random integer x satisfying $\gcd(x, n) = 1$ and registers an account with identification number $\overline{ID} = ID_i \cdot x^2 \bmod n$. Let the corresponding password and parameter of $\overline{ID}$ be $\overline{PW}$ and $\bar{r}$ respectively, and the corresponding parameter of ID_i be r_i. We know $r_i \cdot ID_i \in S_{QR-p} \cap S_{QR-q}$, then $r_i \cdot \overline{ID} = r_i \cdot ID_i \cdot x^2 \in S_{QR-p} \cap S_{QR-q}$. Since the parameter is uniquely determined, hence $r_i = \bar{r}$. We have

$$\begin{cases} r_i \cdot ID_i = PW_i^2 \bmod n & (1) \\ \bar{r} \cdot \overline{ID} = r_i \cdot \overline{ID} = r_i \cdot ID_i \cdot x^2 = \overline{PW}^2 \bmod n & (2) \end{cases}$$

Substituting eq.(1) into eq.(2), we get

$$PW_i^2 \cdot x^2 = \overline{PW}^2 \bmod n$$

or

$$PW_i^2 = (\overline{PW} \cdot x^{-1})^2 \bmod n$$

Hence the password corresponding to ID_i is either $(\overline{PW} \cdot x^{-1}) \bmod n$ or $(-\overline{PW} \cdot x^{-1}) \bmod n$. We notice that in the login phase the system cannot distinguish between the two possible passwords $(\overline{PW} \cdot x^{-1}) \bmod n$ and $(-\overline{PW} \cdot x^{-1}) \bmod n$. Now the intruder can successfully impersonate the legitimate user of ID_i by inputting a password $(\overline{PW} \cdot x^{-1}) \bmod n$ or $(-\overline{PW} \cdot x^{-1}) \bmod n$.

References

[1]Chin-Chen Chang, Tzong-Chen Wu and Chi-Sung Laih, Cryptanalysis of a password authentication scheme using quadradic residues. Computer communications, Vol. 18 No. 1, January 1995, pp 45-47.

[2] C.S. Laih, L. Harn and D. Huang, Password authentication using public-key encryption, Proceeding of 1983 International Carnahan Conference on Security Technology, Zurich, Switzerland, October 1987, pp 35-38.

[3] Chin-Chen Chang, Wen-Yuan Liao, Remote password authentication scheme based upon ElGamal's signature schemem, Computers & Security, Vol. 13, No. 2, Apr, 1994, pp 137-144.

[4] Chun-Li Lin, Tzonelih Hwang, A password authentication scheme with secure password updating, Computers and Security, Vol. 22 No. 1, 2003, pp 68-72.

[5]Lei Fan, Jian-Hua Li, Hong-Wen Zhu, An enhancement of timestamp-based password authentication scheme, Computers and Security, Vol. 21 No. 7, 2002, pp 665-667.