IV. CONCLUSIONS

We have shown that Shieh et al.'s proposed multisignature schemes are vulnerable to insider forgery attacks. From our analysis, we find the following facts.

1) In Shieh et al.'s parallel multisignature scheme, the initiator or the combiner must be trusted by the other signers, because that always has the advantage to successfully plot a forgery attack without being detected by the verifier.

2) Shieh et al.'s serial multisignature scheme cannot convince the verifier that a valid multisignature is truly generated by the participant signers in compliance with the predefined signing sequence.

3) Any verifier cannot be convinced by Shieh et al.'s parallel/serial multisignature schemes that the signed message is indeed signed by the claimed signers, even though the recovered message have been verified successfully.

Therefore, Shieh et al.'s multisignature schemes cannot fulfill the claimed security requirements for authenticating delegates in mobile code systems.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable suggestions that greatly improved the presentation of this paper.

REFERENCES


Security of Park–Lim Key Agreement Schemes for VSAT Satellite Communications

Xun Yi, Chee Kheong Siew, Hung-Min Sun, Her-Tyan Yeh, Chun-Li Lin, and Tzonelih Hwang

Abstract—Park and Lim proposed a modified Yacobi scheme, a modified Diffie–Hellman scheme in two cases, and a modified Diffie–Hellman scheme with ID for key agreement in very small aperture terminal satellite communications. In this paper, we show that the three Park–Lim schemes are insecure against an impersonation attack.

Index Terms—Authentication, encryption, key agreement, satellite communications, very small aperture terminal (VSAT).

I. INTRODUCTION

RECENT advances in technology have given a new thrust to the satellite communication industry by deploying a low-cost very small aperture terminal (VSAT) network for data, voice, and video communications [2]. A typical VSAT network usually consists of a number of remote VSATs that communicate with or through a HUB station via the inbound links (VSAT-to-HUB) and the outbound links (HUB-to-VSAT) [3]. All VSAT signal carriers are received by the HUB station, which acts as a ground processor. The HUB station then retransmits the data information to the destination VSAT via the outbound links.

The VSAT network utilizes the advantages of satellite communications, such as high reliability, quality of transmission, low cost, flat usage rates independent of distance, and simple network installation, operation, and management. In view of that, it is highly suitable for creating broadcasting network. However, satellite communications are vulnerable to relatively easy interception because data are transmitted over open air. For this reason, it is critical to protect data transmitted in satellite communications by way of encryption.

To encrypt data exchanged between the HUB and the VSAT of a user with secret-key cryptosystems, a common secret key should be shared in advance by them. In [1], Park and Lim modified the Yacobi key agreement scheme [4] and Diffie–Hellman key agreement scheme [5] and proposed three new key agreement schemes for VSAT satellite communications. They claimed that the modified Yacobi scheme and the modified Diffie–Hellman scheme can indirectly authenticate both sides by way of a common working key, and that the modified Diffie–Hellman scheme with ID directly enables authentication of both sides.

In this paper, the three Park–Lim schemes are shown to be insecure against an impersonation attack. The rest of this paper is arranged as follows. Section II summarizes the three Park–Lim key agreement schemes. Section III performs an impersonation attack on the three Park–Lim schemes, respectively. Conclusions are drawn in Section IV.

Manuscript received July 30, 2001; revised May 23, 2002.

X. Yi and C. K. Siew are with the Information and Communication Institute of Singapore, School of Electrical and Electronic Engineering, Nanyang Technological University, 639798 Singapore (e-mail: exyi@ntu.edu.sg).

H.-M. Sun is with the Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan 30055, R.O.C. (e-mail: hmsun@cs.nthu.edu.tw).

H.-T. Yeh, C.-L. Lin, and T. Hwang are with the Department of Computer Science and Information Engineering, National Cheng Kung University, Taiwan, 701 Taiwan, R.O.C. (e-mail: hmsun@mail.ncku.edu.tw).

Digital Object Identifier 10.1109/TVT.2003.808752
II. PARK–LIM KEY AGREEMENT SCHEMES

In the following description of the three Park–Lim schemes, we suppose that the HUB station and the VSAT of a user wish to communicate one another in secrecy and need to reach a common secret working key between them.

A. Initial Key Generation and Distribution

A key distribution center generates two big primes $p$ and $q$, computes $n = p \cdot q$, and chooses a pair of public and private keys $(e, d)$ such that $e \cdot d = 1 \pmod{(p-1)(q-1)}$. It also selects an integer $g$, which is the primitive element of both $\mathbb{GF}(p)$ and $\mathbb{GF}(q)$. $(n, g, e)$ are then public, while $(q, d)$ are known only to the center.

For an authorized user $A$ whose identification information is $ID_A$, the center calculates $a_A = ID_A^d \pmod{n}$. Then it stores $(n, g, e, a_A)$. By doing this, it can easily recover $(n, g, e, a_A)$ when the user authenticates himself.

B. Park–Lim Modified Yacobi Scheme

The HUB station chooses a random integer $r_h$ and computes $x_h = g^{r_h} \pmod{n}$, $y_h = (r_h \cdot e + a_A)$, where $a_A = ID_A^d \pmod{n}$ is known only to the HUB station. The VSAT also selects a random integer $r_v$ and calculates $x_v = g^{r_v} \pmod{n}$, $y_v = (r_v \cdot e + a_A)$, where $a_A = ID_A^d \pmod{n}$ is known only to the VSAT. Then the HUB station and the VSAT exchange $(x_h, y_h)$ and $(x_v, y_v)$. After exchange, the HUB station computes $W_{Kh} = (g^{x_h \cdot y_v^{r_h^*}})^{r_v} \pmod{n}$ while the VSAT calculates $W_{Kv} = (g^{y_h \cdot x_v^{-r_v^*}})^{r_v} \pmod{n}$.

It is obvious that $W_{Kh} = W_{Kv}$. Finally, the HUB station and the VSAT reach a common secret working key $W_{Kh} \oplus W_{Kv}$, which may be used to protect both the inbound link (VSAT-to-HUB) and the outbound link (HUB-to-VSAT) between the HUB station and the VSAT. The above procedure can be illustrated in Fig. 1.

1) Note: In [1], the formula for computing $W_h$ in a Park–Lim modified Yacobi scheme is mistaken and should be corrected to $W_{Kh} = (g^{x_h \cdot y_v^{r_h^*}})^{r_v} \pmod{n}$.

C. Park–Lim Modified Diffie–Hellman Scheme

1) First Case: The HUB station chooses a random integer $r_h$ and computes $x_h = ID_A \cdot g^{r_h} \pmod{n}$, while the VSAT selects a random integer $r_v$ and calculates $x_v = ID_A \cdot g^{r_v} \pmod{n}$. Then the HUB station and the VSAT exchange $x_h$ and $x_v$. After exchange, the HUB station computes $W_{Kh} = (ID_A \cdot g^{r_h})^{r_v} \pmod{n}$, while the VSAT calculates $W_{Kv} = (ID_A \cdot g^{r_v})^{r_h} \pmod{n}$. It is obvious that $W_{Kh} = W_{Kv}$. The above procedure is illustrated in Fig. 2.

2) Second Case: The HUB station randomly chooses a private key $s_h$ and computes the corresponding public key $P_h = g^{s_h} \pmod{n}$ for itself. For each VSAT $v$, the HUB station randomly selects a private key $s_v$, and distributes the private–public key pair $(s_h, P_h)$ such that $P_h = g^{s_h} \pmod{n}$ to the VSAT via a secure channel.

During key establishment, the HUB station chooses a random integer $r_h$ and computes $x_h = g^{r_h} \pmod{n}$, $z_h = P_h^{r_h} \pmod{n}$, $y_h = x_h \cdot z_h \pmod{n}$ while the VSAT selects a random integer $r_v$ and calculates $x_v = g^{r_v} \pmod{n}$, $z_v = P_h^{r_v} \pmod{n}$, $y_v = x_v \cdot z_v \pmod{n}$. Next, the HUB station and the VSAT exchange $(x_h, y_h)$ and $(x_v, y_v)$. After exchange, the HUB station computes $W_{Kh} = (y_h \cdot z_v)^{r_h} \pmod{n}$ while the VSAT calculates $W_{Kv} = (y_v \cdot z_h)^{r_v} \pmod{n}$ where $z_h = P_h^{r_h} = g^{r_h} \pmod{n}$ and $z_v = P_h^{r_v} = g^{r_v} \pmod{n}$. It is obvious that $W_{Kh} = W_{Kv}$. The above procedure is depicted in Fig. 3.

3) Note: In [1], $(R_i, R_j)$ in the second case have no definite meanings. If $R_i = r_i$ and $R_j = r_j$, $(r_i, r_j)$ are transmitted over a open channel according to the second case and thereby any eavesdropper can easily intercept $(r_i, r_j)$ and obtain the shared secret working key between the HUB station and the VSAT simply by computing $g^{r_i \cdot r_j} \pmod{n}$. In fact, the above description of the second case is based on the adaption of modified Diffie–Hellman scheme in [1].

D. Park–Lim Modified Diffie–Hellman Scheme With $ID$

The HUB station chooses a random integer $r_h$ and computes $x_h = g^{r_h} \cdot ID_v^{r_h} \pmod{n}$, $z_h = P_h^{r_h} \pmod{n}$, $y_h = x_h \cdot z_h \pmod{n}$ while the VSAT selects a random integer $r_v$ and calculates $x_v = g^{r_v} \cdot ID_v^{r_v} \pmod{n}$, $z_v = P_h^{r_v} \pmod{n}$, $y_v = x_v \cdot z_v \pmod{n}$. Then the HUB station and the VSAT exchange $(x_h, y_h)$ and $(x_v, y_v)$. After exchange, the HUB station computes $W_{Kh} = (y_h \cdot z_v)^{r_h} \pmod{n}$ while the VSAT calculates $W_{Kv} = (y_v \cdot z_h)^{r_v} \pmod{n}$. It is obvious that $W_{Kh} = W_{Kv}$. The above procedure can be illustrated in Fig. 4.

Next, the HUB station authenticates the VSAT if $s_h = x_h^{r_h} / (y_h \cdot g^{ID_v^{r_h}} \cdot ID_v^{r_h} \pmod{n})$ while the VSAT authenticates the HUB station if $s_v = x_v^{r_v} / (y_v \cdot g^{ID_v^{r_v}} \cdot ID_v^{r_v} \pmod{n})$, where $c_v'$ is computed by the HUB station according to $c_v' = h(x_v, ID_v, ID_h, t)$ while $c_h$ is calculated by the VSAT based on $c_h = h(x_h, ID_v, ID_h, t)$.

1) Note: In [1], the formula for computing $W_{hv}$ in adaption of the modified Diffie–Hellman with ID is mistaken and should be corrected to

$W_{hv} = (g^{ID_h} \cdot X_h)^{R_v \cdot S_v} = (g^{ID_h} \cdot X_v)^{R_v \cdot S_h}$

$= g^{R_v \cdot S_v \cdot S_h} \pmod{n}$

III. IMPERSONATION ATTACK AGAINST PARK–LIM SCHEMES

The impersonation attack is a mechanism whereby an attacker attempts to masquerade as a legal user in satellite communications. In the following discussion, we suppose that an attacker has no knowledge of the secret $s_e$ (known only to the VSAT $v$) but attempts to impersonate the VSAT to communicate with the HUB station.
A. Attack to Park–Lim Modified Yacobi Scheme

According to the Park–Lim modified Yacobi scheme, the HUB station chooses a random integer $r_h$ and computes a pair of integers $(x_h, y_h)$ such that $x_h = g^{r_h} \mod n$ and $y_h = (r_h \cdot e + s_h)$. The attacker (the impersonator of the VSA T) also selects a random integer $r_r^*$ and forges a pair of integers $(x_r^*, y_r^*)$ such that $y_r^* = g^{r_r^* \cdot v^*} \mod n$ and $y_r^* = g^{r_r^* \cdot v^*} \mod n$. Then the HUB station and the attacker exchange $(x_h, y_h)$ and $(x_r^*, y_r^*)$. After exchange, based on the Park–Lim modified Yacobi scheme, the HUB station computes the secret working key in the following way:

$$W_{K_h} = g^{x_h \cdot y_r^*} \cdot x_r^* = g^{x_r^* \cdot y_h} \cdot x_h = g^{x_h \cdot y_r^*} \cdot x_r^* \mod n.$$  

The attacker can also calculate the same secret working key in the following way:

$$W_{K_r^*} = (g^{x_r^*} \cdot x_h^{-1})^*h = g^{x_r^* \cdot y_h} \mod n.$$  

It is obvious that $W_{K_h} = W_{K_r^*}$. The above procedure is illustrated in Fig. 5.

Since $W_{K_h} = W_{K_r^*}$, the attacker is able to decrypt any encrypted message sent by the HUB station in the outbound link (HUB-to-VSAT) and impersonate the VSAT to send the HUB station any encrypted message in the inbound link (VSAT-to-HUB) without being detected. Therefore, the HUB station cannot indirectly detect this attack by way of the common secret working key.

In the same way, the attacker can also impersonate the HUB station to communicate with any VSAT, and the VSAT cannot indirectly detect the impersonation attack by way of the common secret working key.

Consequently, the Park–Lim modified Yacobi scheme is insecure against the impersonation attack.

B. Attack to Park–Lim Modified Diffie–Hellman Scheme

1) First Case: Based on the Park–Lim modified Diffie–Hellman scheme (first case), the HUB station chooses a random integer $r_h$ and computes $x_h = g^{r_h} \mod n$.

The attacker (pretending to be the VSAT) also selects a random integer $r_r^*$ and forges $x_r^*$ by computing $x_r^* = ID_h \cdot g^{r_r^* \mod n}$. Then the HUB station and the attacker exchange $x_h$ and $x_r^*$. After exchange, according to the Park–Lim modified Diffie–Hellman scheme (first case), the HUB computes the secret working key in the following way:

$$W_{K_h} = (ID_h \cdot x_r^*)^{x_h} \mod h = g^{x_r^* \cdot x_h} \mod h.$$  

The attacker can also calculate the same secret working key in the following way:

$$W_{K_r^*} = (ID_h \cdot x_r^*)^{x_h} \mod h = g^{x_r^* \cdot x_h} \mod h.$$  

It is obvious that $W_{K_h} = W_{K_r^*}$. The above procedure is depicted in Fig. 6.

2) Second Case: According to the adaptation of the Park–Lim modified Diffie–Hellman scheme in [1], there is a hint that all VSATs know the authentic $P_h$ and the HUB station, as the key distribution center, knows the genuine $P_h$ of all VSATs.

The HUB station chooses a random integer $r_h$ and computes $x_h = g^{r_h} \mod n$, $z_h = P_h^r \mod n$, $y_h = x_h \cdot z_h \mod n$.

Suppose that the attacker intercepts $(x_h, y_h)$ in a previous exchange between the HUB station and the VSAT, where $x_r^* = g^{r_r^* \cdot v^*} \mod n$, $y_r^* = x_r^* \cdot z_h \mod n$, and $z_h = P_r^* \mod n$. From $(x_h, y_h)$ or $(x_r^*, y_r^*)$, the attacker can deduce $z_h = y_r^* \cdot x_r^* \mod n$ or $z_h = y_r^* \cdot x_r^* \mod n$. In fact, $z_h$ never changes for the HUB station and the VSAT. With $z_h$, the attacker chooses a random integer $x_r^*$ and forges $x_h = g^{x_h} \mod n$, $y_h = x_h \cdot z_h \mod n$.

Then the HUB station and the attacker exchange $(x_h, y_h)$ and $(x_r^*, y_r^*)$. After exchange, according to the adaptation of the Park–Lim modified Diffie–Hellman scheme, the HUB station computes the secret working key in the following way:

$$W_{K_h} = (y_r^* \cdot z_h^{-1})^{x_h} \mod n = (x_r^*)^{x_h} \mod n = g^{x_r^* \cdot x_h} \mod h.$$  

The attacker can also calculate the same working key in the following way:

$$W_{K_r^*} = (y_r^* \cdot z_h^{-1})^{x_h} \mod n = (x_r^*)^{x_h} \mod n = g^{x_r^* \cdot x_h} \mod h.$$  

It is obvious that $W_{K_h} = W_{K_r^*}$. The above procedure is illustrated in Fig. 7.

In the above two cases, since $W_{K_h} = W_{K_r^*}$, the HUB station cannot indirectly detect this attack by way of the common secret working key.

In the same way, the attacker can also impersonate the HUB station to communicate with any VSAT without being detected. Consequently, the two cases of Park–Lim modified Diffie–Hellman scheme are insecure against an impersonation attack.

C. Attack to Park–Lim Modified Diffie–Hellman Scheme With ID

On the basis of the Park–Lim modified Diffie–Hellman scheme with ID, the HUB station chooses a random integer $r_h$ and computes three integers $(x_h, y_h, c_h)$ with $x_h = g^{r_h \cdot h^i} \mod n$, $c_h = h(x_h, ID_h, ID_v, t) \mod n$.

The attacker (masquerading as the VSAT) also selects a random integer $r_r^*$ and forges three integers $(x_r^*, y_r^*, c_r^*)$ with $x_r^* = g^{r_r^* \cdot h^i} \mod n$, $c_r^* = h(x_r^*, ID_h, ID_v, t) \mod n$.

After the HUB station and the attacker exchange $(x_h, y_h)$ and $(x_r^*, y_r^*)$, according to Park–Lim modified Diffie–Hellman scheme with ID, the HUB station computes the secret working key in the following way:

$$W_{K_h} = (g^{ID_h} \cdot x_r^*)^{x_h} \mod h = g^{x_r^* \cdot x_h} \mod n.$$  

Authorized licensed use limited to: National Cheng Kung University. Downloaded on October 28, 2009 at 04:06 from IEEE Xplore. Restrictions apply.
The attacker can also calculate the same working key in the following way:

\[ W_K^* = (g^{-ID_v \cdot x_h})^{x_v} = g^{(h \cdot x_h \cdot x_v^a)(mod \; n)}. \]

It is obvious that \( W_K = W_K^* \). The above procedure can be illustrated in Fig. 8.

Since \( W_K = W_K^* \), the HUB station cannot indirectly detect this attack by way of the common working key.

Moreover, although \( c'_v \) is computed by the HUB station based on \( c'_v = h(x'_v, ID_v, ID_h, t) \), the authentication equation holds because \( c'_v = c_v \) and

\[
\frac{x'_v \cdot c'_v}{y'_v \cdot g^{ID_h \cdot c_v} \cdot ID_h} = \frac{x'_v \cdot c'_v}{y'_v \cdot g^{ID_h \cdot c_v} \cdot ID_h} = ID_h^{-c_v} = s_h (mod \; n). 
\]

Therefore, the HUB station cannot directly detect this attack by checking the authentication equation.

In the same way, the attacker can also impersonate the HUB station to communicate with any VSAT without being detected.

Consequently, the Park–Lim modified Diffie–Hellman scheme with ID is insecure against an impersonation attack.

IV. CONCLUSION

Key agreement is an important issue in securing VSAT satellite communications. A secure key agreement scheme should stand up an impersonation attack. In [1], Park and Lim proposed three key agreement schemes for VSAT satellite communications based on Yacobi and Diffie–Hellman schemes. In this paper, we have shown that all three Park–Lim schemes are vulnerable to an impersonation attack.

REFERENCES