ATTACK ON THE KOYAMA-OHTA IDENTITY BASED KEY DISTRIBUTION SCHEME

by

Yacov Yacobi

Bell Communications Research
435 South Street
Morristown, NJ 07960
USA

ABSTRACT

Koyama and Ohta proposed an identity based key distribution scheme. They considered three configurations: ring, complete graph, and star. The most practical configuration is the star which is used in teleconferencing. We show the Koyama-Ohta star scheme to be insecure. Specifically, we show that an active eavesdropper may cut one of the lines, and perform a bidirectional impersonation, thus establishing two separate keys. One with each side.

1. INTRODUCTION

Koyama and Ohta proposed [1] an identity based key distribution scheme. They considered three configurations: ring, complete graph, and star. The most practical configuration is the star which is used in teleconferencing. We show the Koyama-Ohta star scheme to be insecure. Specifically, we show that an active eavesdropper may cut one of the lines, and perform a bidirectional impersonation, thus establishing two separate keys. One with each side.

The same kind of attack is possible for the classic Diffie-Hellman key distribution scheme [2], however, this scheme is not an identity based scheme. Diffie and Hellman do not claim to solve impersonation problems in their scheme.

In order to apply this attack to the complete graph case, the eavesdropper has to manipulate all the communication lines which connect one node to each of the rest. This is much less probable than the attack on the star configuration, which requires the

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 429-433, 1988.

manipulation of just one line.

2. THE SCHEME, [1]

Each of the parties is equipped with a smart card, issued by trusted center. Let p,q and r be large primes, where p and q are secret, known to the center only, and r is public. Let L=lcm(p-1,q-1,r-1). Let e be any (public) number relatively prime to L, and d its inverse modulo L (i.e. $e \cdot d \equiv 1 \ mod \ L$. Let $3 \leq c < L$. Let g be a primitive element of GF(p), GF(q), and GF(r). To make the search for such g practical we demand that p-1=2p', q-1=2q' and r-1=2r', where p', q', and r' are primes.

Let ID_i denote the identification information of user i. The center computes $S_i \equiv ID_i^d \ mod \ nr$, where n=pq. The center stores (n,r,g,e,c,Si) in the smart card of user i. Si,p,q and d are secret.

The Protocol

j picks random $U_j \epsilon [0,n)$, and *sends* $E_j \equiv_n g^{e \cdot U_j}$, to i , (1.1)

i picks random P_i and V_i, *where* $P_i \epsilon [0,nr)$ and $V_i \epsilon [0,n)$, and computes

$$X_i \equiv_{nr} g^{e \cdot P_i}; \ Y_i \equiv_{nr} S_i \cdot g^{c \cdot P_i}; \ Z_{ij} \equiv_n E_j^{P_i}; \ F_i \equiv_n X_i^{e \cdot V_i}. \tag{1.2}$$

i then sends (X_i, Y_i, Z_{ij} and F_i) to j.

j checks whether the following two congruences hold:

$$Y_i^e / X_i^c \equiv_{nr} ID_i \text{ and } Z_{ij} \equiv_n X_i^{U_j}. \tag{1.3}$$

If they do not hold j halts.

j picks random $R_j \epsilon [0,nr)$, computes the following three numbers, and sends them to i:

$$A_{ji} \equiv_{nr} X_i^{e \cdot R_j}; \ B_{ji} \equiv_{nr} S_j \cdot X_i^{c \cdot R_j}; \ C_{ji} \equiv_n F_i^{R_j} \tag{1.4}$$

i checks whether the following two congruences hold:

$B_{ji}^{e}/A_{ji}^{c} \equiv_{nr} ID_j$ and $C_{ji} \equiv_n A_{ji}^{V_i}$ (1.5)

i halts if they do not hold.

i computes conference key

$K_i \equiv_r A_{ji}^{P_i}$ (1.6)

j computes conference key

$K_j \equiv_r g^{e^2 \cdot R_j}$ (1.7)

[]

From (1.2), (1.4) and (1.6) it is clear that $K_i \equiv_r K_j$.

3. THE ATTACK

The eavesdropper cuts the communication line between the honest center of the star (j) and one of the terminals (i). He mediates every communication between the two from now on. When communicating with j he pretends to be i (denoted $\tilde{i}$), and when communicating with i he pretends to be j (denoted $\tilde{j}$). At the end of the attack protocol $\tilde{j}$ establishes a key with i, and $\tilde{i}$ establishes another key with j. The key with j matches the session key of the rest of the group.

Preprocessing:

The eavesdropper choses random P', and computes its inverse modulo r-1 ($\overline{P}$'). He also compute the inverse of e modulo r-1 ($\overline{e}$).

The attack protocol

j picks random secret $U_j \in [0,n)$, and computes

$E_j \equiv_n g^{e \cdot U_j}$ (2.1)

He then sends it to i. $\tilde{i}$ reads it without interfering.

i picks random $P_i \epsilon [0, n \cdot r)$ and $V_i \epsilon [0, n)$, computes

$$X_i \equiv_{n \cdot r} g^{e \cdot P_i}; \;\; Y_i \equiv_{n \cdot r} S_i \cdot g^{c \cdot P_i}; \;\; Z_{ij} \equiv_n E_j^{P_i}; \;\; F_i \equiv_n X_i^{e \cdot V_i}, \tag{2.2}$$

and sends it to j,

$\tilde{j}$ intercepts the message, and modifies it as follows: The new Z_{ij} and F_i equal the original, but the new X_i and Y_i (denoted $\dot{x}_i$ and $\dot{y}_i$ are computed using Chinese Remanidering to have the following properties:

$$\dot{x}_i \equiv_n X_i; \;\; \dot{x}_i \equiv_r g^{e \cdot P} \;\; (\mathit{denoted} \;\; x_i'); \;\; \dot{y}_i \equiv_n Y_i; \;\; \dot{y}_i \equiv_r (ID_i \cdot (x_i')^c)^{\bar{e}}; \tag{2.2'}$$

He then sends $\dot{x}_i$; $\dot{y}_i$; Z_{ij}; F_i to j,

j validates that

$$\dot{y}_i^e / \dot{x}_i^c \equiv_{nr} ID_i \;\; \text{and} \;\; Z_{ij} \equiv_n \dot{x}_i^{U_j}, \tag{2.3}$$

j halts if these congruences do not hold.

j computes the following three numbers:

$$\dot{a}_{ji} \equiv_{nr} \dot{x}_i^{eR_j}; \;\; \dot{b}_{ji} \equiv_{nr} S_j \cdot \dot{x}_i^{c \cdot R_j}; \;\; C_{ji} \equiv_n F_i^{R_j} \tag{2.4}$$

and sends them to i,

$\tilde{i}$ intercepts this communication. He choses some random $\dot{r}_j$. He then modifies the communication as follows: C_{ji} remains unchanged. Using Chinese Remaindering , $\tilde{i}$ computes new $\ddot{a}_{ji}$, and $\ddot{b}_{ji}$, for which the following holds:

$$\ddot{a}_{ji} \equiv_n \dot{a}_{ji} \equiv_n A_{ji}; \;\; \ddot{a}_{ji} \equiv_r X_i^{e\dot{r}_j}; \;\; \ddot{b}_{ji} \equiv_n \dot{b}_{ji} \equiv_n B_{ji}; \;\; \ddot{b}_{ji} \equiv_r (ID_j \cdot X_i^{ce\dot{r}_j})^{\bar{e}}; \tag{2.4'}$$

He sends these three numbers to i.

i verifies that the following congruences hold:

$$\dot{b}_{ji}^{e} / \ddot{a}_{ji}^{c} \equiv_{nr} ID_j \quad ; C_{ji} \equiv_n \ddot{a}_{ji}^{V_i'} \tag{2.5}$$

i halts if the congruences do not hold.

i creates session key

$$K_i \equiv_r \ddot{a}_{ji}^{\overline{P}_i'} \equiv_r g^{e^2 \cdot \dot{r}_j} \tag{2.6}$$

$\tilde{j}$ creates session key

$$\acute{k}_j \equiv_r g^{e^2 \cdot \dot{r}_j} \tag{2.6'}$$

$\tilde{i}$ creates session key

$$\acute{k}_i \equiv_r \dot{a}_{ji}^{\overline{P'}_i'} \equiv_r g^{e^2 \cdot R_j} \tag{2.7'}$$

j creates session key

$$K_j \equiv_r g^{e^2 \cdot R_j} \tag{2.7}$$

▯

REFERNCES

[1] K.Koyama and K.Ohta :"Identity based conference key distribution systems", To appear in the proceedings of **Crypto-87** ,

[2] Diffie and Hellman:" New Directions in Cryptography", **IEEE Trans. on Inf. Th.** , **1976.**