TẤN CÔNG LIM-LEE VÀO CÁC GIAO THỨC DH-KE TRÊN GF(p)

Nguyễn Thanh Sơn[1*], Lều Đức Tân[2]

Tóm tắt: *Bài báo trình bày tấn công theo phương pháp của Lim-Lee lên các giao thức DH-KE trên GF(p) như là: tấn công giao thức HARN, giao thức PHAN, Giao thức Liu-Li. Bài báo cũng đưa ra điều kiện đủ để chống lại tấn công Lim-Lee.*

Từ khóa: Giao thức DH-KE trên GF(p); Tấn công Lim-Lee.

1. ĐẶT VẤN ĐỀ

Vào năm 1997, hai tác giả Chao Hoom Lim và Pil Joong Lee đã đưa ra một phương pháp tấn công của người trong hệ thống nhằm tìm khóa mật của người khác khi họ tham gia các giao thức DH-KE trên GF(p) [2]. Trong tài liệu trên, Lim và Lee đã thực hiện việc tấn công vào một số giao thức DH-KE như giao thức Diffie-Hellman cơ bản, giao thức đối xứng không tương tác (một cải biên của giao thức 2 [5]), giao thức MTI [6],… Tuy nhiên, có một giao thức không được nhắc đến đó là giao thức của Harn công bố từ 1995 (xem [1]). Trong bài này, chúng tôi đưa ra cách tấn công vào giao thức Harn tại mục 3 và hai giao thức công bố sau năm 1997 đó là giao thức của Phan công bố năm 2005 [4] tại mục 4 và giao thức của Jie Liu và Jianhua Li công bố năm 2010 [3] tại mục 5. Do 3 giao thức được xem xét đều sử dụng việc xác thực theo lược đồ chữ ký DSA nên mục 2 trình bày lại lược đồ chữ ký DSA nhằm phục vụ việc xác định chi phi tính toán của các tấn công vào các giao thức nêu trên đồng thời cũng chỉ ra tính chưa tuân thủ đúng thuật toán tạo chữ ký của DSA trong các giao thức nêu trên.

Từ những xem xét trên chúng ta thấy rằng, cho đến nay chưa tồn tại giao thức DH-KE nào trên GF(p) không bị tổn thương trước tấn công của Lim và Lee. Cuối cùng, trong mục 6, chúng tôi chỉ ra một điều kiện cho tham số p đủ để chống được tấn công của Lim và Lee.

2. MỘT SỐ KẾT QUẢ LIÊN QUAN ĐẾN CHI PHÍ TẤN CÔNG

2.1. Một số ký hiệu

$t_m(n)$ là chi phí trung bình cho một phép nhân rút gọn theo modulo n;

$t_{exp}(t, n)$ là chi phí trung bình cho một phép tính $a^e \bmod n$ với e < t. $t_{inv}(n)$ là chi phí trung bình cho một phép tính $a^{-1} \bmod n$;

t_H là chi phí trung bình cho một phép tính hàm H: $\{0,1\}^\infty \to \{0,1\}^h$;

$t_{DSAVer}(p, q)$ là chi phí cho một phép kiểm tra cặp số (r, s) có là chữ ký hợp lệ của người (sử dụng tham số bí mật của mình) ký lên thông báo M theo lược đồ DSA;

|| là phép ghép nối các thông báo để tạo thành thông báo mới;

ord(g) là cấp của g.

Một số quy đổi: $t_m(n^2) = 3.t_m(n)$; $t_{exp}(t, n) = 1{,}5.\log_2(t) \times t_m(n)$.

2.2. Lược đồ chữ ký DSA

Tham số miền (p, q, g) trong đó p, q là hai số nguyên tố với q | p – 1 và g ∈ GF*(p) thỏa mãn ord(g) = q.

Tập các thông báo: $\{0,1\}^\infty$.

Hàm tóm lược thông báo: H: $\{0,1\}^\infty \to \{0,1\}^l$, *l* được gọi là độ dài tóm lược.

Tham số mật của người ký: x ∈ [1, q).

Tham số công khai của người ký: $y = g^x \bmod p$.

Chữ ký lên thông báo M của người có tham số mật x là cặp $(r, s) \in [1, q)^2$, ký hiệu là *DSASig*(M, x), như một hàm được xác định theo thuật toán sau.

Thuật toán 1. (Tạo chữ ký DSA)

Input: M, x.

Output: *DSASig*(M, x).

1. $k \in_R [1, q)$.
2. $r \leftarrow (g^k \bmod p) \bmod q$; if (r = 0) then goto 1.
3. $h \leftarrow H(M)$.
4. $s \leftarrow k^{-1}(h + x.r) \bmod q$; if (s = 0) then goto 1.
5. Return (r, s).■

Việc chấp nhận (r, s) là chữ ký lên thông báo M của người có tham số công khai y là thông báo thuộc tập {"*Accept*", "*Reject*"}, ký hiệu là *DSAVer*(M, (r, s), y), như một hàm được xác định theo thuật toán sau.

Thuật toán 2. (Kiểm tra chữ ký DSA)

Input: M, (r, s), y.

Output: *DSAVer*(M, (r, s), y).

1. If $(r, s) \notin [1, q)^2$ then return "*Reject*".
2. $w \leftarrow s^{-1} \bmod q$.
3. $h \leftarrow H(M)$.
4. $u \leftarrow h.w \bmod q$
5. $v \leftarrow r.w \bmod q$
6. $r' \leftarrow (g^u.y^v \bmod p) \bmod q$
7. If (r' = r) then return "*Accept*".
8. Else return "*Reject*".■

Từ thuật toán 2 ta có

$$t_{DSAVer}(p, q) = t_H + t_{inv}(q) + 2.t_m(q) + t_m(p) + 2.t_{exp}(q, p) \quad (1)$$

2.3. Thuật toán tìm $l = \log_g a$ trên nhóm G với điều kiện $l \le M$

Thuật toán 3. (Thuật toán Daniel Shank)

Input: $a \in G$ và số nguyên dương M thỏa mãn tồn tại $l \in [0, M)$ sao cho $g^l = a$.

Output: *l*.

1. $m \leftarrow \lceil \sqrt{M} \rceil$; $b \leftarrow 1$; $S \leftarrow \{\}$. (*1 là phần tử đơn vị của G*)
2. For i from 0 to m – 1 do:
   2.1 $S \leftarrow S \cup \{(b, i)\}$.
   2.2 $b \leftarrow b.g$.

(*Kết thúc bước 2 thì* $b = g^m$)

3. $c \leftarrow b^{-1}$; $j \leftarrow 0$; $d \leftarrow a$. (b^{-1} *là phần nghịch đảo của b trong G*)
4. While $(d \notin S1)$ do:

(*S1 là tập gồm các thành phần thứ nhất của các phần tử của S*)

   4.1 $j \leftarrow j + 1$.
   4.2 $d \leftarrow d.c$.

5. If (d = b ∈ S1 with $(b, i) \in S$) then *l* = i + j.m.
6. Return *l*.■

Từ điều kiện *l* < M và $m = \lceil \sqrt{M} \rceil$ nên luôn tồn tại 0 ≤ i, j < m sao cho *l* = i + j.m và

điều này có nghĩa

$$a = g^{i+j.m} \text{ hay } a.(g^{-m})^{j} = g^{i} \quad (2)$$

Theo cách thiết lập tập S trong bước 2 thì S1 chính là tập tất cả các phần tử g^i với $0 \le i < m$.

Giá trị d tính được trong vòng thứ j của bước 4 chính là $a.c^j$. Do giá trị b tính được sau vòng for của bước 2 chính là g^m nên $c = g^{-m}$ hay $a.c^j = a.(g^{-m})^j$.

Tóm lại thuật toán 3 là đúng đắn với chi phí tính toán bao gồm:

- m phép toán nhóm trang bị cho cấu trúc nhóm tại bước 2;
- 1 phép tìm phần tử nghịch đảo tại bước 3;
- j < m phép toán nhóm tại bước 4;
- j < m phép toán xác định điều kiện ($d \notin S1$) tại bước 4.

Để thuận lợi trong việc xác định điều kiện ($d \notin S1$) và trích ra giá trị i khi $d = b \in S1$ tại bước 5 thì S sẽ được xắp xếp theo thứ tự của thành phần thứ nhất (việc làm này cần đến $m.\log_2 m$ phép so sánh trong nhóm) còn điều kiện ($d \notin S1$) được thực hiện với $\log_2 m$ phép so sánh trong nhóm.

Giới hạn phạm vi xem xét với G là nhóm con của GF*(p) chúng ta có phép toán trang bị cho cấu trúc nhóm (là phép nhân) có chi phí là $O((lnp)^2)$, còn phép so sánh có chi phí là $O(lnp)$ cho nên có thể coi $\log_2 m$ phép so sánh có chi phí cùng bậc với 1 phép nhân. Điều trên cho ta kết quả sau.

Bổ đề 1.

Chi phí tính toán cho việc tìm logarit rời rạc với điều kiện giá trị này nhỏ hơn M theo thuật toán 3 là $O(\sqrt{M})$ phép nhân trên GF(p).■

3. TẤN CÔNG VÀO GIAO THỨC HARN

3.1. Giao thức Harn

<table>
<tr><td colspan="2">Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$</td></tr>
<tr><td>A giữ tham số mật x_A.</td><td>B giữ tham số mật x_B.</td></tr>
<tr><td colspan="2">Bước 1. A tạo và truyền các thông tin thỏa thuận khóa cho B.</td></tr>
<tr><td>A.1 $v_1, v_2 \in_R [1, q)$
A.2 $m_1 = g^{v_1} \bmod p$.
A.3 $m_2 = g^{v_2} \bmod p$.
A.4 $r_A = (m_1.m_2 \bmod p) \bmod q$.
A.5 $h_A = H(m_1 || m_2)$.
A.6 $v = (v_1 + v_2)^{-1} \bmod q$.
A.7 $s_A = v.(h_A + x_A.r_A) \bmod q$.
A.8 Send (m_1, m_2, s_A) to B.</td><td>(Khi này (r_A, s_A) chính là chữ ký theo lược đồ DSA của A lên thông báo $m_1 || m_2$ với khóa phiên $v = v_1 + v_2$)</td></tr>
<tr><td colspan="2">Bước 2. B tạo và truyền các thông tin thỏa thuận khóa cho A.</td></tr>
<tr><td>(Khi này, (r_B, s_B) chính là chữ ký theo lược đồ DSA của B lên thông báo $n_1 || n_2$ với khóa phiên $w = w_1 + w_2$)</td><td>B.1 $w_1, w_2 \in_R [1, q)$.
B.2 $n_1 = g^{w_1} \bmod p$.
B.3 $n_2 = g^{w_2} \bmod p$.
B.4 $r_B = (n_1.n_2 \bmod p) \bmod q$.
B.5 $h_B = H(n_1 || n_2)$.
B.6 $w = (w_1 + w_2)^{-1} \bmod q$.
B.7 $s_B = w.(h_B + x_B.r_B) \bmod q$.
B.8 Send (n_1, n_2, s_B) to A.</td></tr>
<tr><td colspan="2">Bước 3. A xác thực B và tính khóa chung.</td></tr>
</table>

A.9 $r_B = (n_1.n_2 \bmod p) \bmod q$. A.10 $M_B = n_1 \| n_2$. A.11 If $Ver_{DSA}(M_B, (r_B, s_B), y_B) =$ "$Accept$" then: A.11.1 $K_{A1} = (n_1)^{v_1} \bmod p$. A.11.2 $K_{A2} = (n_2)^{v_2} \bmod p$. A.11.3 $K_{A3} = (n_2)^{v_1} \bmod p$. A.11.4 return (K_{A1}, K_{A2}, K_{A3}). A.12 Else break protocol.	
Bước 4. B xác thực A và tính khóa chung.	
(*Khi này, ta có* $K_{A1} = K_{B1}$. $K_{A2} = K_{B2}$. $K_{A3} = K_{B3}$. ***Chú ý:*** *Công thức tính khóa thứ 3 của B không giống như của A.*)	B.9 $r_A = (m_1.m_2 \bmod p) \bmod q$. B.10 $M_A = m_1 \| m_2$. B.11 If $Ver_{DSA}(M_A, (r_A, s_A), y_A) =$ "$Accept$" then: B.11.1 $K_{B1} = (m_1)^{w_1} \bmod p$. B.11.2 $K_{B2} = (m_2)^{w_2} \bmod p$. B.11.3 $K_{B3} = (m_1)^{w_2} \bmod p$. B.11.4 return (K_{B1}, K_{B2}, K_{B3}). B.12 Else break protocol.

Chú ý 1. Theo thuật toán 2 thì $Ver_{DSA}(M_A, (r_A, s_A), y_A)$ ở B.11 hoặc tương tự $Ver_{DSA}(M_B, (r_B, s_B), y_B)$ ở B.11 có thể là "*Reject*". Để tránh lỗi trên, theo chúng tôi các bước 1 và 2 cần viết lại như sau.

Bước 1 (và hoàn toàn tương tự đối với bước 2)

A.1 $v_1, v_2 \in_R [1, q)$ such that $v_1 + v_2 \in [1, q)$.

A.2 $m_1 = g^{v_1} \bmod p$.

A.3 $m_2 = g^{v_2} \bmod p$.

A.4 $r_A = (m_1.m_2 \bmod p) \bmod q$; If $(r_A = 0)$ then goto A.1.

A.5 $h_A = H(m_1 \| m_2)$.

A.6 $v = (v_1 + v_2)^{-1} \bmod q$.

A.7 $s_A = v.(h_A + x_A.r_A) \bmod q$; If $(s_A = 0)$ then goto A.1.

A.8 Send (m_1, m_2, s_A) to B.

3.2. Tấn công vào giao thức của Harn

Đối với giao thức Harn, người tấn công có thể là A hoặc B. Ở đây, chúng tôi chỉ trình bày dưới góc độ A là người tấn công và chỉ cần đảo ngược A với B ta sẽ thu được tấn công còn lại.

Cho u là một ước nào đó của p – 1. Khi này, A muốn tìm giá trị $x_B \bmod u$ sẽ thực hiện qua các giai đoạn sau.

3.2.1. Giai đoạn chuẩn bị

Tìm $\alpha \in GF^*(p)$ sao cho $ord(\alpha) = u$, tính

$$\beta = \alpha^{-1} \bmod p \quad (3)$$

3.2.2. Giai đoạn thực hiện giao thức Harn đối với B

Toàn bộ các bước đối với A được thực hiện như trong giao thức chuẩn, chỉ trừ hai bước A.2 và A.3 sẽ được thay như sau.

$$m_1 = \alpha.g^{v_1} \bmod p \quad (4)$$

$$m_2 = \beta.g^{v_2} \bmod p \quad (5)$$

Với việc làm như trên ta có kết quả sau.

Mệnh đề 1. *Giao thức được thực hiện thành công với sự chấp nhận của cả A lẫn B tuy nhiên, các khóa thỏa thuận của hai người là không như nhau. Cụ thể các khóa do A tính được là*

$$\begin{aligned} K_{A1} &= g^{v_1.w_1} \bmod p, \\ K_{A2} &= g^{v_2.w_2} \bmod p, \\ K_{A3} &= g^{v_1.w_2} \bmod p. \end{aligned} \quad (6)$$

Còn do B tính được là

$$\begin{aligned} K_{B1} &= \alpha^{w_1 \bmod u}.g^{v_1.w_1} \bmod p, \\ K_{B2} &= \beta^{w_2 \bmod u}.g^{v_2.w_2} \bmod p, \\ K_{B3} &= \alpha^{w_1 \bmod u}.g^{v_1.w_2} \bmod p. \end{aligned} \quad (7)$$

Chứng minh

Do B thực hiện hoàn toàn theo giao thức gốc nên việc kiểm tra của A theo các bước A.9, A.10 luôn thỏa mãn điều kiện của A.11 tức là A chấp nhận (n_1, n_2, s_B) là thông báo thỏa thuận của B. Ngược lại, theo A.4, (4), (5) và (3) thì giá trị

$$\begin{aligned} r_A &= (m_1.m_2 \bmod p) \bmod q \\ &= (\alpha.\beta.g^{v_1+v_2} \bmod p) \bmod q \\ &= (g^{v_1+v_2} \bmod p) \bmod q. \end{aligned}$$

Như vậy, (r_A, s_A) chính là chữ ký theo lược đồ DSA do A thực hiện trên thông báo $h = H(m_1||m_2)$ với khóa phiên là $v = (v_1 + v_2) \bmod q$ cho nên hiển nhiên $Ver_{DSA}(h, (r_A, s_A)) = "Accept"$ tức là B cũng chấp nhận (m_1, m_2, s_A) là thông báo thỏa thuận của A.

Từ B.2, B.3, A.11.1, A.11.2 và A.11.3 ta thu ngay được (6).

Ngược lại từ 3.2, 3.3, B.11.1, B.11.2 và B.11.3 ta thu ngay được (7). Mệnh đề đã được chứng minh.■

3.2.3. Giai đoạn tìm x_B

Giai đoạn này được thực hiện với giả thiết B gửi hai bản mã bằng một hệ mật đối xứng nào đó, trong đó, một bản được mã hóa với khóa thỏa thuận K_1 (hoặc K_3) bản còn lại được mã hóa với khóa thỏa thuận K_2. Khi này, A sẽ tìm được khóa mật x_B của B với chi phí tính toán cho trong mệnh đề sau.

Mệnh đề 2. *Với giả thiết như đã nêu ở trên thì A tìm được x_B với chi phí bằng*

$$O\left(max\left\{min\{u, q\}, \sqrt{q/u}\right\}\right) \text{ (phép nhân trên GF(p))} \quad (8)$$

Chứng minh

Giả sử c là bản mã của một thông báo "có nghĩa" được mã hóa với khóa thỏa thuận K_1 (hoặc K_3). Khi này, A có thể giải mã thử với các khóa

$$K_1(j_0) = K_{A1}.\alpha^{j_0} \bmod p \text{ (hoặc } K_3(j_0) = K_{A3}.\alpha^{j_0} \bmod p) \ (j_0 = 0, 1, \ldots)$$

cho đến khi bản giải mã có nghĩa. Từ $j_0 < u$ và $j_0 \le w_1 < q$ nên A đã tìm được $w_1 \bmod u = j_0$ với độ phức tạp là

$$O(\min\{u, q\}) \text{ (phép giải mã)} \quad (9)$$

Do $w_1 = (w_1 \bmod u) + (w_1 \operatorname{div} u).u$ nên để tìm w_1 ta chỉ cần tìm $w_1 \operatorname{div} u$ là đủ. Từ

giá trị đã biết $n_1 = g^{w_1} \bmod p$ được truyền theo bước B.8 ta có

$$n_1 . g^{-(w_1 \bmod u)} \equiv g^{u.(w_1 \operatorname{div} u)} \pmod p \text{ hay}$$

$$n_1 . g^{-(w_1 \bmod u)} \equiv g^{u.(w_1 \operatorname{div} u)} \equiv (g^u)^{(w_1 \operatorname{div} u)} \pmod p.$$

Đồng dư thức trên có nghĩa $w_1 \operatorname{div} u$ chính là logarit của $n_1 . g^{-(w_1 \bmod u)} \bmod p$ theo cơ số $g^u \bmod p$. Từ $w_1 < q$ nên $w_1 \operatorname{div} u < q/u$, theo bổ đề 1 thì chi phi cho việc tìm $w_1 \operatorname{div} u$ sẽ là

$$O\left(\sqrt{q/u}\right) \text{ (phép nhân trên GF(p))} \quad (10)$$

Nếu coi một phép giải mã và phép nhân trong GF(p) có chi phí như nhau, từ (9) và (10) ta có việc tính w_1 có độ phức tạp

$$O\left(\max\left\{\min\{u, q\}, \sqrt{q/u}\right\}\right) \text{ (phép nhân)}$$

Lập luận hoàn toàn tương tự khi một thông báo mật do B gửi cho A nếu dùng khóa thỏa thuận K_2 thì A có thể giải mã thử với các khóa $K_2(j_0) = K_{A2} . \beta\alpha^{j_0} \bmod p$ (j_0 = 0, 1, …) cho đến khi bản giải mã có nghĩa để tìm ra $w_2 \bmod u = j_0$. Tiếp đó, tính $w_2 \operatorname{div} u$, theo bổ đề 1 cần chi phí là $O\left(\sqrt{q/u}\right)$, vậy tổng chi phí cho việc tìm w_2 cũng là $O\left(\max\left\{\min\{u, q\}, \sqrt{q/u}\right\}\right)$.

Như vậy, A đã tính được $w_1 + w_2$ và từ phương trình tính s_B trong bước B.7, A tính được x_B theo công thức

$$x_B = \left(s_B(w_1 + w_2) - H(n_1 || n_2)\right)(r_B)^{-1} \bmod q$$

với chi phí $O((lnq)^3)$.

Do $\max\left\{\min\{u, q\}, \sqrt{q/u}\right\} \geq \sqrt[3]{q}$ (dấu = xảy ra khi $u = \sqrt[3]{q}$) và $\lim_{q\to\infty} \frac{(lnq)^3}{\sqrt[3]{q}} = 0$ nên chi phí cho việc tìm x_B bằng

$$O\left(\max\left\{(lnq)^3, \min\{u, q\}, \sqrt{q/u}\right\}\right) = O\left(\max\left\{\min\{u, q\}, \sqrt{q/u}\right\}\right)$$

Mệnh đề đã được chứng minh.■

4. TẤN CÔNG VÀO GIAO THỨC PHAN

4.1. Giao thức Phan

Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$	
A giữ tham số mật x_A.	B giữ tham số mật x_B.
Bước 1. A tạo và truyền các thông tin thỏa thuận khóa.	
A.1 $v \in_R [1, q)$. A.2 $m_1 = g^v \bmod p$. A.3 $m_2 = (y_A)^v \bmod p$. A.4 Send (m_1, m_2) to B.	
Bước 2. B tạo và truyền các thông tin thỏa thuận khóa; tính cặp khóa chung (K_{B1}, K_{B2}); Chứng minh theo lược đồ chữ ký DSA rằng, mình đã dùng thông tin thỏa thuận khóa là n_1, n_2 và tính được cặp khóa chung (K_{B1}, K_{B2}).	
	B.1 $w \in_R [1, q)$. B.2 $n_1 = g^w \bmod p$. B.3 $n_2 = (y_B)^w \bmod p$. B.4 $r_B = n_1 \bmod q$. B.5 $K_{B2} = (m_1)^{w.x_B} \bmod p$. B.6 $K_{B1} = (m_2)^w \bmod p$.

	B.7 $h = H(n_1 \| \| K_{B2} \| \| K_{B1})$. B.8 $s_B = w^{-1}.(h + x_B.r_B) \bmod q$. B.9 Send (n_1, n_2, s_B) to A.
Bước 3. A tính cặp khóa chung (K_{A1}, K_{A2}) và xác thực B cũng có cặp khóa đó.	
A.5 $K_{A1} = (n_1)^{v.x_A} \bmod p$. A.6 $K_{A2} = (n_2)^v \bmod p$. A.7 $r_B = n_1 \bmod q$. A.8 $h = H(n_1 \| \| K_{A2} \| \| K_{A1})$. A.9 If $Ver_{DSA}(h, r_B, s_B) = "Acept"$ then: A.9.1 $h = H(m_1 \| \| K_{A1} \| \| K_{A2})$. A.9.2 $r_A = m_1 \bmod q$. A.9.3 $s_A = v^{-1}.(h + x_A.r_A) \bmod q$. A.9.4 Send s_A to B. A.10 Else break protocol.	
Bước 4. B xác thực A có cặp khóa chung giống mình.	
	B.7 $r_A = m_1 \bmod q$. B.8 $h = H(m_1 \| \| K_{B1} \| \| K_{B2})$. B.9 If $Ver_{DSA}(h, r_A, s_A) = "Reject"$ then break protocol.

Chú ý 2. Cũng giống như giao thức của Harn, giao thức của Phan cũng mắc lỗi về tạo chữ ký DSA. Tuy nhiên, việc sửa được lỗi cho giao thức của Phan là không đơn giản như của Harn.

- Việc tạo ra $r_A \neq 0$ đối với A là đơn giản, người này chỉ cần thêm vào cuối dòng A.2 lệnh "If ($m_1 \bmod q = 0$) then goto A.1." (Tương tự đối với B). Theo chúng tôi nên thực hiện bổ xung trên.

- Việc tạo $s_A \neq 0$ đối với A cũng như $s_B \neq 0$ đối với B là không luôn luôn thực hiện được vì giá trị này chỉ được tính sau khi có các khóa thỏa thuận K_{B1}, K_{B2} đối với B và K_{A1}, K_{A2} đối với A. Biết rằng điều kiện $s \neq 0$ được đặt ra trong DSA nhằm tránh để lộ khóa mật x từ công thức xác định s. Tuy nhiên, trong giao thức trên công thức xác định s_A lại còn phụ thuộc vào tham số $h = H(m_1 \| \| K_{A1} \| \| K_{A2})$ mà chỉ A và B mới có thể biết cho nên nó sẽ không phải là lỗi trong giao thức. Đến đây, chúng ta cần hiểu: hàm Ver_{DSA} dùng trong giao thức không kiểm tra điều kiện ($s \in [1, q)$) như trong thuật toán 2.■

4.2. Tấn công vào giao thức của Phan

Đối với giao thức Phan, người tấn công là A. Cách thức và chi phí tấn công được nêu trong mệnh đề sau.

Mệnh đề 3

A luôn tính được x_B với chi phí là

$$O\left(lnq.max\{min\{u, q\}, \sqrt{q/u}\}\right) \text{ (phép nhân trong GF(p))} \quad (11)$$

Chứng minh

Tại bước A.3 của mình, A lấy $m_2 = \alpha.(y_A)^v \bmod p$ với ord(α) = u.

Khi này, khóa thỏa thuận K_2 do A và B tính đều như nhau, tức là

$$K_{A2} = K_{B2} = g^{v.w.x_B} \bmod p$$

Trong khi đó, K_{B1} do B ở bước B.6 sẽ là

$$K_{B1} = (m_2)^w \bmod p = (\alpha.(y_A)^v)^w \bmod p = \alpha^w.g^{v.w.x_A} \bmod p$$

còn K_{A1} do A tính ở bước A.5 sẽ là

$$K_{A1} = (n_1)^{v.x_A} \bmod p = g^{v.w.x_A} \bmod p$$

Khi này, sau khi thực hiện đến bước A.7 thì A tiến hành tìm j_0 đầu tiên ($j_0 = 0, 1, ...$) sao cho $Ver_{DSA}(h, r_B, s_B) = "Accept"$ với $h = H(n_1||K_{A2}||\alpha^{j_0}.K_{A1})$. Giá trị j_0 tìm được chính là w mod u. Hiển nhiên, chi phí thêm ra cho việc làm trên là

$O(\min\{u, q\})$ (phép nhân + tính hàm H + tính hàm Ver_{DSA})

Biết rằng hàm Ver_{DSA} cần thực hiện 2 phép lũy thừa modulo p với số mũ không quá q nên chi phí cho việc tính hàm này là $O(ln q)$ phép nhân trong GF(p), còn việc tính hàm H do kích thước đầu vào luôn bằng 3 kích thước của p nên có thể coi như bằng việc tính một số hữu hạn phép nhân vậy biểu thức trên trở thành

$O(ln q.\min\{u, q\})$ (phép nhân trong GF(p))

Tiếp đến, giống như trong chứng minh mệnh đề 2 từ $n_1 = g^w \bmod p$, A tính được w div u với chi phí

$O(\sqrt{q/u})$ (phép nhân trong GF(p))

còn chi phí để tìm x_B từ phương trình tính s_B trong điều kiện biết w là $O((ln q)^3)$.

Tóm lại, chi phí phải tính toán thêm của A để tìm x_B sẽ cho bởi công thức (11) và mệnh đề đã được chứng minh.■

5. TẤN CÔNG VÀO GIAO THỨC CỦA LIU VÀ LI

5.1. Giao thức Liu-Li

<table>
<tr><td colspan="2">Tham số dùng chung: p, q, g, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$</td></tr>
<tr><td>A giữ tham số mật x_A.</td><td>B giữ tham số mật x_B.</td></tr>
<tr><td colspan="2">Bước 1. A tạo và truyền các thông tin thỏa thuận khóa.</td></tr>
<tr><td>A.1 $v_1, v_2 \in_R [1, q)$.
A.2 $m_A = g^{v_1} \bmod p$.
A.3 $n_A = (y_A)^{v_2} \bmod p$.
A.4 Send (m_A, n_A) to B.</td><td></td></tr>
<tr><td colspan="2">Bước 2. B tạo và truyền các thông tin thỏa thuận khóa; tính cặp khóa chung (K_{B1}, K_{B2}); Chứng minh theo lược đồ chữ ký DSA rằng, mình đã dùng thông tin thỏa thuận khóa là m_B, n_B và tính được cặp khóa chung (K_{B1}, K_{B2}).</td></tr>
<tr><td></td><td>B.1 $w_1, w_2 \in_R [1, q)$.
B.2 $m_B = g^{w_1} \bmod p$.
B.3 $n_B = (y_B)^{w_2} \bmod p$.
B.4 $r_B = m_B \bmod q$.
B.5 $K_{B1} = (m_A)^{w_2.x_B} \bmod p$.
B.6 $K_{B2} = (n_A)^{w_1} \bmod p$.
B.7 $h = H(m_B||K_{B1}||K_{B2})$.
B.8 $s_B = w_1^{-1}(h + x_B.r_B) \bmod q$.
B.9 Send (m_B, n_B, s_B) to A.</td></tr>
<tr><td colspan="2">Bước 3. A tính cặp khóa chung (K_{A1}, K_{A2}) và xác thực B cũng có cặp khóa đó.</td></tr>
<tr><td>A.5 $K_{A1} = (m_B)^{v_2.x_A} \bmod p$.
A.6 $K_{A2} = (n_B)^{v_1} \bmod p$.
A.7 $r_B = m_B \bmod q$.
A.8 $M = m_B||K_{A2}||K_{A1}$.
A.9 If $Ver_{DSA}(M, (r_B, s_B)) = "Acept"$ then:</td><td>(khi này ta có:
$K_{A1} = g^{x_A.v_2.w_1} \bmod p = K_{B2}$.
$K_{A2} = g^{x_B.v_1.w_2} \bmod p = K_{B1}$.)</td></tr>
</table>

A.9.1 $h = H(m_A \| K_{A1} \| K_{A2})$. A.9.2 $r_A = m_A \bmod q$. A.9.3 $s_A = v_1^{-1}(h + x_A.r_A) \bmod q$. A.9.4 Send s_A to B. A.9.5 return (K_{A1}, K_{A2}). A.10 Else break protocol.	
Bước 4. B xác thực A có cặp khóa chung giống mình.	
	B.7 $r_A = m_A \bmod q$. B.8 $M = m_A \| K_{B2} \| K_{B1}$. B.9 If $Ver_{DSA}(M, (r_A, s_A)) = "Reject"$ then break protocol. B.10 return (K_{B2}, K_{B1}).

Chú ý 3. Giao thức của Liu và Li cũng gặp phải những tính huống giống như của giao thức của Phan cho nên đối với giao thức này chúng tôi đề nghị:

- Thêm vào cuối dòng A.2 lệnh "If ($m_A \bmod q = 0$) then goto A.1.". Thêm vào cuối dòng A.2 lệnh "If ($m_B \bmod q = 0$) then goto B.1.

- Hàm Ver_{DSA} dùng trong giao thức không kiểm tra điều kiện ($s \in [1,q)$) như trong thuật toán 2.

5.2. Tấn công vào giao thức Liu-Li

5.2.1. Phương pháp tấn công

Để tấn công vào giao thức Liu-Li, A thay giá trị $n_A = (y_B)^{v_2} \bmod p$ bằng $n_A = (y_B)^{v_2}.\beta \bmod p$ tại bước A.3. Với sự thay đổi trên ta có

$$K_{A1} \equiv K_{B2} \pmod p \text{ và } K_{A2}.\beta^{w_2} = K_{B1} \pmod p$$

Với kỹ thuật giống hệt như tấn công đối với giao thức Phan, cụ thể một số bước được sửa đổi như sau

A.8 $M = m_B \| K_{A2} \| K_{A1}$; $j = 0$.

A.9 While ($Ver_{DSA}(M, (r_B, s_B)) = "Acept"$) do:

A.9.1 $K_{A2} \leftarrow K_{A2}.\beta \bmod p$.

A.9.2 $M \leftarrow m_B \| K_{A2} \| K_{A1}$.

A.9.3 $j \leftarrow j + 1$.

A.10 $h = H(m_A \| K_{A1} \| K_{A2})$.

A.11 $r_A = m_A \bmod q$.

A.12 $s_A = v_1^{-1}(h + x_A r_A) \bmod q$.

A.13 Send s_A to B.

A.14 return (j, K_{A1}, K_{A2}).

5.2.2. Chi phí tấn công

Với sửa đổi trên A sẽ thỏa thuận được khóa với B là cặp (K_{A1}, K_{A2}), ngoài ra còn thu được giá trị $j = x_B \bmod u$. Như vậy, với chi phí đưa ra trong (3.10) thì A tìm được x_B.

Mệnh đề 4

Với tấn công theo phương pháp đưa ra trong 4.2.1 thì A luôn tính được x_B với chi phí là

$O(lnq.max\{min\{u, q\}, \sqrt{q/u}\})$ (phép nhân trong GF(p)) ■

6. ĐIỀU KIỆN ĐỦ ĐỂ CHỐNG LẠI TẤN CÔNG CỦA LIM VÀ LEE

Trong mục này, chúng tôi chỉ ra kết quả sau.

Mệnh đề 5

Nếu (p, q, g) là bộ tham số an toàn cho lược đồ chữ ký DSA và thêm vào nữa p thỏa mãn điều kiện sau

Với mọi ước nguyên tố lẻ r của p – 1 đều thỏa mãn

$$r \geq q \tag{12}$$

Thì tấn công Lim-Lee để tìm khóa mật x_B là <u>không thể</u> (theo nghĩa người tấn công không thể thực hiện được trong thời gian thực).

Chứng minh

Biết rằng, trong các ứng dụng mật mã có độ an toàn dựa trên tính khó giải của bài toàn logarit trên GF(p) thì tham số q cần được chọn sao cho việc bài toán logarit rời rạc trên GF(p) là không thể. Trong đó, việc thực hiện $\lceil\sqrt{q}\rceil$ đối với người giải là không thể.

Các tham số khóa mật x_B và khóa phiên k_B luôn được chọn đủ lớn ít nhất là không thể tìm được theo phương pháp vét cạn (việc thực hiện x_B phép toán cơ bản là không thể đối với người giải).

Với điều kiện (12) thì chỉ xảy ra hai khả năng đối với u đó là:

- u = 2. Khi này, theo (4) thì của tấn công Lim-Lee có chi phí là $\lceil\sqrt{q/2}\rceil \approx \lceil\sqrt{q}\rceil$ nên sẽ không thể.

- $u \neq 2$. Theo điều kiện (2) thì $u \geq q$ cho nên $x_B \bmod u = x_B$, vì vậy tấn công Lim-Lee cũng không thể.

Tóm lại, kết luận đã được chứng minh.■

7. KẾT LUẬN

Bài báo đã trình bày tấn công theo phương pháp của Chao Hoom Lim và Pil Joong Lee vào một số giao thức DH-KE, bao gồm các giao thức sau: giao thức HARN, giao thức PHAN, giao thức Liu-Li, đồng thời chúng tôi cũng chỉ ra tính chưa tuân thủ đúng thuật toán tạo chữ ký số của DSA (thiếu bước kiểm tra điều kiện) trong các giao thức trên. Cuối cùng, trong bài báo, chúng tôi cũng trình bày điều kiện đủ cho tham số p để chống lại tấn công Lim-Lee.

TÀI LIỆU THAM KHẢO

[1]. L. Harn. *"Modified Key Agreement Protocol Base on the Digital Signature Standard"*. Electronics Letters, Vol.31(6), 1995, pp. 448-449

[2]. Chao Hoom Lim and Pil Joong Lee. *"A Key Recovery Attack on Discrete Log-based Schemes Using a Prime Order Subgroup"*. EUROCRYPT 1997, pp. 249-263.

[3]. Jie Liu and Jianhua Li. *"A Better Improvement on the Integreated Diffie-Hellman – DSA Key Agreement Protocol"*. IEEE Communications Letters 2010; 11: 114-117.

[4]. Phan, *"Fixing the Integratied Diffie-Hellman DSA Key Exchange Protocol",* IEEE Communications Letters 2005; 9: 570-572.

[5]. C.H.Lim and P.J.Lee, *"Several practical protocols for authentication and key exchange"*, Information Processing Letters, 53, 1995, pp.91-96.

[6]. T.Matsumoto, Y.Takashima and H.Imai, *"On seeking smart public-key distribution systems"*, The Transactions of the [EICE of Japan, E69, 1986, pp.99-106.

ABSTRACT

LIM-LEE'S ATTACK ON PROTOCOLS DH-KE ON GF(p)

The article describes attacks by the Lim-Lee method on protocols DH-KE on GF(p) such as the attack on HARN protocol, PHAN protocol, Liu-Li protocol. In the article, we also point out compliance incorrect with DSA algorithm in the protocols above. The article shows condition against Lim-Lee's attack.

Keywords: Protocol DH-KE on GF(p); Lim-Lee's attack.

Nhận bài ngày 19 tháng 3 năm 2020
Hoàn thiện ngày 26 tháng 4 năm 2020
Chấp nhận đăng ngày 12 tháng 6 năm 2020

Địa chỉ: [1]Cục Quản lý mật mã dân sự và kiểm định sản phẩm mật mã, Ban Cơ yếu chính phủ;
[2]Học viện Kỹ thuật mật mã, Ban Cơ yếu chính phủ.
*Email: vuphongthanhson@gmail.com.