情報保護學會論文誌
第16卷 第6號, 2006. 12

Yong-Lee의 익명 핑거프린팅 프로토콜의 안전성 취약점 및 개선 방안

손 기 욱,[1†] 이 윤 호,[2] 원 동 호[2‡]

[1]국가보안기술연구소, [2]성균관대학교 정보통신공학부 정보보호연구소

Weakness and Improvements of Yong-Lee's Anonymous Fingerprinting Protocol

Kiwook Sohn,[1†] Yunho Lee,[2] Dongho Won[2‡]

[1]National Security Research Institute
[2]Information Security Group School of Information and Communication Engineering Sungkyunkwan University

요 약

2005년, Yong과 Lee는 buyer-seller 핑거프린팅 프로토콜을 제안하면서, 대칭(symmetric) 암호계와 가환(commutative) 암호계를 이용하기 때문에 속도가 빠르고 익명성을 갖는다고 주장한 바 있다. 그러나 이 방식은 공격자가 man-in-the-middle 방법을 이용하여 공격할 경우 정당한 사용자의 핑거프린트가 포함된 콘텐츠를 얻을 수 있는 문제가 있다. 본 논문에서는 Yong-Lee 방식의 안전성 취약점을 살펴보고 이를 막을 수 있는 방안을 제시한다.

ABSTRACT

In 2005, Yong and Lee proposed a buyer-seller fingerprinting protocol using symmetric and commutative encryptions. They claimed that their protocol was practical and anonymous since they used symmetric and commutative encryptions. However, an attacker can get the content embedded with one or more honest buyers' fingerprints using man-in-the-middle attack. In this letter, we point out the weakness and propose methods for improving to their protocol.

Keywords : *Fingerprinting, Anonymous Buyer-Seller Protocol, Watermarking, Man-in-the-middle Attack*

Ⅰ. 서 론

2005년 Yong과 Lee는 대칭 암호계 및 가환 암호계를 기반으로 하는 핑거프린팅 프로토콜을 제안하였다[1]. 이 방식은 이전 방식[3],[4]과는 달리 대칭키 암호방식을 이용하여 콘텐츠를 암호화하기 때문에 속도가 빠르다는 장점이 있다. 또한, 대칭키 암호방식을 위한 비밀키는 가환 암호계를 이용하여 전달하도록 하고 있다.

본 논문에서는 Yong-Lee 방식의 안전성 취약점을 살펴보고, 이를 해결하기 위한 몇가지 방안을 제시하도록 한다.

접수일: 2006년 7월 4일 : 채택일: 2006년 10월 25일
† 주저자, kiwook@etri.re.kr
‡ 교신저자, dhwon@security.re.kr

Ⅱ. Yong-Lee의 핑거프린팅 프로토콜

Yong-Lee 프로토콜의 참여자는 다음과 같다. B와 CP는 각각 구매자와 판매자를 의미하며 RC는 신뢰할 수 있는 등록기관 그리고 J는 재판관을 나타낸다.

2.1 용어

- $item$: 핑거프린팅할 디지털 콘텐츠 원본
- $\oplus$: exclusive-OR 연산
- SE, SE^{-1}: 대칭키 암호화, 복호화
- CE, CE^{-1}: 가환 암호화, 복호화
- E: 공개키 암호방식
- H: 단방향 해쉬 함수

2.2 가환 암호방식(Commutative Encryption)

키를 k, 메시지를 m이라고 했을 때 암호계 $CE(k,m)$은 다음 조건을 만족할 때 가환성을 갖는다고 한다.

$$c = CE(k_1,(CE(k_2,m))) = CE(k_2,(CE(k_1,m)))$$

즉, 두 개의 키 k_1,k_2를 이용하여 연속적으로 암호화한 결과 c는 k_1,k_2 순서와 무관하게 $CE^{-1}(k_1,CE^{-1}(k_2,c))$나 $CE^{-1}(k_2,CE^{-1}(k_1,c))$로 복호화할 수 있다. Yong-Lee 방식에 사용할 수 있는 가환 암호계는 [2]에서 제안한 방식 등이 사용될 수 있다. 단, 스트림 암호방식도 가환 암호계에 속하지만 Yong-Lee 방식에는 적용할 수 없다.

2.3 등록 절차

B와 RC는 모두 각자의 공개키, 개인키 쌍을 가지고 있다. B의 개인키를 x_B라고 했을 때 공개키 $y_B = g^{x_B}$이다. RC는 자신의 개인키를 이용하여 인증서를 발급하며, 발급된 인증서는 RC의 공개키를 이용하여 검증할 수 있다. 등록과정은 다음과 같다.

① B는 $x_1 + x_2 = x_B$를 만족하는 $x_1, x_2 \in_R Z_p$를 선택하여 $(y_B, y_1 = g^{x_1}, E_{RC}(x_2))$를 RC로 전송한다.

② RC는 전송받은 데이터를 이용하여 $y_1 g^{x_2} = y_B$가 만족하는지 확인하고 y_1에 대한 인증서 $Cert(y_1)$을 발급한다.

2.4 익명 핑거프린팅 프로토콜

B는 $y_1, Cert(y_1)$을 CP에게 전송하면서 디지털 콘텐츠 $item$을 요청한다. CP는 요청 접수와 함께 $Cert(y_1)$을 검증한 후 B의 핑거프린트 두 개 F_B^0, F_B^1 및 $item$과 동일한 사본 두 개 $item^0$, $item^1$을 생성한다.

콘텐츠 암호화

CP는 $item^0$와 $item^1$을 각각 t 개의 프레임으로 분할한 후 F_B^0, F_B^1를 삽입한다.

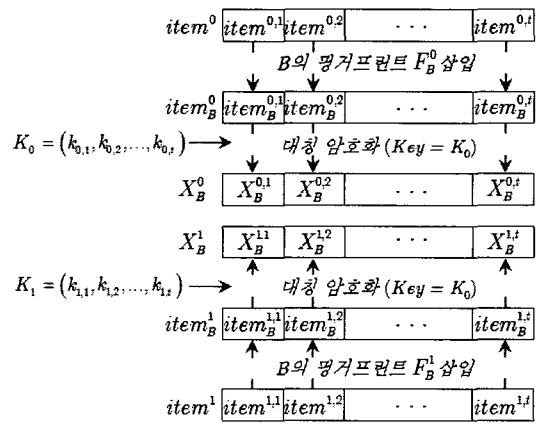
$$item_B^0 = (item^{0,1} \oplus F_B^0, ..., item^{0,t} \oplus F_B^0) \quad (1)$$

$$item_B^1 = (item^{1,1} \oplus F_B^1, ..., item^{1,t} \oplus F_B^1) \quad (2)$$

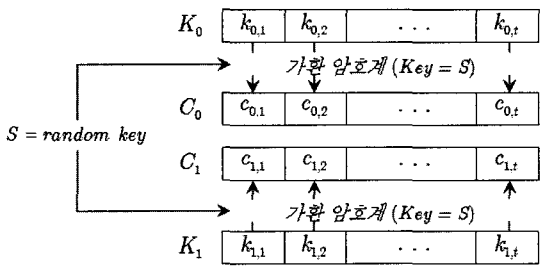
그런 후 두 개의 비밀키 벡터 $K_0 = (k_{0,1}, ..., k_{0,t})$, $K_1 = (k_{1,1}, ..., k_{1,t})$을 생성하여 $item_B^i$를 구성하는 $2t$ 개의 프레임 각각을 다음 식 (3),(4)와 같이 암호화하고 X_B^0, X_B^1를 B에게 전송한다([그림 1] 참조).

$$X_B^0 = (SE(k_{0,1}, item_B^{0,1}), ..., SE(k_{0,t}, item_B^{0,t})) \quad (3)$$

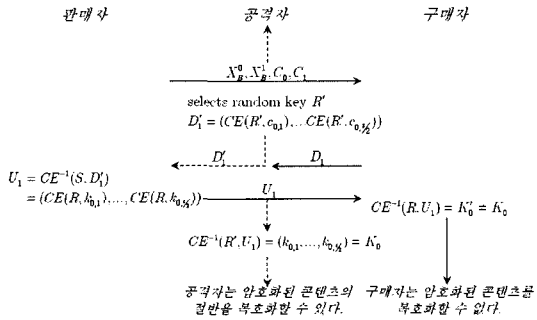
$$X_B^1 = (SE(k_{1,1}, item_B^{1,1}), ..., SE(k_{1,t}, item_B^{1,t})) \quad (4)$$



[그림 1] 핑거프린트가 삽입된 콘텐츠의 암호화



〔그림 2〕 콘텐츠 암호화 키의 암호화



〔그림 3〕 Man-in-the-middle 공격법을 이용한 공격

키벡터 암호화

CP는 임의의 비밀키 S를 정하고 가환암호계 CE를 이용하여 두 개의 키벡터 K_i를 다음과 같이 암호화한 후 C_0, C_1을 B에게 전송한다(〔그림 2〕 참조).

$$C_0 = (c_{0,1}, \ldots, c_{0,t}),\ c_{0,j} = CE(S, k_{0,j}) \quad (3)$$

$$C_1 = (c_{1,1}, \ldots, c_{1,t}),\ c_{1,j} = CE(S, k_{1,j}) \quad (4)$$

Buyer-Seller 프로토콜

구매자-판매자 프로토콜은 다음과 같이 진행된다.

① B는 임의의 비트열 $L_B = (l_1, \ldots, l_t),\ l_i = 0,1$과 임의의 비밀키 R을 선택한다.

② B는 C_0, C_1으로부터 $C' = (c_{l_1,1}, \ldots, c_{l_t,t})$을 생성한다.

③ B는 비밀키 R과 가환암호계 CE를 이용하여 C'을 암호화하고 이를 두 벡터로 분할한 $D_1 = (d_1, \ldots, d_{t/2})$과 $D_2 = (d_{(t/2)+1}, \ldots, d_t)$를 CP에게 전송한다. 단, $d_i = CE(R, c_{l_i,i})$이다.

④ CP는 자신이 선택한 임의의 비밀키 S를 이용하여 D_1을 복호화한 결과 $U_1 = CE^{-1}(S, D_1)$을 계산하고 이를 B에게 전송한다.

⑤ B는 자신의 비밀키 R로 U_1을 복호화하면 $t/2$개의 복호화 키를 얻게 된다.

⑥ B는 J의 공개키로 L_B를 암호화한 결과 $T_B = E_J(L_B)$ 및 서명값 $P_B = Sign(T_B)$를 CP에게 전송한다.

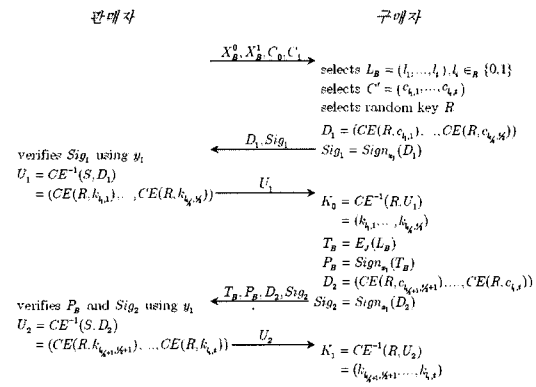
⑦ B는 D_2를 CP에게 전송한다.

⑧ CP는 B의 익명 공개키 y_1을 이용하여 서명을 검증하고, 자신의 비밀키 S를 이용하여 D_2를 복호화한 값 $U_2 = CE^{-1}(S, D_2)$를 계산하여 B에게 전송한다.

⑨ B는 U_2를 복호화하여 암호화된 콘텐츠 X_B^0, X_B^1을 복호화하는데 필요한 모든 비밀키를 얻을 수 있다.

Ⅲ. Yong-Lee 방식의 안전성 취약점

공격자 M은 잘 알려진 man-in-the-middle 공격법을 이용하여 1 명 이상의 정당한 구매자의 핑거프린트가 삽입된 콘텐츠를 가로챌 수 있다.



〔그림 4〕 세 번째 방법을 이용하여 개선된 프로토콜

암호화된 콘텐츠 X_B^0, X_B^1과 암호화된 비밀키 C_0, C_1은 공중통신망을 통해 전송되기 때문에 공격자도 쉽게 얻을 수 있다. 이후 공격자는 임의의 비밀키

R'을 선택하여 임의의 $j \in 0,1$에 대해 $D_1' = CE(R', C_j)$을 계산하여 정당한 구매자가 전송하는 D_1 대신 CP에게 전송한다.

CP는 D_1과 D_1'을 구별할 수 없기 때문에 자신의 비밀키 S로 복호화하여 다시 전송한다. 이렇게 복호화된 결과 $U_1' = CE^{-1}(S, D_1')$도 공중 통신망을 통해 전송되므로 공격자도 쉽게 얻을 수 있고, 공격자는 자신이 선택한 임의의 키 R'을 이용하여 복호화하면 전체 콘텐츠의 절반을 복호화할 수 있는 비밀키 $K_j = CE^{-1}(R', U_1)$를 구할 수 있다. 이러한 공격을 최소 2번 반복하면 다른 정상 사용자들의 핑거프린트가 삽입된 콘텐츠를 얻을 수 있게 된다. 공격과정은 [그림 3]과 같다.

Ⅳ. 개선 방안

이 문제를 해결하는 방법은 크게 두가지로 생각할 수 있다. 하나는 CP가 D_1, D_2의 송신자를 확인할 수 있도록 하는 것이고 다른 하나는 정당한 구매자 B만 C_1, C_2를 얻을 수 있게 하는 것이다. 해결 방법은 다음과 같다.

Method 1

CP는 U_1, U_2를 B의 익명 공개키 y_1으로 암호화하여 전송한다.

Method 2

CP는 임의의 치환벡터 p를 이용하여 C_0, C_1을 치환하고, 프로토콜이 종료되었을 때 B의 익명 공개키 y_1으로 p를 암호화하여 전송한다.

Method 3

B는 D_1, D_2를 전송할 때 자신의 익명 개인키 x_1을 이용하여 D_1, D_2에 대한 서명을 추가하여 전송한다.

첫 번째 방법은 공개키 암호화/복호화 연산이 많아지는 단점이 있고 두 번째 방법은 콘텐츠의 길이 t에 따라 안전성이 결정되는 단점이 있어 세 번째 방법이 가장 적합하다고 할 수 있다.

[표 1]은 세가지 방법을 비교한 것이고, [그림 4]는 세 번째 방법을 이용한 개선된 프로토콜을 나타냈다.

[표 1] 개선 방안 비교

연산	방법1	방법2	방법3
공개키 연산	t	1	0
전자 서명	0	0	2
치환	0	1	0

Ⅴ. 결 론

Yong-Lee의 익명 핑거프린팅 프로토콜은 대칭키 암호계와 가환 암호계를 이용하여 속도가 빠르다는 장점이 있지만 man-in-the-middle 공격에 취약하다. 이러한 문제점은 구매자의 익명 공개키를 이용한 암호화 또는 익명 개인키를 이용한 전자 서명을 적용함으로써 간단하게 해결할 수 있다.

참 고 문 헌

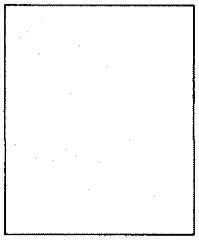
[1] S.Yong and S.Lee, "An Efficient Fingerprinting Scheme with Symmetric and Commutative Encryption," IWDW 2005, LNCS 3710, pages 54-66, 2005.

[2] F.Bao, R.H.Deng and P.Feng, "An Efficient and Practical Scheme for Privacy Protection in the E-Commerce of Digital Goods," ICICS' 00, LNCS 2836, pages 162-170, 2001.

[3] C.C.Chang and C.Y.Chung, "An Enhanced Buyer-Seller Watermarking Protocol," Proc. of ICCT 2003, pages 1779-1783, 2003.

[4] J.G.Choi, J.H.Park and K.R.Kwon, "Analysis of COT-based Fingerprinting Schemes: New Approach to Design Practical and Secure Fingerprinting Scheme," IHW 2004, LNCS 3200, pages 253-265, 2004.

〈著者紹介〉



손 기 욱 (Kiwook Sohn)
1990년 2월 : 성균관대학교 정보공학과(공학사)
1992년 2월 : 성균관대학교 대학원 정보공학과(공학석사)
2002년 2월 : 성균관대학교 대학원 전기전자컴퓨터공학부(공학박사)
1992년 3월-1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월-현재 : 국가보안기술연구소 선임연구원
관심분야 : 사이버위협대응기술, 키관리기술

이 윤 호 (Yunho Lee)
1991년 2월 : 성균관대학교 정보공학과(공학사)
1993년 2월 : 성균관대학교 대학원 정보공학과(공학석사)
1993년 3월-2000년 4월 : 한국통신 연구개발본부 전임연구원
2000년 5월-2005년 1월 : KBS인터넷(주) 기술지원팀장
2005년 3월-현재 : 성균관대학교 컴퓨터공학과 박사과정 재학중
2006년 6월-현재 : (주)애니온소프트 기술이사
〈관심분야〉 암호이론, 정보보호 응용, 전자투표, 워터마킹

원 동 호 (Dongho Won)
1976년-1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 : 한국전자통신연구원 전임연구원
1985년-1986년 : 일본 동경공업대 객원연구원
1988년-2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 : 국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
〈관심분야〉 암호이론, 정보이론, 정보보호