情報保護學會論文誌
第18卷 第5號, 2008. 10

Nakazato-Wang-Yamamura '07의 프라이버시가 강화된 크레덴셜 시스템에 대한 크레덴셜 위조 공격*

양 대 헌[1†], 이 경 희[2‡]
[1]인하대학교 정보통신대학원, [2]수원대학교 전기공학과

Credential Forging Attack against Privacy Enhancing Credential System in Nakazato-Wang-Yamamura '07*

DaeHun Nyang[1†], KyungHee Lee[2‡]
[1]The Graduate School of Information Tech & Telecomm, InHa University
[2]Department of Electrical Engineering, The University of Suwon

요 약

이 논문에서는 ASIAN 2007에서 Nakazato, Wang, Yamamura 등이 발표한 프라이버시가 강화된 크레덴셜 시스템에서 크레덴셜 발급자인 서버의 도움 없이도 사용자와 검증자가 공모하는 경우에 크레덴셜을 위조할수 있음을 보인다. 이 공격은 크레덴셜의 생성과정에서 사용하는 서버의 비밀키를 겹선형 사상의 성질을 이용해서 우회하는 방법을 이용한다. 또한, 이 공격방법의 이론적인 영향과 실질적인 영향을 고찰해 본다.

ABSTRACT

We present an attack which forges a credential without the help of the credential issuer in the protocol designed by Nakazato, Wang and Yamamura at ASIAN 2007. The attack avoids using the credential issuer's private key by taking advantage of the property of bilinear pairing. Implication of this collusion attack by user and verifiers also discussed.

Keywords : Cryptanalysis, Anonymity, Credential, Bilinear Pairing

Ⅰ. 서 론

인터넷 등 통신기술의 발전에 따라 프라이버시 보호에 대한 관심이 증가하고 있다. 네트워크에서 사용자의 프라이버시 보호를 위해서는 여러 가지 조건들이 요구되며 주로 익명 채널, 익명 크레덴셜 시스템(또는 Pseudonym 시스템), 그룹 서명 및 링 서명과 같은 분야에서 프라이버시 보호를 위한 연구가 이루어지고 있다.

접수일 : 2008년 7월 1일; 수정일 : 2008년 9월 11일;
채택일 : 2008년 10월 7일
*본 연구는 정보통신부 및 정부통신연구 진흥원의 IT신성장 동력 핵심기술 개발 사업의 일환으로 수행하였음. (2008-F-036-01, 익명성 기반의 U-지식 정보보호 기술 개발) (KRF-2004-015-D00389)
† 주저자, nyang@inha.ac.kr
‡ 교신저자, khlee@suwon.ac.kr

이 중 이 논문에서 다루고자 하는 주제는 익명 크레덴셜 시스템으로, 1985년 David Chaum에 의해 처음 소개 되었다. 이후 [1-5] 등에서 다양한 연구 결과를 내놓고 있다. 익명 크레덴셜 시스템은 보통 기관, 사용자로 구성 되는데, 이때 사용자는 가명(Pseudonym)이라는 것으로 인식된다. 다른 기관에서는 다른 가명을 사용하므로 기관간의 공모 등에 의해서 사용자를 식별할 수 없다. 또한, 어떤 특별한 한 기관은 가명으로 동작하는 사용자가 자신이 정당한 사용자임을 증명하기 위해 사용하는 크레덴셜을 발급하게 되는데, 사용자는 이 크레덴셜을 직접 보여주지 않고 단지 크레덴셜의 소유여부만을 영지식 증명으로 증명함으로써 다른 기관 또는 같은 기관에 있는 자신의 권한을 획득하게 된다. 익명 크레덴셜의 요구사항은 매우 다양한데, 이 논문의 주제와 관련되어서 그 중 몇 가지를 나열해 보면 다음과 같다.

- 익명성(anonymity) : 크레덴셜이나 이의 소유에 대한 증명과정에서 사용자의 신원을 알 수 없어야 한다.
- 위조불가능(unforgeability) : 발급기관 이외에 크레덴셜을 발급할 수 없어야 한다.
- 연결불능성(unlinkability) : 사용자는 매 트랜잭션마다 다른 가명을 사용하게 되는데, 이때 이들 가명이 같은 사용자의 가명인지 알 수 없어야 한다.
- 변환가능성(Transferability) : 한 기관에서 발급한 익명 크레덴셜을 다른 기관에서 사용할 수 있도록 사용자 스스로 변형할 수 있어야 한다.

2007년 ASIAN 2007 학술대회에서 J. Nakazato, L. Wang, A. Yamamura등은 "Privacy Enhancing Credentials"라는 제목의 논문에서 겹선형 사상을 이용한 새로운 크레덴셜 시스템을 제안했다.[1] 이 논문에서는 NWY07 프로토콜에서 크레덴셜 발급자 없이 사용자와 검증자가 공모함으로써 정당한 크레덴셜을 발급할 수 있음을 보이고, 이 공격의 의미를 짚어 본다.

Ⅱ. NWY07 프로토콜 리뷰

이 논문에서는 다음과 같은 표기법을 사용한다.

$\mathbb{G}_1$: 위수로 큰 소수 q를 갖는 덧셈군
$\mathbb{G}_2$: 위수로 큰 소수 q를 갖는 곱셈군
P : $\mathbb{G}_1$ 의 생성자, $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$

겹선형 사상 $\hat{e}()$은 다음과 같은 성질을 만족해야 한다.

- Bilinear : 주어진 모든 $Q, R \in \mathbb{G}_1$ 과 $a, b \in \mathbb{Z}_q$ 에 대해서,
- Non-degenerate : $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$
- Computable : 모든 $Q, R \in \mathbb{G}_1$ 에 대해서 $\hat{e}(Q, R)$의 계산은 쉬워야 한다.

프로토콜에 대한 자세한 설명은 NWY07을 참조하기 바란다[1].

2.1 시스템 매개 변수 및 키 설정

모든 사용자와 기관이 공유하는 시스템 매개 변수는 다음과 같다 : $(\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, Q, F, H(\bullet))$, 여기서 P, Q, F: $\mathbb{G}_1$의 non-trivial elements 이고, H: $0,1^* \rightarrow \mathbb{G}_1$인 해시 함수이다.

크레덴셜 발급자 S, 사용자 U, 검증자 V_j 의 공개키/비밀키 쌍은 각각 다음과 같다 :

$(x_S, R_S), (x_U, x_U), (x_j, R_j)(j = 1, \cdots, n)$, 여기서 $R_S = x_S P$, $R_U = x_U P$, $R_j = x_j P$이고 비밀키 x_S, x_U, x_j은 $\mathbb{Z}_q^*$에서 랜덤하게 선택한다. 따라서 공개키들은 모두 $\mathbb{G}_1$의 원소가 된다.

2.2 크레덴셜 발급 및 사용 프로토콜

크레덴셜을 발급 받기 위해 사용자는 $(X = x_U Q, U)$를 서버에게 전송하고 서버는 [그림 1]에서와 같이 (S, I)를 크레덴셜로 사용자에게 전송한다.

발급 받은 크레덴셜을 이용해서 서비스 요청을 하기위해 사용자는 크레덴셜을 이용해 티켓이라는 것을 만들게 되는데, 이를 생성하는 방법은 [그림 2]에서와 같다.

크레덴셜을 이용해 생성한 티켓으로 서비스 권한을 획득한 뒤, 사용자와 검증자는 [그림 3]에서와 같이 키 교환을 수행하고 여기서 얻은 키 K를 이용해 이후의 트랜잭션을 보호하게 된다.

Ⅲ. 크레덴셜 생성을 위한 공모 공격

NWY07에서는 다음과 같이 크레덴셜의 위조불가능성(Unforgeability)을 정의하고 있으며, 자신들의 프로토

콜에서 크레덴셜의 위조는 불가능하다고 언급했다.[1]

"Unforgeability : Nobody can forge a valid credential to generate a valid ticket with V_j without collaboration with S"

이 절에서는 위의 위조 불가능성이 이 프로토콜에서는 만족되지 않음을 V_j와 U가 또는 V_i와 V_j가 공모해서 S의 도움 없이 V_j가 유효한 크레덴셜을 만들어 낼 수 있음을 보임으로써 증명한다.

3.1 위조 크레덴셜 생성

이제 S의 도움 없이 유효한 크레덴셜을 만들어 내는 알고리즘을 A라 하자. V_j는 알고리즘 A를 실행하고 이의 결과로 유효한 크레덴셜을 출력한다.

알고리즘 A

Input : 시스템 매개 변수들, S, U, V_j의 공개키들, V_j의 비밀키 x_j (V_j가 실행하므로 접근 가능)
Output : 위조한 크레덴셜 (Y_1, Y_2, W_j, j)
Begin
1. 공모한 사용자 또는 공모한 다른 검증자 V_i로부터 ($X = x_U Q$, U) 수신
2. $b \in \mathbb{Z}_q^*$에서 랜덤하게 선택
3. $Y_1 = b(X + F)$
4. $Y_2 = b^{-1} R_S$
5. $W_j = b^{-1} x_j R_S$
6. Output (Y_1, Y_2, W_j, j)
End

위의 공모를 위해 사용자가 자신의 비밀키를 노출 시킬 필요는 없다. 또한, V_j는 크레덴셜 발급자 S의 비밀을 이용하지 않았음을 알 수 있다. 이제 이렇게 위조된 크레덴셜이 유효한 크레덴셜인지 확인해 보자. 먼저 사용자는 [그림 1]의 발급 프로토콜에 따르면 이 크레덴셜의 진위여부를 다음과 같이 시험한다.

1 : $\hat{e}(Y_1, Y_2) \stackrel{?}{=} \hat{e}(X+F, R_S)$
2 : $\hat{e}(W_j, P) \stackrel{?}{=} \hat{e}(R_j, Y_2)$

각각의 확인 과정에 위조한 크레덴셜을 대입해 보면 다음과 같다.

$$1 : \hat{e}(Y_1, Y_2) = \hat{e}(b(X+F), b^{-1} R_S) = \hat{e}(X+F, R_S)^{b(1/b)} = \hat{e}(X+F, R_S)$$

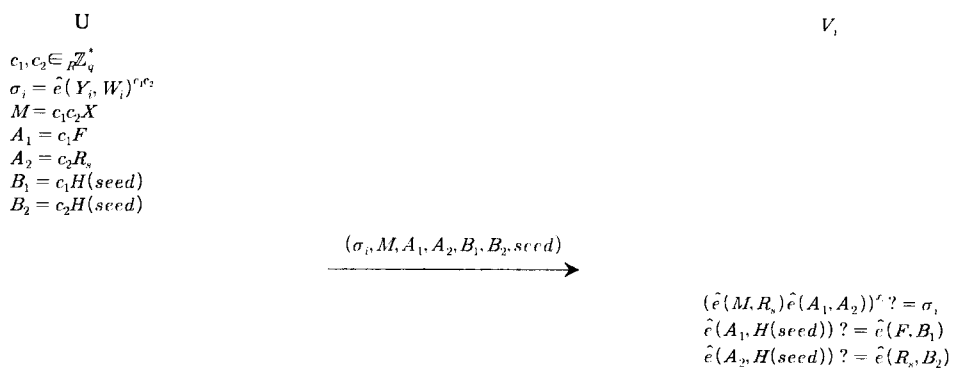
$$2 : \hat{e}(W_j, P) = \hat{e}(b^{-1} x_j R_S, P) = \hat{e}(x_j R_S, b^{-1} P)$$
$$= \hat{e}(x_j x_S P, b^{-1} P) = \hat{e}(x_S x_j P, b^{-1} P)$$
$$= \hat{e}(x_S R_j, b^{-1} P) = \hat{e}(R_j, b^{-1} x_S P)$$
$$= \hat{e}(R_j, b^{-1} R_S) = \hat{e}(R_j, Y_2)$$

따라서 유효한 크레덴셜로 인정받을 수 있게 된다.

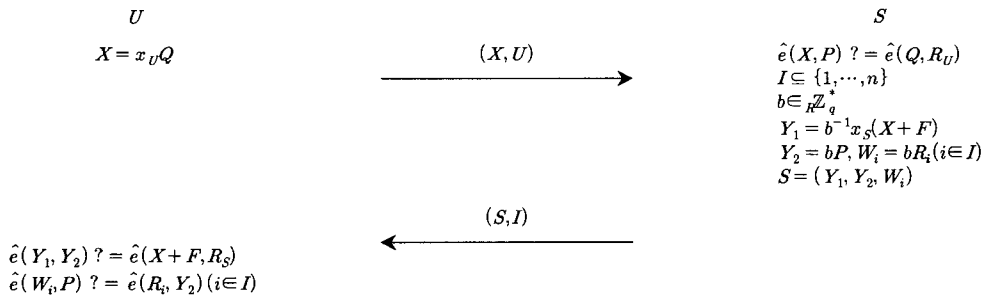
3.2 위조한 크레덴셜을 이용한 서비스 요청

이제 이 크레덴셜이 [그림 2]의 프로토콜을 이용한 서비스 요청에 통과할 수 있는지 살펴보자.

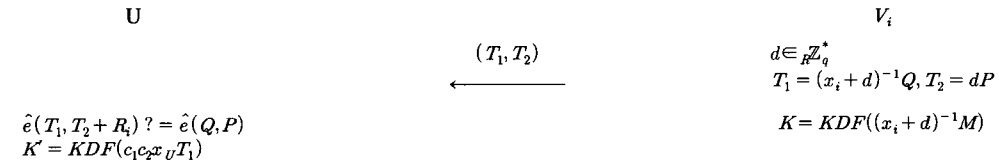
[그림 2]의 프로토콜에서 사용자는 위조한 크레덴셜의 일부인 Y_1과 W_j를 이용해서 서비스를 [그림 2]에서와 같이 요청하게 되고, 검증자 V_j는 다음의 세 가지가 같은지 확인 한다.



[그림 1] 티켓 생성 프로토콜



〔그림 2〕 크레덴셜 발급 프로토콜



〔그림 3〕 키 교환 프로토콜

1 : $(\hat{e}(M, R_S)\hat{e}(A_1, A_2))^{x_j} ? = \sigma_j$

2 : $\hat{e}(A_1, H(seed)) ? = \hat{e}(F, B_1)$

3 : $\hat{e}(A_2, H(seed)) ? = \hat{e}(R_S, B_2)$

위의 세 가지 식 중 2번, 3번은 위조한 크레덴셜과 관련이 없으므로, 항상 통과한다. 다만 1번의 시험에는 위조한 크레덴셜로 만든 티켓 $(\sigma_j, M, A_1, A_2, B_1, B_2)$을 사용하므로 확인해 보아야 하는데, 이를 위 식에 대입해 보면 다음과 같다.

$$
\begin{aligned}
1 : & (\hat{e}(M, R_S)\hat{e}(A_1, A_2))^{x_j} \\
&= (\hat{e}(c_1 c_2 X, R_S)\hat{e}(c_1 F, c_2 R_S))^{x_j} \\
&= (\hat{e}(X, R_S)\hat{e}(F, R_S))^{c_1 c_2 x_j} \\
&= \hat{e}(X+F, R_S)^{c_1 c_2 x_j} \\
&= \hat{e}((X+F), x_j R_S)^{c_1 c_2} \\
&= \hat{e}(b(X+F), b^{-1} x_j R_S)^{c_1 c_2} \\
&= \hat{e}(Y_1, W_j)^{c_1 c_2} = \sigma_j
\end{aligned}
$$

마지막으로 [그림 3]의 키 교환 과정이 남아있지만, 이 과정에서도 크레덴셜을 이용하지 않으므로 항상 통과하게 된다.

Ⅳ. 공격의 의미

이론적인 관점에서의 의미와 실용적인 관점에서의 의미로 나누어 살펴볼 수 있다. 이론적인 관점에서는 앞서 언급한 것처럼, 저자들이 주장하는 위조불가능성은 성립하지 않으며, 일반적으로도 크레덴셜을 발급하는 기관도 모르게 유효한 크레덴셜이 발급될 수 있다는 것은 커다란 문제라고 할 수 있다. 또한, 분쟁이 생겼을 때 위조한 크레덴셜과 진짜 크레덴셜이 구별 불가능하다고 할 수 있으며, 이는 분쟁 해결이 불가능함을 의미한다. 예를 들어, 사용자와 쇼핑몰이 공모해서 위조 크레덴셜을 만든 후 쇼핑몰이 이 크레덴셜로 인해 피해를 입었다고 주장하여 크레덴셜 발급기관에 소송을 걸 수 있을 것이다.

검증자가 발급하는 위조 크레덴셜이 자신에게 쓰이는 크레덴셜임을 감안한다면, 실용적으로 보았을 때 매우 위협적인 공격이 아닐 수도 있을 것이다. 하지만, 위의 프로토콜이 다양한 비즈니스 모델에서 이용될 수 있음을 고려한다면 의미 있는 공격으로 이용될 수도 있을 것이다. 한 가지 예를 들어 보면, 크레덴셜을 발급하는 S는 일종의 익명 선불카드사가 될 수 있고, 검증자는 S에서 발행하는 선불카드를 처리해서 지불 받을 수 있는 쇼핑몰이 될 수 있다. 선불 카드사는 자신의 선불카드 사용을 장려하기 위해서 쇼핑몰에서 해당 선불카드로 결제한 기록을 제출하면 장려금을 주는 비즈니스 모델을 생각할 수 있다. 이때 쇼핑몰은 사용자와 공모하여 크레덴셜을 위조하고(사용자에게 장려금의 일부를 돌려주는 조건으로) 이를 증거로 선불 카드사에 장려금을 요청할 수 있을 것이다. 선불 카드사가 사용자로 부터

얻을 수 있는 최대한은 익명 크레덴셜이지만, 이는 진짜 크레덴셜과 구별 불가능하므로 분쟁의 해결이 쉽지 않게 된다. 이 외에도 프로토콜이 가져야 하는 기본적인 성질 즉, 위조불가능성이 만족되지 않음으로 인해 발생할 수 있는 문제는 비지니스 모델에 따라 더 있을 것으로 생각한다.

V. 결 론

이 논문에서는 사용자로부터 사용자의 비밀키가 아닌 비밀키에 대한 일종의 commitment 값인 $X_U Q$를 얻은 검증자가 스스로 크레덴셜을 발급할 수 있음을 보임으로써 NWY07에서 주장하는 위조불가능성이 만족되지 않고 있음을 보였다. 또한, 이렇게 발행한 크레덴셜을 이용한 서비스 요청이 유효함을 보였고, 이 공격이 가지는 의미를 이론적인 면과 실용적인 면에서 고찰해 보았다. 향후에는 많은 추가 비용이 없이 이 공격을 피할 수 있는 방법을 연구할 예정이다.

참고문헌

[1] Junji Nakazato, Lihua Wang and Akihiro Yamamura, "Privacy Enhancing Credentials", ASIAN 2007, LNCS 4846, pp. 55-61, 2007.

[2] David Chaum, Security without identification : transaction systems to make big brother obsolete, Communications of the ACM 28 (1985), no. 10.

[3] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf, Pseudonym systems, Selected Areas in Cryptography (Howard M. Heys and Carlisle M. Adams, eds.), Lecture Notes in Computer Science, vol. 1758, Springer, 2000.

[4] Jan Camenisch and Anna Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, EUROCRYPT (Birgit Pfitzmann, ed.), Lecture Notes in Computer Science, vol. 2045, Springer, 2001.

[5] Jan Camenisch and Anna Lysyanskaya, Dynamic accumulators and application to efficient revocation of anonymous credentials, CRYPTO (Moti Yung, ed.), Lecture Notes in Computer Science, vol. 2442, Springer, 2002.

〈著者紹介〉

양 대 헌 (DaeHun Nyang) 정회원

1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 정보통신대학원 조교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희 (KyungHee Lee)

1993년 2월 : 연세대학교 컴퓨터과학과 학사
1998년 8월 : 연세대학교 컴퓨터과학과 석사
2004년 2월 : 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월 : LG소프트(주) 연구원
2000년 12월~2005년 2월 : 한국전자통신연구원 선임연구원
2005년 3월~현재 : 수원대학교 조교수
<관심분야> 생체인식, 정보보호, 컴퓨터비젼, 인공지능, 패턴인식