情報保護學會論文誌
第17卷 第1號, 2007. 2

새로운 인증-암호화 모드 NAE에 대한 위조 공격*

정기태,[1†] 이창훈,[1] 성재철,[2] 홍석희,[1‡] 은희천[3]
[1]고려대학교 정보보호기술연구센터, [2]서울시립대 수학과, [3]고려대학교 정보수학과

Forgery Attack on New Authenticated Encryption

Kitae Jeong,[1†] Changhoon Lee,[1] Jaechul Sung,[2] Seokhie Hong,[1‡] Hichun Eun[3]
[1]Center for Information Security Technologies, Korea University,
[2]Department of Mathematics, University of Seoul,
[3]Department of Information and Mathematics, Korea University

요 약

본 논문에서는 JCCI 2003에 제안된 새로운 인증-암호화 모드 NAE[1]에 대한 위조 공격을 제안한다. NAE는 CFB 모드와 CTR 모드를 결합시킨 변형된 형태로, 하나의 기반이 되는 블록암호 키를 가지고 최소한으로 블록암호를 호출하는 인증-암호화 기법이다. 그러나 본 논문에서는 단순 암호문 조작으로 NAE에 대해 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다.

ABSTRACT

This paper represents a forgery attack on new authenticated encryption mode NAE[1] which was proposed at JCCI 2003. NAE is a new authenticated encryption mode which is combined with CFB mode and CTR mode. And it provides confidentiality. In this paper, we show that it is possible to make a valid ciphertext-tag pair only by modifying a ciphertext.

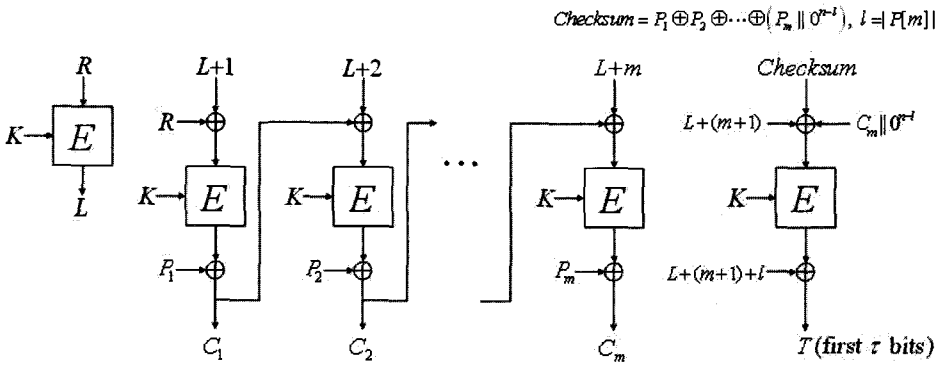
Keywords : *Forgery attack, Modes of operation, Block cipher, NAE*

Ⅰ. 서 론

블록암호는 메시지의 기밀성을 제공하는 가장 대표적인 알고리즘이지만, 본질적으로 n-비트 고정된 길이만큼의 평문만을 암호화하도록 설계되었기 때문에 n-비트 길이보다 더욱 긴 임의의 메시지를 블록암호를 이용하여 암호화하기 위한 방법이 필요하다. 이를 위해 긴 메시지를 여러 개의 n-비트 블록들로 나누어 블록들 간의 연관성을 주는 방식을 사용하는데, 이 사용 방식을 블록암호 운영모드(Mode of Operation)라 일컫는다. 이러한 운영모드는 메시지의 기밀성(Confidentiality)을 유지할 뿐만 아니라, 메시지의 무결성(Integrity) 및 메시지의 출처 인증까지 보장할 수 있기 때문에 금융권 및 다양한 정보 서비스 응용분야에 사용되고 있다.

일반적으로 운영모드는 크게 메시지의 기밀성만 제공하는 암호화 모드(Encryption mode), 메시지의 무결성만 제공하는 인증 모드(Authentication mode), 그리고 메시지의 기밀성과 무결성을 동시에 제공하는 인증-암호화 모드(Authenticated encryption mode)로 분류할 수 있다. 블록암호 DES[7]가 미연방 표준 알고리즘으로 선

접수일: 2007년 1월 15일; 채택일: 2007년 1월 24일
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2006-(C1090-0603-0025))
† 주저자, kite@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr



〔그림 1〕 NAE의 암호화

정된 초기에는 주로 기밀성만을 보장하는 암호화 모드들에 대한 연구가 주로 이루어졌고 1980년에 이르러 DES의 4가지 표준 운영모드(ECB, CBC, OFB, CFB)가 FIPS-81로 선정되었다[8]. 그러나 DES의 안전성에 대한 문제가 제기되면서, NIST에서는 2000년 블록암호 Rijndael을 DES를 대체할 표준 블록암호 AES (Advanced Encryption Standard)로 선정하였다[9]. 이러한 새로운 블록암호 도래와 더불어, NIST는 기존의 모드를 개선하고 AES에 적합한 새로운 모드를 개발하기 위해 2000년과 2001년에 공개 워크샵을 개최하였고, 공개 워크샵에서 제안된 모드들에 대한 안전성과 효율성을 다각적으로 검토하여 현재 3개의 권고 모드를 Special Publication (SP) 800-38 시리즈를 통해 제안하고 있다. SP 800-38A[10]에는 기밀성을 제공하는 5가지 표준 모드(ECB, CBC, OFB, CFB, CTR)를 포함하고 있으며, SP 800-38B[11]에는 무결성을 제공하는 모드로서 CMAC(=OMAC1)을 표준으로 권고하고 있다. SP 800-338C[12]에는 CTR 모드와 CBC-MAC을 함께 사용하여 기밀성과 무결성을 동시에 제공하는 CCM 모드를 표준으로 권고하고 있는데 이것은 IEEE 902.11 WLAN 표준으로 채택된 알고리즘이다. 그리고 최근에 NIST는 또 다른 인증-암호화 모드 GCM을 SP 800-38D[13]로 선정하였다. 이 모드는 tag 크기가 상대적으로 작을 때는 실질적인 공격이 가능하지만, CCM 모드와 달리 병렬처리가 가능하기 때문에 구현 성능이 좋은 모드이다. 이처럼 NIST는 지속적으로 SP 800-38 시리즈를 업데이트할 예정이다.

본 논문에서는 JCCI 2003에 제안된 새로운 인증-암호화 모드 NAE[1]에 대한 위조 공격을 제안한다. CCM 모드가 CTR 모드와 CBC-MAC을 함께 사용하는 모드인데 반해, NAE는 CFB 모드와 CTR 모드를 결합시킨 형태로, 하나의 기반이 되는 블록암호 키를 가지고 최소한으로 블록암호를 호출하는 인증-암호화 기법이다. 본 논문에서는 NAE에 대하여 단순 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다.

먼저 2절에서는 NAE에 대하여 살펴보고, 3절에서는 한 블록 메시지를 갖는 NAE와 여러 개의 블록 메시지를 갖는 NAE에 대해 각각 위조 공격을 수행한다. 그리고 마지막 4절에서는 본 논문의 결과를 요약한다.

Ⅱ. 인증-암호화 모드 NAE

2.1 표기

본 논문에서는 다음과 같은 표기를 사용한다.

- $\{0,1\}^*$: 임의의 길이의 수열의 집합 ($\{0,1\}^n$:길이 n의 모든 수열의 집합)
- $|A|$: 수열 A의 비트 길이 ($A \in \{0,1\}^*$)
- $\|A\|_n = \max\{1, \lceil |A|/n \rceil\}$: A의 n-비트 블록 개수
- $A\|B$: 수열 $A, B(\in \{0,1\}^*)$의 연결 (concatenation)
- $0^i(1^i)$: i개의 0(1)로 구성된 수열
- $A \oplus B$: 두 수열 $A, B(\in \{0,1\}^*)$의 비트 단위 XOR (만약 두 스트링의 길이가 다른 경우에 $A \oplus B$는 A의 처음 l 비트와 B의 처음 l 비트의 비트 단위 XOR을 나타낸다. 이때 $l = \min\{|A|, |B|\}$이다.)
- $E: K \times \{0,1\}^n \to \{0,1\}^n$: n-비트 블록암호
- K: 키 집합, P: 평문 집합, C: 암호문 집합
- $\tau \in [0, \cdots, n]$: 태그 길이
- R: n-비트 nonce

2.2 NAE(New Authenticated Encryption)

본 소절에서는 NAE를 구체적으로 기술한다. 제안된 모드의 암호화 알고리즘은 [그림 1]과 같다.

2.2.1 키 생성 및 세션 셋업

블록암호를 위한 키 집합 K를 랜덤하게 선택한다. 키 K는 송신자와 수신자 모두에게 제공된다. 송신자와 수신자는 각각 블록암호 암호화와 복호화에 관련된 키 셋업을 수행한다.

2.2.2 암호화 알고리즘: $NAE_E(R, K, P)$

$P = P[1]\|\cdots\|P[m]$; $L \leftarrow E_K(R)$;
$C[1] \leftarrow E_K(R \oplus (L+1)) \oplus P[1]$;
for $i \leftarrow 2$ to m do
  $C[i] \leftarrow E_K((L+i) \oplus C[i-1]) \oplus P[i]$;
$C \leftarrow C[1]\|\cdots\|C[m]$; $l \leftarrow |P[m]|$;
$Checksum \leftarrow P[1] \oplus \cdots \oplus P[m-1] \oplus (P[m]\|0^{n-l})$;
$T \leftarrow E_K(Checksum \oplus (C[m]\|0^{n-l}) \oplus (L+m+1)) \oplus (L+m+1+l)$;
$T \leftarrow$ first τ bits of T;
return $C\|T$

2.2.3 복호화 알고리즘: $NAE_D(R, K, C\|T)$

$C\|T = C[1]\|\cdots\|C[m]\|T$; $L \leftarrow E_K(R)$;
$P[1] \leftarrow E_K(R \oplus (L+1)) \oplus C[1]$;
for $i \leftarrow 2$ to m do
  $P[i] \leftarrow E_K((L+i) \oplus C[i-1]) \oplus C[i]$;
$P \leftarrow P[1]\|\cdots\|P[m]$; $l \leftarrow |C[m]|$;
$Checksum \leftarrow P[1] \oplus \cdots \oplus P[m-1] \oplus (P[m]\|0^{n-l})$;
$T' \leftarrow E_K(Checksum \oplus (C[m]\|0^{n-l}) \oplus (L+m+1)) \oplus (L+m+1+l)$;
$T' \leftarrow$ first τ bits of T';
if $T = T'$ then return P
  else return INVALID

Ⅲ. NAE에 대한 위조 공격

본 절에서는 NAE에 대하여 단순한 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보인다. NAE에 대한 위조 공격은 한 블록 메시지와 $m(>1)$개 블록 메시지에 대하여 각각 수행된다.

3.1 한 블록 메시지에 대한 위조 공격 ($m=1$)

공격자에게 송신자가 수신자에게 보낸 n-비트 메시지 P에 대한 유효한 암호문-태그 쌍 $C\|T$을 얻는다고 가정한다. 이때, 공격자는 임의의 n-비트 값 α에 대하여 암호문 C를 $C \oplus \alpha$로 단순 조작하여 새로운 암호문-태그 쌍 $C \oplus \alpha \| T^*$를 수신자에게 보낸다. 여기서 $C \oplus \alpha$는 n-비트 메시지 $P \oplus \alpha$에 대한 암호문을 의미한다. 그러면 다음과 같은 이유로 수신자는 $C \oplus \alpha \| T^*$를 유효한 암호문-태그 쌍으로 받아들인다.

T와 새로운 태그 T^*는 암호화 알고리즘 $NAE_E(R,K,P)$에 의해 각각 다음과 같다.

$$T = E_K(Checksum \oplus C \oplus (L+2)) \oplus (L+2+n)$$
$$T^* = E_K(Checksum^* \oplus (C \oplus \alpha) \oplus (L+2)) \oplus (L+2+n)$$

여기서 $Checksum = P$이고 $Checksum^* = P \oplus \alpha$이다. 따라서 T^*는 다음에 의해 T와 같게 된다.

$$\begin{aligned} T^* &= E_K(Checksum^* \oplus C \oplus \alpha \oplus (L+2)) \oplus (L+2+n) \\ &= E_K(P \oplus \alpha \oplus C \oplus \alpha \oplus (L+2)) \oplus (L+2+n) \\ &= E_K(P \oplus C \oplus (L+2)) \oplus (L+2+n) \\ &= E_K(Checksum \oplus C \oplus (L+2)) \oplus (L+2+n) \\ &= T \end{aligned}$$

이는 새로운 암호문-태그 쌍 $C \oplus \alpha \| T^*$가 유효함을 의미하고 수신자는 $C \oplus \alpha \| T^*$를 유효한 암호문-태그 쌍으로 받아들이게 된다. 따라서 공격자는 단순한 암호문 조작으로 NAE에 대해 유효한 암호문-태그 쌍을 생성할 수 있다.

3.2 $m(>1)$개 블록 메시지에 대한 위조 공격

m개 블록 메시지에 대한 위조 공격은 한 블록 메시지에 대한 위조 공격과 유사하다. 공격자가 송신자가 수신자에게 보낸 $(n \times m)$-비트 메시지 $P = P_1\|P_2\|\cdots\|P_m$에 대하여 유효한 암호문-태그 쌍 $C_1\|C_2\|\cdots\|C_m\|T$을 얻는

다고 가정한다. 이때 공격자는 임의의 n-비트 값 α에 대하여 암호문 $C_1\|C_2\|\cdots\|C_m$을 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)$로 단순 조작하여 새로운 암호문-태그 쌍 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)\|T^*$를 수신자에게 보낸다. 여기서 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)$는 $(n\times m)$-비트 메시지 $P=P_1\|P_2\|\cdots\|(P_m\oplus\alpha)$에 대한 암호문을 의미한다. 그러면 다음과 같은 이유로 수신자는 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)\|T^*$를 유효한 암호문-태그 쌍으로 받아들인다.

T와 새로운 태그 T^*는 암호화 알고리즘 $NAE_E(R,K,P)$에 의해 각각 다음과 같다.

$$T=E_K\big(Checksum\oplus C_m\oplus(L+m+1)\big)\oplus(L+m+1+n)$$

$$T^*=E_K\big(Checksum^*\oplus C_m\oplus\alpha\oplus(L+m+1)\big)\oplus(L+m+1+n)$$

여기서 $Checksum=P_1\oplus\cdots\oplus P_m$이고 $Checksum^*=P_1\oplus P_2\oplus\cdots\oplus P_m\oplus\alpha$이다. 따라서 T^*는 다음에 의해 T와 같게 된다.

$$\begin{aligned}T^*&=E_K\big(Checksum^*\oplus C_m\oplus\alpha\oplus(L+m+1)\big)\oplus(L+m+1+n)\\&=E_K\big(P_1\oplus\cdots\oplus P_m\oplus\alpha\oplus C_m\oplus\alpha\oplus(L+m+1)\big)\oplus(L+m+1+n)\\&=E_K\big(P_1\oplus\cdots\oplus P_m\oplus C_m\oplus(L+m+1)\big)\oplus(L+m+1+n)\\&=E_K\big(Checksum^*\oplus C_m\oplus\alpha\oplus(L+m+1)\big)\oplus(L+m+1+n)=T\end{aligned}$$

이는 새로운 암호문-태그 쌍 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)\|T^*$가 유효함을 의미하고 수신자는 $C_1\|C_2\|\cdots\|(C_m\oplus\alpha)\|T^*$를 유효한 암호문-태그 쌍으로 받아들인다. 따라서 공격자는 단순한 암호문 조작으로 NAE에 대해 유효한 암호문-태그 쌍을 생성할 수 있다.

Ⅳ. 결론

본 논문에서는 JCCI 2003에 제안된 새로운 인증-암호화 모드 NAE[1]에 대한 위조 공격을 제안하였다. NAE는 CFB 모드와 CTR 모드를 결합시킨 형태로, 하나의 기반이 되는 블록암호 키를 가지고 최소한으로 블록암호를 호출하는 인증-암호화 기법이다. 본 논문에서는 NAE에 대하여 단순 암호문 조작으로 유효한 암호문-태그 쌍을 생성할 수 있음을 보였다. 이는 NAE가 위조 공격에 매우 취약함을 의미하므로 실생활에 절대 사용되어서는 안 된다.

참고문헌

[1] 신상욱, 류희수, "새로운 인증된 암호화 기법", JCCI 2003 [S9-692], April, 2003.

[2] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm", *Advances in Cryptology- ASIACRYPT* 2000, LNCS 1976, Springer-Verlag, pp. 531-545, 2000.

[3] M. Bellare, J. Kilian and P. Rogaway, "The security of the cipher block chaining message authentication code", *Journal of Computer and System Sciences*, vol. 61, no. 3, 2000.

[4] J. Black and P. Rogaway, "CBC-MACs for arbitrary-length messages: The three key construction", *Advances in Cryptology-CRYPTO 2000*, LNCS 1880, Springer-Verlag, pp. 197-215, 2000.

[5] D. McGrew and J. Viega, "The Galois/Counter mode of operation (GCM)", Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes/, 2004.

[6] D. Whiting, R. Housley and N. Ferguson, "Counter with CBC-MAC (CCM)", Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes, 2002.

[7] *National Bureau of Standards*, "Data Encryption Standard", FIPS Pub. 46, 1977.

[8] *National Bureau of Standards*, "DES modes of operation", FIPS Pub. 81, 1980.

[9] FIPS Publication 197, "Advanced encryption standard(AES)", 2001. http://csrc.nist.gov/encryption/aes.

[10] NIST Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques", http://src.nistgov/CryptoToolkit/modes/800-38_Series_Publications/SP800-38A.pdf.

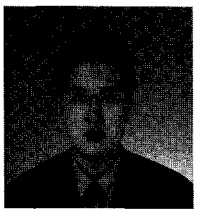
[11] NIST Special Publication 800-38B, "Recommendation for Block Cipher Modes of Ope- ration: The CMAC Mode for Authentica- tion",

http://csrc.nist.gov/CryptoToolkit/modes/800-38_Series_Publications/SP800-38B.pdf.

〔12〕 NIST Special Publication 800-38C, "Recommendation for Block Cipher Modes of Ope- ration: The CCM Mode for Authentication and Confidentiality", ttp://csrc.nist.gov/CryptoToolkit/modes/80038_Series_Publications/SP800-38C.pdf.

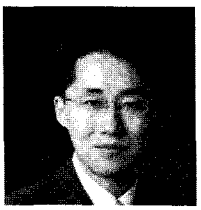
〔13〕 NIST Special Publication 800-38D, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", http://csrc.nist.gov/CryptoToolkit/modes/800-38_Series_Drafts/GCM/GCM_public_comments.pdf.

〈著者紹介〉



정 기 태 (Kitae Jeong) 학생회원
2004년 2월: 고려대학교 수학과 학사
2006년 2월: 고려대학교 정보보호대학원 석사
2006년 3월~현재: 고려대학교 정보보호대학원 박사과정
<관심분야> 블록 암호, 스트림 암호 및 해쉬 함수의 분석 및 설계

이 창 훈 (Changhoon Lee) 학생회원
2001년 2월: 한양대학교 수학과 학사
2003년 2월: 고려대학교 정보보호대학원 석사
2003년 3월~현재: 고려대학교 정보보호대학원 박사수료
<관심분야> 대칭키 암호의 분석 및 설계



성 재 철 (Jaechul Sung) 종신회원
1997년 8월: 고려대학교 수학과 학사
1999년 8월: 고려대학교 수학과 석사
2002년 8월: 고려대학교 수학과 박사
2002년 8월~2004년 1월: 한국정보보호진흥원 선임연구원
2004년 2월~현재: 서울시립대학교 수학과 조교수
<관심분야> 암호 알고리즘 설계 및 분석

홍 석 희 (Seokhie Hong) 종신회원
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 2월: 고려대학교 수학과 박사
1999년 8월~2004년 2월: (주) 시큐리티 테크놀로지스 선임연구원
2003년 2월~2004년 2월: 고려대학교 시간강사
2004년 4월~2005년 2월: K.U.Leuven 박사후연구원
2005년 3월~현 재: 고려대학교 정보보호대학원 조교수
<관심분야> 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식

은 희 천 (Hichun Eun)
1969년 2월: 고려대학교 수학과 학사
1974년 2월: 고려대 수학과 석사
1982년 2월: 고려대 수학과 박사
1982년 3월~현재: 고려대학교 과학기술대학 정보수학과 교수