직접적 인증을 제공하는 안전하고 효율적인 키동의 프로토콜

이 형 규[†] · 이 경 호[††] · 차 영 태[†††] · 심 주 걸[††††] · 원 동 호[†††††]

요 약

본 논문에서 우리는 프로토콜의 체계적 설계를 위해 이산대수에 기반한 키분배 프로토콜의 안전성을 분석하였다. 또한, Diffie-Hellman 문제를 이용하여 기존의 Station-to-Station 프로토콜 보다 효율적인 키동의 프로토콜을 제안한다. 제안한 프로토콜은 분석된 안전성을 만족하고, 직접적인 인증을 제공하도록 설계되었다.

The Secure and Efficient Key Agreement Protocol with Direct Authentication

Hyung-Kyu Lee[†] · Kyung-Ho Lee[††] · Young-Tae Cha[†††] · Joo-Geol Sim[††††] · Dong-Ho Won[†††††]

ABSTRACT

In this paper, we analyzed the security of key distribution protocol based on discrete logarithm for the purpose of designing key distribution protocol systematically. We also propose the efficient key agreement protocol with direct authentication. In comparison with Station-to-Station protocol, it provides the direct authentication using the Diffie-Hellman problem without signature.

1. 서 론

Diffie와 Hellman에 의해 공개키 암호 방식의 개념이 소개된 이후, 공개키 암호 방식은 현대 정보화 사회의 많은 문제점을 해결할 수 있는 토대를 제공해 주었다. 하지만, 공개키 암호방식은 공개키의 공개로 인한 문제점을 해결하기 위해 공개키 기반구조(Public Key Infrastructure : PKI)를 필요로 한다. 따라서 PKI의 핵심기관인 인증기관(Certification Authority : CA)의 역할은 공개키 암호방식의 안전성에 중요한 영향을 미친다. 또한 이와 더불어 현대 암호기술의 안전성이 오직 키에만 의존하는 것을 요구하므로, 키관리 기술 또한 매우 중요하게 취급되고 있다. 따라서 본 논문에서는 키관리의 핵심인 키분배와 인증기관(CA)을 중심으로 키동의 프로토콜의 안전성을 분석한다. 특히, 직접적 인증[7]을 제공하는 키동의(Key Agreement) 프로토콜의 안전성과 이에 근거한 키동의 프로토콜을 제안한다.

본 논문은 다음과 같은 형태로 구성된다. 2장에서는 키 분배 프로토콜의 안전성을 수행전, 수행시, 수행후로 나누어 분석하고, 3장에서는 키분배 프로토콜에 대한 고려사항, 4장에서는 직접적 인증을 제공하기 위한 효율적인 프로토콜의 설계방법, 5장에서는 새로운 키

※ 본 고는 1999년 삼성전자의 위탁과제(O-I-98131)와 한국과학재단의 공모과제(97-01-13-01-05)에 의해 연구되었음.
† 준 회 원 : 성균관대학교 대학원 전기·전자 및 컴퓨터 공학부
†† 정 회 원 : 성균관대학교 대학원 전기·전자 및 컴퓨터 공학부
††† 정 회 원 : 삼성종합기술원 디지틀 통신 연구소 전문연구원
†††† 정 회 원 : 성균관대학교 대학원 전기·전자 및 컴퓨터 공학부
††††† 종신회원 : 성균관대학교 전기·전자 및 컴퓨터 공학부 교수
논문접수 : 1999년 7월 20일, 심사완료 : 1999년 10월 29일

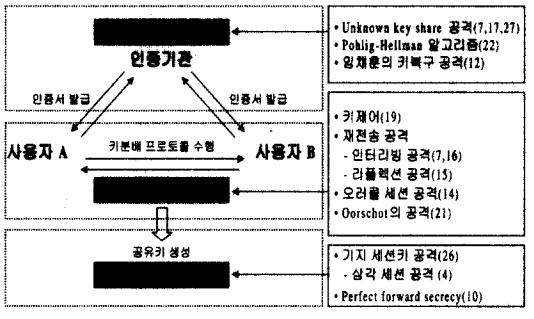
동의 프로토콜의 제안 및 안전성과 효율성을 분석하고 마지막으로 6장에서 결론을 내린다.

2. 키분배 프로토콜의 안전성

안전성을 논하기 위해 본 논문에서 사용되는 기호 및 약어는 <표 1>과 같다.

〈표 1〉 프로토콜에 사용되는 기호 및 약어

프로토콜 관련정보	주 체	표 기	비 고
공개키 정보(P)	A,B	P_A, P_B	A와 B의 공개키
비밀키 정보(S)	A,B	S_A, S_B	A와 B가 선택한 비밀키
인증서	A,B	$Cert_A$, $Cert_B$	A와 B의 공개키 인증서
전송정보(I)	A→B		A에서 B로 전송되는 전송정보
	B→A		B에서 A로 전송되는 전송정보
랜덤정보(R)	A,B	r_A, r_B	A와 B가 선택한 랜덤 정보
세션키(K)			A와 B의 세션키 생성함수
일방향 해쉬 함수(h)	-	h	공개된 일방향 해쉬 함수
개인 식별 정보(ID)	A,B	ID_A, ID_B	A와 B의 개인 식별 정보
파라미터	-	p	모듈러를 나타내는 소수로써 p=qw+1
	-	q, w	q는 q|p-1인 큰 소수 w는 w|p-1인 임의의 작은 소수들의 곱
	-	α	Z_p^*상에서 α는 q를 위수로 갖는 소수-위수 서브그룹의 생성원
		ord	위수를 나타내며 ord(α)=q



(그림 1) 키분배 프로토콜의 안전성

본 절에서는 안전성에 영향을 줄 수 있는 요인들을 체계적으로 살펴보기 위해 키분배 프로토콜의 안전성을 수행전, 수행시, 수행후로 나누어 분석한다. 즉, 시스템 파라미터의 선정과 인증서 발급과정에서부터 비밀정보(비밀키 및 세션키)의 노출로 인한 향후 프로토콜의 안전성에 이르기까지 공격자들의 공격방법과 연계하여 살펴본다. 도식화하면 (그림 1)과 같다.

2.1 키분배 프로토콜 수행전 안전성

공개키의 공개로 인한 공개키 암호방식의 잠재적인 문제점을 해결하기 위해 공개키 기반구조(Public Key Infrastructure : PKI)가 등장하게 되었다. 공개키 기반구조는 공개키의 위변조 문제를 해결하기 위해 공개키에 해당하는 비밀키의 소유주와 공개키를 연결시켜주는 전자 인증서(Certificate)의 발행과 획득, 조회, 검증 등을 수행할 수 있도록 하는 인증서 관리 기반 구조를 가진다. 이러한 인증서 관리의 핵심기관을 인증기관(Certification Authority)이라 부르며, 안전성에 대한 많은 문제들이 인증기관의 올바른 기능 수행과 밀접하게 관련되어 있다[7, 12, 17, 27]. 이 절에서는 주로 인증기관의 역할이 올바르게 수행되지 않을 경우에 가능한 공격방법들에 대해 논한다.

(1) 미지 키공유 공격(Unknown Key Share Attack)

미지 키공유 공격은 [7]에서 처음 개념이 제시되었고 공격자가 세션키를 모른다는 점에서 이러한 종류의 공격방법을 미지 키공유 공격이라 부른다[27]. 미지 키공유 공격은 공격자가 정당한 사용자와 동일한 공개키에 대한 인증서를 발급받아 공격하는 방법[7, 27]과 정당한 사용자의 공개키를 변형한 것을 자신의 공개키로 사용하여 공격하는 방식으로 나눌 수 있다[17]. 이러한 미지 키공유 공격의 대부분은 공개키의 인증서가 그 공개키에 해당하는 비밀키를 알고 있는 사용자에게만 발급되지 않는다는 가정에서 비롯된다. 이 공격은 한 사용자가 공유한 키로써 메시지를 보내면 메시지를 받은 다른 사용자는 그 메시지를 공격자가 보내온 것으로 오인하게 된다. 이러한 공격은 은행거래 등과 같은 메시지 교환에는 치명적일 수 있다는 점에서 매우 중요하게 취급될 수 있다. [23]에 소개된 Nyberg-Rueppel형 One-pass 키분배 프로토콜에 대해 미지 키공유 공격은 다음과 같이 수행될 수 있다.

Nyberg-Rueppel형 One-pass 키분배 프로토콜에 대한 공격과정

$P_A = \alpha^{-s_A}$이며, R, $r \in_R \{1, 2, \ldots, q-1\}$이다.

[프로토콜]

사용자 A는 $e=\alpha^{R-r} \bmod p$, $y=r+e \cdot s_A \bmod q$를 계산하여 B에게 보낸다.

- $A \rightarrow B : e \parallel y \parallel Cert_A$

[세션키 생성]

- A의 세션키 생성 : $K=P_B^R \bmod p$
- B의 세션키 생성 : $K=(\alpha^y P_A^e e)^{-s_B}=\alpha^{-R \cdot s_B} \bmod p$

[공격과정]

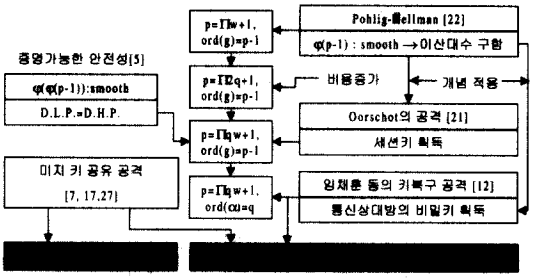
위의 프로토콜에 대해 [17]의 공격 방법을 적용하면 다음과 같다.

- 공격자는 전송정보 $e \parallel y \parallel Cert_A$를 가로채어 $g^R=g^y \cdot P_A^e \cdot e \bmod p$을 구한다.
- 공격자는 g^R을 이용하여 $e'=g^{R-r} \bmod p$와 $y'=r'+e' \cdot s_E \bmod q$를 계산한다.
- 공격자는 B에게 $e' \parallel y' \parallel Cert_E$를 보낸다.

따라서, 사용자 A가 공유한 키를 사용하여 사용자 B에게 메시지를 보내면 B는 그 메시지가 공격자 E로부터 온 것으로 착각하게 된다. 이러한 미지 키공유 공격을 막기 위한 가장 근본적인 방법은 공격자가 분배된 세션키를 알 수 없다는 점에 착안하여 키확인 과정을 가지는 것이다.

(2) 서브그룹 제한 공격(Subgroub Confinement Attack)

이산대수문제에 기반한 암호시스템에서 파라미터의 안전성에 관한 대부분은 Pohlig-Hellman 알고리즘과 관련되어 있다[22]. 이러한 Pohlig-Hellman의 알고리즘에 기초하여 위수가 낮은 서브그룹상에서 이산대수문제를 풀 수 있도록 프로토콜을 조작하는 공격방법을 서브그룹 제한 공격(Subgroup Confinement Attack)이라 한다[2, 12, 20, 21, 28]. 즉, 큰 소수 p에 대해, p-1이 작은 소인수들로 이루어진 경우에는 이산대수를 풀 수 있는 방법이 존재하고 따라서, q|p-1인 또 다른 큰 소수 q가 존재해야 한다(예, p=qw+1, ord(g)=p-1). 하지만 이러한 형태의 소수도 모듈러 w에 대해 이산대수에 관한 정보를 노출시킨다. 이러한 이유로 [21]에서 소수-위수 서브그룹의 사용이 제기되었다. 소수-위수 서브그룹은 그룹 Z_p^*의 서브그룹으로 q를 위수로 가지는 α를 생성원으로 하며 계산효율성과 소수생성이 편리하다는 장점을 가진다. 하지만 소수-위수 서브그룹을 사용하더라도 다른 사용자의 비밀키를 아는 것이 가능하다[12]. 이러한 안전성 문제 역시, 앞에서 언급한 대로 인증기관의 역할과 밀접한 관계가 있다.



(그림 2) 공개파라미터 설정과 인증기관의 역할

(그림 2)는 위에서 언급된 안전한 파라미터의 안전성과 인증기관의 역할에 대해 기존의 논문을 토대로 체계적으로 나타내고 있다. 이상에서 알 수 있듯이 안전한 파라미터의 사용과 인증기관의 역할이 올바르게 행해지면 이산대수에 기반한 대부분의 키분배 프로토콜은 프로토콜의 수행전 안전성에 있어서 많은 문제점을 해결할 수 있다.

2.2 키분배 프로토콜 수행시 안전성

안전한 공개 파라미터의 선택과 올바른 인증기관의 역할은 공개정보만을 이용한 수동적인 공격자에 대해 프로토콜을 안전하게 수행할 수 있도록 한다. 하지만, 이러한 프로토콜의 수행전 안전성이 만족되더라도 프로토콜의 수행시 존재하는 다양한 공격 방법에 의해 안전성이 위협받을 수 있다. 이 절에서는 합법적인 사용자로 가장한 후 정보의 재전송 또는 수정을 할 수 있는 신분위장 공격자(Impersonation attacker)에 대해, 프로토콜의 설계시 부주의로 일어날 수 있는 공격방법들을 대상으로 프로토콜의 안전성을 점검한다. 특히, 직접적 인증을 제공하기 위해, 주로 인증에 대한 공격방법들을 분석한다.

(1) 재전송 공격

재전송 공격(Replay Attack)은 공격자가 합법적인 사용자를 가장하여 현재 또는 과거에 사용된 메시지를 재사용 하는 공격방법이다. 이것은 보통 인증이나 키전송 프로토콜에서 많이 일어나며 타임스탬프(Time stamp)나 논스(Nonce)를 사용함으로써 해결된다. 재전송의 방법은 과거의 프로토콜에서 도청한 메시지의 재

전송과 중간 공격자에 의한 외부 프로토콜에서 얻은 메시지의 재사용 등 다양한 형태로 존재한다. 특히, 중간 공격자가 정당한 사용자로 가장하여 메시지를 재전송 하는 공격을 인터리빙 공격(Interleaving Attack)이라 하고, A에게서 받은 메시지를 다시 A에게로 재전송 하는 공격방법을 리플렉션 공격(Reflection Attack)이라 한다[15, 16].

(2) 오러클 세션 공격

오러클 세션 공격은 신분인증을 속이기 위해 공격자가 정당한 사용자를 오러클처럼 이용하여 공격을 위한 정보를 제공하도록 만드는 공격방법이다. 이 공격방법은 Shamir에 의해 SECURICOM '89에서 언급된 마피아 공격(Marfia Fraud)과 유사하고, 임채훈 등이 제안한 Schnorr의 개인식별 프로토콜을 변형한 상호 인증 키 분배 프로토콜의 안전성을 기술하기 위해 설명되었다[14]. 이러한 오러클 세션 공격을 막기 위해 프로토콜은 메시지 근원지/수신지 증명을 제공하여야 하며 보통, 개인식별정보(ID)가 해쉬함수나 서명의 입력에 사용되어야 한다.

(3) 키동의 프로토콜에서 키제어

키제어 문제는 [19]에서 Mitchell 등이 기존의 키동의 프로토콜의 문제점으로 지적하였다. 즉, 키동의 프로토콜은 두 사용자의 세션키가 한 사용자에 의해 미리 결정될 수 없도록 하는 키분배 프로토콜을 의미하지만, 세션키 생성에 해쉬함수 등을 이용하는 프로토콜들에 대해서는 상당한 정도로 세션키 생성이 한 사용자에 의존될 수 있다는 것을 지적하였다. 이러한 문제점을 해결하기 위해 Mitchell 등은 키재료에 대한 커미트먼트(Commitment)를 제안하고 있다.

2.3 프로토콜 수행 후 고려사항

프로토콜 수행 후에 일어날 수 있는 안전성에 관한 중요한 개념으로서 기지 세션키 공격(Known Key Attack : KKA)과 Perfect Forward Secrecy(PFS)는 프로토콜의 설계시 중요하게 취급되고 있다. 기지 세션키 공격은 과거의 세션키의 노출이 현재의 프로토콜에서 세션키에 대한 중요한 정보(예, 비밀키로만 이루어진 항($g^{s_A s_B}$))를 제공하는 것을 의미하며[8, 13, 26], Perfect Forward Secrecy는 사용자의 비밀키 노출이 과거의 세션키에 대한 정보를 노출하지 않음으로써 과거의 세션키의 지속적인 안전성을 의미한다[7, 10]. 기지 세션키 공격과 Perfect Forward Secrecy의 개념이 혼합된 공격방법은 [4]에서 기지키 삼각세션 공격(Known Key Triangle Attack : KKTA)으로 묘사되었다. 이것은 사용자의 비밀키를 아는 공격자가 과거 세션키의 부분키들을 각각 다른 두 세션으로부터 구할 수 있음으로 해서 과거의 세션키를 구하는 공격방법이다.

3. 키분배 프로토콜에 대한 고려사항

키분배 프로토콜이 전자상거래 등에 널리 활용되기 위해서는 사용자 요구사항을 충족 시켜야 할 것이다. 따라서, 본 논문에서는 전자상거래의 활성화를 위해 다음과 같은 요소를 중점적으로 고려한다. 키분배에 대한 중요한 고려사항들은 [1, 7, 23] 등에도 언급되고 있다.

- **직접적 인증(Direct Authentication)**
  키분배 프로토콜의 수행시에 일어나는 사용자 인증(특히, 명시적 인증)이 두 사용자가 공유된 키를 서로 확인하는 키확인 과정에 의해서가 아니라 키 공유 이전에 일어날 수 있도록 프로토콜을 설계하는 것을 직접적 인증이라 한다[7]. 키공유 이전에 통신 상대방에 대한 인증은 사용자 측면의 요구사항을 고려한 것으로 실제, [7, 14]에서 제기된 키분배 프로토콜은 이러한 목적을 이루기 위해 설계되었다.

- **키확인(Key confirmation)의 필요성**
  중요한 정보의 암호화가 통신 상대방에게 함부로 전송되어지는 것은 공격에 이용되기 쉽기 때문에 정확한 키 공유 사실을 확인하는 키확인 과정은 매우 중요하다. 보통, 키분배 프롤토콜은 당사자 이외에는 세션키를 생성할 수 없을 것이라는 내재적 인증(Implicit Key Authentication)만을 많이 다루지만, 앞에서 언급된 것처럼 내재적 인증만을 가지고 미지키공유 공격을 막을 수 없는 경우가 존재하기 때문에, 그러한 공격을 쉽게 막기 위해 키확인 과정이 더욱 필요하다고 할 수 있다. 또한, 통신에서 공유키의 확인 과정을 가지는 것은 통신 지연 등으로 인한 사용자들의 불안감을 해소시키고, 정확한 세션의 시작을 알릴 수 있는 장점도 가지고 있다. 실제로 SSL(Secure Socket Layer) 3.0에서는 키분배에 대한 완료 메시지(Finished message)를 이용해서 키확

인 과정을 제공하고 있다[9].

- **인증기관(Certificate Authority)의 역할**
  본 논문에서 언급된 안전성에 관한 중요한 부분들이 인증기관의 역할과 상당 부분 관련되어 있다. 즉, 인증기관의 역할이 올바르게 수행되지 않으면 안전한 키분배 프로토콜을 설계하더라도 안전성에 중요한 영향을 끼칠 수 있다[7, 12, 17, 27]. 따라서, 엄격한 공개키에 대한 관리는 향후 사용자들의 프로토콜 수행에 기반이 되는 안전성을 제공하여 전자상거래를 위한 사용자들의 좀 더 적극적인 자세를 유도할 수 있을 것이다.

- **메시지 수신지/근원지 증명**
  프로토콜에 사용되는 메시지에 대해 근원지와 수신지를 증명할 수 있도록 함으로써, 공격자가 신분위장을 할 수 있는 가능성을 최대한으로 줄일 수 있다. 특히, 이것은 직접적인 인증을 제공하고 마피아 공격을 막기 위해 메시지의 재전송 등과 함께 본 논문에서 중요하게 고려된다[1, 14]. 이러한 개념을 적용하면 Rivest 등이 [24]에서 제안한 Interlock protocol에 대한 공격유형에도 안전한 프로토콜을 설계할 수 있다[3].

4. 직접적 인증을 제공하는 효율적인 키동의 프로토콜의 수행 및 설계

앞에서 분석된 다양한 공격방법들에 안전하고 직접적 인증을 제공하는 효율적인 이산대수형 키동의 프로토콜을 설계하기 위해 다음과 같은 요구사항들을 도출하였다. 요구사항들은 본논문에서 분석된 프로토콜들의 안전성에 기초하였다.

(1) 인증서 발급과정

요구사항 1 (인증기관의 역할) : 인증기관은 사용자가 안전한 공개키 파라미터를 선택하고 해당 비밀키를 정확히 알고 있는가에 대해 검사한다.

위에서 언급한 소수 위수 서브그룹의 사용과 공개키의 유효성은 다음과 같은 과정에 의해 진행된다.

- **단계 1 (공개키 전송)** : 사용자 A는 비밀키 $s_A \in_R Z_q$를 선택하고, $y_A = \alpha^{s_A} \bmod p$를 계산하여 ID와 함께 인증기관인 CA에게 전송한다.

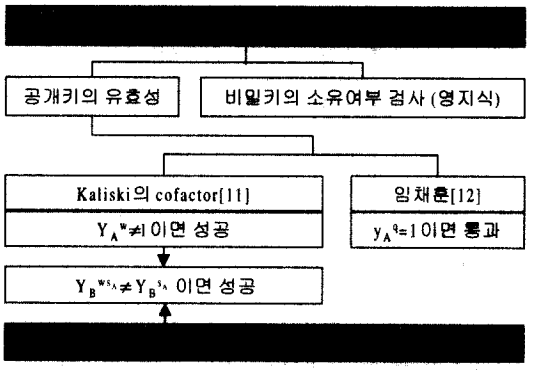
$$A \rightarrow CA : ID_A, y_A$$

- **단계 2 (공개키 유효성 검사)** : 인증기관은 사용자 A에게서 전송 받은 공개키 y_A에 대해 A가 정확한 비밀키 s_A를 소유하고 있는지에 대해 검사한 후 아래와 같이 인증서를 발급한다.

$$CA \rightarrow A : Cert_A$$

  - 경우 1 : 정보의 노출방지를 위해 영지식 개인식별 프로토콜을 사용하여 정확한 비밀키 소유여부에 대한 사용자 인증을 수행한다.
  - 경우 2 : 공개키가 유효한 조건을 따르는지 검사한다.
    ① $y_A^q = 1$이면 성공, $y_A^q \neq 1$이면 실패.
    ② $y_A^w \neq 1$이면 성공, $y_A^w = 1$이면 실패.

일반적으로 인증기관은 경우 1의 방법으로 사용자의 공개키에 대한 검사과정을 수행하며, 경우 2는 설계된 프로토콜의 특성(특히, 공개키의 형태)에 따라 적절하게 사용될 수 있다. 또한, 경우 2의 ②번을 사용하면, 공개키 발급과정이 아니라, 키분배 프로토콜의 수행과정에서, 생성된 세션키를 사용하여 공개키 유효성을 검사할 수 있다[11]. 아래의 (그림 3)은 위에서 언급된 인증기관의 역할을 도식화한 것이다.



(그림 3) 공개키 검사과정

(2) 키분배 프로토콜의 설계

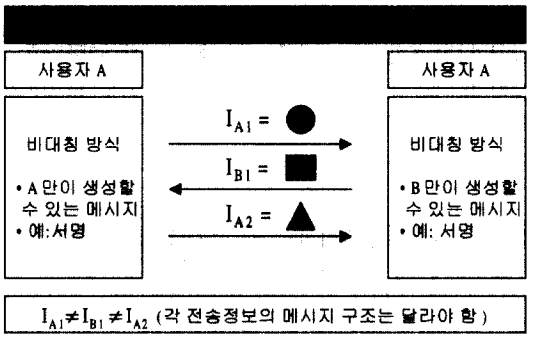
직접적인 인증을 제공하고 효율적인 Diffie-Hellman (DH)형 키동의 프로토콜을 설계하기 위해 다음과 같은 요구사항들을 도출한다.

요구사항 2 (위탁) : 키재료를 보내기 앞서 해쉬함수를 이용하여 키재료와 인증 및 식별 정보에 대한 위탁(Commitment)을 수행한다.

키제어의 문제점을 해결하고, 서명과 같은 또다른 비대칭 암호화 방식을 사용하지 않기 위해 해쉬함수를 사용하여 키재료와 인증 및 식별정보에 대한 커미트먼트(Commitment)를 수행한다.

요구사항 3 (재전송 방지) : 각 라운드의 전송정보는 다른 메시지 구조를 갖고, 비밀키를 사용한 비대칭 정보와 랜덤정보를 가지고 다른 라운드와 연결되어야 한다.

요구사항 3은 재전송 공격을 막기 위해 [15, 16]에서 언급된 공격방법에 기초하였으며, 이와 같은 설계에 의해 공격자는 기존의 재전송 공격을 막을 수 있다. 이해를 돕기 위해 3-move 요구-응답 프로토콜을 예로 들어 요구사항 3을 아래 (그림 4)와 같이 나타낼 수 있다.



(그림 4) 재전송 공격 방지를 위한 메시지 생성과 구조

요구사항 4 (직접적 인증) : 사용자가 커미트먼트의 유효성을 검증하면 통신상대방을 확인할 수 있도록 프로토콜을 설계한다.

요구사항 4는 요구사항 3과 연계되며, 따라서 메시지 재전송과 같은 공격들에 안전한 효율적인 인증을 제공하게 된다.

요구사항 5 (기지 세션키 공격(KKA))과 Perfect Forward Secrecy(PFS)) : 세션키가 임의의 비밀 랜덤 정보로만 생성되도록 설계한다.

세션키가 임의의 랜덤정보로만 구성된다면 기지 세션키 공격과 Perfect Forward Secrecy는 자연적으로 해결된다. 하지만, MTI/A(0)와 MTI/B(0) 프로토콜은 세션키가 사용자의 비밀키 정보를 포함하고 있으므로 과거의 세션키 또는 사용자의 비밀키를 아는 능동적인 공격자에 약점을 가지고 있다.

요구사항 6 (키확인) : 생성된 세션키를 확인하는 키확인 과정을 둔다.

키확인 과정으로써 키분배의 완료를 알리고 미지 키 공유 공격을 근본적으로 막을 수 있다.

5. 제안하는 키동의 프로토콜

이 프로토콜은 직접적인 인증을 제공하기 위해 각 사용자의 공개키로 생성된 Diffie-Hellman 정보를 사용한다. 키재료로 사용되는 랜덤수 r_A, r_B는 Z_q^*상에서 선택된다.

5.1 Diffie-Hellman 방식의 인증 정보를 사용한 새로운 프로토콜

서명을 사용하지 않고 해쉬함수(hash function)만을 사용함으로써 훨씬 효율적으로 직접적인 인증을 제공할수 있다. 프로토콜은 다음과 같다. $r_A, r_B \in_R \{1, 2, \cdots, q-1\}$이다.

- $A \rightarrow B$: ID_A, $Cert_A$, $T_A = h(\alpha^{r_A}, P_B^{s_A})$
- $B \rightarrow A$: ID_B, $Cert_B$, α^{r_B}, $T_B = h(\alpha^{r_B}, P_A^{s_B}, T_A)$
- $A \rightarrow B$: α^{r_A}, $h(K)$
- $B \rightarrow A$: $h(K, \alpha^{r_A})$

사용자들은 각각 상대방이 전송한 해쉬값을 검사하고, 그 해쉬값들이 검사과정을 만족하면, $\alpha^{r_B r_A}$ 또는 $\alpha^{r_A r_B}$를 세션키로 사용하는데 동의할 수 있다. $h(K)$와 $h(K, \alpha^{r_A})$는 획득한 세션키에 대한 키확인 메시지이다.

5.2 제안한 프로토콜의 안전성 및 효율성

제안하는 키동의 프로토콜은 Diffie-Hellman 문제의 안전성에 바탕을 두고 있다. Diffie-Hellman 문제는 다음과 같이 정의된다.

Diffie-Hellman 문제 : g^x mod p와 g^y mod p가 주어졌을 때 g^{xy}를 결정하는 문제

따라서, 능동 공격자도 Diffie-Hellman 문제를 풀수 없다면 신분위장을 할 수 없으며 또한, 서명을 사용하지 않고 해쉬함수만을 사용하여 직접적 인증을 제공하기 때문에 효율적이다. 특히, 제안된 프로토콜은 랜덤 정보로만 세션키를 생성하므로 Perfect forward secrecy를 만족하고 Known key attack에도 안전하다. 세션키가 랜덤정보로만 이루어지지 않은 프로토콜들은 설계시 많은 주의를 필요로 한다. 위에서 언급했듯이, [18]에서 제안된 MTI/(A), (B)는 두 사용자의 비밀키가 노출된다면 Perfect forward secrecy를 만족하지 못하며, MTI/(A)는 기지키 삼각세션 공격(Known key triangle attack)을 막을 수 없다. 또한, 키확인 과정을 제외하면 위의 프로토콜은 커미트먼트(commitment)에 의해 3-move 비대칭 프로토콜을 구성한다. 안전성 및 효율성을 좀 더 세부적으로 살펴보면 다음과 같다.

[마피아 공격과 오러클 세션공격]

마피아 공격에 의해 공격자 E는, 사용자 A와 통신하고 있는 사용자 J와 공모하여, 사용자 B에게 사용자 A로 가장할 수 있다. 이러한 공격은 사용자 I의 메시지에 수신지 또는 근원지 정보가 포함되지 않았기 때문에 가능하다. 따라서, 직접적 인증을 제공하기 위해 STS 프로토콜은 분배된 키를 사용하는 암호화와 서명정보를 연결시킨 반면, 제안하는 프로토콜은 해쉬함수와 Diffie-Hellman 방식의 인증정보를 이용하여 개인식별의 기능을 제공하고 있다. 또한, 3-move 비대칭 프로토콜이므로 공격자 E는 자신이 프로토콜의 시작자(Initiator)가 되어 오러클 세션 공격을 시도할 수 없으며 해쉬함수를 이용한 커미트먼트 T_A에 의해 키제어 문제도 해결한다[19]. 즉, 공격자 E가 사용자 B에게 A로 위장하기 위해서는 사용자 A가 사용자 B에게 위의 프로토콜을 이용하여 키동의 프로토콜을 시작해 주어야 한다. 하지만, 이러한 세션에서 공격자는 통신선로의 중간에 위치하여 정보를 전달해주는 역할밖에 수행할 수 없으며, 자신이 프로토콜의 시작자가 되어 A와 통신한다면 B에게 재전송 할수 있는 메시지를 A로부터 얻을 수 없다. 이것은 각 라운드의 메시지 구조가 다르고, 3-move 프로토콜이기 때문에 가능하다. 또한, 커미트먼트 T_A에 의해 사용자 B는 자신의 키재료를 보내기 전까지 사용자 A의 키재료를 알 수 없으며, 역으로 사용자 A는 사용자 B의 키재료를 받은 후 커미트먼트에 해당하는 키재료를 보내야 하기 때문에 키제어 문제도 해결할 수 있다.

[효율성]

STS 프로토콜은 직접적 인증을 제공하기 위해 또다른 비대칭 암호방식인 서명을 사용한다[7]. 일반적으로 비대칭 암호방식을 사용한 서명은 계산량이 많고, 실제적인 키동의 프로토콜도 복잡해 진다. 본 논문에서 제안하는 프로토콜은 서명을 사용하지 않고 해쉬함수만을 사용하여 직접적 인증을 제공하도록 설계하였다. 이를 위해 커미트먼트에 Diffie-Hellman 방식의 인증정보를 입력하여 통신상대방에 대한 인증기능을 제공하도록 하였다. Diffie-Hellman 방식을 인증정보로 사용하는 것은 세션키 생성과 동일한 방법이라는 점에서 서명과 같은 또 다른 공개키 방식을 사용하는 것보다 효율성과 편리성이 훨씬 뛰어나다. 또한, Diffie-Hellman 방식에 의한 인증은 그 자체에 송신자와 수신자의 인증정보가 내포되어 있으므로 임채훈의 프로토콜[14]처럼 수신자의 ID를 전송정보에 사용하지 않아도 마피아 공격에 안전하다. 특히, 제안하는 프로토콜은 모듈러 지수승을 계산 효율성의 척도로 삼을 때 [14]에서 제안된 임채훈의 상호 인증 키분배 프로토콜보다 모듈러 지수승이 훨씬 적기 때문에 계산량 측면에서 효율적이라 할수 있다.

제안 프로토콜의 특성을 위에서 언급된 다른 프로토콜들과 비교하여 간단히 정리하면 <표 2>와 같다.

<표 2> 제안 프로토콜의 특성

분류	안전성			직접적 인증	비고
	KKTA	PFS	키제어		
STS [7]	○	○ (s_A, s_B 모두 노출시)	×	○	서명
MTI/A(0) [18]	×	× (s_A, s_B 모두 노출시)	×	×	Diffie-Hellman
MTI/B(0) [18]	○	× (s_A, s_B 모두 노출시)	×	×	Diffie-Hellman
MTI/C(0) [18]	○	○ (s_A, s_B 모두 노출시)	×	×	Diffie-Hellman
임채훈의 프로토콜 [14]	○	× (s_A 또는 s_B의 노출시)	×	○	Schnorr
제안 프로토콜	○	○ (s_A, s_B 모두 노출시)	○	○	Diffie-Hellman

6. 결 론

본 논문은 프로토콜의 수행전, 수행시, 수행후에 일어날 수 있는 안전성에 관한 문제를 광범위하게 분석하고, 이를 바탕으로 안전한 키동의 프로토콜의 체계적 설계 방법과 설계방법을 적용한 키동의 프로토콜을 제안하였다. 제안된 프로토콜들은 직접적인 인증과 미지 키공유 공격을 막기 위한 키확인 기능을 제공하며, 완전한 의미의 키동의 프로토콜을 수행하기 위한 키제어 방지 기능 및 메시지 재전송 공격에 안전하도록 설계되었다. 또한, 본 논문에서는 키분배 프로토콜에 대한 공격이 보통 프로토콜의 수행 정보만을 가지고 일어나지 않고 파라미터의 설정 단계에서부터 인증서 발급, 과거나 현재의 중요정보 노출로 인한 문제까지 확장된다는 것을 체계적으로 살펴봄으로써 향후, 전자상거래 등에 활용하기 위한 시스템 구축시, 키관리 측면과의 연계에 많은 도움을 줄 수 있을 것이라 생각된다.

참 고 문 헌

[1] M. Abadi and R. Needham, "Prudent Engineering Practice for Cryptographic Protocols," IEEE Software Engineering Vol.22, No.1, pp.6-15, Jan. 1996.

[2] R. Anderson and S. Vaudenay, "Minding your p's and q's," Advances in Cryptology-Asiacrypt '96, Springer-verlag, Vol.LNCS 1163, pp.15-25, 1996.

[3] S. M. Bellovin and M.Merritt, "An attack on the Interlock Protocol When Used for Authentication," in IEEE Transactions on Information Theory Vol.40, No.1, pp.273-275, Jan. 1994.

[4] M. Burmester, "On the risk of opening distributed keys," Advances in Cryptology-Crypto '94, Springer-verlag, Vol.LNCS 839, 1994.

[5] B. DenBoer, "Diffie-Hellman is as strong as discrete log for certain primes," Advances in Cryptology-Crypto '88, Springer-verlag, Vol.LNCS 403, pp.530-539, 1988.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol.IT-22, No.6, pp.644-654, 1976.

[7] W. Diffie, P. C. vanOorschot and M. J. Wiener, "Authentication and Authenticated Key Exchange," Designs, Codes and Cryptography, Vol.2, pp.107-125, 1992.

[8] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," Communications of the ACM, Vol.24, No.8, 1981.

[9] A. O. Freier, P. Karlton and P. C. Kocher "The SSL protocol verson 3.0," Internet draft, March, 1996, (Netscape Communications Corporation-http://home.netscape.com/eng/ssl3/index.html)

[10] C. G. Günther, "An identity-based key-exchange protocol," Advances in Cryptology-Eurocrypt '89 Vol.LNCS434, pp.29-37, 1990.

[11] B. S. Kaliski Jr, "Compatible cofactor multiplication for Diffie-Hellman primitivies," Electronics Letters 10th, Vol.34, No.25, December, 1998.

[12] C. H. Lim and P. J. Lee, "A key recovery attack on discrete log-based schemes using a prime order subgroup," Advances in Cryptology-Crypto '97, Springer-verlag, Vol.LNCS 1294, pp. 249-263, 1997.

[13] 이필중, 임채훈, "일반화된 Diffie-Hellman 키이분배방식의 안전성 분석", 한국정보통신학회논문지, 제16권 제7호, pp.575-597, 1997.

[14] 임채훈, 이필중, "상호 신분 인증 및 디지털 서명 기법에 관한 연구", 통신정보보호학회논문지, 제2권 제1호, pp.16-33, 1992.

[15] C. Mitchell, "Limitations of challenge-response entity authentication," Electronic Letters, Vol.25 No.17, pp.195-196, 1989.

[16] A. J. Menezes, P. C. vanOorschot and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, pp.530-531.

[17] A. Menezes, M. Qu and S. A. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," Workshop on Selected Areas in Cryptography (SAC '95), pp.22-32, 1995.

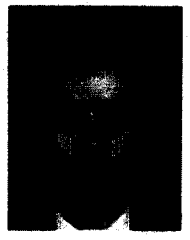
[18] T. Matsumoto, Y. Takashima and H. Imai, "On seeking smart public key distribution systems," Trans. IEICE Japan. Vol.69, No2, pp.99-106, 1986.

[19] C. J. Mitchell, M. Ward and P. Wilson, "Key control in key agreement protocols," Electronics

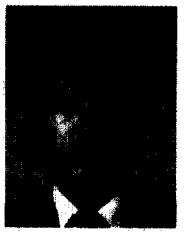
Letters 14th, Vol.34, No.10, May, 1998.
[20] 오수현, 이형규, 김승주, 원동호, "이산대수 문제에 기반한 암호 방식의 안전성에 관한 연구", 통신정보보호학회지 제9권 제1호, pp.43-68, 1999.
[21] P. C. vanOorschot and M. J. Wiener, "On Diffie-Hellman Key Agreement with Short Exponents," In Advances in Cryptology-Eurocrypt '96, Springer-verlag, Vol.LNCS 1070, pp.332-343, 1996.
[22] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," IEEE Trans. Inform. Theory, Vol.IT-24(1), pp.106-110, 1978.
[23] R. A. Rueppel and P. C. vanOorschot, "Modern Key Agreement Techniques," Computer Communications, Vol.17, No.7, pp.458-465, July, 1994.
[24] R. L. Rivest and A. Shamir, "How to Expose an Eavesdropper," Communications of the ACM, Vol.27, No.4, pp.393-395, Apr. 1984.
[25] C. P. Schnorr, "Efficient identification and signatures for smart cards," Advances in Cryptology-Crypto '89, Springer-verlag, Vol.LNCS 435, pp. 239-252, 1989.
[26] Y. Yacobi, "A key distribution paradox," Advances in Cryptology-Crypto '90, Springer-verlag, Vol.LNCS 537, pp.245-255, 1990.
[27] S. B. Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station(STS) Protocol," University of Waterloo Dept. of Combinatorics and Optimization, research report, CORR. 98-42.
[28] T. Wu. "The Secure Remote Password Protocol," Internet Society Symposium on Network and Distributed System Security, 1998.

이 형 규
e-mail : hklee@dosan.skku.ac.kr
1996년 성균관대학교 산업공학과 졸업(학사)
1998년~현재 성균관대학교 대학원 전기전자 및 컴퓨터공학부 석사과정 재학
관심분야 : 인증 및 키분배, VPN, IPsec

이 경 호
e-mail : khlee@dosan.skku.ac.kr
1991년 성균관대학교 정보공학과(학사)
1993년 성균관대학교 대학원 정보공학과(공학석사)
1993년~현재 성균관대학교 대학원 전기전자 및 컴퓨터 공학부(박사과정)
관심분야 : 암호화, 인증



차 영 태
e-mail : cha@sait.samsung.co.kr
1985년 서울대학교 전기공학과 졸업(학사)
1987년 서울대학교 대학원 전기공학과(공학석사)
1994년 펜실베니아 주립대학교 대학원 전자공학과(공학박사)
1994년~현재 삼성종합기술원 디지틀 통신 연구소 전문연구원
관심분야 : 데이터 통신 & 디지틀 통신, 암호, 네트워크 보안, 에러수정 코드, 다중엑세스 프로토콜의 성능분석, 고속 데이터 네트워크 등



심 주 걸
e-mail : pmp47@chollian.net
1979년 중앙대학교 전자공학과(학사)
1991년 건국대학교 전자공학과(석사)
1997년~현재 성균관대학교 전기전자 및 컴퓨터 공학부(박사과정)
1999년~현재 한국정보보호센터 기술전문위원
관심분야 : 보안정책, 암호

원 동 호
e-mail : dhwon@dosan.skku.ac.kr
1976년 성균관대학교 전자공학과(학사)
1978년 성균관대학교 대학원 전자공학과(공학석사)
1988년 성균관대학교 대학원 전자공학과(공학박사)
1978년~1980년 한국전자통신연구소 연구원
1985년~1986년 일본 동경공대 객원연구원
1996년~현재 성균관대학교 공과대학 전기전자 및 컴퓨터공학부 정교수
관심분야 : 암호이론, 정보이론