DBpia

논문 99-24-5A-18 한국통신학회논문지 '99-5 Vol.24 No.5A

패스워드 기반 인증 프로토콜 K1P의 재전송 공격에 대한 안전성 개선에 관한 연구

정회원 권 태 경*, 송 주 석*

A Study on the Security against Replay Attacks in the Password-based Authentication Protocol K1P

Taekyoung Kwon*, Jooseok Song* *Regular Members*

요 약

안전한 컴퓨터 통신의 실현을 위해서 요구되는 인증 프로토콜은 다양한 종류의 프로토콜 공격에 대한 안전성이 검증되어야 한다. 이와 같은 공격의 한 종류인 재전송 공격은 그 형태가 다양하게 분류될 수 있지만, 실제로 재전송되는 메시지가 본래 메시지와 같은 데이터와 구조를 갖기 때문에 대부분의 형식 기법으로는 발견해내기가 어렵다. 따라서 논문 [3]의 재전송 공격 분류를 토대로 프로토콜을 검증할 필요가 있다. 본 논문에서는 Paul Syverson이 정의한 재전송 공격의 분류를 토대로 이미 제안한 바 있는 패스워드 기반 인증 프로토콜 K1P[1,2]의 안전성을 검토 및 개선하는 한편 논문 [3]의 오류를 지적하도록 한다.

ABSTRACT

Authentication protocols required for securing computer communications, should be verified in terms of security against various protocol attacks. A replay attack which is one of those attacks, is classified into a lot of kinds. However, it is not so easy to detect it by formal methods because such a replayed message has data and structures equal to those of a message for the protocols. Therefore, it is recommended to verify the protocols with a taxonomy of [3] for a basis. In this paper, we improve the password-based authentication protocol K1P[1,2] on security against replay attacks on the basis of the Syverson's taxonomy, and comment on some mistake of [3].

I. 서 론

여러 사용자들이 원격으로 컴퓨터 자원에 접근할 수 있도록 하는 분산 환경에서는 사용자들의 신분을 확인하기 위한 인증(authentication) 기술이 시스템의 안전을 위해서 절대적으로 필요하다. 인증 프로토콜은 이와 같은 인증 기술의 구체적인 집합체로서 암호화 기술을 통하여 안전한 인증이 가능하도록 여러 단계의 메시지와 절차를 정의하는 규약이다.

1978년에 제안된 Needham-Shroeder 프로토콜[6]을 효시로 하여 다양한 종류의 프로토콜들이 계속해서 제안 및 적용되고 있다. 그러나 이러한 프로토콜들은 처음 제안되었을 때의 예상과는 달리 각기 다양한 공격에 의해서 그 취약점들이 드러나고 또한 개선되는 것을 반복하여 왔다. 그 예로써 Needham-Shroeder 프로토콜[6]은 Denning과 Sacco에 의해서 취약점이 발견되었으며[7], 이 프로토콜에 근간한 인증 시스템인 커베로스(Kerberos) 시스템 역시 그 취약점이 발견되었다[11]. 또한 패스워드 기

* 연세대학교 컴퓨터과학과(ktk@emerald.yonsei.ac.kr)
논문번호 : 98475-1028, 접수일자 : 1998년 10월 28일

www.dbpia.co.kr

반 인증 프로토콜인 GLNS 프로토콜[11]과 EKE 프로토콜[10]은 각각 Tsudik 등에 의해서 문제점이 발견되었으며[12,14], 논문 [14]에서 확장한 EKE 프로토콜은 Ding에 의해서 취약점이 발견되었다[15]. 이와 같이 인증 프로토콜의 안전성 여부가 계속해서 거론되는 것은 암호화 프로토콜의 안전성을 검증하는데 많은 어려움이 따르기 때문이다.

인증 프로토콜에 대한 공격에 대해서는 논문 [3]과 [5]에서 구체적으로 분류하고 있다. 또한 논문 [1], [2], [11], [15] 등에서는 패스워드 추측 공격에 대해서 분류하고 있다. 특히 논문 [3]에서는 인증 프로토콜에 대한 재전송 공격(replay attack)을 매우 명확하게 분류하였으며 또한 안전성의 분석 방법에 대한 고찰을 하였다. 이 논문에서는 현재 가장 널리 사용되는 인증 프로토콜 분석 방법인 형식 논리 모델링 기법이 재전송 공격에 대한 취약점을 발견하는데 한계가 있음을 언급하고 있는데, 따라서 이렇게 분석된 인증 프로토콜에 대해서는 구체적으로 재전송 공격에 대한 안전성을 검토할 필요가 있다.

선행 논문인 [1]과 [2]에서 제안된 패스워드 기반 인증 프로토콜 K1P는 대표적인 형식 논리 기법중 하나인 GNY 논리를 이용하여 검증된 바 있다. 따라서 본 논문에서는 논문 [3]에서 Paul Syverson이 정의한 재전송 공격의 분류를 토대로 하여 K1P의 재전송 공격에 대한 안전성을 검토한 후 발견된 취약점을 개선하도록 한다. 먼저 2장에서는 재전송 공격의 분류에 대해서 살펴보도록 하며, Syverson의 분류에서 발생할 수 있는 오류를 지적하고 수정하도록 한다. 3장에서는 K1P가 재전송 공격에 대해서 안전한지를 경험적인 방법을 통해서 검토한다. 4장에서는 K1P의 상호 인증 프로토콜에서 발견된 취약점을 개선한 후, 5장에서 결론을 맺는다.

Ⅱ. 재전송 공격의 분류

먼저 본 논문에서 사용될 표기법을 간단히 요약하면 [표 1]과 같다.

표 1. 표기법 요약

A, B	통신 참가자의 시스템 주체
A^*	A로 위장한 공격자
$na1$	A가 생성한 첫 난수
K_A	A의 공개키
K_{AS}	A와 S의 공유키, 즉 비밀키
$\|X\|$	X의 비트 길이
$h(M)$	메시지 M의 해쉬값
$k(M)$	입력값 M으로부터 정해진 크기의 세션키를 생성하기 위한 키 변환 함수
F_A	A가 전송한 메시지의 부분값
,	concatenator
$A \rightarrow B : X$	A가 메시지 X를 B에게 전송
S	서버의 시스템 주체
na	A가 생성한 난수
P_A	A가 선택한 패스워드, 즉 공유 비밀
K_S	S의 공개키
K	세션키
$\{M\}_K$	메시지 M을 암호키 K로 암호화한 결과
$f(M)$	미리 정의된 간단한 함수
$\oplus$	XOR 연산자
'	새로운 세션
''	새로운 라운드

2.1 Syverson의 분류

인증 프로토콜은 암호화 기술을 이용하여 메시지의 비밀성과 무결성을 보장하도록 하는 암호화 프로토콜의 대표적인 예로서 내부적으로 사용되는 암호화 알고리즘의 안전성보다는 프로토콜의 메시지와 전송 절차에 대한 안전성 문제를 프로토콜 자체의 안전성 문제로 다루게 된다. 따라서 암호화 알고리즘 자체는 안전하다고 가정하며 단지 메시지의 구성과 전송 절차 설계에 그 초점을 맞추게 되는 것이다. 이와 같은 관점에서 인증 프로토콜의 안전성 문제는 수년간에 걸쳐 논의되어 왔으며 실제로 이것을 분석하기 위한 방법들이 다양하게 제안되었다. 이것은 크게 경험적인 분석 기법(empirical analysis)과 형식적인 분석 기법(formal analysis)으로 나누어 볼 수 있겠다. 경험적인 기법은 프로토콜에 대해서 가능한 공격 등을 시도하여 직접 결과를 얻어내는 방법이며, 형식적인 기법은 형식 논리이나 대수 시스템 모델링 등을 통하여 정형화된 결과를 얻어내도록 하는 방법이다[17,19]. 그러나 경험적인 분석 기법과 형식적인 분석 기법에는 각각 한계가 있으며 따라서 일반적으로 두 방법을 병행하여 인증 프로토콜의 안전성을 평가한다.

인증 프로토콜에 대한 재전송 공격이란 어느 프로토콜 세션에서 이미 사용된 메시지를 어느 세션에서 재전송하여 프로토콜의 안전성을 파괴하는 행위를 일컫는다. 그러나 이렇게 단순해 보이는 재전송 공격은 다양하게 분류될 수 있으며, 형식적인 기

www.dbpia.co.kr

법으로 발전해 내는데는 한계가 있다[4]. 논문 [3]에서 Syverson은 재전송 공격을 구체적으로 분류하였다. 다음 표에서는 Syverson의 총분류를 요약하고 있다. 본 논문에서는 분류의 가시성을 위하여 각 분류 항목에 대해서 명확한 레이블을 부여하도록 한다.

표 2. Syverson의 총분류

분 류	비 고
I. 외부 공격 (External Attacks)	현재 프로토콜 세션의 외부로부터의 메시지를 재전송
A. 인터리빙 (Interleaving)	둘 이상의 프로토콜 세션을 반드시 동시에 수행
(a) 메시지 굴절 (Deflection)	메시지를 정해진 개체가 아닌 다른 개체에게 전송
(i) 반사 (Reflection)	메시지를 그 메시지의 전송자에게 되돌려 전송
(ii) 제3자 메시지 굴절	메시지를 제3자에게 전송
(b) 직렬 재전송 (Straight Replay)	메시지를 정해진 개체에게 재전송
B. 전형적 재전송 (Classic Replay)	둘 이상의 프로토콜 세션이 개별적으로 수행
(a) 메시지 굴절	메시지를 정해진 개체가 아닌 다른 개체에게 전송
(i) 반사	메시지를 그 메시지의 전송자에게 되돌려 전송
(ii) 제3자 메시지 굴절	메시지를 제3자에게 전송
(b) 직렬 재전송 (Straight Replay)	메시지를 정해진 개체에게 재전송
II. 내부 공격 (Internal Attacks)	현재 프로토콜 세션의 내부 메시지를 재전송
(a) 메시지 굴절	메시지를 정해진 개체가 아닌 다른 개체에게 전송
(i) 반사	메시지를 그 메시지의 전송자에게 되돌려 전송
(ii) 제3자 메시지 굴절	메시지를 제3자에게 전송
(b) 직렬 재전송 (Straight Replay)	메시지를 정해진 개체에게 재전송

Syverson은 이와 같은 재전송 공격 분류를 메시지 생성(origination)과 메시지 도착(destination)의 각 측면에서 구체적으로 분류하였다. 즉, [표 2]의 총 분류는 메시지 생성과 도착에 따라 분류되는 항목들의 결합체이다. 따라서 각 분류 항목을 생성 분류법과 도착 분류법으로 나누어 살펴볼 필요가 있다.

(1) 생성 분류(Origination Taxonomy)

이 분류법은 메시지를 생성하는 측면에서의 프로토콜 세션 실행에 초점을 두고 있다. 따라서 이 분류법을 통해서 메시지의 재전송이 프로토콜의 어느 부분에서 발생할 수 있는가를 살펴볼 수 있다.

재전송 공격의 생성 분류는 [표 2]의 항목들 중에서 I, II, A, B 항목에 해당한다. 즉, I-A 및 I-B 항목으로 세부 분류되는 I 항목과 II 항목으로 구성된다.

I 항목의 외부 공격이란 현재 수행중인 프로토콜 세션에서 생성되는 메시지가 아닌 외부의 메시지가 유입되는 공격을 통칭한다. 따라서 둘 이상의 프로토콜 세션이 필요하다. I-A 항목의 인터리빙 공격은 현재 수행중인 프로토콜과 동시에 수행되고 있는 다른 프로토콜 세션의 메시지가 유입되는 것을 말하며, I-B 항목의 전형적 재전송 공격은 이미 수행이 끝난 다른 프로토콜 세션의 메시지가 유입되는 것을 말한다. 즉, I-A 항목은 논문 [5]에서 정의한 병렬 세션 공격(parallel session attacks)이나 신탁 세션 공격(oracle session attacks)의 동기화된 수행 형태를 의미하며, II-B 항목은 메시지의 도청을 통해서 저장된 다른 프로토콜 세션의 메시지가 차후에 재전송되는 형태를 의미한다. II-B 항목의 대표적인 예로는 Needham-Shroeder 프로토콜[6]에 대해서 이루어진 Denning-Sacco 공격[7]을 들수 있다.

II 항목의 내부 공격이란 현재 수행중인 프로토콜 세션의 내부에서 전송되는 메시지가 재전송되는 공격을 통칭한다. 즉, I 항목에서는 둘 이상의 프로토콜 세션이 필요한 반면 II 항목은 단 하나의 프로토콜 세션으로 이루어진다는 명백한 차이점이 있다. 내부 공격은 논문 [16]에서 지적한 Neuman-Stubblebine 프로토콜에 대한 공격을 예로 들 수 있는데 이 프로토콜은 반복되는 인증의 효율성을 고려한 프로토콜로서[9] 공격자가 프로토콜의 두 번째 메시지를 네 번째 메시지로 위장하여 타인의 권한을 취득하거나 위조 세션키를 생성할 수도 있다.

(2) 도착 분류(Destination Taxonomy)

이 분류법은 메시지가 도착하는 측면에 초점을 두고 있다. 따라서 이 분류법을 통해서 메시지가 프로토콜 세션의 어느 개체에게 재전송될 수 있는가를 살펴볼 수 있다.

재전송 공격의 도착 분류는 [표 2]의 항목들 중에서 (a), (b), (i), (ii) 항목에 해당한다. 즉, (a)-(i) 및 (a)-(ii) 항목으로 세부 분류되는 (a) 항목과 (b) 항목으로 구성된다.

(a) 항목의 메시지 굴절이란 메시지를 프로토콜 세션에서 수신하도록 정해진 개체가 아닌 다른 개체에게 재전송하는 공격을 통칭한다. 즉, 메시지가 원래의 목적지로 가지 않고 다른 곳으로 전송되도

www.dbpia.co.kr

록 만드는 것이다. (a)-(i) 항목의 반사 공격은 메시지를 그 메시지의 전송자에게 되돌려 보내는 것을 의미하며, (a)-(ii) 항목의 제3자 메시지 굴절은 메시지가 그 메시지의 전송자나 수신자가 아닌 제3의 개체에게 재전송되는 것을 의미한다.

(b) 항목의 직렬 재전송이란 메시지가 프로토콜 세션에서 수신하도록 정해진 개체에게 전송되지만 전송 지연을 수반하게 되는 재전송 공격을 통칭한다. 그러나 이것은 단일 프로토콜 세션일 경우 강제 지연(forced delay) 공격과의 구분이 모호할 수 있으므로 명확한 정의를 필요로한다. 즉, 강제 지연 공격이란 공격자가 송수신 개체의 중간에 개입하여 메시지를 갈취한 후 일정한 시간이 지난 후 정해진 개체에게 단순히 중계하는 공격을 일컬으며, 따라서 이것은 재전송 공격으로 분류할 수 없다[19]. 다음의 2.2절에서는 이와 같은 문제에 대해서 검토하도록 한다.

2.2 직렬 재전송 공격의 재정의

논문 [3]에 따르면 직렬 재전송 공격이란, 어느 메시지가 정해진 개체에게 지연되어 전송되거나 메시지의 특성을 바꾸는 텍스트가 추가되는 경우라고 정의된다. 그러나 앞절에서 설명한 바와 같이 이와 같은 형태의 공격이 단일 프로토콜 세션의 같은 라운드에서 이루어질 경우에는 오히려 강제 지연 공격의 형태가 된다. 결과적으로 논문 [3]에서는 Yahalom 프로토콜 드래프트에 대한 재전송 공격 예제에서 강제 지연 공격을 직렬 재전송 공격으로 오판하여 분석하였다. 구체적으로 살펴보면 다음과 같다. 먼저 Yahalom 프로토콜 드래프트 버전은 다음과 같이 표기된다.

$$\begin{array}{l} 1.\ A \rightarrow B:\ A, na \\ 2.\ B \rightarrow S:\ B, nb, \{A, na\}_{K_{BS}} \\ 3.\ S \rightarrow A:\ nb, \{B, K, na\}_{K_{AS}}, \{A, K, nb\}_{K_{BS}} \\ 4.\ A \rightarrow B:\ \{A, K, nb\}_{K_{BS}}, \{nb\}_{K} \end{array} \quad (2.1)$$

이 프로토콜은 다음과 같이 재전송 공격에 노출된다[3].

$$\begin{array}{l} 1.\ A \rightarrow B^{*}:\ A, na \\ \quad 1'.\ B^{*} \rightarrow A:\ B, na \\ \quad 2'.\ A \rightarrow S^{*}:\ A, na', \{B, na\}_{K_{AS}} \\ \quad 2''.\ A^{*} \rightarrow S:\ A, na, \{B, na\}_{K_{AS}} \\ \quad 3'.\ S \rightarrow B^{*}:\ na, \{A, K, na\}_{K_{BS}}, \{B, K, na\}_{K_{AS}} \\ 2.\ - \\ 3.\ S^{*} \rightarrow A:\ ns, \{B, K, na\}_{K_{AS}}, \{A, K, na\}_{K_{BS}} \\ 4.\ A \rightarrow B^{*}:\ \{A, K, na\}_{K_{BS}}, \{ns\}_{K} \end{array} \quad (2.2)$$

먼저 단계 1과 1'에서 공격자는 B로 위장하여 I-A-(a)-(i) 항목의 반사 공격 형태로 A가 전송한 메시지 1을 단계 1'에서 A에게 재전송하였다. 여기서 단계 1과 1'는 각각 서로 다른 프로토콜 세션에 해당한다. 즉, 외부 공격의 인터리빙 분류 형태를 갖게 되며 명확한 재전송 공격이라고 할 수 있다. 단계 3'와 3에서는 I-A-(a)-(ii) 항목의 제3자 메시지 굴절에 해당하는 재전송이 이루어진다. 즉, 공격자는 단계 3'에서 B로 위장하여 S가 전달한 메시지의 암호문 $\{A, K, na\}_{K_{BS}}$, $\{B, K, na\}_{K_{AS}}$를 갈취한 후 다시 S로 위장하여 A에게 전송하였다. 결국 이 메시지는 $S \rightarrow B^{*} \rightarrow S^{*} \rightarrow A$의 순서로 B가 아닌 A, 즉 제3자에게 전송된 것이다. 이 공격 역시 외부 공격의 인터리빙 분류 형태를 갖는 것으로서 명확한 재전송 공격이다.

논문 [3]에서는 이와 함께 단계 2'와 2''에서 암호문 $\{B, na\}_{K_{AS}}$를 이용한 직렬 재전송 공격이 이루어지고 있다고 분석하고 있다. 즉, 공격자가 S와 A로 위장하여 단계 2'에서 S가 받아야 할 메시지를 가로챈 후 단계 2''에서 다시 S에게 전송한 것으로서 메시지가 $A \rightarrow S^{*} \rightarrow A^{*} \rightarrow S$의 순서로 S에게 지연되어 전달되므로 논문 [3]의 모호한 정의만으로는 직렬 재전송으로 오판되기 쉽다. 그러나 단계 2'와 2''는 같은 세션의 같은 라운드이므로 메시지의 재전송보다는 메시지의 지연된 중계로 분석하는 것이 타당하다. 여기서 라운드란 시간 단위별로 가능한 병렬 연결을 총칭한다[8]. 즉, 암호문 $\{B, na\}_{K_{AS}}$는 재사용된 것이라기보다 단지 중계 지연된 것이므로 재전송 공격이라고 할 수 없다. 따라서 단일 프로토콜 세션일 경우에는 서로 다른 라운드에서만 메시지의 재전송이 가능하다고 할 수 있다.

결국 여기서 암호문 $\{B, na\}_{K_{AS}}$는 강제 지연된 것이며 이것이 단계 2'와 2''에서의 취약점이 되지는 않는다. 오히려 이 단계에서의 결정적인 취약점은 단계 1'의 평문 na가 단계 2''에서 II-(a)-(ii) 항목의 제3자 메시지 굴절 형태로 재전송된 것이다. 이와 같은 논문 [3]의 오류는 직렬 재전송 공격의 모호한 정의에서 비롯된 것이며, 따라서 직렬 재전송 공격을 다음과 같이 프로토콜 라운드를 고려하여 명확하게 재정의할 필요가 있다.

[정의 1] 직렬 재전송 공격은 메시지가 서로 다른 프로토콜 라운드나 서로 다른 프로토콜

www.dbpia.co.kr

세션에서 정해진 개체에게 지연되어 전송되거나 메시지의 특성을 바꾸는 텍스트가 추가되는 경우를 의미한다.

따라서 본 논문에서는 이와 같은 명확한 분석을 토대로 하여 Yahalom 프로토콜 드래프트의 단계 1, 2, 3에서 발생할 수 있는 각각의 재전송 공격에 대한 안전성을 보강하도록 한다. 먼저 단계 1의 반사 공격을 무의미하게 만들기 위해서는 na를 전송자의 비밀키, 즉 K_{AS}로 암호화하도록 한다. 이 경우 단계 1'에서와 같은 반사 공격은 무의미하게 된다. 한편 단계 2''에서와 같은 제3자 굴절 역시 무의미하게 하기 위해서는 단계 2의 nb역시 K_{BS}로 암호화된 암호문에 포함되도록 한다. 또한 단계 3에서와 같은 제3자 굴절을 무의미하게 만들기 위해서 단계 3의 각 암호문의 구조를 서로 비대칭적으로 구성하도록 한다. 이와 같이 수정된 프로토콜은 다음과 같다.

$$\begin{aligned}
&1.\ A \rightarrow B:\ A, \{na\}_{K_{AS}} \\
&2.\ B \rightarrow S:\ B, \{nb, A, na\}_{K_{BS}} \\
&3.\ S \rightarrow A:\ \{B, K, na, nb\}_{K_{AS}}, \{A, K, nb\}_{K_{BS}} \\
&4.\ A \rightarrow B:\ \{A, K, nb\}_{K_{BS}}, \{nb\}_{K}
\end{aligned} \tag{2.3}$$

이와 같이 본 논문에서 수정된 Yahalom 프로토콜 드래프트 (2.3)은 (2.2)와 같은 복합적인 형태의 재전송 공격에 대해서 안전하다. 기타 재전송 공격의 구체적인 예는 논문 [3], [4], [5], [7], [16] 등을 참고하여 살펴볼 수 있다.

Ⅲ. K1P에 대한 재전송 공격 검토

선행 논문인 [1]과 [2]에서는 패스워드 기반 인증 프로토콜인 K1P를 제안하였다. 특히 [1]에서는 대표적인 형식 분석 방법인 GNY 논리[18]을 이용하여 프로토콜 분석을 한 후 타 패스워드 기반 프로토콜들과 효율성 비교를 하였으며, [2]에서는 K1P를 더욱 확장하여 다양한 환경에서 적용될 수 있는 프로토콜들을 제시하였다. 그러나 선행 논문에서의 프로토콜 안전성 분석은 패스워드 추측 공격에 대해서 초점이 맞추어졌으며 특히 재전송 공격에 있어서도 메시지 재전송을 통한 온라인 및 오프라인 패스워드 분석에 대한 안전성만을 다루었다. 따라서 K1P에 대한 재전송 공격을 경험적 분석 기법을 통해서 검토할 필요가 있다. K1P는 직접 인증 프로토콜과 상호 인증 프로토콜로 구성되며 논문 [2]에서 확장된 프로토콜은 모두 직접 인증 프로토콜의 구조에 기반하므로 본 장에서는 직접 인증 프로토콜과 상호 인증 프로토콜에 대해서 검토하도록 한다. 프로토콜의 검토 순서는 [표 2]의 분류를 따르도록 한다.

3.1 직접 인증 프로토콜에 대한 재전송 공격

K1P 직접 인증 프로토콜은 패스워드를 기반으로 하는 클라이언트-서버 환경에서 적용하기에 적합하며 다음과 같이 두가지 종류가 있다[1].

(i)

$$\begin{aligned}
&1.\ A \rightarrow S:\ A,\ \{na1, na2, P_A \oplus na1\}_{K_S} \\
&2.\ S \rightarrow A:\ na1 \oplus na2 \oplus K,\ h(P_A \oplus na1, K, na2) \\
&3.\ A \rightarrow S:\ h(P_A \oplus na2, K, na1)
\end{aligned} \tag{3.1-i}$$

(ii)

$$\begin{aligned}
&1.\ A \rightarrow S:\ A,\ \{na, P_A \oplus na\}_{K_S} \\
&2.\ S \rightarrow A:\ na \oplus ns,\ h(P_A \oplus na, ns) \\
&3.\ A \rightarrow S:\ h(P_A \oplus ns, K, na) \\
&\quad (a)\ K = k(h(na, ns)) \\
&\quad (b)\ K = k(g^{xy} \bmod n) \\
&\quad (na = g^x \bmod n,\ ns = g^y \bmod n)
\end{aligned} \tag{3.1-ii}$$

프로토콜 (3.1-i)에서는 패스워드 P_A를 통해서 S가 A를 쉽게 인증하고 세션키 K를 안전하게 분배할 수 있으며, 패스워드 추측 공격에 대해서 안전하다. 프로토콜 (3.1-ii)에서는 해쉬 함수나 Diffie-Hellman 방식[9], 즉 지수적 키 교환 (exponential key exchange) 방법을 통해서 A와 S가 서로 합의하에 세션키를 공동으로 생성할 수 있다. 프로토콜 (3.1-i)와 (3.1-ii)는 세션키 생성 방법이 다를 뿐 사실상 같은 구조를 갖고 있으므로 (3.1-i)에 대한 재전송 공격을 검토하도록 한다.

(1) 외부 공격의 인터리빙

[표 2]의 I-A 항목에 해당하는 인터리빙 공격 가능성을 검토한다. 이 공격을 위해서는 적어도 두 프로토콜 세션을 열어야 하며 또한 두 세션을 동시에

www.dbpia.co.kr

수행해야 한다.

먼저 I-A-(a) 항목의 메시지 굴절 공격을 살펴보면, 단계 1의 메시지는 S의 공개키로 암호화된 만큼 굴절시킬 수 없으며 단계 2와 3의 메시지는 메시지 1의 논스값을 암호화하였으므로 굴절시킬 수 없다. 따라서 반사 공격이나 제3자 메시지 굴절 공격이 불가능하다.

I-A-(b) 항목의 직렬 재전송 공격을 살펴보면, 프로토콜의 각 메시지는 현재 세션에서 생성된 난수를 암호화하여 포함하고 있을 뿐만 아니라 각 개체의 신원에 바인딩되어 있으므로 외부 세션 메시지의 직렬 재전송 공격이 불가능하다.

(2) 외부 공격의 전형적 재전송

I-B 항목의 전형적 재전송 공격을 살펴본다. 이 공격을 위해서는 이미 수행이 끝난 이전 프로토콜 세션에서 도청된 메시지가 새로운 세션에서 재사용된다.

I-B-(a) 항목의 메시지 굴절 공격을 살펴보면, 인터리빙 공격에서와 같은 이유로 각 메시지는 굴절될 수 없다.

I-B-(b) 항목의 직렬 재전송 공격을 살펴보면, 공격자는 이전 세션에서 도청한 메시지 1을 새로운 세션을 열어서 S에게 전송할 경우 S의 응답 메시지 2를 얻을 수 있지만 일시 패드(One-time pad)[1,2,19]인 $na1 \oplus na2$를 모르는 공격자는 세션키를 얻거나 메시지 3으로 응답할 수 없다. 비록 공격자가 이전 세션의 세션키를 분석하여 일시 패드를 알아냈더라도 이 일시 패드로 암호화된 새로운 세션키를 발견할 수 있을 뿐 각 논스값을 알 수 없기 때문에 메시지 3을 구성할 수 없다. 따라서 이 공격은 역시 불가능하다. 이것은 선행 논문 [1]에서 메시지 1의 재전송을 통한 패스워드 추측 공격의 형태로 분석되었다.

(3) 내부 공격

두 개체 사이에 단지 3단계로 메시지를 교환하도록 하는 직접 인증 프로토콜은 각 단계의 메시지가 각각 방향성과 서로 다른 구조를 가지며 또한 메시지가 패스워드와 식별자를 포함하여 인증성을 보유하므로 내부적으로 굴절시키거나 직렬 재전송 할 수 없다.

3.2 상호 인증 프로토콜에 대한 재전송 공격

K1P 상호 인증 프로토콜은 패스워드를 기반으로 하고 안전성 센터의 설치가 가능한 통신망 환경에서 적용하기에 적합하며 다음과 같이 구성된다.

$$
\begin{aligned}
&1.\ A \rightarrow B:\ \{A, B, na1, na2, P_A \oplus na1\}_{Ks}\\
&2.\ B \rightarrow S:\ \{A, B, na1, na2, P_A \oplus na1\}_{Ks},\\
&\qquad\quad \{B, A, nb1, nb2, P_B \oplus nb1\}_{Ks}\\
&3.\ S \rightarrow B:\ na1 \oplus na2 \oplus K, h(P_A \oplus na1, K, na2, A \oplus B),\\
&\qquad\quad nb1 \oplus nb2 \oplus K, h(P_B \oplus nb1, K, nb2, A \oplus B)\\
&4.\ B \rightarrow A:\ na1 \oplus na2 \oplus K, h(P_A \oplus na1, K, na2, A \oplus B),\\
&\qquad\quad \{f(F_A), nb1 \oplus nb2\}_K\\
&5.\ A \rightarrow B:\ \{f(nb1 \oplus nb2)\}_K
\end{aligned}
\qquad (3.2)
$$

이 프로토콜의 특징은 메시지 1의 부분값을 정해진 함수로 처리한 결과 $f(F_A)$와 이미 구성한 일시 패드 $nb1 \oplus nb2$를 세션키 K로 암호화하여 세션키 분배 확인을 위한 도전-응답(challenge-response)값으로 이용한다는 점이다[1].

(1) 외부 공격의 인터리빙

먼저 I-A-(a) 항목의 메시지 굴절 공격을 살펴보면, 단계 1과 2의 메시지는 S의 공개키로 암호화되어 있을 뿐만 아니라 A와 B의 식별자가 메시지 주체의 패스워드와 함께 암호화된 메시지 내부에 포함되어 있으므로 굴절시킬 수 없으며 단계 3와 4의 메시지는 메시지 1과 2의 논스값과 A와 B의 식별자를 각각의 패스워드와 함께 암호화하였으므로 역시 굴절시킬 수 없다. 따라서 반사 공격이나 제3자 메시지 굴절 공격이 불가능하다.

I-A-(b) 항목의 직렬 재전송 공격을 살펴보면, 직접 인증 프로토콜에서와 같이 프로토콜의 각 메시지가 현재 세션의 난수를 암호화하여 포함하고 있을 뿐만 아니라 각 개체의 신원에 바인딩되어 있으므로 이와 같은 직렬 재전송 공격은 불가능하다.

(2) 외부 공격의 전형적 재전송

I-B-(a) 항목의 메시지 굴절 공격을 살펴보면, 인터리빙 공격의 경우와 마찬가지로 각 메시지는 굴절될 수 없다.

I-B-(b) 항목의 직렬 재전송 공격을 살펴보면, 공격자가 이전 세션에서 도청한 메시지 1을 새로운 세션을 열어서 B에게 전송할 경우 B는 메시지 2를 S에게 전송하고 프로토콜은 진행된다. 이 때 일시 패드(One-time pad)[1,2,19]인 $na1 \oplus na2$를 모르는 공격자는 세션키를 얻거나 메시지 5로 상호 인증을 진행할 수 없다. 그러나 Denning-Sacco 공격[7]과 같이 공격자가 이전 세션의 세션키를 분석하였

www.dbpia.co.kr

을 경우는 다르다. 이 경우에는 이전 세션의 일시 패드, 즉 도청한 메시지 1에 의해서 만들어지는 일시 패드를 이전 세션의 메시지 3에서 XOR 연산을 하여 쉽게 얻을 수 있다. 이렇게 일시 패드를 알아냈을 경우에는 (3.3)의 단계 4'에서와 같이 새로운 세션키를 알아낼 수 있을 뿐만 아니라 메시지 5를 구성하여 B와 함께 상호 인증한 후 통신을 할 수 있게 된다.

.....

3. $S \rightarrow B$: $na1 \oplus na2 \oplus K, h(P_A \oplus na1, K, na2)$, $nb1 \oplus nb2 \oplus K, h(P_B \oplus nb1, K, nb2)$
4. $B \rightarrow A^*$: $na1 \oplus na2 \oplus K, h(P_A \oplus na1, K, na2)$, $\{f(F_A), nb1 \oplus nb2\}_K$
4'. A^* : $(na1 \oplus na2 \oplus K) \oplus (na1 \oplus na2) = K$
5. $A^* \rightarrow B$: $\{f(nb1 \oplus nb2)\}_K$

(3.3)

결국 I-B-(b) 항목의 재전송 공격에 노출된다는 사실을 발견할 수 있다. 본 논문의 4장에서는 이와 같은 취약점을 개선하도록 한다.

(3) 내부 공격

상호 인증 프로토콜 역시 직접 인증 프로토콜과 마찬가지로 각 단계의 메시지가 각각 방향성과 서로 다른 구조를 가지며 또한 메시지가 패스워드와 식별자를 포함하여 인증성을 보유하므로 내부적으로 굴절시킬 수 없다.

Ⅳ. 상호 인증 프로토콜의 개선

이와 같이 K1P는 상호 인증 프로토콜이 I-B-(b) 항목의 재전송 공격에 노출된다. 이것은 선행 논문에서 발견하지 못한 취약점으로서 본 논문에서 개선되어야 할 사항이다. 본 장에서는 개선된 상호 인증 프로토콜을 제안하고 검증하도록 한다.

4.1 개선된 상호 인증 프로토콜

3.2-(2)절의 (3.3)에서와 같이 상호 인증 K1P에서 과거 세션에서 사용된 세션키의 분석으로 말미암아 일시 패드가 노출되는 경우 이 때 사용된 메시지 1을 재전송하면 단계 4에서 새로운 세션키를 복호화하여 단계 5에서 상호 인증을 이룰 수 있으며 또한 불법적인 통신을 계속 진행할 수 있다는 문제점이 있다. 그 이유는 일시 패드로 암호화된 세션키의 확인과 상호 인증이 단계 4와 5에서 A와 B 사이에 공유 비밀 없이 이루어지기 때문으로 분석된다. 여기서 공유 비밀이란 패스워드를 일컫는다. 그러나 직접 인증 프로토콜에서는 단계 2에서 일시 패드로 암호화된 세션키에 대한 확인이 인증 확인과 함께 단계 3에서 공유 비밀을 포함하여 이루어지기 때문에 이러한 재전송 공격에 노출되지 않는다. 즉, 공격자는 단계 2에서 노출된 일시 패드를 이용하여 새로운 세션키를 복호화하더라도 공유 비밀을 모르기 때문에 단계 3의 메시지를 구성하여 인증 절차를 마치는 것이 불가능한 것이다. 반면에 상호 인증 프로토콜의 단계 4와 5는 프로토콜의 효율상 A와 B의 공유 비밀을 알고 있는 S의 참여 없이 세션키와 인증 확인을 이루기 때문에 공격자가 쉽게 메시지 4를 복호화한 후 메시지 5를 구성할 수 있는 것이다.

따라서 이와 같은 문제를 해결하기 위해서는 세션키 분석에 따른 일시 패드의 노출을 막기 위해서 일반적인 관용 암호화 방식을 사용할 수 있도록 하면 된다. 즉, 단계 3에서 세션키를 일시 패드가 아닌 일시 키[11]를 통해서 암호화한 후 분배하도록 하여 해결할 수 있다. 개선된 상호 인증 프로토콜은 다음과 같다.

1. $A \rightarrow B$: $\{A, B, na1, na2, P_A \oplus na1\}_{K_s}$
2. $B \rightarrow S$: $\{A, B, na1, na2, P_A \oplus na1\}_{K_s}$, $\{B, A, nb1, nb2, P_B \oplus nb1\}_{K_s}$
3. $S \rightarrow B$: $\{na1, K\}_{k(h(P_A \oplus na1, na2, A \oplus B))}$, $\{nb1, K\}_{k(h(P_B \oplus nb1, nb2, A \oplus B))}$
4. $B \rightarrow A$: $\{na1, K\}_{k(h(P_A \oplus na1, na2, A \oplus B))}$, $\{f(F_A), nb1 \oplus nb2\}_K$
5. $A \rightarrow B$: $\{f(nb1 \oplus nb2)\}_K$

(4.1)

단계 1과 2는 기존의 상호 인증 K1P와 같이 이루어지며, 단계 3에서 A와 B를 인증한 후 새로운 세션키를 생성한 S는 기존 K1P에서와 같이 해쉬값을 계산한다. 그리고 이 값을 키 생성 함수 $k()$를 사용하여 암호화 알고리즘에 맞는 크기의 키로 변환한 후 논스값과 세션키를 암호화한다. 단계 4와 5는 기존의 상호 인증 K1P와 같이 이루어진다.

4.2 프로토콜 검증

개선된 상호 인증 프로토콜은 기존 프로토콜과 메시지를 구성하는 요소들이 같으며 단지 달라진 것이 있다면 단계 3에서 세션키를 암호화하는 방법이다. 그러나 세션키의 암호화를 위해서 사용된 일시 키 역시 기존 프로토콜에서 무결성 보장을 위한

www.dbpia.co.kr

해쉬값을 그대로 이용하였다. 따라서 기존 프로토콜이 갖는 안전성을 그대로 유지할 수 있다[1].

기존 프로토콜의 취약점인 I-B-(b) 항목의 재전송 공격에 대한 안전성 여부를 살펴보면, 이전 세션의 세션키가 노출되었을 경우 공격자는 이전 세션의 메시지 3을 이용하여 K를 암호화한 키를 발견할 수 없다. K에 대한 알려진 평문 공격을 시도하더라도 난수 na를 알 수 없으므로 많은 계산량을 요구한게 된다. 따라서 공격자가 도청한 메시지 1을 재전송하더라도 새로운 세션의 단계 4에서 새로운 세션키를 복호화하는 것은 계산적으로 불가능하며 결국 단계 5를 수행할 수 없으므로 개선된 상호 인증 프로토콜은 I-B-(b) 항목의 재전송 공격에 대해서도 안전하다.

4.3 프로토콜 효율성 평가

패스워드 기반 인증 프로토콜은 기존 인증 프로토콜과는 달리 불안전한 공유 비밀을 보호하기 위해서 많은 오버헤드를 수반한다[1,2,12,13,14]. 따라서 프로토콜의 효율성을 고려하여야 할 것이다. 본 절에서는 선행 논문 [1]에서 검토한 효율성 비교 결과와 마찬가지로 모든 패스워드 추측 공격에 대해서 안전한 것으로 알려져 있는 상호 인증 프로토콜인 GLNS nonce 프로토콜과 Gong의 Optimal 프로토콜을 비교 대상으로 삼아 개선된 상호 인증 K1P의 효율성을 [표 3]과 같이 검토한다.

[표 3]은 각 프로토콜의 단계, 난수 생성 횟수, 그리고 공개키 암호화, 대칭키 암호화, 일방향 해쉬 등의 각종 암호화 관련 연산 횟수를 정량적으로 비교한다. 이와 같은 항목에 대한 비교는 $f()$나 $h()$와 같은 함수가 프로토콜의 전체 성능에 미치는 영향이 미약한 반면 [표 3]의 비교 항목들은 연산 횟수가 늘어날 경우 프로토콜의 전체 성능에 미치는 영향이 크기 때문이다.

[표 3]에는 기존 상호 인증 K1P의 항목들도 포함하였다. 물론 개선된 상호 인증 K1P와 기존 프로토콜과의 차이점은 개선된 프로토콜이 관용 암호화 연산을 A, B와 S 사이에서 한번씩 더 수행한다는 것이다. 따라서 개선된 K1P는 여전히 GLNS nonce 프로토콜보다 프로토콜 단계수가 2회 적을 뿐만 아니라 난수 생성 횟수가 절반 이상 적다. 또한 GLNS의 효율성을 개선한 Gong의 Optimal 프로토콜보다도 난수 생성 횟수가 적다. 암호화 관련 연산 횟수는 A, B와 S 사이에서 개선된 K1P의 관용 암호화 연산이 GLNS나 Optimal 프로토콜보다 1회씩 적은 반면 해쉬 연산이 1회씩 많다. 결과적으로 개선된 K1P는 기존 K1P 상호 인증 프로토콜보다 관용 암호화 연산 횟수가 조금 늘어났지만, GLNS나 Optimal 프로토콜보다는 더 효율적이다.

표 3. 프로토콜의 효율성 비교

프로토콜	프로토콜 단계	난수 생성 횟수		암호화 관련 연산 횟수			
					Pub.	Conv.	Hash.
개선된 상호 인증 K1P	5	A	2	A-S	1	1	1
		B	2	B-S	1	1	1
		S	0	A-B	0	2	0
상호 인증 K1P[1,2]	5	A	2	A-S	1	0	1
		B	2	B-S	1	0	1
		S	0	A-B	0	2	0
GLNS nonce[11]	7	A	4	A-S	1	2	0
		B	4	B-S	1	2	0
		S	1	A-B	0	2	0
Gong Optimal[13]	5	A	5	A-S	1	2	0
		B	5	B-S	1	2	0
		S	0	A-B	0	2	0

V. 결 론

본 논문에서는 먼저 논문 [3]에서 Syverson이 분류한 재전송 공격을 면밀히 검토한 후, 직렬 재전송 공격에 대한 논문 [3]의 오류를 지적하고 재정의하는 한편 Yahalom 프로토콜 드래프트의 안전성 강화 방법에 대해서 살펴보았다. 그리고 이 분류를 통하여 선행 논문인 [1]과 [2]에서 제안한 바 있는 패스워드 기반 인증 프로토콜 K1P의 재전송 공격에 대한 안전성 여부를 검토하였다. 여기서 K1P의 상호 인증 프로토콜이 분류표인 [표 2]의 I-B-(b) 항목에 해당하는 재전송 공격에 노출된다는 사실을 발견하였으며, 이것을 해결하는 한편 효율성을 고려하도록 상호 인증 프로토콜을 개선하였다. 개선된 상호 인증 K1P는 여전히 효율적인 패스워드 기반 인증 프로토콜로서 패스워드가 사용되는 분산환경에서 적용될 수 있는 인증 프로토콜이다.

그러나 본 논문에서는 재전송 공격에 대한 안전성 분석이 경험적인 기법을 토대로 하여 비형식적으로 이루어졌다. 따라서 이와 같이 재전송 공격 여부를 발견하고 모델링 할 수 있는 형식적인 기법이 마련되어야 할 것이다. 재전송 공격에 대한 검증은 현재 NRL 프로토콜 분석기[9]를 제외한 나머지 일

www.dbpia.co.kr

반적인 형식적 기법으로는 어렵다고 알려져 있다[3,4]. 따라서 재전송 공격을 고려한 보다 폭넓은 기능의 형식적인 분석 방법 개발이 요구된다. 결과적으로 설계된 프로토콜의 재전송 공격에 대한 안전성 분석을 보다 형식적인 방법으로 이룰 수 있는 연구를 향후 진행해야 하겠다.

참 고 문 헌

[1] 권태경, 송주석, "패스워드 기반 인증 프로토콜 K1P의 확장," 한국통신학회 논문지, 제23권 제7호, pp. 1851-1859, Jul. 1998

[2] 권태경, 송주석, "추측 공격에 대해서 안전하고 효율적인 패스워드 기반 인증 프로토콜," 한국정보과학회 논문지(A), 제24권 제8호, pp. 795-806, Aug. 1997

[3] P.Syverson, "A Taxonomy of Replay Attacks,"

[4] L.Gong, "Variations on the Themes of Message Freshness and Replay or, the Difficulty of Devising Formal Methods to Analyze Cryptographic Protocols," Proceedings of the Computer Security Foundations Workshop VI, pp. 131-136, 1993

[5] R.Bird, I.Gopal, A.Herzberg, P.A.Janson, S.Kutten, R.Molva, M.Yung, "Systematic Design of a Family of Attack-Resistant Authentication Protocols," IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, pp. 679-693, June 1993

[6] R.Needham, M.Schroeder, "Using Encryption For Authentication in Large Networks of Computers," Communications of the ACM, vol. 21, no. 12, pp.993-999, Dec. 1978

[7] D.Denning, G.Sacco, "Timestamps in Key Distribution Protocols," Communications of ACM, vol. 24, no. 8, pp. 533-536, Aug. 1981

[8] L.Gong, "Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations," Distributed Computing, vol. 9, no. 3, pp.131-145, 1995

[9] B.Schneier, *Applied Cryptography*, 2nd Ed., John Wiley & Sons, 1996

[10] S.Bellovin, M.Merrit, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," Proceedings of the IEEE Symposium on Security and Privacy, pp. 72-84, 1992

[11] L.Gong, M.Lomas, R.Needham, J.Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks," IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, pp. 648-656, June 1993

[12] G.Tsudik, E.Van Herreweghen, "Some Remakrs on Protecting Weak Keys and Poorly-Chosen Secrets from Guessing Attacks," 1993 IEEE Symposium on Reliable Distributed Systems, pp. 136-142, 1993

[13] L.Gong, "Optimal Authentication Protocols Resistant to Password Guessing Attacks," Proceedings of the 8th IEEE Computer Security Foundations Workshop, pp. 24-29, June 1995

[14] M.Steiner, G.Tsudik, M.Waidner, "Refinement and Extension of Encrypted Key Exchange," ACM Operating System Review, vol. 29, no. 3, pp. 22-30, 1995

[15] Y.Ding, P.Horster, "Undetectable On-line Password Guessing Attacks," ACM Operating Systems Review, vol. 29, no. 4, pp. 77-86, Oct. 1995

[16] P.Syverson, "On Key Distribution Protocols for Repeated Authentication," ACM Operating Systems Review, vol. 27, no. 4, pp. 24-40, Oct. 1993

[17] M.Burrows, M.Abadi, R.Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, Feb. 1990

[18] L.Gong, R.Needham, R.Yahalom, "Reasoning about Belief in Cryptographic Protocols," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp.234-248, 1990

[19] A.Menezes, P.van Oorschot, S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997

www.dbpia.co.kr

권 태 경(Taekyoung Kwon) 정회원
통신학회논문지 제23권 제7호 p.1859 참조

송 주 석(Jooseok Song) 정회원
통신학회논문지 제23권 제7호 p.1859 참조

www.dbpia.co.kr