이동 통신 환경에서의 종단간 키 교환 프로토콜

심학섭[0] 임수철 김선형 김태윤
고려대학교 컴퓨터학과
{100tpig[0], causal, shaklim, tykim}@netlab.korea.ac.kr

An End-to-End Key Exchange Protocol in Mobile Communication Environment

Hak-Sub Sim[0] Soo-Chul Lim Sun-Hyoung Kim Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

본 논문에서는 이동 통신 환경에 적합한 키 교환 프로토콜의 기본적인 보안 요소와 요구되는 사항들을 살펴보고 기존의 키 교환 프로토콜들을 분석하여 제시한 보안 요소의 만족여부를 살펴본다. 또한 이를 기반으로 이동 통신 환경에 적합한 End-to-End 키 교환 프로토콜을 제안하고 이를 기존의 키 교환 프로토콜들과 비교 분석한다. 제안된 키 교환 프로토콜은 이동 통신 단말기에서의 공개키 연산과 교환되는 메시지 수를 줄여 기존의 키 교환 프로토콜과 비교해 볼 때 보다 더 효율적이다.

1. 서 론

이동 통신의 가입자가 크게 늘면서 이동 통신 단말기 사용의 폭이 넓어졌다. 이러한 이동 통신이 무선 통신망을 사용함으로써 야기되는 문제점들로 인해 m-commerce와 같은 사용자를 위한 서비스가 안전하게 제공되기 어렵다. 또한 이동 통신 단말기의 소형화로 인한 낮은 계산 능력과 처리량의 한계도 문제가 되고 있다.

본 논문에서는 이러한 문제점들을 고려하여 요구되는 기본적인 보안 사항을 만족시키고 적은 메시지 교환과 이동 통신 단말기에서의 낮은 계산량을 보이는 키 교환 프로토콜을 제안하고자 한다.

우선 기존의 키 교환 프로토콜들을 분석하고 제시한 보안 요소들을 어떻게 만족시키는지 살펴본다. 이러한 프로토콜들을 기반으로 End-to-End 보안을 지원하는 키 교환 프로토콜을 제안한다. 제안한 키 교환 프로토콜은 VM(Varadharajan-Mu) 프로토콜[1]을 개선한 키 교환 프로토콜로서 보다 향상된 성능을 보여준다.

본 논문의 구성은 다음과 같다. 2장에서는 이동 통신 환경에서 키 교환 프로토콜이 고려해야할 사항들을 살펴보고, 기존의 키 교환 프로토콜들을 분석한다. 3장에서는 새로운 키 교환 프로토콜을 제안하고 분석하며 4장에서 제안한 프로토콜과 기존의 프로토콜들을 비교 및 성능평가를 하고 5장에서 결론을 내린다.

2. 관련 연구

2.1 키 교환 프로토콜에서의 보안 요소

키 교환 프로토콜은 기밀성, 무결성, 인증, 부인방지 등과 같은 다음의 기본적인 보안 요소들을 만족해야 한다[2].

▪기밀성(Confidentiality)

허가되지 않거나 의도되지 않은 사용자로부터 정보를 보호하는 것으로, 기밀성 제공을 위한 기본적인 기술로는 데이터 암호화를 사용한다.

▪무결성(Integrity)

교환되는 정보는 악의적인 목적에 의해 중간에 변경되거나 임의로 생성 및 파괴되어서는 않된다. 메시지 다이제스트를 이용해 정보의 변경 여부를 확인할 수 있다.

▪인증(Authentication)

기본적인 보안 요소로서 통신에 참여하는 상대 개체의 신원을 검증하는 것이다. 자신을 입증할 수 있는 정보를 교환함으로써 서로 상대를 인증한다. 신뢰할 수 있는 인증기관에서 자신을 인증한 인증서를 주로 사용한다.

▪부인방지(Non-repudiation)

보안에 관련된 행동이나 자신이 보낸 정보들을 나중에 부인할 수 없도록 하는 것으로, 디지털 서명과 같은 암호학 기술들이 사용된다.

2.2 이동 통신 환경에서의 요구 사항

이동 통신 단말기의 소형화로 인하여 사용자의 이동성이 증가하고 사용이 편리해졌으나 그만큼 이동 통신 단말기의 전원 보유량이 감소해 계산 능력과 처리량이 줄어들었다. 다음과 같은 사항들을 줄임으로써 이동 통신 단말기의 부하를 감소시킬 수 있다.

▪공개키 연산량

연산량이 많이 드는 공개키의 사용을 줄이기 위해 복잡한 계산은 기지국으로 넘겨 이동 통신 단말기에서의 연산량을 줄인다.

▪메시지 교환 횟수

쓸데없는 정보의 유출을 막고 통신으로 인한 부하를 줄이기 위해 교환되는 메시지의 수를 줄인다.

2.3 기존의 키 교환 프로토콜

본 절에서는 공개키를 이용한 기존의 키 교환 프로토콜들을 분석한다. 기본적인 프로토콜의 표기 형식은 <표 1>과 같다.

<표 1> 기호의 정의

기호	정의
$B, M, M1$	식별자 (M:이동국, B:기지국)
N_X	X가 생성한 난수
PK_X	X의 공개키
PK_X^{-1}	X의 개인키
$Cert(X)$	X의 인증서
$h(M)$	메시지 M을 압축하는 일방향 해쉬 함수
$\{M\}_K$	키 K를 사용하여 메시지 M을 암호화
$\{M\}_{PK_X^{-1}}$	X의 개인키를 사용하여 메시지 M을 전자서명

2.3.1 MSR(Modulo Square Root) + DH(Diffie-Hellman) 프로토콜

BCY 키 교환 프로토콜을 Carlsen이 개선하여 제안한 프로토콜로 Link 범위의 보안을 지원한다[3].

(1) $B \rightarrow M$: $B, N_B, PK_B, Cert(B)$

(2) $M \rightarrow B$: $\{x\}_{PK_B}, \{N_B, M, PK_M, Cert(M)\}_x$

이 프로토콜은 사용자 인증 및 기밀성을 제공한다.

2.3.2 BY(Beller and Yacobi) 프로토콜

Beller와 Yacobi가 제안한 Link 범위의 키 교환 프로토콜을 Boyd와 Mathuria가 취약점을 보완해 다음과 같은 개선된 프로토콜을 제안하였다[4].

(1) $B \rightarrow M$: $B, PK_B, Cert(B), N_B$

(2) $M \rightarrow B$: $\{x\}_{PK_B}, \{M, PK_M, Cert(M)\}_x,$
$\{h(B, M, N_B, x)\}_{PK_M^{-1}}$

(3) $B \rightarrow M$: $\{N_B\}_x$

MSR+DH 프로토콜과 비교해 볼 때 전자서명이 사용되어 부인방지와 무결성이 추가되었다.

2.3.3 AD(Aziz-Diffie) 프로토콜

Aziz와 Diffie가 제안한 Link 범위의 키 교환 프로토콜[5]이 Boyd와 Mathuria에 의해 취약점이 발견되면서 다음과 같은 개선된 키 교환 프로토콜이 제안되었다[4].

기지국과 이동국 각각 정보를 생성해 교환한 후에 서로 교환한 정보를 이용해 세션키를 생성한다.

(1) $M \rightarrow B$: $Cert(M), N_M, alg\_list$

(2) $B \rightarrow M$: $Cert(B), N_B, \{x_B\}_{PK_M}, sel\_alg,$
$\{h(x_B, M, N_M, sel\_alg)\}_{PK_B^{-1}}$

(3) $M \rightarrow B$: $\{x_M\}_{PK_B}, \{h(x_M, B, N_B)\}_{PK_M^{-1}}$

* alg_list : 이동국이 선택한 공개키 알고리즘 리스트
* sel_alg : alg_list에서 기지국이 선택한 알고리즘

모든 보안요소를 만족하나 이동국에서의 많은 공개키 연산으로 인하여 부하가 심하다.

2.3.4 VM(Varadharajan-Mu) 프로토콜

Varadharajan과 Mu에 의해 제안된 End-to-End 범위의 키 교환 프로토콜이다[1].

Diffie-Hellman 키 교환 기법을 이용해 서로 교환한 공개키로 이동국과 기지국간의 공유 세션키를 생성한다.

•단계 1 : $M1 \leftrightarrow B$

(1) $M1 \rightarrow B$: $M1_{sub}, B, Cert(M1), N_{M1}, PK_{M1}, T_{M1},$
$\{h(M1_{sub}, B, N_{M1})\}_{PK_{M1}^{-1}}$

(2) $B \rightarrow M1$: $B, M1_{sub}, Cert(B), PK_B, T_B, N_B,$
$\{h(B, M1_{sub}, N_{M1}, N_B)\}_{PK_B^{-1}}$

(3) $M1 \rightarrow B$: $M1_{sub}, B, \{h(M1_{sub}, M2, B, N_B)\}_{K_{M1,B}},$
$\{M2\}_{K_{M1,B}}$

•단계 2 : $B \leftrightarrow M2$

(4) $B \rightarrow M2$: $B, M2_{sub}, Cert(B), PK_B, T_B,$
$Cert(M1), PK_{M1}, T_{M1}, N_B', N_{M1},$
$\{h(B, M2_{sub}, N_B', N_{M1})\}_{PK_B^{-1}}$

(5) $M2 \rightarrow B$: $M2_{sub}, B, N_{M1}, N_{M2},$
$\{h(M2_{sub}, B, N_{M1}, N_{M2}, N_B')\}_{K_{M2,B}},$
$\{h(M1, M2, N_{M1}, N_{M2})\}_{K_{M1,M2}}$

•단계 3 : $M1 \leftrightarrow M2$

(6) $B \rightarrow M1$: $B, M1_{sub}, Cert(M2), PK_{M2}, T_{M2}, N_{M1},$
$N_{M2}, N_B'', \{M1_{sub}'\}_{K_{M1,B}}, \{h(B, M1_{sub},$
$M1_{sub}', N_{M1}, N_{M2}, N_B'')\}_{K_{M1,B}}, \{h(M1,$
$M2, N_{M1}, N_{M2})\}_{K_{M1,M2}}$

(7) $M1 \rightarrow M2$: $N_{M2}, \{M1, M2, N_{M2}+1\}_{K_{M1,M2}}$

* X_{sub} : X의 임시 식별자
* T_X : X의 공개키 유효 기간
* PK_X : X의 Diffie-Hellman 공개키 ($g^{k_X} \bmod p$)
* PK_X^{-1} : X의 개인키 (k_X)
* $K_{X,Y}$: X와 Y가 공유하는 세션키 $(g^{k_Y})^{k_X} \bmod p = (g^{k_X})^{k_Y} \bmod p$

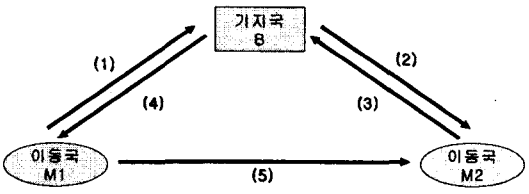
앞의 프로토콜들과 달리 End-to-End 범위의 보안을 위해 설계되었으며 결점이 없다. 그러나 이동국과 기지국간의 세션키를 생성하기 위해 이동국에서 많은 공개키 지수 연산을 수행하므로 현재의 이동 통신 환경에는 부적합하다[4].

3. 제안한 종단간 키 교환 프로토콜

이번 장에서는 기존의 VM 프로토콜을 개선하여 요구되는 보안 사항을 만족하고 이동 통신 환경에 적합한 End-to-End 범위의 키 교환 프로토콜을 제안하고 분석한다.

3.1 통신 절차 및 가정

제안하는 프로토콜은 <그림 1>과 같은 절차로 이루어지며,



<그림 1> 키 교환 과정

다음과 같은 가정하에 이루어진다.

•기지국의 인증 정보($Cert(B)$)는 항상 브로드캐스트되며, 기지국의 인증정보를 받은 이동국은 이를 검증한다.

▪기지국으로부터 인증정보를 받은 이동국은 기지국의 공개키와 자신의 개인키를 이용해 세션키를 생성하며, 이 과정은 통신이 이루어지지 않는 유휴(idle) 시간 동안 이루어져 직접적인 통신에 관련한 연산에는 영향을 주지 않는다.

3.2 제안한 키 교환 프로토콜

제안하는 프로토콜은 VM 프로토콜과 마찬가지로 Diffie-Hellman 키 교환 기법을 이용해 세션키를 생성하며 다음의 3단계로 이루어진다.

▪단계 1 : $M1 \leftrightarrow B$

(1) $M1 \rightarrow B$: $M1, B, Cert(M1), PK_{M1}, N_{M1}, \{M2\}_{K_{M1,B}}, \{h(M1, M2, B, N_{M1})\}_{PK_{M1}^{-1}}$

이동국 M1은 통신하고자 하는 상대방의 식별자 $M2$를 이미 생성한 세션키 $K_{M1,B}$로 암호화해서 보내고, 자신이 생성한 난수 N_{M1}과 각자의 식별자들을 포함한 전자서명 값을 기지국 B에게 보낸다.

▪단계 2 : $B \leftrightarrow M2$

(2) $B \rightarrow M2$: $B, M2, Cert(B), PK_B, Cert(M1), PK_{M1}, N_B, N_{M1}, \{h(B, M2, N_B, N_{M1})\}_{K_{M2,B}}$

기지국 B는 등록되어 있는 이동국 M2에게 M1의 인증서와 난수 N_{M1}, 그리고 자신이 생성한 난수 N_B를 보내며 이러한 정보를 해쉬한 값을 이미 공유한 세션키 $K_{M2,B}$로 암호화해서 보낸다.

(3) $M2 \rightarrow B$: $M2, B, N_{M2}, \{h(M2, B, N_B, N_{M1}, N_{M2})\}_{K_{M2,B}}, \{h(M1, M2, N_{M1}, N_{M2})\}_{K_{M1,M2}}$

이동국 M2는 기지국 B로부터 받은 M1의 공개키를 이용해 이동국 M1과 M2사이에 공유하는 세션키 $K_{M1,M2}$를 생성한다. 자신이 생성한 난수 N_{M2}와 기지국 B로부터 받은 정보를 해쉬한 값을 기지국과 공유한 세션키 $K_{M2,B}$로 암호화해서 보낸다. 또한 세션키 $K_{M1,M2}$로 이동국간의 정보를 암호화해 전송한다.

▪단계 3 : $M1 \leftrightarrow M2$

(4) $B \rightarrow M1$: $B, M1, Cert(M2), PK_{M2}, N_{M2}, N_B, \{h(B, M1, N_{M1}, N_{M2}, N_B)\}_{PK_B^{-1}}, \{h(M1, M2, N_{M1}, N_{M2})\}_{K_{M1,M2}}$

기지국 B는 M2로부터 받은 인증서와 난수 N_{M2}를 이동국 M1에게 보내고, 보내는 정보에 대해 자신이 서명을 한다. 또한 키 $K_{M1,M2}$로 암호화된 값을 그대로 M1에게 보낸다.

(5) $M1 \rightarrow M2$: $\{M1, M2, N_{M1}, N_{M2}, N_B\}_{K_{M1,M2}}$

이동국 M1은 기지국으로부터 받은 M2의 공개키를 이용해 세션키 $K_{M1,M2}$를 생성하게 되고 이동국간의 공유 세션키를 가지게 된다. 기지국으로부터 받은 M2의 정보를 세션키로 암호화하여 전송함으로써 마지막 인증 과정을 마친다.

3.3 제안한 키 교환 프로토콜의 분석

서로 공유하는 세션키 $K_{M1,B}, K_{M2,B}, K_{M1,M2}$로 데이터를 암호화함으로써 전송되는 정보를 보호해 기밀성을 유지한다. 또한 각각의 단계에서 교환되는 데이터는 그 데이터를 해쉬한 값을 포함하고 있어 무결성을 만족시킨다.

세션키 생성을 위해 교환한 인증서, 개인키로 서명한 서명값, 그리고 데이터를 암호화한 세션키를 확인해 상대방을 인증할 수 있으며, 단계1과 단계3 과정에서 개인키를 사용하여 전자서명을 함으로써 부인방지를 할 수 있다.

이동국에서는 단계1에서 전자서명을 하고, 단계3 과정에서 기지국이 서명한 값을 검증한다. 또한 이동국간의 공유 세션키 $K_{M1,M2}$를 계산하기 위한 공개키 지수 연산을 단계2 과정에서 한번, 단계3 과정에서 한번씩 이루어진다.

4. 성능 평가

제안한 프로토콜은 (1)에서 서명, (4)에서 검증을 하며 이동국간의 공유 세션키를 생성할 때 각각 한번씩 공개키 지수 연산을 한다. <표 2>에서 보듯이 이러한 연산량은 End-to-End 범위의 VM 프로토콜과 비교해 볼 때 보다 더 효율적이다.

<표 2> 키 교환 프로토콜 비교

프로토콜	보안 범위	기밀성	무결성	인증	부인 방지	공개키 연산량	메시지 교환횟수
MSR+DH	Link	∧	×	○	×	암:1	2
BY	Link	○	∧	○	∧	암:1 서:1	3
AD	Link	○	○	○	○	복:1 검:1 암:1 서:1	3
VM	E2E	○	○	○	○	서:1 검:2 지:4	7
제안한 프로토콜	E2E	○	○	○	○	서:1 검:1 지:2	5

* ○: High, ∧: Low, ×: None
* 암: 암호화, 복: 복호화, 서: 전자서명, 검: 전자서명 검증
지: 세션키 생성을 위한 공개키 지수 연산

5. 결론

본 논문에서는 이동 통신 환경의 키 교환 프로토콜이 고려해야할 사항들을 제시하고 기존의 키 교환 프로토콜들을 분석하였다. 그 중 End-to-End 범위의 VM 프로토콜을 개선하여 이동 통신 환경에 적합한 종단간 키 교환 프로토콜을 제안하였다. 이동국에서의 공개키 계산량을 줄이고 교환되는 메시지의 수를 줄여 개선된 효율성을 보여주었다.

참고문헌

[1] V. Varadharajan and Y. Mu, "On the Design of Security Protocols for Mobile Communications", ACISP'96 conference, Springer-Verlag, pp. 134-145, 1996.

[2] N. Asokan, "Security Issues in Mobile Computing", CS 690B-Research Proposal, 1995.

[3] U. Carlsen, "Optimal Privacy and Authentication on a Protable Communications System", ACM Operating System Review, 28 (3), pp. 16-23, 1994.

[4] C. Boyd and A. Mathuria, "Key Establishment Protocols for Secure Mobile Communications: A Selective Survey", Information Security and Privacy, LNCS Vol. 1438, Springer-Verlag, pp. 344-355, 1998.

[5] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, vol. 1, pp. 25-31, 1994.