이동 시스템 기반 보안 프로토콜의 취약성 분석[1)]

김일곤[0], 김현석, 전철욱, 이지연, 최진영
고려대학교 컴퓨터학과
{igkim[0], hskim, cwjeon, jylee, choi}@formal.korea.ac.kr,

The Vulnerability Analysis of a Security Protocol in Mobile Systems

Il-Gon Kim[0], Hyun-Suk Kim, Chul-Wuk Jeon, Ji-Yeon Lee, Jin-Young Choi,
Dept. of Computer Science & Engineering, Korea University

요약

무선 이동 시스템을 기반으로 안전한 키 교환 및 사용자 인증을 위한 다양한 보안 프로토콜이 제시되고 있다. 무선 이동 시스템 기반 보안프로토콜은 유선기반 보안프로토콜과 다르게 공개키와 대칭키가 혼합된 암호화 방식을 사용하고 있다. 본 논문에서는 이동 시스템 환경에서 동작하는 BCY 프로토콜의 안전성을 분석하기 위한 기술에 대해 언급하고, Casper/CSP 언어 및 FDR 도구를 이용하여 보안 취약성을 분석하고자 하였다.

1. 서론

이동 통신의 활성화와 더불어, 무선 인터넷을 기반으로한 뱅킹, 증권거래, 쇼핑 등 전자 상거래 서비스의 응용 영역이 점차 확대되고 있다. 이에 따라, 무선 이동 통신 기반의 안전한 키 교환 및 사용자 인증을 위한 다양한 보안 프로토콜이 제시되고 있다. 무선 인터넷 환경에서 사용되는 보안 프로토콜은 이동 단말기의 부족한 계산 능력, 메모리 크기, 대역폭등의 제한성으로 갖고 있기 때문에 기존 유선 기반 보안 프로토콜과 다른 특성을 갖고 있다[]. 이동 단말기의 제한된 계산능력과 보안성을 함께 고려하여 공개키 기반 암호알고리즘과 대칭키 기반 암호알고리즘을 혼합한 보안 프로토콜들이 사용되고 있다(MSR 프로토콜[1], BCY 프로토콜[2], AzizDiffie 프로토콜[3] 등) 그 중에서도 BCY 프로토콜은 무선 이동 통신 기반에서 사용되는 대표적인 프로토콜로서 새롭게 제시되는 보안프로토콜의 안전성을 비교하기 위해 사용되는 벤치마킹 보안 프로토콜로 널리 알려져 있다.

새로운 보안프로토콜의 제안과 더불어, 보안 프로토콜 설계상의 안전성을 분석하기 위한 다양한 연구가 진행되어 오고 있다. 이런 연구는 크게 정리 증명과 모델체킹 기법으로 나누어 볼 수 있다. 첫번째 방법의 경우, BAN[4], GNY[5]와 같은 보안 로직을 이용하여 정해진 규칙에 따라 상호 호스트간의 신뢰성을 증명하게 된다. 두번째 방법의 경우, 해당 프로토콜의 인증 동작을 정형 명세 언어로 설계 한 후, 다양한 보안 속성을 만족시키는지 체크하게 된다. ESTELLE, Murphi, NRL Protocol Analyser[6]와 FDR[7]은 위와 같은 방법을 이용하게 된다. 특히 FDR을 이용한 모델 체킹 기법은 보안 프로토콜의 안전성을 분석하기 위해 널리 사용되어오고 있는 방법으로, 그 효율성을 인증 받고 있다.

본 논문에서는 Casper를 이용하여 BCY 프로토콜에서 사용되는 공개키 및 대칭키 기반 보안 프로토콜의 취약성을 분석하기 위한 기술에 대해 언급하고, FDR 모델체킹 도구를 이용하여 BCY 프로토콜의 안전성을 분석한 결과에 대해 기술하고자 한다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 BCY 프로토콜에 대해 간략히 소개하고, 제 3장에서는 프로토콜을 명세하고 검증하기 위한 CASPER/CSP 언어와 FDR 도구를 이용한 보안프로토콜 취약성 분석 방법에 대해 소개하고, 제 4장에서는 BCY 프로토콜 명세 및 검증 결과를 보여주고, 마지막으로 제 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. BCY(Beller-Chang-Yacobi) 프로토콜

BCY 프로토콜은 공캐키 방식과 대칭키 방식을 혼합한 보안 프로토콜로서, Diffie-Hellman 및 MSR+DH 키 교환 프로토콜을 사용하고 있다[2]. BCY 프로토콜의 안전성을 검증하기 위해 GNY 로직을 이용한 연구논문[8]을 바탕으로 BCY 프로토콜의 키 교환 및 인증 절차를 설명하고자 한다.

BCY 프로토콜 동작 절차

Msg 1 : V -> U : {V, Kvd+, Kvm+}Ks-
Msg 2 : U -> V : {Ru}{Kvm+, {{U, Ku+}Ks-}Ru
Msg 3 : V -> U : {dataV}SK1
Msg 4 : V -> U : {dataU}SK2

앞에서 언급한 BCY 프로토콜에서 V는 서비스 제공자 이며, U는 무선 이동통신 사용자를 의미하게 된다. 그리고 메시지 순서상에는 명시하지 않았지만, S는 인증서를 방행하는 제3의 인증기관을 나타낸다. 즉, Ks- 는 인증기관의

1) 고려대학교 특별연구비에 의하여 수행되었음

개인키를 의미하게 된다. 메시지에 표기된 보다 상세한 기호는 표 1을 참조하기 바란다.
서비스 제공자 V가 Msg1을 사용자 U에게 전송한 후에, 사용자는 KK2 = {Kvd+}Ku- 를 생성하고, 세션키 SK2 = {Ru}KK2를 계산하게 된다. 이와 마찬가지로, 서비스 제공자가 Msg2를 수신한 후, KK1 = {Ku+}Kvd- 를 생성하고, 세션키 SK1 = {Ru}{KK1}을 계산하게 된다.
SK1과 SK2는 Diffie-Hellman 키 교환 방식을 나타내기 때문에 KK1=KK2, SK1=SK2의 관계가 성립한다.

표 1. BCY 프로토콜 기호 및 의미

기호	의미
U	사용자의 식별자
V	서비스 제공자의 식별자
S	인증기관의 식별자
Rx	X 호스트에서 생성한 임의 난수
Kx+	X 호스트의 공개키
Kx-	X 호스트의 개인키
KK	키 암호화 키(KK1 = KK2)
SK	세션키(SK1 = SK2)

3. Casper/CSP 및 FDR을 이용한 보안 프로토콜 분석 방법

CSP(Communication Sequential Processes) 통신 프로토콜의 행위를 정형적으로 명세하기 위해 개발된 프로세스 알제브라 언어의 일종이다[9]. CSP 언어는 프로세스의 동시성(Concurrency) 행위를 표현할 수 있기 때문에, CSP를 이용하여 보안 프로토콜의 행위를 명세하고 FDR 모델체킹 도구를 이용하여 취약성을 분석하기 위한 많은 연구가 진행되었다[7]. 하지만 CSP 언어 명세의 복잡성으로 인해 정형적 명세 표현에 많은 시간과 노력을 필요로 한다. 이에 따라, 보안 프로토콜의 행위를 보다 간단히 표현하기 위해 Casper 도구가 개발되었다[10]. Casper를 이용하여 보안 프로토콜의 행위와 검증하고자 하는 속성을 명세한 후, Casper 컴파일 기능을 이용하여 자동으로 CSP 언어로 변환할 수 있다. 마지막으로 자동 생성된 CSP 모델을 FDR 도구에 입력한 후, 비밀성, 인증 등과 같은 보안속성을 만족하는지 검사하게 된다. 만일 해당 보안속성을 위반하는 이벤트를 CSP 모델에서 찾게 되면, 반례를 보여주기 때문에 보안 취약점을 분석하고 개선하는데 도움을 준다.

4. BCY 명세 및 검증 결과

4.1 BCY 명세

제2장에서 기술한 BCY 프로토콜을 토대로, Casper를 이용하여 BCY 프로토콜의 행위 및 보안요구사항을 명세하였다. 본 논문에서는 추가적으로 인증기관 S의 행위도 Casper 모델에 추가하였다. Casper 모델은 기본적으로 8개의 헤더로 나누어 지지만, 본 논문에서는 페이지 사정상 #Protocol description, #Specification, #Intruder Knowledge 및 #Equivalences 섹션 부분에 대해서만 기술하도록 하겠다. 그림 1은 BCY 프로토콜에 대한 Casper 명세를 보여주고 있다. 그리고 본 논문에서는 암호 알고리즘은 안전하기 때문에 공격자가 암호키를 알지 못한 상태에서 암호문을 통해 암호키와 평문을 알아내는 것은 불가능하다고 가정하고 있다.

```
#Protocol description
0.      -> v : u
1a. s -> v : {v, pkvd, pkvm}{SSK(s)} % digV
1b. s -> u : {u, pku}{SSK(s)} % digU
2.  v -> u : digV % {v, pkvd, pkvm}{SSK(s)}
3.  u -> v : {ru}{pkvm},
             {digU % {u, pku}{SSK(s)}}{ru}
4.  v -> u : {{{dataV}{ru}}{pku}}{skvd}
5.  u -> v : {{{dataU}{ru}}{pkvd}}{sku}

#Specification
Secret(v, ru, [u])
Secret(u, ru, [v])
Agreement(v, u, [ru, pku, skvd])
Agreement(u, v, [ru, pkvd, sku])

#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Vendor, User, Sam, Mallory,
Nm, PKvd, PKvm, PKu, PKm, SKm, SPK(Sam), Rm}

#Equivalences
forall nu, pkvd, pku, skvd, sku, ru .
{{{nu}{ru}}{pkvd}}{sku} = {{{nu}{ru}}{pku}}{skvd}

forall nv, pkvd, pku, skvd, sku, ru .
{{{nv}{ru}}{pku}}{skvd} = {{{nv}{ru}}{pkvd}}{sku}
```

그림 1. Casper를 이용한 BCY 프로토콜 명세

#Protocol description 섹션 헤더는 보안 프로토콜상의 메시지 전송을 표현하기 위해 사용된다. s는 인증기관, v는 서비스 제공자 이고 u는 이동 단말기 사용자를 의미한다. 0번 메시지에서는 명시적으로 사용자 u가 서비스 제공자 v와 통신을 해야 한다는 사실을 알려주고 있다. pkvd와 pkvm은 v의 두 공개키를 나타내며, pku는 u의 공개키를 의미한다. SSK(s)는 s 인증기관의 개인키를 나타내게 되며, {v, pkvd, pkvm}{SSK(s)} % digV 는 인증기관 s의 개인키로 서명된 인증서를 의미하게 된다. 이와 마찬가지로, {u, pku}{SSK(s)} % digU 도 인증기관 s의 개인키로 서명된

인증서를 표현하고 있다.
#Specification 섹션 헤더는 검증하고자 하는 보안속성을 표현하는데 사용된다. Secret 기호는 비밀성을 나타내며, Agreement 기호는 인증 속성을 표현하는 부분이다. 예를 들어, Secret(v, ru, [u])는 "서비스 제공자 v는 임의 난수 ru를 사용자 u 하고만 공유하고 있다고 믿는다"는 의미로 해석되며, Agreement(v, u, [ru, pku, skvd])는 "서비스 제공자 v는 사용자 u에게 ru, pku, skvd 정보를 이용하여 인증을 받는다"는 의미로 해석된다.
#Information knowledge는 공격자의 사전지식을 표현하기 위해 사용된다. 공격자의 사전지식을 어떻게 구성하느냐에 따라, 보안 취약점 탐지 유무가 결정된다. 본 논문에서 BCY 프로토콜에 대한 공격자 호스트의 이름은 Mallory 이며, 그는 모든 호스트의 공개키, 자신의 개인키 그리고 Ru와 동일한 기능을 하는 자신의 임의난수 세션키 Rm을 알고 있다고 가정하고 있다.
#Equivalences는 메시지 표현상의 상호 교환 법칙을 적용하기 위해 사용된다. 예를 들어, 메시지 {{m}k1}k2 와 {{m}k2}k1는 같은 의미로 해석되기 때문에 수학적으로 다음과 같이 표현할 수 있다.

$$\forall k1, k2, m \bullet \{\{m\}k1\}k2 = \{\{m\}k2\}k1$$

위의 표현식은 #Equivalence 섹션 헤더 부분에 다음과 같이 명세하게 된다.

forall k1, k2, m . {{m{k1}}{k2} = {{m}{k2}}{k1}

그림 1의 #Equivalence 부분에 기술된 내용의 Diffie-Hellman 키 교환 방식을 표현하고 있다. 따라서, SK1 = SK2 이기 때문에 {{ru}{pkvd}}{sku} = {{ru}{pku}}{skvd} 로 나타낼 수 있다. 결과적으로, #Protocol description 헤더에 기술된 4, 5번 메시지는 각각 {{{nu}{ru}}{pkvd}}{sku} = {{{nu}{ru}}{pku}}{skvd}와 {{{nv}{ru}}{pku}}{skvd} = {{{nv}{ru}}{pkvd}}{sku}로 해석될 수 있다. 그림 1의 명세상에, 만일 #Equivalence 섹션에 Diffie-Hellman 키 교환 방식에 대한 내용을 기술하였을 경우, 어떠한 공격 취약점도 찾아내지 못하게 된다.

4.2 검증 결과

FDR 모델체커 도구를 이용해서 BCY 프로토콜이 위에서 언급한 비밀성 및 인증 속성을 만족하고 있는지 확인해 보았다. 그 결과 비밀성(Secret(v, ru, [u]), Secret(u, ru, [v])) 및 인증 속성(Agreement(u, v, [ru, pkvd, sku]))을 위반하는 보안 취약점을 발견 할 수 있었다.

인증 속성 보안 취약점

1a. S -> I(V) : {V, PKvd, PKvm}{SSK(S)}
1b. S -> I(U) : {U, PKu}{SSK(S)}
0. -> V : User
1a.I(S) -> V : {V, PKvd, PKvm}{SSK(S)}
2. V -> I(U) : {V, PKvd, PKvm}{SSK(S)}
3. I(U) -> V : {Rm}{PKvd}, {{U, PKu}{SSK(S)}}{Rm}
4. V -> I(U) : {{{Nv}{Rm}}{PKm}}{SKu}

위의 보안 취약점에서 I(V) 기호는 Vendor로 위장하거나 Vendor가 수신하는 메시지를 가로채는 공격자를 의미하게 된다. 결국, BCY 프로토콜의 보안 취약점은 공격자가 V의 공개키 PKvd를 가로채서 다시 이용하는 재사용 공격(replay attack)이 가능하다는 것을 확인할 수 있었다. 이 공격을 방어하기 위해서는 메시지에 타임 스탬프(timestamp)를 표기하거나 혹은 인증서버에서 인증서 만료일을 알려주는 메시지를 보내주어 특정 시간이 지난 후에, V의 공개키를 재사용하는 취약점을 막아주어야만 한다.

5. 결론 및 향후 연구 방향

본 논문에서는 Casper, CSP/FDR을 이용하여, 무선 이동통신망환경에서 동작하는 BCY 프로토콜의 취약점을 분석해 보았다. BCY 프로토콜과 같은 무선 보안 프로토콜은 유선 보안프로토콜과 달리 공개키와 대칭키를 혼합한 암호화 방식을 사용하기 때문에, 공격 취약점 분석을 위해서는 보다 정확한 추상화 모델을 구성하기 무엇보다 중요한 과제임을 파악할 수 있었다. 그리고 FDR 도구를 이용한 안전성 분석 결과, 공개키를 이용한 공격자의 재사용 공격을 재확인할 수 있었다.
향후 연구방향으로는 BCY 프로토콜과 같은 다양한 무선 이동 보안프로토콜의 취약점을 분석하고 보안성이 향상된 프로토콜을 제안하고 검증하고자 한다.

6. 참고문헌

[1] M.O.Rabin, "Digitalized signatures and public key functions as intractable as factorization," MIT Lab. Computer Sci., TR 212, Jan. 1979.
[2] M.J.Beller, L.-F.Chang and Y.Yacobi, "Privacy and authentication on a portable communications system," *Proceedings of the International Computer Symposium*, Vol. 1, pp.821-829, 1994.
[3] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Personal Commun., First Quarter 25 -31, 1994. Jonatban Hassell, *O'Reilly RADIUS book*, 2002.
[4] M. Abadi, M. Burrows, and R. Needham. "A Logic of Authentication," *In Proceeding of the Royal Society, Series A*, 426, 1871, pages 233-271, December 1989
[5] L.Gong, R.Needham and R.Yahalom, "Reasoning about Belief in Cryptographic Protocols," *Proceedings 1990. IEEE Symposium on Research in Security and Privacy.*
[6] P.E.Varner, "Formal Methods as an Environmental Catalyst for Emergent Security in System Design and Construction," December 12, 2002.
[7] T.Coffey and R.Dojen, "Analysis of a mobile communication security protocol," *Proceeding of the 1st international symposium on Information and communication technologies*, pp.322-328, 2003.
[8] Formal Systems(Europe) Ltd. Failure Divergence Refinement-FDR2 User Manual, Aug. 1999.
[9] C.A.R. Hoare, *Communicating Sequential Processes*, Prentice-Hall, 1985.
[10] G.Lowe. Casper: A compiler for the analysis of security protocols. 10th IEEE Computer Security Foundations Workshop, 1997.