모델체킹을 이용한 Carlsen BCY 프로토콜 검증

김현석° 전철욱 김일곤 최진영

고려대학교 컴퓨터학과
{hskim°, cwjeon, igkim, choi}@formal.korea.ac.kr

Verification of the Carlsen BCY Protocol Using Model Checking

Hyun-Seok Kim chul-wook Jeon Il-Gon Kim Jin-Young Choi

Dept. of Computer Science Korea University

요 약

인터넷을 통한 통신의 안전성을 확보하기 위해서는 전송될 정보를 암호화해야 한다. 따라서 통신의 주체간에는 공통적인 키의 공유와 상대방의 신원 확인을 위한 절차가 필요하다. 정형검증기법은 이러한 네트워크상에서 통신의 안전성을 확보하기 위한 수단으로 사용되며, 본 논문에서는 무선환경기반 보안 프로토콜인 Carlsen BCY 프로토콜을 모델 체커인 FDR을 사용하여 검증하였다.

1. 서 론

통신 및 네트워크 기술의 발전은 전자 상거래, 원격지 사용자간의 통신, 응용서버와의 통신 등의 서비스를 창출하였다. 이에 따라 오늘날의 공개된 인터넷을 통한 통신의 안전성을 확보하기 위해서는 전송될 정보를 암호화해야 한다. 따라서 통신의 주체간에는 공통적인 키의 공유와 상대방의 신원확인을 위한 절차가 필요한 것이다. 그러나 이러한 네트워크 환경에서 안전한 통신을 확보하는 것은 쉽지 않다. 보안프로토콜은 이러한 안전하지 않은 네트워크상에서 통신의 안전성을 확보하기 위해 사용된다.

일반적인 사용자 인증기술은 사용자 ID 와 패스워드에 의해 이루어진다. 하지만 이 방식은 이것은 도청, 재전송 공격 등에 매우 취약하며 유선환경에서 많은 취약성을 가지고 있다.

무선 인터넷에서 통신 상대자간에는 통신을 통해 정보를 교환하고 있는 상대가 실제 의도한 상대인지 확인하는 인증 과정이 반드시 필요한데 이러한 인증 기능은 사용자가 응용서버로부터 서비스를 받기 위해서도 필요하다.

따라서 암호화키를 공유하는 문제와 사용자 인증 문제는 안전한 정보 교환과 개인 정보보호를 위해 해결해야 할 중요한 문제이고, 이를 위해서는 보다 효율적인 보안프로토콜 구현이 절실히 필요하며 이러한 보안프로토콜을 구현하기 전에 설계단계에서부터 사용자와 개발자에게 안전성과 신뢰성을 제공하기 위한 기술이 요구되고 있다. 그러한 요구를 만족시키기 위해 진행되는 노력 중 대표적으로 정형 기법이라는 연구가 있으며 이는 정형 명세와 정형 검증의 두 가지 방법으로 구분된다.

정형 명세는 개발하고자 하는 시스템의 동작 및 시스템이 만족해야 하는 특성을 정형적인 표현방법을 이용해 모델링하는 방법이고, 정형 검증은 정형적으로 명세된 시스템을 대상으로 그 시스템이 정확한지 혹은 그 시스템의 요구사항으로 주어지는 특성을 만족하는지를 논리적으로 증명하는 방법이다.

그 중 정형 검증은 정리증명과 모델체킹 기법으로 구분되며, 전자는 BAN[1], GNY[2]와 같은 보안 로직을 이용하여 특정한 논리식으로 시스템을 명세하고 정확한 논리 증명단계로써 정확성을 증명하는 방식이고, 후자는 프로토콜의 인증과정을 유한상태기계의 형식으로 모델링하고 그 모델이 만족해야하는 요구사항이나 특성을 모델에서 만족되는지를 검증도구를 이용해 자동으로 증명하는 방식으로 ESTEREL, Murphi, NRL protocol Analyzer[3]와 FDR[4]과 같은 방법이 있다.

본 논문에서는 정형검증 도구 중 FDR 이라는 모델체킹 도구를 이용, 무선환경기반 보안프로토콜인 BCY 프로토콜[5]의 취약성을 재분석한 Carlsen BCY 프로토콜[6]에 대한 위험성을 분석하여 보안 프로토콜의 안전성을 향상시키고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 Carlsen BCY 프로토콜에 대해서 설명하고 3 장에서는 프로토콜을 명세하고 검증하기 위한 CSP 언어[7]와 Casper[8] 및 FDR 도구에 대해 소개하며, 4 장에서는 Casper 와 FDR 을 이용하여 Carlsen BCY 프로토콜의 분석 및 결과에 대해 살펴보고, 5 장에서는 결론 및 향후 연구방향을 제시하고자 한다.

2. The Carlsen BCY (Carlsen and M.J.Beller, L.-F.Chang and Y.Yacobi) 프로토콜

비밀키 방식과 공개키 방식의 조합을 도입한 방법들 중 하나인 BCY 프로토콜의 목적은 핸드폰과 같은 저전력 이동 단말기에서 인증을 제공하는 것이며 이동 통신에서 공개키 암호화방법을 통해 구현하고 있다. Carlsen BCY 프로토콜에서 명세하는 표현방식은 기존의 BCY 프로토콜에서 rv(서비스제공자의 랜덤한 난수값)와 TSx(만료시간)를 추가하였으며 그림 1 과 같다

U	사용자 ID 정보	Kx+	X 의 공개키
V	서비스제공자 ID 정보	Kx-	X 의 비밀키
SK	세션키	KK	키 암호화 키
SK1	{{ru}Ku+}Kvd-	SK2	{{ru}Kvd+}Ku-
rx	랜덤한 난수값	TSx	만료시간

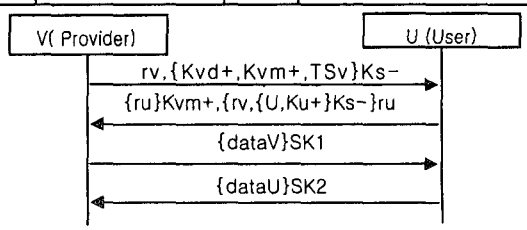

그림 1. Carlsen BCY 프로토콜의 표현방식

V(서비스제공자)는 S(인증기관)으로부터 인증받은 키를 이용해 두개의 공개키(Kvd+, Kvm+)를 암호화 및 복호화하여, V(서비스제공자)와 U(사용자)간의 데이터 암호화에 사용하였다. 이때 두 개의 공개키는 각각 Diffie-Hellman key [9]와 MSR (Modular Square Root) encryption [10]에 의해 생성되었으며 전자는 대칭키에 관한 기술을, 후자는 이동 환경에서의 암호화에 관한 기술을 말한다.

그림 1 의 프로토콜의 메시지 송수신 단계는 다음과 같다. 최초 V 는 자신의 두 공개키 정보와 시간정보를 인증기관의 비밀키로 암호화하고 이와 함께 V 의 난수값을 U 에게 전송한다. 여기서 사용자는 인증기관으로부터 인증서를 가지고 있으며 이에 대한 복호화 과정을 통해 U는 인증서 내용을 소유하게 되고 이 메시지에 대해 U는 V의 난수값 정보와 V의 공개키에 대한 정보를 알 수 있게 된다. 다음으로 메시지를 받은 U 는 V 에게 V 의 공개키로 암호화된 U 가 생성한 ru 라는 난수값과 그 난수값으로 암호화된 ru,{U, Ku+}Ks-를 전송하는데 이 값은 다시 U 의 ID 와 사용자의 공개키를 인증기관의 비밀키로 암호화한 값이며 V 로부터 받은 rv 와 함께 U 의 난수값으로 암호화하여 전송한다. 이 메시지를 전송받은 V 는 U 의 ID 정보와 사용자의 공개키에 대한 정보를 알 수 있게 된다. 이렇게 V와 U간의 키교환이 이루어진 후, 다음 단계에서 V는 U 에게 데이터를 보내기 위해 SK1 라는 세션키값으로 암호화하는데 이값은 {{ru}}{Kvd+}Ku-라는 값으로 이루져 있다. 이는 V의 공개키 Kvd+키를 U의 비밀키 Ku-로 암호화한 값으로 ru를 암호화했다. 이렇게 암호화된 데이터를 U는 V로 부터 알게 된 Kvd+로 ru 값을 복호화하고 ru 값으로 복호화한 dataV 의 값을 알게 된다. 마찬가지로 U 가 V 에게 데이터를 보내기 위해서는 SK2 라는 세션키 값으로 데이터를 암호화하는데 이 값은{{ru}}{Ku+}Kvd- 라는 값으로 이루어져 있고 이는 U 의 공개키 Ku+키를 V 의 비밀키 Kvd-로 암호화한 값으로 ru 를 암호화했다. 이렇게 암호화된 데이터를 V 는 U 로부터 알게 된 Ku+로 ru 값을 복호화하고 ru 값으로 복호화한 dataU 의 값을 알게 된다. 여기서 이 두 세션키 SK1 과 SK2 값은 Diffie-Hellman 키분배프로토콜에 의해 동일한 세션키 값을 보이고 있음을 알 수 있다.

3. CSP, Casper and FDR

3. 1 CSP(Communicating Sequential Process)

CSP는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용되어졌으나, 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP 에서 제공하는 pure synchronization(|||)과 Interleaving parallelism(||) 개념을 사용하여 분산 시스템 환경하에서 동작하는 클라이언트 서버와 공격자 모델을 정형적으로 표현할 수 있는 장점을 갖고 있다. 예를 들어, 분산시스템 환경하에서 동작하는 보안 시스템은 다음과 같이 간략히 표현할 수 있다.

SYSTEM = CLIENT1 ||| CLIENT2||| SERVER || INTRUDER

3. 2 Casper(A Compile for the Analysis of Security Protocols)

CSP 와 FDR 을 이용한 보안프로토콜 명세시 명확하고 세부적인 표현에 있어 machine-based 이 아닌 수작업에 전적으로 의존한다는 점에서 매우 방대한 시간이 소요된다는 단점을 가지고 있어 비용 대 효과면에서 다소 비효율적인 방법론이라 할 수 있다. 이러한 점을 개선한 도구로서 추상적인 표현만으로 CSP 명세소스를 자동으로 생성해주는 개발도구가 바로 Casper 이다.

3. 3 FDR(Failure Divergence Refinement)

모델체킹 도구로서, CSP 언어로 생성된 파일을 통해 구현된 보안 모델에 대해 비밀성, 인증성과 같은 보안 속성의 만족여부를 체킹하는 도구이다. 이를 통해 해당 속성을 만족시키지 못할 경우 반례를 보여주어, 공격 시나리오의 가능형태를 분석해 준다. 즉 보안 프로토콜이 반드시 갖추어야 할 요구사항인 비밀성, 무결성, 인증, 부인방지와 같은 보안속성의 만족여부에 대한 검사 도구이다.

4. Casper/FDR 을 이용한 BCY Protocol 분석 및 결과

4.1 Carlsen BCY Protocol 분석

본 논문에서는 Carlsen BCY 프로토콜을 모델체킹 도구를 이용해 모델링하였는데 그림 2 는 Carlsen BCY 프로토콜을 Casper 표현방식으로 모델링한 것으로 8 가지 항목 중 자유변수 영역과 프로토콜 기술영역, 침입자 영역, 카동치성에 대한 표현이다

```
#Free variables
v, u : Agent
s : Server
pkvd, pkvm, pku : PublicKey
skvd, skvm, sku : SecretKey
SPK :  Server -> ServerPublicKey
SSK :  Server -> ServerSecretKey
tsv : TimeStamp
dataV, dataU : Nonce
ru,rv: Nonce
InverseKeys = (pkvd, skvd), (pkvm, skvm), (pku, sku),
(SPK, SSK), (ru, ru), (rv, rv)

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

#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Provider, 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 2 . Casper 를 이용한 Carlsen BCY 프로토콜 명세

V 는 서비스제공자, U 는 사용자로서 각각 Agent 로 나타내고, pkvd, pkvm, pku 는 공개키, skvd, skvm, sku 는 공개키 각각에 대한 비밀키, SPK 와 SSK 는 인증기관의 공개키 함수와 비밀키 함수이며, tsv 는 만료시간을 나타내는 값, V 와 U 가 전송하고자 하는 data 는 각각 dataV, dataU 이며, Inverse-Keys 는 암호화 함수에 대응하는 복호화 함수를 나타낸다. 또한 마지막 영역은 Diffie-Hellman key 분배프로토콜이 적용된 부분이다

4.2 Carlsen BCY 프로토콜 검증 결과

기존의 BCY 프로토콜에서는 두 개체간의 최신 인증서를 미보유함에 따라 공개키가 노출되어 궁극적으로 정보노출이라는 결과를 초래하였다. 따라서 Carlsen BCY 프로토콜에서는 두 개체간 키에 대한 비밀성과 개체간 상호 ID 에 대한 인증을 만족해야하며 이는 다음과 같이 표현할 수 있다

Secret(V,ru,[U])
Secret(U,pkvm,[V])
Agreement(v,u,[ru,pku,skvd])

첫번째 표현은 " V 는 ru 정보를 오직 U 와만 알고 있다" 라고 풀이할 수 있고 두번째 표현은 " U 는 pkvm 정보를 오직 V 와만 알고 있다 " 로 풀이할 수 있다. 세번째 표현은 " V 는 ru,pku,skvd 정보를 통해 U 로부터 자신의 개체를 인증받는다" 라고 풀이할 수 있다

모델 체커를 이용해 비밀성과 개체인증 속성의 만족여부를 확인한 결과 첫번째 표현에서 V 가 생성한 랜덤한 정보(rv)에 대해 비밀성 속성을 만족하지 않았고 이에 따라 결국 두 개체간의 데이터가 누설되었다.

위 비밀성 요구사항의 반례에 대해 FDR 의 interpret 기능을 통해 분석한 결과는 그림 3 과 같다.

```
0.   -> Provider : User
1. Provider -> I_User : Rv, {Pkvd, Pkvm, 0}{Ks}
1. I_Provider -> User : Rv, {Pkvd, Pkvm, 0}{Ks}
   Time is 0
2. User -> I_Provider : {Ru}{Pkvm}, {Rv, {User, Pku}{Ks}}{Ru}
2. I_User -> Provider : {Ru}{Pkvm}, {Rv, {User, Pku}{Ks}}{Ru}
3. Provider -> I_User : {{{Provider}{Ru}}{Pku}}{Skvd}
3. I_Provider -> User : {{{Provider}{Ru}}{Pku}}{Skvd}
   Provider believes Rv is a secret shared with User
   The intruder knows Rv
```

그림 3. FDR 을 이용한 반례의 분석결과

U 가 V 에게 정상적인 데이터 전송을 했다고 간주했으나 I_Provider 에 의해 Rv 정보가 노출되었다. 결과적으로 문제점은 V 의 identity 가 인증서 내에 포함되지 않았기 때문에, BCY 프로토콜의 문제점으로 분석되었던 Timestamp 를 추가하였으나 U 가 공개키 Pkvm 을 불신함으로써 인증기관으로부터의 최신 인증서를 소유하지 않은 악의적인 침입자로부터의 공개키 획득을 통한 침입과 인증서 자체의 공유키 노출시 사용자와 서비스 제공자와의 모든 data 및 키의 노출을 통한 침입이 가능하게 된다는 점이다. 이러한 문제점을 해결하기 위해서는 인증서내 V 에 대한 identity 정보를 추가함으써 해결될 수 있고, 세션키 자체에 대해서는 인증기관으로부터 인증된 인증서라 하더라도 인증서의 세션키에 포함되는 키에 대한 정보 또한 암호화함으로써 해결될 수 있다.

5. 결론 및 향후 연구방향

무선 네트워크 기술의 보안 취약점은 무선 네트워크 사용의 중요한 장애요인이다. 이에 본 논문에서는 네트워크 보안이라는 주제로 무선환경에서는 어떠한 보안프로토콜이 어느 정도 신뢰성을 주는지에 대해 모델체킹 도구를 이용하여 Carlsen BCY 프로토콜이라는 보안프로토콜의 안전성을 분석해 보았다. 기존의 BCY 프로토콜에서 취약점으로 제기된 인증서의 시간정보부재의 문제점은 단순한 시간정보 추가를 통해서 해결될 수 없으며 각 개체의 상호인증을 위한 정보가 함께 전송되어 키 암호화를 지원해야한다.

요컨대 이동환경에서의 보안프로토콜은 서비스 제공자와 사용자간의 개체확인을 위한 최신화된 정보와 키 암호화 키에 대한 관리가 가장 중요하다고 할 수 있다. 향후 연구방향으로 무선환경 보안프로토콜로서 패스워드 기반의 키 교환 및 인증프로토콜에 대한 연구 및 분석을 해 보고자 한다

6. 참고문헌

[1]M. Abadi, M. Burrows, and R. Needham, A Logic of Authentication. In Proceeding of the Royal Society, Series A,426, 1871,pp.233-271, December 1989.

[2]Li Gong, Roger Needham, Raphael Yahalom, Reasoning about Belief in Cryptographic Protocols, *Proceedings* 1990 IEEE Symposium on Research in Security and Privacy, 1990.

[3] Philip E.Varner, Formal Methods as and Environmental Catalyst for Emergent Security in System Design and Construction, December 12, 2002.

[4]Gavin Lowe, Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR, 1996

[5] M. J. Beller, L. F. Chang, and Y. Yacobi, Privacy and Authentication on a Potable Communication System, Proceedings of GLOBECOM' 91, pp.1922-1927, IEEE Press, 1991.

[6]Tom Coffey , Reiner Dojen , Tomas Flanagan, Formal verification: an imperative step in the design of security protocols, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.43 n.5, pp.601-618, December 5, 2003.

[7]C.A.R. Hoare, Communicating Sequential Processes, Prentice-Hall, 1985.

[8]G. Lowe, Casper: A compiler for the analysis of security protocols. 10th IEEE Computer Security Foundations Workshop, 1997.

[9]W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol.22, pp. 644-645, 1976.

[10]M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorisation, *Technical* Report MIT/LCS/TR-212, MIT, 1979.