Diffie-Hellman기반 M-Commerce 프로토콜 분석

김현석[O]* 김일곤* 최진영* 노정현* 유희준**
*고려대학교 컴퓨터학과
{hskim[O], igkim, choi, jhnoh}@formal.korea.ac.kr
**삼성전자 무선통신 사업부
heejun.yoo@samsung.com

Analysis of the M-Commerce Protocol based on Diffie-Hellman

Hyun-Seok Kim[O]* Il-Gon Kim* Jin-Young Choi* Jung-Hyun Noh*
*Dept. of Computer Science and Engineering, Korea University
Hee-Jun Yoo**
**R&D lab. of Mobile & Communication Division, Samsung Electronics CO.,LTD.

요약

최근 모바일 단말기를 이용한 전자상거래 서비스가 활발해 짐에 따라, 사용자 및 서비스 제공자간의 통신 안전성 확보가 중요한 문제로 인식되고 있다. 지금까지 제안된 대부분의 모바일 프로토콜들은 상호 안전한 키 교환을 위해 Diffie-Hellman 알고리즘을 사용하고 있다. 본 논문에서는 BCY 및 ASK 프로토콜을 통해서 Diffie-Hellman 알고리즘 기반 모바일 프로토콜의 상호 키 교환 및 인증절차를 살펴보고, Casper 및 FDR 도구를 이용하여 무선환경기반 M-Commerce 프로토콜의 안전성을 분석하였다.

1. 서론

전자상거래에서 거래정보, 개인정보, 개인의 금융정보, 금융거래나 상거래를 위한 비밀번호 등 중요한 디지털 정보가 수없이 생성되고 또한 여기저기 저장되게 된다. 이런 중요한 정보를 암호화함으로써 도용이나 오용을 막을 수 있고 위험으로부터 소비자나 상거래 쇼핑몰을 보호할 수 있다. 특히 무선 통신 환경에서 정확한 사용자 인증 및 안전한 데이터 전송은 안전성을 확보하기 위한 중요 기반 기술이라 하겠다. 최근에 많은 전자인증기술이 도입되었고 이러한 인증기술에 대한 신뢰성 문제를 검증하기 위한 노력이 제기되고 있다.

대표적으로 정형 기법을 이용한 프로토콜 안전성 분석 연구가 진행되어 오고 있다. 정형기법은 정형 명세와 정형 검증의 두 가지 방법으로 구분된다. 정형 명세는 설계자가 구현하고자 하는 시스템의 설계도를 정형적으로 명세하는 방식이고, 이렇게 명세된 설계가 정확한지 그리고 그 설계가 중요한 특성들을 만족하는지를 증명하는 것이 정형 검증이다. 기본적으로 정형 검증을 하기 위해서는 정형명세가 반드시 필요하다. 이 두 분류에 따라 정형 기법은 다시 논리 증명과 모델 체킹기법으로 구분할 수 있다. 이는 시스템의 정확성 증명을 위한 도구와 원리를 기준으로 나눈 것으로 그 중 정형 검증은 정리증명과 모델체킹 기법으로 구분되며, 전자는 BAN[1], GNY와 같은 보안 로직을 이용하여 특정한 논리식으로 시스템을 명세하고 정확한 논리 증명단계로써 정확성을 증명하는 방식이고, 후자는 프로토콜의 인증과정을 유한상태기계의 형식으로 모델링하고 그 모델이 만족해야 하는 요구사항이나 특성을 모델에서 만족되는지를 검증도구를 이용해 자동으로 증명하는 방식으로 ESTEREL, Murphi, NRL protocol Analyzer[2]와 FDR[3]과 같은 방법이 있다.

본 논문에서는 정형검증도구를 이용, 무선환경에서 Diffie-Hellman 키 교환 알고리즘 기반 전자상거래 프로토콜의 보안 취약점을 분석 하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 두 프로토콜의 주요 세션키 교환 알고리즘으로서 Diffie-Hellman 기반의 BCY프로토콜 및 ASK 프로토콜을 분석하며, 3장에서는 프로토콜을 명세하고 검증하기 위한 Casper, FDR 도구에 대해 소개하며, 4장에서는 ASK프로토콜의 검증결과를 토대로 Diffie-Hellman의 보안 취약점에 대해 살펴보고, 5장에서는 결론 및 향후 연구방향을 제시하고자 한다.

2. Diffie-Hellman 기반 M-Commerce 프로토콜

2. 1 Diffie-Hellman 키교환 알고리즘[4]

이 알고리즘은 제한된 영역에서 이산대수 계산의 어려움을 보안의 기초에 둔 것으로, 대부분의 키교환 알고리즘은 Diffie-Hellman 알고리즘을 사용하며, 실수에서 로그는 매우 쉽게 계산할 수 있지만 유한체 위에서 정의된 로그는 계산하기 매우 어렵다는 특성을 이용한다.

이러한 Diffie-Hellman 알고리즘의 연산 과정은 간단하다. 키를 교환하고자 하는 양 party(A, B)가 prime n 과 g 의 사용에 동의하였다고 할 때, 프로토콜은 다음과 같이 동작한다.

A : X = g**x mod n (x 는 large random integer)
B : Y = g**y mod n (y 는 large random integer)
=>이때 A, B 는 각각 X 와 Y 를 상대방으로 전달한다.

A : k = Y**x mod n
B : kp = X**y mod n
=>이때 k 와 kp 는 g**(xy) mod n 과 동일하다.

2.2 The BCY (M.J.Beller., L.-F.Chang, and Y.Yacobi) 프로토콜[5]

비밀키 방식과 공개키 방식의 조합을 도입한 방법들 중 BCY 프로토콜은 핸드폰과 같은 저전력 이동단말기에서 인증을 제공하여 고객과 판매자간의 상거래를 가능하도록 하는데 목적이 있다.

표 1 프로토콜 표현 기호

U	고객 ID정보	Kx+	X의 공개키
V	판매자ID정보	Kx-	X의 비밀키
SK	세션키	KK	Diffie-Hellman키
SK1	{{ru}Ku+}Kvd-	SK2	{{ru}Kvd+}Ku-
rx	랜덤한 난수값	CertX	인증기관의 인증서
DataX	전송하고자 하는 데이터 정보		

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. U -> V : {dataU}SK2

그림 1 BCY 프로토콜

위 표와 메시지 순서도는 각각 BCY 프로토콜의 기호와 프로토콜의 단계를 나타낸다

V(판매자)는 제3의 S(인증기관)으로부터 분배된 인증서정보로 두개의 공개키(Kvd+, Kvm+)를 암호화하여, V(판매자)와 U(고객)의 데이터 암호화에 사용하였다. 이때 두 개의 공개키는 각각 Diffie-Hellman과 MSR(Modular Square Root)알고리즘을 사용하였으며, 전자는 대칭키에 관한 기술이며, 후자는 이동 환경에서의 암호화에 관한 기술을 말한다. 그림 1의 프로토콜의 메시지 송수신 단계는 다음과 같다. 최초 판매자는 자신의 두 공개키 정보를 인증기관에서 분배된 인증서의 형태로 고객에게 전송한다. 여기서 고객 또한 제3의 인증기관으로부터 인증서를 가지고 있으며 이에 대한 복호화 과정을 통해 고객은 판매자의 두 공개키에 대한 정보를 알 수 있게 된다. 다음으로 메시지를 받은 고객은 판매자에게 판매자의 공개키로 암호화된 고객으로부터 전달된 ru라는 난수값과 이 난수값으로 암호화할 {U,Ku+}Ks-를 전송하는데 이 값은 제 3의 인증기관으로부터 고객에게 분배한 인증서로서 고객의 ID와 고객의 공개키를 인증기관의 비밀키로 암호화한 값이며 고객의 난수값으로 암호화하여 전송한다. 이 메시지를 전송받은 판매자는 고객의 ID정보와 고객의 공개키에 대한 정보를 알 수 있게 된다.

이렇게 판매자와 고객간의 키교환이 이루어진 후, 다음 단계에서 판매자는 고객에게 특정 데이터를 보내기 위해 SK1라는 세션키값으로 암호화 하는데 이 값은 {{ru}}{Kvd+}Ku-라는 값으로 이루져 있다. 이는 판매자의 공개키 Kvd+키를 고객의 비밀키 Ku-로 암호화한 값으로 ru라는 고객의 난수값을 암호화했다. 이 두 공개키는 실제로 Diffie-Hellman 키값을 형성하게 되며, 이 키를 통해 암호화된 특정 데이터를 고객은 판매자 Kvd+로 ru값을 복호화하고, 다시 ru값으로 복호화하여 dataV의 값을 알 수 있게 된다. 마찬가지로 고객이 판매자에게 데이터를 보내기 위해서는 SK2라는 세션키값으로 데이터를 암호화하는데 암호화와 복호화 과정은 동일하다. BCY 프로토콜에서 적용된 Diffie-Hellman 알고리즘은 이 두 세션키 SK1과 SK2값의 각각 ru를 제외한 값에 의해 구현이 되며 결과적으로 동일한 세션키 값을 이용해 상호 인증하도록 지원한다.

2.3 The ASK (Aydos, Sunar, and Koc).프로토콜[6]

Msg 1. V -> U : Kv+

Msg 2. U -> V : Ku+

Msg 3. V -> U : {CertV, Rv}KK1

Msg 4. U -> V : {CertU, Rv}KK2

그림 2 ASK 프로토콜

그림 2의 ASK 프로토콜의 기호는 표1을 통해 참조할 수 있으며 메시지 송수신 단계는 다음과 같다. BCY 프로토콜과 마찬가지로 제3의 인증기관으로부터 판매자와 고객에게 인증서가 전달되고 각각의 인증서에는 공개키가 암호화되어 있다. 먼저 판매자는 인증서로 전달된 자신의 Kv+(공개키)를 전달하고 고객은 그 공개키로 Diffie-Hellman 키인 KK1={Kv+}Ku-를 생성한다. 동일하게 고객은 인증서로 전달된 자신의 Ku+(공개키)를 전달하고 판매자는 그 공개키로 Diffie-Hellman키인 KK2={Ku+}Kv-를 생성한다. 이렇게 두 키를 생성하여 판매자는 판매자의 인증서와 난수값 rv 를 암호화하여 고객에게 전달하고, 고객은 고객의 인증서와 판매자로부터 받은 난수값 rv를 암호화하여 전달함으로써 상호인증을 받고자 한다. ASK 프로토콜에서 적용된 Diffie-Hellman 알고리즘은 이 두 Diffie-Hellman 키 KK1과 KK2값의 각각의 값에 의해 직접 구현이 되며 결과적으로 동일한 세션키 값으로 인증을 구현한다.

앞서 언급된 BCY 프로토콜과의 차이점은 ASK는 Diffie-Hellman 키값 자체를 세션키로 사용함에 반해, BCY는 난수정보를 포함한 Diffie-Hellman 키의 조합에 의한 키값을 세션키로 사용한다는 것이다.

3. Casper 및 FDR 도구를 이용한 분석 방법

3. 1 Casper(A Compile for the Analysis of Security Protocols)[7]

CSP와 FDR을 이용한 보안프로토콜 명세시 명확하고 세부적인 표현에 있어 수작업에 전적으로 의존한다는 점에서 매우 방대한 시간이 소요된다는 단점을 가지고 있어 비용 대효과면에서 다소 비효율적인 방법론이라 할 수 있다. 이러한 점을 개선한 도구로서 추상적인 표현만으로 CSP명세소스를 자동으로 생성해주는 개발도구가 바로 Casper 이다.

3. 2 FDR(Failure Divergence Refinement)

모델체킹 도구로서, CSP언어로 생성된 파일을 통해 구현된 보안 모델에 대해 비밀성, 인증성과 같은 보안 속성의 만족여부를 체킹하는 도구이다. 이를 통해 해당 속성을 만족시키지 못할 경우 그 반례를 제시함으로써 공격 시나리오의 가능형태를 분석해 준다. 즉 보안 프로토콜이 반드시 갖추어야 할 요구사항인 비밀성, 무결성, 인증, 부인방지와 같은 보안속성

의 만족여부에 대한 검사 도구이다.

4. Casper/FDR을 이용한 M-Commerce 프로토콜 보안성 분석

4.1 M-commerce 프로토콜 분석

M-Commerce 프로토콜의 궁극적인 목적은 첫째, 정보의 기밀성 제공, 둘째, 지불정보의 무결성 확보, 셋째, 판매자와 고객 쌍방의 확인이며 이 프로토콜에 적용된 Diffie-Hellman 알고리즘의 목적은 두 사용자가 키를 안전하게 교환하고 계속해서 메시지의 암호화에 사용할 수 있도록 하는 것이다. 본 논문에서는 지면관계상 ASK 프로토콜을 모델체킹 도구를 이용해 모델링하였는데 그림 3은 ASK 프로토콜을 Casper표현 방식으로 모델링한 것으로 8가지 항목 중 기술영역, 침입자 영역, 키 동치성에 대한 표현이다.

```
#Protocol description
0.    -> v : u
1a.s -> v : {v, pkv}{SSK(s)} % digV
1b.s -> u : {u, pku}{SSK(s)} % digU
2. v -> u : pkv
3. u -> v : pku
4. v -> u : {{digV % {v, pkv}{SSK(s)}, rv}{pku}}{skv}
5. u -> v : {{digU % {u, pku}{SSK(s)}, rv}{pkv}}{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}
```

그림 3 . Casper를 이용한 ASK 프로토콜 명세

v는 판매자, u는 고객으로서 각각 Agent로 나타내고 pkvd, pkvm, pku는 공개키이며 skvd, skvm, sku는 공개키 각각에 대한 비밀키를 말한다. SPK와 SSK는 인증기관의 공개키 함수와 비밀키 함수이며, v와 u가 전송하고자 하는 데이터는 각각 dataV, dataU를 나타낸다. 마지막 키동치성 영역은 Diffie-Hellman 키 분배프로토콜의 구현을 위해 Casper로 명세한 부분이다.

4.2 검증 결과

첫번째 프로토콜인 BCY 프로토콜에서는 두 개체간의 최신 인증서를 미보유함에 따라 공개키가 노출되어 궁극적으로 정보노출이라는 결과를 초래하였다. 또한 ASK 프로토콜에서는 두 개체간 키에 대한 비밀성과 개체간 상호 ID에 대한 인증에 대해 동일한 취약점을 노출시켰다.

두 프로토콜이 만족해야 할 속성은 다음과 같다.

#Specification
Secret(v, rv, [u])
Agreement(v, u, [rv, pku, skv])

첫번째 표현은 "v는 rv 정보를 오직 u 하고만 알고 있다"라고 풀이할 수 있고, 세번째 표현은 "v는 ru, pku, skvd 정보를 통해 u 로부터 자신의 개체를 인증한다"라고 풀이할 수 있다. 모델 체커를 이용해 비밀성과 개체인증 속성의 만족여부를 확인한 결과 첫번째 표현에서 V가 생성한 랜덤한 정보(rv)에 대해 비밀성 속성을 만족하지 않았고 이에 따라 결국 두 개체간의 데이터가 노출되었다.

결과적으로 두 프로토콜에 적용된 Diffie-Hellman 키 교환은 중간자 공격(man-in-the-middle attack)에 취약하다. 이 공격에서, 공격자는 판매자의 공개 값을 가로채고 공격자 자신의 공개값을 고객에게 보낸다. 고객이 그의 공개 값을 전달할 때, 공격자는 그녀 자신의 값으로 대체하고 판매자에게 그 값을 전달한다. 공격자와 판매자는 하나의 공유된 키를 합의하고 공격자와 고객은 다른 공유된 키를 합의한다. 이러한 교환 후에, 공격자는 판매자나 고객에 의해서 만들어진 어떤 메시지를 단순히 복호화하고, 복호문을 읽고 나서 읽고 적당한 키로 다시 암호화하고 그것들을 변경한 후에 적당한 상대방에게 전달한다. 이러한 취약성은 Diffie-Hellman 키 교환이 참가자들을 인증하지 않기 때문이다.

5. 결론 및 향후 연구방향

본 논문에서는 Diffie-Hellman기반 두 프로토콜의 공통적인 취약성을 파악함으로써 이동환경에서의 비적합성을 논의하고자 하였다. 즉 두 프로토콜은 위 알고리즘을 이용하여 공통적인 세션키를 생성, 개체인증 및 데이터 보호를 하고자 하였으나 결과적으로 신뢰성 문제의 검증에서 취약성이 발견되었다. 요컨대 이동환경에서의 전자상거래는 고객과 판매자간의 개체확인을 위한 키정보 대한 관리가 가장 중요하다고 할 수 있다. 향후 연구방향으로 Fair Exchange 계열의 E-Commerce 프로토콜에 대한 연구 및 분석을 하고자 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]Philip E.Varner, Formal Methods as and Environmental Catalyst for Emergent Security in System Design and Construction, December 12, 2002.

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

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

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

[6]M. Aydos, B. Sunar, and C.K. Koc, "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication," presented at the 2nd Int. Workshop Discrete Algorithms and Methods for Mobility, Dallas, TX, Oct. 1998.

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