스마트카드를 이용한 안전한 인터넷 전화 설계

박진호* 정진욱**
*대덕대학 인터넷정보기술계열 **성균관대학교 전기전자 및 컴퓨터공학부

요 약

스마트카드는 메모리와 프로세서를 내장하여 간단한 연산이 가능하도록 하는 카드 형태의 장치로 안전성을 제공하여야 하는 인증 시스템에 이용되기도 한다. 본 논문에서는 인터넷 전화에서 상호 인증과 비밀 통신이 가능하도록 하기 위해 키 교환 과정 중에 스마트 카드를 이용하는 방법에 대해 제안하였다. 대하여 알아본다.

Design of Secure Internet Phone using Smart Card

Jinho Park* Jinwook Chung**

ABSTRACT

The smart card including memory and processor is able to simple process such as privilege unauthorized access and used to Authentication System for security. In this paper, we propose using the smart card in the key exchange phase when secure Internet phones conversation, so certainly guarantee to mutual authentication and secret communication.

1. 서 론

세계는 점점 하나의 지구를 표방하면서 주위의 가족과 친척은 세계 곳곳에 퍼져 있으며, 기업은 기업대로 많은 현지 생산 거점과 무역 상사를 세계 무대에 펼쳐 놓았다. 이들은 그들이 가까운 거리에 있는 것처럼 이야기하고 업무 협조가 이루어지기를 원하므로, 원거리까지의 통신은 근거리에서의 통신 못지 않게 그 빈도가 많아졌다. 원거리 통신시 비용의 절감을 위하여 텔리텍스, 팩시밀리 등을 이용하기도 하지만, 직접 대화에 비해 일의 효율성은 낮다. 이런 연유로 전화의 이용을 무조건 억제할 수는 없으며, 음성 전화 통화에서의 비용 절감의 필요성이 대두되었다. 인터넷은 원거리에서와 근거리에서의 통신비용의 차이가 없는 장점으로 인하여 그 활용은 전화에까지 이용되며 이것이 바로 인터넷 전화이다.

원거리에서의 값싼 가격의 국제 통화가 가능하도록 하는 게이트웨이로 사용되거나 기존의 사설 교환기(PBX)를 대체하는 등의 인터넷 전화의 보급은 급격히 늘고 있으며, 전자 상거래에서의 인터넷을 통한 상품 주문과 통신 판매원과의 직접 연결 서비스 또는 가상 콜 센터를 구성할 수 있는 여러 장점으로 인터넷 전화는 계속적으로 널리 이용될 것이다[1]. 그러나, 인터넷 전화 시장의 활성화에는 몇 가지 해결해야 할 문제를 안고 있다. 첫째로는 표준화된 규격이 없음으로 인하여 서로 다른 제품간의 호환이 불가능하다는 점이며, 둘째로는 인터넷의 성격 상 생길 수 있는 패킷의 손실과 데이터의 보호에 대한 철저한 대비가 없다는 점이다. 이와 같은 문제점을 해결하기 위해, 여러 인터넷 전화 제공 사업자간의 제품 호환이 가능하도록 하는 표준화에 대한 논의가 이루어지고 있으며[2][3][4][5], 정확하고 빠른 데이터 전송을 위한 압축 및 전송 프로토콜에 대한 연구 역시 활발하나, 인터넷 전화의 음성 데이터의 보호에 대한 연구는 미진하다. 또 스마트 카드를 이용한 원거리에서의 패스워드 인증과 네트워크 가입자 신분확인에 대한 연구는 이루어졌으며[6], 디지털 이동 통신에서의 가입자 및 단말기의 인증에 스마트 카드를 이용하고자 하는 노력이 GSM(Global Systems for Mobil communications)을 통해 이루어지고 있다[7]. 본 논문에서는 스마트 카드를 인터넷 전화에 응용하기 위해서 카드가 수행하여야 할 기능들과 그 동작 시나리오에 대해 논의하고자 한다.

2. 인터넷 전화의 보안 기능

인터넷의 다양한 응용의 한 분야인 인터넷 전화는 그 서비스에 대한 요구사항이 커질수록 전세계적으로 통용 가능하도록 하여야 하는 필연성도 커질 것이다. 이런 연유로 ITU에서는 H.323 권고에 음성/비디오 등의 통합 데이터를 인터넷에서 전송하기 위한 규약을 포함하였으며, 이를 준수하는 인터넷 전화 제품이 출시되었다. 그러나 이 초기 권고에는 암호화와 관련된 내용을 포함하고 있지 않았으며, 이를 H.235 권고로 최근 발표하였다[4]. 이 외에 IETF(Internet Engineering Task Force)에서의 iptel(Internet Telephony) Working Group과 VON(Voice On the Network)에서 인터넷 전화 표준에 대한 논의가 활발히 진행 중이다[2][3].

인터넷 전화에서의 보안은 사용자끼리의 음성 데이터의 암호화에 의한 기밀성(confidentiality)의 제공 뿐만 아니라 상대방의 신원을 확인하는 인증(authentication)을 포함하여야 한다. PGP에서 개발하여 발표한 안전한 인터넷 전화인 PGPfone에서도 기밀성과 인증을 위해 패킷의 블록 암호화 기법과 공개키 방식의 Difffe-Hellman 키 교환 방식을 이용한다[4].

3. 스마트 카드를 이용한 안전한 인터넷 전화

인터넷 전화는 아래와 같은 과정을 거쳐서 PC-to-PC 서비스 모드를 제공할 수 있다.

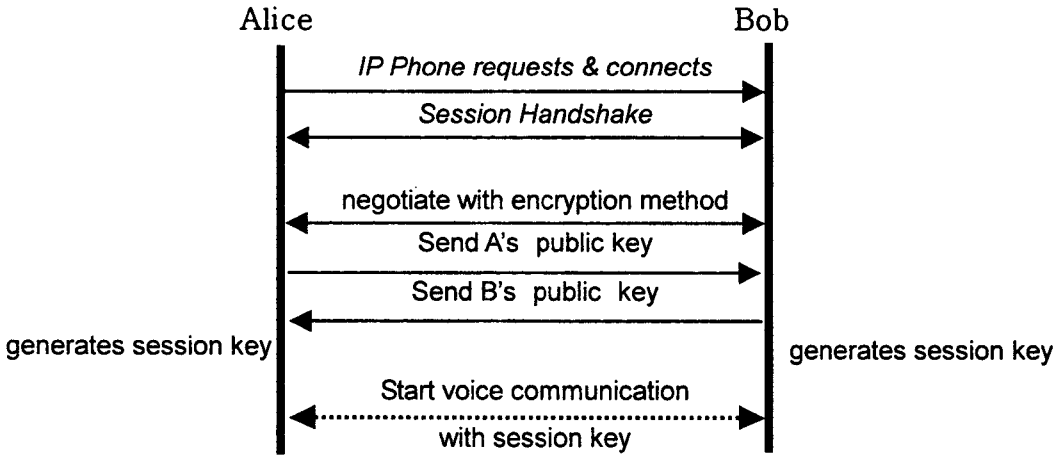
• 단계 1)

아날로그인 사람의 음성을 마이크 입력으로 받아서 디지털 형식으로 변환하고, 이에 대한 압축을 거친 후 패킷 단위로 나눈다. 이 패킷 제어 정보를 가진 별도의 제어 패킷을 생성하고 이를 상대방에게 전송한다.

• 단계 2)

이를 수신하면, 먼저 제어 패킷을 해석하여 제어 정보 등을 알아내고 제어 정보를 통해 음성 패킷의 해석과 아울러 압축 해제 과정을 거친 후 사람이 들을 수 있는 음성으로 재변환하여 스피커 또는 이어폰으로 출력한다.

안전한 비밀 통신을 위해서는 전화를 거는 사람이 먼저 인터넷 전화 연결 요구를 상대방에게 보내고 이에 대한 허가에 의해 한 세션이 연결된다. 이 후 암호 방법에 대한 협상이 이루어지며 서로의 음성 통신에 이용할 키를 얻은 과정까지 마치면 비로소 해당 키로 비밀 통신이 이루어진다.



(그림 1) 안전한 인터넷 전화의 기본 메커니즘

메시지의 암호에 이용되지는 않고 단순히 세션키의 분배에만 사용되는Diffie-Hellman 키 교환은 안전한 인터넷 전화에서 매우 적합하다. 그러나 이 세션키는 별도의 동작 없이 계속적으로 유지되는 값으로 불순한 의도를 가진 사람에 의한 키의 재사용(replay attack)에 대한 대비를 위해 주기적인 키 교환과 상호 인증을 위한 별도의 메커니즘을 필요로 한다.

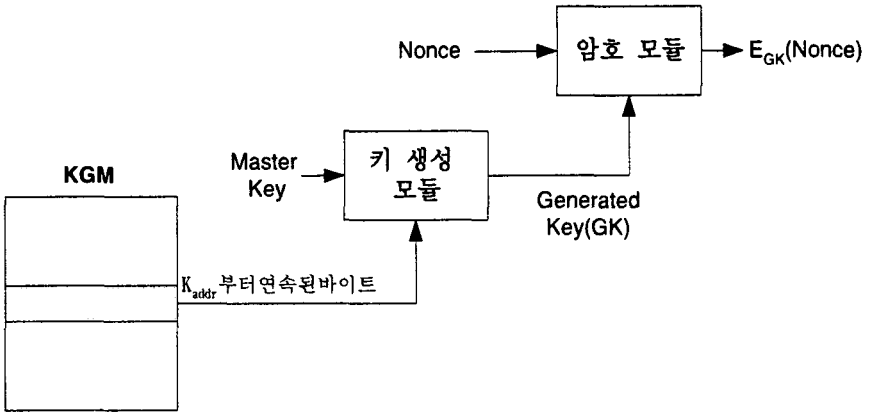
3.1 스마트 카드를 이용하는 안전한 키 교환

인터넷 전화에서 상호 인증 과정과 안전한 키 교환을 위한 스마트 카드는 다음과 같은 기능을 수행하여야 한다.

- 난수 발생 및 저장 기능
- 암호화/복호화 기능
- 키 생성 행렬(KGM : Key Generation

Matrix)에 의한 키 생성 기능
- 두개의 난수에 의한 키 생성 기능
- 인증 코드(MAC : Message Authentication Code) 생성 기능
- 강력한 접근 제어 기능

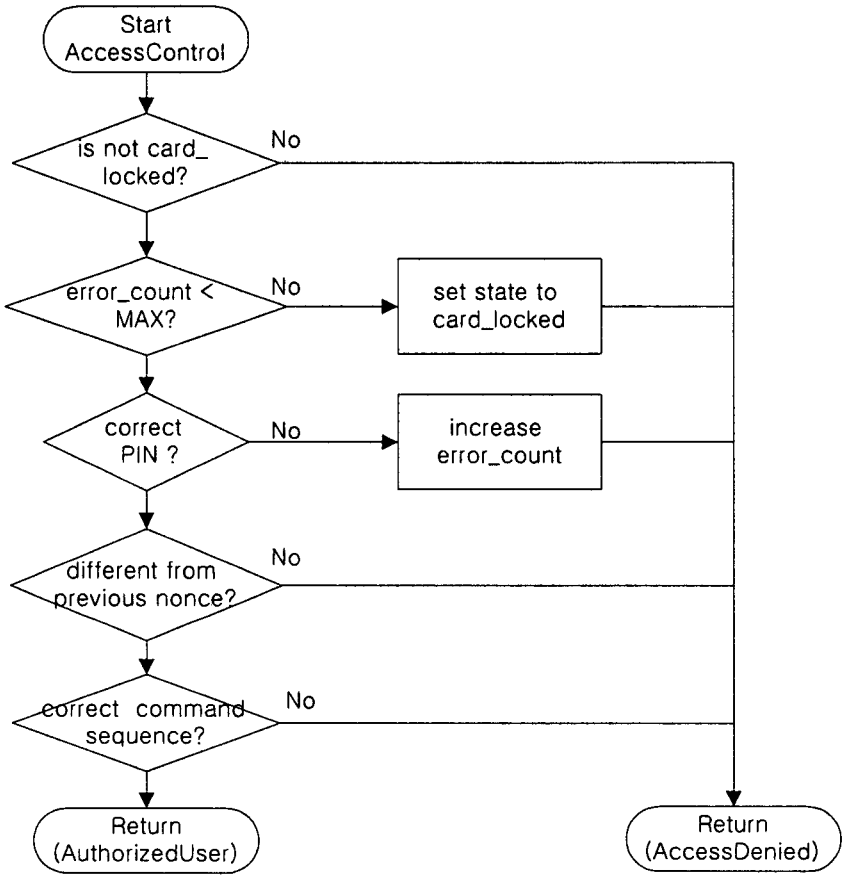
이용하여 계속적으로 안전한 인터넷 전화의 이용이 가능할 것이다. 초기 과정에서 생성된 키(GK)는 초기의 난수 암호화에 사용하며 이후의 스마트 카드의 암호 키(KSC)는 서로 교환된 난수를 사용하여 생성되며, 이는 비밀 통신의 세션키 암



(그림 2) 키 생성 행렬에 의한 초기 암호화 키 생성 과정

키 생성 행렬은 초기 스마트 카드의 숨겨진 영역(사용자가 접근할 수 없는 특정 EEPROM 영역)에 이미 저장되어 있으며, 이는 임의의 수들의 나열이다. 암호화 키를 노출하지 않고 스마트 카드 내부적으로 계산하기 위해 키 생성 행렬을 사용하였다. 키 생성 행렬을 사용하는 경우 카드에 저장되어 있는 행렬의 크기가 작아서 전체 선택 가능한 키 영역이 줄어드는 단점이 있지만, 이 때 생성되는 키는 세션키와 직접적인 관련이 없으며 사용자는 간단한 시작 주소(주로 1K미만의 숫자)의 공유로 초기 키 교환이 가능하다는 장점이 있다. 키 생성 모듈의 하나의 입력으로는 카드에 저장된 마스터 키(Master Key)를 사용하고, 다른 입력은 사용자가 입력한 키 생성 행렬의 시작 주소(Kaddr)로부터 연속된 바이트를 사용하여 새로운 키 GK를 생성한다. 마스터키는 카드의 발급시 동일한 값으로 주고 마스터키의 노출이 의심스러운 경우에 모든 카드에 새로운 마스터키를 내려주어 카드를 교체하지 않고 동일한 카드를 호화에 사용된다. 키 생성 행렬에 의한 초기 암호화 키 생성 과정은 <그림 2>와 같다.

모든 동작은 카드의 비밀번호(PIN : Personal Identification Number)를 확인한 후 이루어지므로 이는 사용자에 의해 안전하게 보관되어야 하며, 불법적인 사용을 막기 위해 카드 내의 모든 동작은 이 값을 확인한 후 이루어진다. 카드의 분실 시에도 카드의 비밀번호를 알지 못하면 카드로부터 어떠한 정보를 얻어낼 수 없으며, 일정 횟수 이상 다른 비밀번호를 입력하면 카드는 자동으로 자신의 카드를 잠김 상태로 두어 비밀 번호 추측에 의한 접근 시도는 불가능하다. 또 메시지의 재사용으로 인한 공격을 막기 위해 스마트 카드는 자신이 발생한 난수를 EEPROM 영역에 저장하여 동일한 명령의 수행에 대한 요구를 거부하거나, 일련의 명령이 정해진 순서가 아닐 경우 이를 거부할 수 있다. 이와 같이 스마트 카드에서 수행되는 접근 제어는 <그림 3>에서의 기능들을 수행하게 된다.



(그림 3) 스마트 카드의 접근 제어 방법

인터넷 전화를 요구하는 쪽에서는 다음의 단계를 거친다. 이 과정은 <그림 4>에 표시하였다.

● 단계 1) 난수 발생 및 암호화 과정

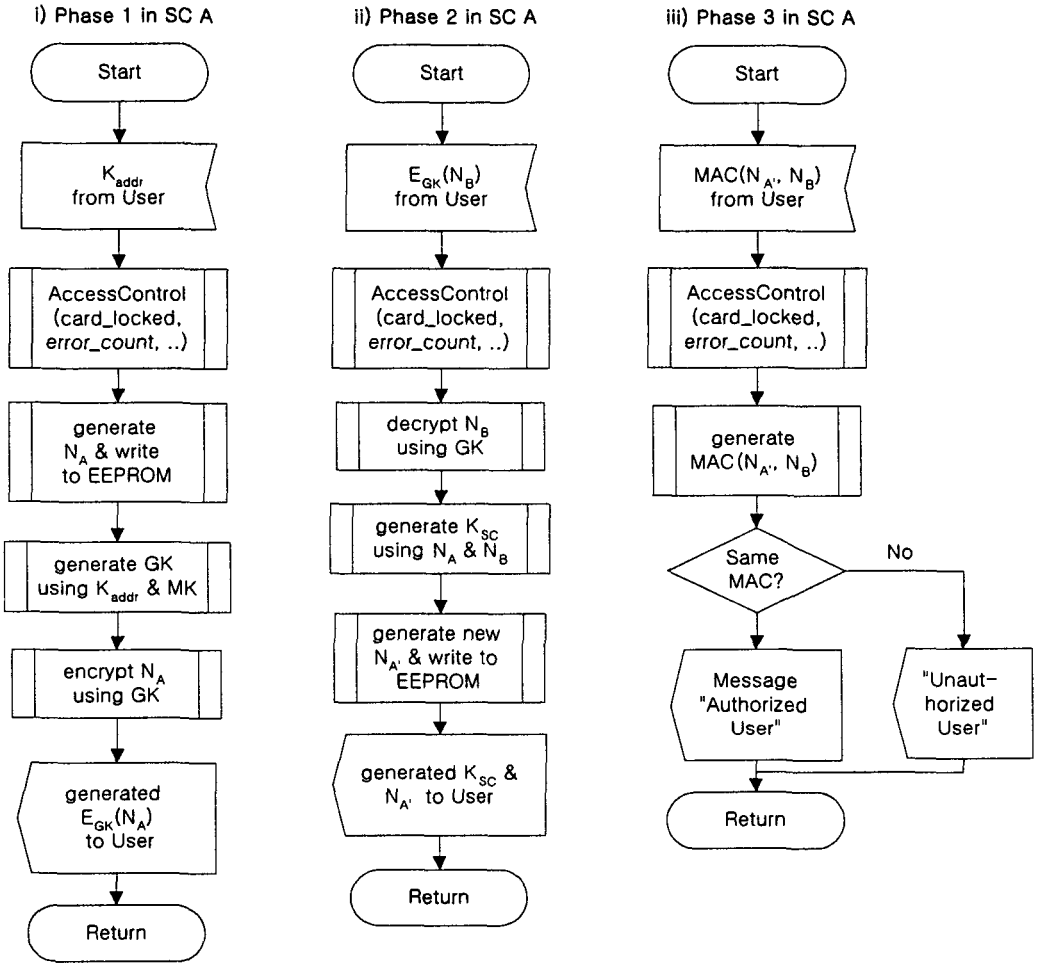
자신의 난수를 발생하여 초기 입력인 키 주소와 카드 내부의 마스터키를 이용하여 키를 생성하고 이 키로 난수를 암호화한다.

● 단계 2) 키의 생성 과정

상대방으로부터의 암호화된 난수를 입력받으면 이를 복호화하고 키 생성 알고리즘에 의해 키를 생성하고, 키 공유를 인증하기 위한 다른 난수를 발생하여 이를 생성된 키와 함께 출력으로 보낸다.

● 단계 3) 인증 코드의 확인 과정

상대방으로부터 받은 인증 코드를 자신이 계산한 값과 비교하여 동일한지를 확인한다.



(그림 4) 연결을 요구하는 쪽(Alice)의 동작 순서

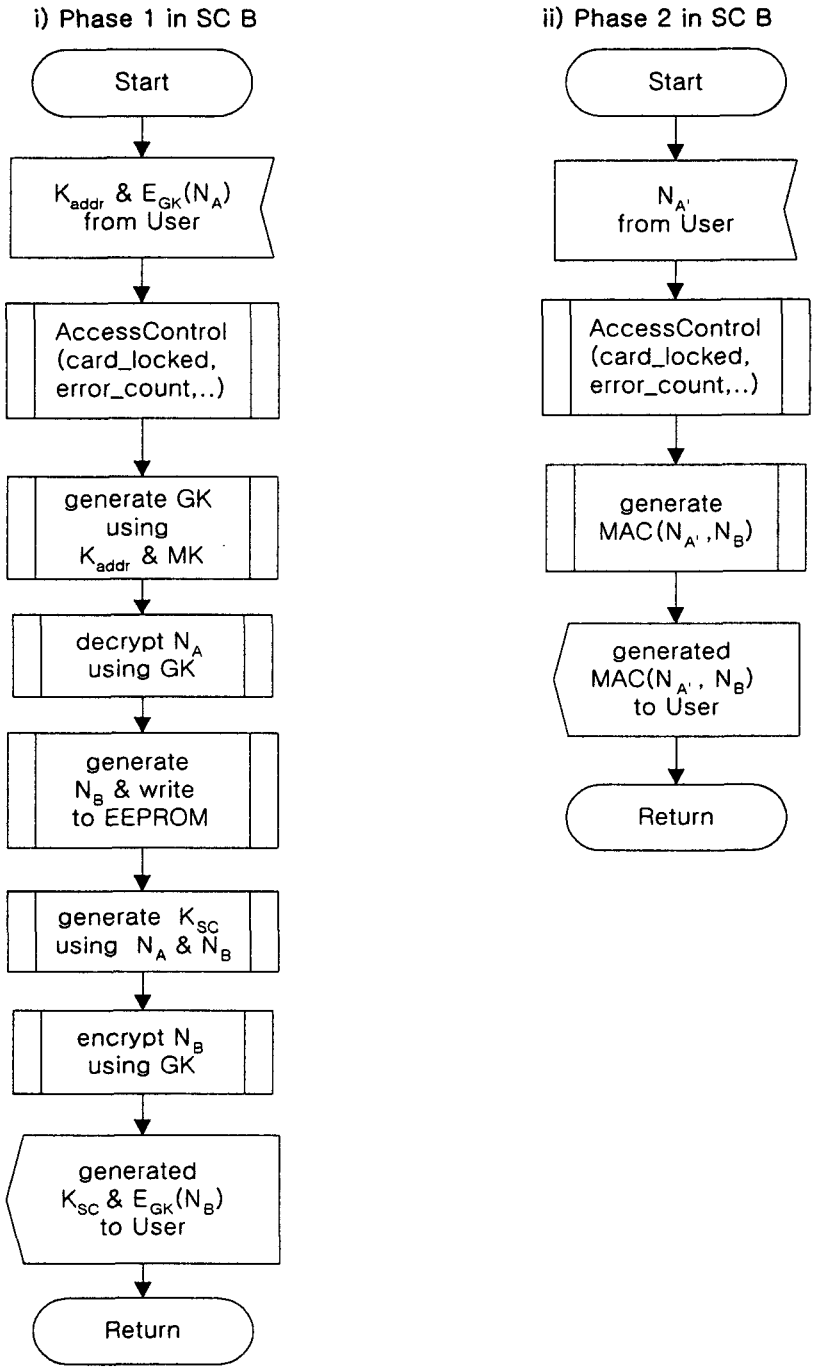
인터넷 전화를 요구받은 쪽에서는 다음의 순서로 동작한다. 이 과정은 <그림 5>에 표시하였다.

● 단계 1) 난수의 복호화 과정 및 키의 생성 과정

초기 입력인 키 주소와 카드 내부의 마스터키를 이용하여 키를 생성하고 상대방으로부터의 암호화된 난수의 복호화를 수행하고 자신의 난수를 암호화하고, 두 난수를 이용하여 키를 생성한다. 생성한 키와 암호화된 자신의 난수를 출력한다.

● 단계 2) 인증 코드의 생성

상대방으로부터 받은 새로운 난수를 이용하여 인증 코드를 생성하여 출력한다.



(그림 5) 연결을 허락하는 쪽(Bob)의 동작 순서

3.2 키 교환 및 인증 동작 절차

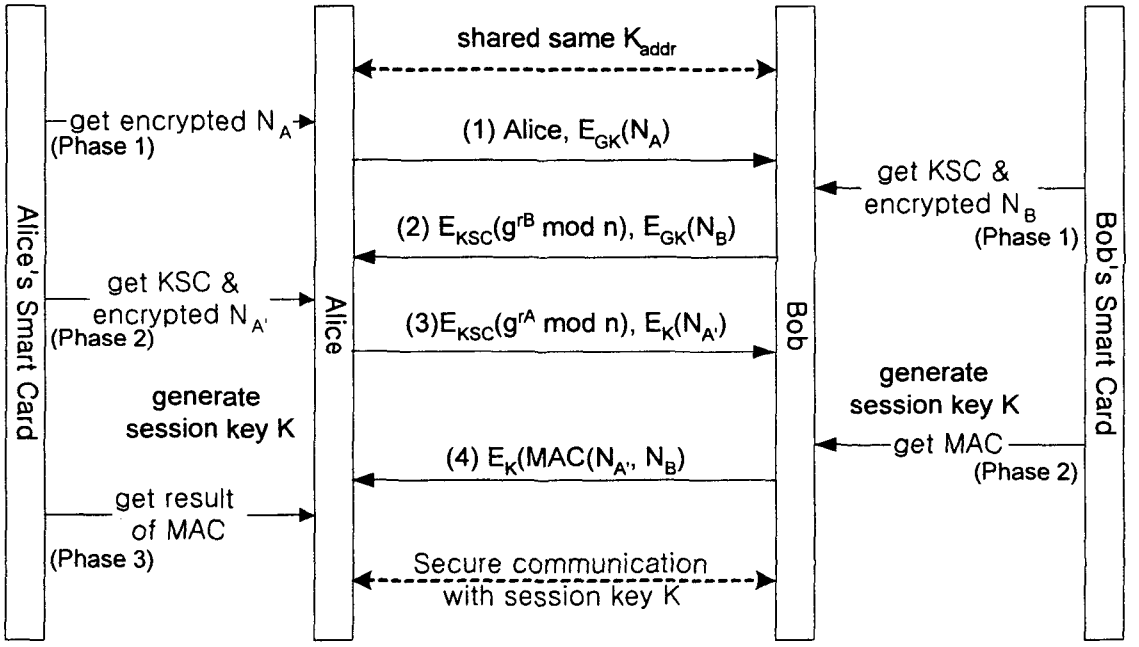
스마트 카드의 동작을 포함하는 키 교환과 인증 과정은 다음과 같으며 <그림 6>에서 이를 도시하였다. 먼저 두 사용자는 자신의 비밀번호가 입력된 스마트 카드를 가지고 있으며, Diffie-Hellman 키 교환을 위한 지수 g와 모듈로 연산을 위한 n을 공유하고 초기 난수 암호화에 이용하기 위한 시작 키 주소 Kaddr를 공유하여야 한다.

1) 통신을 원하는 한쪽(앨리스)이 먼저 자신의 스마트 카드로부터 암호화된 임의의 수 EGK(NA)를 획득하고 이를 상대방(밥)에게 전송한다.

Alice, EGK(NA)

2) 이를 수신한 밥은 앨리스로부터의 메시지임을 확인하기 위해 암호화된 EGK(NA)를 스마트 카드의 입력으로 주고 그가 생성한 키(KSC)와 이 키의 생성에 사용한 암호화된 난수 EGK(NB)를 받는다. 또, 세션키로 사용할 grB mod n을 계산하여 스마트 카드만이 계산할 수 있는 키(KSC)로 비밀키 방식의 암호화를 수행하고 다음을 앨리스에게 전송한다.

EKSC(grB mod n), EGK(NB)



<그림 6> 스마트 카드를 이용한 상호 인증 및 키 교환 과정

3) 앨리스는 암호화된 난수 EGK(NB)를 스마트 카드의 입력으로 사용하여 비밀키(KSC)를 얻어서 암호화된 세션키 일부인 grB mod n을 복호화하고, 나머지 세션키인 grA mod n를 생성함은 물론 세션키 K (grA*rB mod n)를 계산한다. 이후 동일한 세션키를 생성하였음을 확인하기 위한 과정으로 카드의 출력 값인 새로운 난수 NA'를

세션키로 암호화하여 밥에게 전송한다.

EKSC (grA mod n), EK(NA')

4) 밥은 카드로부터의 키 KSC를 이용하여 앨리스와의 비밀 통신시 사용할 세션키 K를 계산하고, 자신이 이를 정확히 계산하였음을 앨리스에게 알리기 위한 다음의 암호화된 메시지를 앨리스에게 보낸다.

EK(MAC(NA', NB))

5) 앨리스는 이를 복호화하고 카드로부터 정확한 인증 코드임을 확인 받는다.

이 과정을 모두 마치면 두 사람은 Diffie-Hellman방식에 의한 세션키 K를 생성할 수 있으며, 상호 인증의 효과를 얻는다. 세션키를 암호화하는데 이용한 비밀키 KSC는 스마트 카드의 내부 알고리즘에 의해 생성되어 외부에 전혀 노출되지 않는 값이다. 그리고 이 키 생성의 근본이 되는 난수 NA와 NB도 카드에 의해 생성되며, 이 난수의 암호화 키 GK를 생성하기 위한 키 주소 Kaddr역시 키 생성 행렬의 시작 키 주소로 일부분만 노출되는 값이며 나머지 부분은 카드만이 알 수 있는 값이다. 또, 비밀 통신 당사자가 아닌 사람이 비밀 통신의 키 정보를 획득하기 위해서는 스마트 카드의 운영체제를 공격하여 강력한 접근 제어 기능을 모두 통과하여야 하므로 카드로부터 해당 정보의 획득은 거의 불가능하다. 하지만 비밀 통신을 시작하기 전에 서로간의 시작 키 주소 Kaddr의 값은 매우 안전한 방법으로 공유되어야 한다.

키 생성 행렬을 저장하고 있는 스마트 카드를 이용하는 이유는 공개키를 유지해야 하는 키 분배 센터의 역할을 줄이고, 기존의 EKE에서의 패스워드에 비해 매우 간단한 값을 공유하기 위함이다. 이 프로토콜은 스마트 카드가 초기 발급되어야 하는 단점으로 인해 비밀 통신을 하고자 하는 제한된 그룹에서의 사용이 적절하며, 다수 가입자에게 인터넷에서의 비밀 통신을 제공하기 위해서는 재구성되어야 한다.

4. 결 론

지금까지 비밀 통신시 키 분배 센터의 개입 없이 안전하게 서로의 키를 교환하기 위해 스마트 카드를 이용하는 방법에 대해 제안하였다. 이 안전한 인터넷 전화를 구현함에 있어 사용되는 스마트 카드의 내부적인 기능과 이로부터의 안전한 키를 생성하여 음성 통신에 사용할 Diffie-Hellman 키의 암호화 및 복호화 과정과 상호 인증에 대해 기술하였다.

본 논문에서 제안한 프로토콜은 저 비용의 인터넷 전화가 일반화되어 원거리 사업장과의 업무 연락 시 노출될 수 있는 기업 비밀의 보호에 탁월한 능력을 발휘할 것 것이다. 또, 인터넷 전화를 근간으로 하는 프로토콜이지만 그 구조는 안전한 통신을 보장하려는 무선 통신에서도 적용이 가능하다.

프로그램과 데이터의 저장을 위한 EEPROM과 RAM 영역의 제한, 낮은 성능의 CPU 사용으로 인하여 자원의 활용이 제한적인 스마트 카드에서 효과적으로 동작할 수 있는 암호 알고리즘의 개발과 안전한 키 생성 행렬의 구성은 추후 연구 사항이다.

참고문헌

[1] http://www.pulver.com/

[2] VON(Voice On the Network), http://www.von.com/

[3] Internet Engineering Task Force, http://www.ietf.org

[4] ITU-T Recommendation H.235 : Security

and Encryption for H Series (H.323 and *other H.245 based) multimedia terminals*

[5] ITU-T Recommendation H.323 : Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service

[6] C.C. Chang, T.C.Wu, "A remote password authentication with smart cards", IEE proc., Part E, 138(3), pp165-168, May 1991

[7] GSM Card Technology, http://www.orga.com/applications/telecomm/

[8] S.M.Bellovin, M.Merritt, "Encrypted Key Exchange : Password-based protocols secure against dictionary attacks," in Proc. of the ComputerSociety Symposium on Research in Security and Privacy, pp. 72-84, May 1992.

[9] S.M.Bellovin, M.Merritt, "Augmented Encrypted Key Exchange," in Proc. of the First ACM Conference on Computer and Communications Security, pp. 244-250, Nov. 1993.

[10] MIT Distribution page for PGPfone : http://web.mit.edu/network/pgpfone/

[11] W.Diffie, M.E.Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, v.IT-22, n.6, pp 644-654, Nov 1976

[12] D.P.Jablon, "Strong Password-Only Authenticated Key Exchange", ACM Computer Communication Review, Oct. 1996

[13] R.Kaufman, R.Perlman, M. Speciner, 'Network Security private communication in a public world', Prentice-Hall, 1995

[14] B.Schneier, 'Applied Cryptography', second edition, John Wiley & Sons, 1996

박 진 호

1995 대전대학교 전자계산학과(공학사)
1997 대전대학교 컴퓨터공학과(공학석사)
1997 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부(박사수료)
2000 ~ 2002 송호대학 정보산업계열 전임강사
2002 ~ 현재 대덕대학 인터넷정보기술계열 전임강사
관심분야 : 네트워크 관리, 보안

정 진 욱

1974 성균관대학교 전기공학과(공학사)
1979 성균관대학교 전자공학과(공학석사)
1991 서울대학교 전자계산학과(이학박사)
1993~1985 한국과학기술연구소(KIST) 실장
1996~현재 한국정보처리학회 회장
1996~현재 정보보호 추진분과위원회 자문위원
1985~현재 성균관대학교 전기 전자 및 컴퓨터공학부 교수
관심분야 : 네트워크 관리, 망 보안, 컴퓨터교육