情 報 保 護 學 會 誌
第17卷 第3號, 2007. 6

일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향

최동현*, 김승주**, 원동호***

요 약

최근 인터넷과 같은 통신 기술이 급속도로 발전함에 따라, 많은 서비스들이 온라인을 통해서 이루어지고 있다. 그러나 인터넷은 개방형 네트워크이기 때문에 공격자에 의한 시스템 침입, 도청 등과 같은 여러 공격이 쉽게 발생된다. 특히 기존에 오프라인 상에서 이루어지던 은행 거래와 상거래가 인터넷 뱅킹과 전자상거래와 같이 온라인상에서 이루어짐에 따라 그 위험 수준은 더욱 높아지고 있다. 이러한 환경에서 사용자 인증은 안전한 통신을 위한 필수적인 요소라 할 수 있다. 대표적인 인증 방법으로 ID/Password 방식이 사용된다. 하지만 ID/Password의 경우 추측이나 도청에 의해 쉽게 공격될 수 있는 단점을 가지고 있다. 이러한 단점을 극복할 수 있는 인증 기법이 매번 새로운 패스워드를 생성하는 일회용 패스워드(OTP: One-Time Password) 기술을 활용한 인증 방법이다. 본 논문에서는 이러한 OTP 기술 분석 및 표준화 동향에 대해 소개하고자 한다.

Ⅰ. 서 론

최근 인터넷과 같은 통신 기술 및 컴퓨터의 계산 능력이 급속도로 발전함에 따라, 많은 비즈니스들이 온라인을 통해서 이루어지고 있다. 이에 따라 지식 및 정보 등 다양한 분야에 있어 누구나 많은 혜택을 누릴 수 있게 되었다. 그러나 인터넷은 개방형 네트워크이기 때문에 공격자에 의한 시스템 침입, 도청 등과 같은 여러 가지 공격에 취약하다. 특히 기존에 오프라인 상에서 이루어지던 은행 거래와 상거래가 인터넷 뱅킹과 전자상거래와 같이 온라인상에서 이루어짐에 따라 전송되는 정보의 중요도가 높아지고 있으며, 만약 공격이 발생할 경우 그 피해수준 역시 높아지고 있다. 이러한 환경에서 사용자 인증은 안전한 인터넷 사용을 위한 필수적인 요소라고 할 수 있다. 사용자 인증이란, 어떤 사용자가 실제로 정당한 사용자인지를 판단하는 과정으로, 대표적인 방식으로 ID/Password가 있다.

하지만, ID/Password 인증 방식은 password와 같은 단순한 인증 정보를 활용하기 때문에 네트워크 환경에서 커다란 문제점을 가지고 있다. 사용자가 아이디와 비밀번호를 외우기 쉬운 정보로 설정하거나, 고정된 비밀번호를 사용하기 때문에 공격자에 의해서 쉽게 추측될 수 있는 문제점이 있다. 또한 도청에 의해 쉽게 노출될 가능성이 높기 때문에 악의적인 공격자가 이를 이용하여 정당한 사용자로 위장할 수도 있다[4,5].

이러한 단점을 극복할 수 있는 인증 기법이 매번 새로운 패스워드를 생성하는 일회용 패스워드 기술을 활용한 인증 방법이다. 이러한 일회용 패스워드는 국내에서 주로 인터넷 뱅킹에서 사용되어 왔으며, 최근에는 온라인 게임에 접속하거나 게임 아이템, 음악, 동영상을 구매할 경우에도 사용되고 있다. 이처럼 일회용 패스워드에 대한 수요가 늘어나고 있으며, 보다 다양한 분야에서 사용되고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 OTP 기술의 필요성 및 OTP 기술에 대해 알아본다. 3장에서는 OTP기술의 국제 표준화 동향에 대하여 알아보고, 마지막으로 4장에서 결론을 내리고자 한다.

본 연구는 정보통신부 및 정보통신진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
* 성균관대학교 정보통신공학부 정보보호연구소 dhchoi@security.re.kr
** 성균관대학교 정보통신공학부 정보보호연구소 skim@security.re.kr
*** 성균관대학교 정보통신공학부 정보보호연구소 dhwon@security.re.kr

Ⅱ. OTP 기술

사용자를 인증하는 방법에는 크게 세 가지가 있다. 첫째는 사용자가 알고 있는 것(what you know)을 이용해서 인증하는 방법으로서 사용자가 특정 정보를 알고 있는지를 검증하는 방식이다. 대표적인 예로는 ID/Password 방식이 있다. 두 번째는 사용자의 특징(what the user is)을 이용해서 인증하는 방법으로 사용자가 가지는 지문, DNA 등을 검증하는 방식이다. 마지막으로 사용자가 가지고 있는 것(what you have)을 이용한 방식으로 사용자가 ID 카드, H/W토큰, S/W 토큰 등을 소유하고 있는지를 검증하는 인증 방식이 있다. OTP는 이러한 세 가지 방법 중 마지막인 사용자가 가지고 있는 것을 이용한 인증 방법으로 사용자가 인증을 받고자 할 때 매번 새로운 패스워드를 생성해주는 방식이다. 이번 장에서는 OTP 기술의 필요성 및 OTP 기술에 대해서 서술한다.

2.1. OTP 기술의 필요성

해킹 기술의 다변화, 고도화 및 대중화로 ID/Password 인증 방식의 안전성이 저하 되고 있다. 이를 반영하듯 피싱, 서버 해킹 및 악성 코드를 이용한 ID/Password 유출, 인터넷 뱅킹 해킹을 통한 불법 인출 사건 및 온라인 게임 해킹을 통한 개인정보유출과 같은 피해 사례가 급증하고 있다.

또한 〔표 1〕에서 보는 바와 같이 패스워드의 형태별 해독 시간이 짧기 때문에 인증방식으로 사용하기에는 매우 취약하다. 이러한 취약점을 보완하고자 password의 자리 수 제한, 특수 문자 사용 또는 주기적인 교체권고 등의 방법이 제안되고 있지만 이는 근본적인 해결책이 될 수 없다.

〔표 1〕 패스워드의 형태와 검출 시간[3]

No	문자 구성	경우의 수	자릿수	총 경우의 수	검색 시간
1	• 숫자	10	6	1,000,000	최대 약 2초
2	• 숫자	10	7	10,000,000	최대 약 5초
3	• 숫자	10	8	100,000,000	최대 약 50초
4	• 숫자	10	10	10,000,000,000	최대 약 1시간 30분
5	• 영소(대)문자 1 ‖ 숫자 5	26 ‖ 10	6	2,600,000	최대 약 3초
6	• 영소(대)문자 1 ‖ 숫자 6	26 ‖ 10	7	26,000,000	최대 약 12초
7	• 영소(대)문자 1 ‖ 숫자 7	26 ‖ 10	8	260,000,000	최대 약 2분
8	• 영소(대)문자 2 ‖ 숫자 4	26 ‖ 10	6	6,760,000	최대 약 3초
9	• 영소(대)문자 2 ‖ 숫자 5	26 ‖ 10	7	67,600,000	최대 약 31초
10	• 영소(대)문자 2 ‖ 숫자 6	26 ‖ 10	8	676,000,000	최대 약 5분 10초
11	• 영소(대)문자 3 ‖ 숫자 3	26 ‖ 10	6	17,576,000	최대 약 7 초
12	• 영소(대)문자 3 ‖ 숫자 4	26 ‖ 10	7	175,760,000	최대 약 1분 30초
13	• 영소(대)문자 3 ‖ 숫자 5	26 ‖ 10	8	1,757,600,000	최대 약 15분 30초
14	• 영소(대)문자	26	6	308,915,776	최대 약 2분 30초
15	• 영소(대)문자	26	7	8,031,810,176	최대 약 1시간 10분
16	• 영소(대)문자	26	8	208,827,064,576	최대 약 1일 10시간
17	• 영소문자, 영대문자	52	6	19,770,609,664	최대 2시간 30분
18	• 영소문자, 영대문자	52	7	1,028,071,702,528	최대 6일 20시간
19	• 영소문자, 영대문자	52	8	53,459,728,531,456	최대 약 280일
20	• 영소문자, 영대문자, 숫자	62	6	56,800,235,584	최대 약 7시간
21	• 영소문자, 영대문자, 숫자	62	7	3,521,614,606,208	최대 약 20일 3시간
22	• 영소문자, 영대문자, 숫자	62	8	218,340,105,584,896	최대 약 1,120일
23	• 영소문자, 영대문자, 숫자, 특수문자(32개)	94	6	689,869,781,056	최대 약 3일 15시간
24	• 영소문자, 영대문자, 숫자, 특수문자(32개)	94	7	64,847,759,419,264	최대 약 370일
25	• 영소문자, 영대문자, 숫자, 특수문자(32개)	94	8	6,095,689,385,410,816	10,000일 이상

이러한 ID/Password 방식의 한계를 극복하기 위해서는 비밀번호의 개수를 굉장히 많이 늘리거나 매번 바뀌는 비밀번호를 생성해야 한다. 여기서, 매번 바뀌는 비밀번호를 생성하는 방법이 OTP기술이다.

2.2. OTP 기술

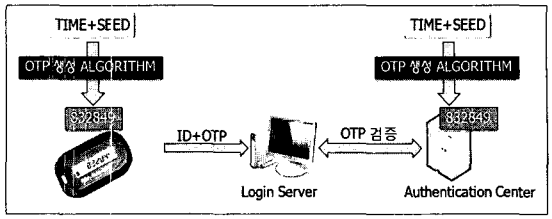
OTP는 사용자가 인증을 받고자할 때 매번 새로운 패스워드를 생성해주는 방식이다. OTP는 One Time Password의 약자로써, OTP 토큰과 인증 서버간 시간이나 seed와 같은 비밀 정보를 공유하고 이러한 정보를 해쉬 함수와 같은 알고리즘을 통해 일회용 패스워드를 생성하는 방식을 말한다.

OTP인증 과정은 다음과 같다. [그림 1]에서와 같이 OTP 토큰은 인증 서버와 공유하고 있는 시간 정보와 seed값을 해쉬와 같은 알고리즘을 통해 OTP 값을 생성하고 이를 Login Server로 ID와 함께 전송한다. ID와 OTP를 전송받은 Login Server는 해당 정보를 Authentication Center에 전송하고 OTP를 검증한다. Authentication Center는 수신한 ID를 확인하고 해당되는 시간 정보와 seed 정보를 OTP 토큰이 가지고 있는 알고리즘과 동일한 알고리즘을 이용해서 패스워드를 생성하고 이 값과 수신한 OTP 값이 동일한지 여부를 확인하여 Login Server에 검증 결과를 알려준다.

OTP는 질의응답(Challenge-Response) 방식, 시간동기화(Time-Synchronous) 방식, 이벤트 동기화(Event-Synchronous) 방식, 조합 방식 등의 네 가지 방식으로 나눌 수 있다.

2.2.1. 질의응답 방식

질의응답은 사용자가 서버가 제시한 질의 값을 알고리즘에 입력해 응답 값을 얻고 해당 응답 값을 서버에 전송하여 자신을 인증하는 방식이다. 인터넷 뱅킹에서 사용되는 보안카드가 바로 질의응답 방식이다. '11번 , 23번 비밀번호를 입력하세요?'의 질문에서 '11, 23'이라는 숫자가 질의 값이며, 이에 해당하는 응답 값은 보안카드의 11번의 앞자리 비밀번호, 23번의 뒷자리 비밀번호가 된다. 실제로 운용되는 OTP 장치는 보통 6자리 질의 값과 6자리 응답 값을 사용한다. 인증 서버가 임의의 난수를 생성하여 사용자에게 전송하면 사용자는 해당 질의 값을 입력하고, 그 결과로 얻은 응답 값을 다시 입력해야 하는 방식이다. 이 방식은 사용자의 입력 내용



[그림 1] OTP 인증 과정

이 많아서 불편하다.

2.2.2. 시간동기화 방식

질의응답 방식이 가지고 있는 단점인 사용자의 번거로움을 개선하기 위해 개발된 방식으로 임의의 난수 대신에 시간을 OTP 생성 입력 값으로 사용한다. 사용자 서버와 OTP 장치 간에 동기화된 시간 정보를 기준으로 특정 시간 간격(보통 1분)마다 변하는 OTP를 생성하게 된다. 이러한 방식을 적용한 제품으로는 RSA의 '시큐어아이디(SecureID)', 바스코의 '디지패스(Digipass)' 등이 있으며 많은 OTP 장치가 바로 이 방식을 사용하고 있다. 하지만, 이 방식의 경우 특정 시간 간격마다 비밀번호가 변하기 때문에, 입력 중에 비밀번호가 변하는 단점이 있다. 그렇다고 시간 간격을 길게 잡을 경우, 공격의 가능성이 커지게 되는 단점을 가지고 있다. 또한 시간 동기가 어긋날 경우 인증에 실패할 수 있기 때문에 추가적으로 시간 동기를 맞추는 알고리즘을 필요로 한다.

2.2.3. 이벤트 동기화 방식

이벤트 동기화 방식은 서버와 OTP 장치가 시간 정보 대신에 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 사용자가 일회용 비밀번호를 생성할 경우, 카운터 값을 OTP 알고리즘에 입력 값으로 사용하여 패스워드를 생성하고, 패스워드를 생성한 후에는 카운터 값을 증가시켜서 저장해두었다가 다음번에 알고리즘 입력으로 사용한다. 이 방식의 경우 OTP 장치에서 여러 번 패스워드만 생성하고 해당 패스워드를 인증 값으로 사용하지 않으면, OTP 장치와 서버 간의 카운터 값이 달라져 OTP 장치를 다시 초기화해야하는 단점을 가지고 있다.

2.2.4. 조합 방식

시간동기화와 이벤트 동기화 방식의 단점을 보완하

기 위해서 두 가지 방식을 조합하여 OTP 생성 방식이다. 이 방식은 OTP 생성 입력 값으로 시간 값과 카운트 값을 모두 사용하는 방식이다. 특정 시간 간격마다 비밀번호가 다시 생성되며, 또한 같은 시간 내에서 OTP 생성 요청이 다시 발생하면 카운트 값을 증가시켜 새로운 패스워드를 생성하도록 하는 방법이다. 이렇게 함으로써, 동일한 시간간격 내에서도 새로운 패스워드를 생성할 수 있게 되고 이를 통해 OTP의 안전성을 높일 수 있다.

Ⅲ. OTP 표준화 동향

OTP는 최초 Bellcore사가 개발한 기술로 당시 S/KEY 라는 명칭으로 발표되어 IETF에 의해서 표준화 되었다. 그 후에는 인증관련 업계에서 표준화를 주도하고 있으며 대표적으로 RSA진영과 OATH진영이 있다. 두 진영은 OTP관련 표준을 IETF를 통해 경쟁적으로 표준화를 진행하고 있다[2].

3.1. S/KEY[1]

OTP는 Bellcore사에 의해서 최초로 개발된 기술로 당시 S/KEY 라는 명칭으로 발표되었다. 그 후 S/KEY는 IETF의 표준 문서인 RFC 1760으로 1995년에 등록되었다. 하지만 S/KEY라는 명칭이 등록상표로 자유롭게 사용할 수 없었기 때문에 표준 명칭으로는 부적합했다. 같은 해 IETF는 S/KEY 기술 표준화 목적으로 IETF내 One Time Password Authentication WG를 설립하고 기술 명칭을 S/KEY에서 OTP로 변경한다. 이를 바탕으로 RFC 1938이 표준으로 제안되었다. 이후 생성한 패스워드의 표현 형식 등 몇 가지 사항을 개선한 후 제안된 RFC 2289가 표준이 되었다.

S/KEY는 일방향 함수를 사용하여 패스워드를 생성하게 되어 있다. 먼저 난수 r값을 생성하고 이 값에 대하여 식(1)처럼 일방향 함수 f를 n+1번 수행하여 X_{n+1}을 구한다. 그리고 r과 X_{n+1}을 각각 OTP사용자와 검증자에게 시스템 최초 설정시 전달하여 저장해 둔다.

$$X_{n+1} = \underbrace{f(f(...f(r)...))}_{n+1개} \quad (1)$$

이렇게 설정된 상태에서 사용자가 검증자에게 인증을 받을 필요가 생기면 자신의 사용자 번호인 id와 일방향 함수 f를 n번 수행한 X_n을 생성하고 이를 인증 정보로 인증 검증자에게 전달하게 된다. 인증 검증자는 전달 받은 인증 정보 중 X_n을 식(2)처럼 일방향 함수 f를 이용해서 1회 더 계산함으로써 X'_{n+1}을 구한다. 인증 검증자는 이렇게 얻은 값과 시스템 최초 설정시 저장되어 있는 X_{n+1}값을 비교하여 같으면 인증 요구자를 인증하게 된다. 인증이 성공적으로 이뤄지게 되면 인증 검증자는 저장되어 있는 X_{n+1}을 X_n으로 대체한다.

$$X'_{n+1} = f(X_n) \quad (2)$$

3.2. OATH 진영[8]

OATH(Open AuTHentication)는 인증관련 업계에서 "개방", "표준화", "상호 운용성"을 확립하기위해 설립된 조직으로 관련업계 간의 상호 협력을 추진하고 있다. 특히 강력한 인증의 보편적인 채택을 목표로 하여 현재의 개방형 표준화에 적극적으로 참여하고 있으며, 이를 통해 OTP의 개방형 참조 구조를 개발하고 있다. OATH는 미국의 VeriSign사의 제안에 의해서 2004년 2월에 설립되었다. 참여사로는 VeriSign, ActivIdentity, Incard, IBM, VASCO, Entrust 등의 업체가 있다. 또한, 이를 채택하고 있는 업체로는 Cryptocard, PassGo 등이 있다.

대표적인 표준화작업으로는 2005년 12월에 발표된 HMAC을 기본으로 한 OTP표준인 RFC 4226이 있다[6]. 이외에도 HOTP 알고리즘을 기반으로 질의/응답 방식의 인증과 서명을 위한 OATH 알고리즘을 제안한 "IETF Mutual OATH Challenge/Response Specification Draft", XKMS 프로토콜을 기반으로 공유 비밀 값인 OTP 변수들의 공급 방법을 제안한 "IETF Bulk Provisioning Protocol Draft" 그리고 서로 다른 타입의 인증 장치 간 보안 토큰의 공유를 위한 전송 포맷과 OTP키와 같은 비밀 정보의 공유 방법을 제안한 "IETF Symmetric Key Container Draft"가 있다.

현재 OATH는 제안한 Draft의 업데이트 및 새로운 Draft의 제안 등 활발한 활동을 하고 있다. 특히 이벤트 기반의 OTP인 HOTP의 경우 알고리즘의 확장을 통해 시간 기반 OTP의 표준제안을 준비 중이다.

3.3. RSA 진영[9]

1986년에 설립된 RSA는 보안 솔루션을 제공하는 업

〔표 2〕 OATH 와 RSA 진영에서 제안중인 표준

OATH 진영	RSA 진영
• IETF HMAC-SHA1 OTP (RFC 4226) - HMAC 기반의 이벤트 방식의 OTP	• IETF CT-KIP (RFC 4578) - 암호 토큰의 안전한 초기화와 환경설정을 위한 기술
• IETF Mutual OATH Challenge/Response Specification Draft - HOTP를 기반으로 질의/응답 방식의 인증과 서명을 위한 알고리즘	• OTP-PKCS #11 - OTP토큰에 의해 생성된 OTP의 복구와 검증을 위한 기술
• IETF Bulk Provisioning Protocol Draft - XKMS 프로토콜 기반의 공유 비밀값 공급 방법 제안	• OTP-Kerberos - OTP로 Kerberos 비밀번호 대체 방법
• IETF Symmetric Key Container Draft - 다른 타입의 인증장치간의 보안 토큰의 공유를 위한 전송 포맷 및 비밀정보 공유방법 제안	• OTP-Validation Service - OTP 자격 증명 정보의 검증을 위한 웹서비스 프로토콜 정의
	• EAP-POTP - OTP 토큰을 사용하기에 적합한 일반적인 EAP 방식 제안

체로 마이크로소프트사와 협력관계를 맺고 있다. RSA는 SecureID라는 시간동기 방식의 OTP를 통해 전 세계 수천 개의 기업에 사용자 인증 솔루션을 제공하고 있다. 또한, IETF, OASIS 등에서 보안 분야의 표준 개발에서 주요한 역할을 하고 있다.

대표적인 표준화작업의 예로는 암호 토큰의 안전한 초기화와 환경설정을 위한 클라이언트-서버 프로토콜에 관한 기술을 다룬 RFC 4758인 CT-KIP (Cryptographic Token Key Initialization Protocol)이 있다[7]. 이외에도 OTP 토큰에 의해 생성된 OTP의 복구와 검증을 위해 사용할 수 있는 "OTP-PKCS #11", OTP 토큰에 의해 생성된 OTP의 복구와 검증을 위해 사용할 수 있는 일반적인 Microsoft사의 CryptoAPI함수와 알고리즘을 제안한 OTP_CAPI, 사전 인증에서 OTP로 Kerberos 비밀번호를 대체하기 위한 방법인 OTP-Kerberos, OTP 자격 증명 정보의 검증을 위한 웹서비스 프로토콜을 정의한 "OTP-Validation Service" 그리고 OTP 토큰을 사용하기에 적합한 일반적인 EAP 방식을 제안한 "EAP-POTP"가 있다.

3.4. 국내 OTP 동향

현재 국내에서 진행 중이거나 완료된 OTP 표준화 활동은 없다. 다만 2006년 5월 인터넷 뱅킹 해킹 사건의 후속 대책으로 내놓은 '전자금융거래종합대책'에서 고객이 이용하는 거래수단별로 보안등급을 구분하고, 보안 수준 1등급을 맞추기 위해 OTP 또는 HSM 도입을 시중은행에 지시한 상태이다.

또한 전자금융거래 안전성 강화정책의 일환으로 금융보안전담기구인 '금융보안연구원'을 설립되었다. 금융보안연구원에서는 전자금융거래 보안성을 강화하기 위해 각 금융기관이 도입하는 OTP를 한 곳에서 통합관리하는 OTP 통합인증센터를 설립 운영할 예정이다.

Ⅳ. 결 론

본 논문에서 우리는 OTP 기술 분석 및 표준화 동향에 대해서 서술하였다. OTP는 ID/Password 인증 방법을 대체하며 여러 분야로 사용이 확대되고 있다. 하지만 국내의 경우 이러한 OTP 기술과 관련한 표준화 활동이 현재는 전무한 상태에 있다. OTP 사용이 확산되고 있는 과정에서 이러한 표준화가 진행되지 않는 다면 과거 교통카드 인프라 확산 당시와 같이 표준화는 사실상 불가능 하게 될 것이다. 표준화 실패에 의한 피해를 막기 위해서 OTP 기술에 대한 표준화 연구가 시급히 진행되어야 할 것이다. 이러한 OTP기술의 표준화는 OTP를 사용하는 사용자의 불편을 줄여주고, 국내 기술의 해외 진출 경쟁력 확보에도 도움이 될 것이다.

참고문헌

〔1〕 N. Haller, C. Metz, P. Nesser, M. Straw, , "A One-Time Password System," RFC 2289, IETF, 1998

〔2〕 금융보안연구원, "금융보안 주간정보", 제1권 4호 Jan 2007

[3] 신동휘, 최윤성, 박상준, 김승주, 원동호, "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석", 정보보호학회논문지 17(2), Feb 2007
[4] 박중길, 김영진, 김영길, 백규태, 백기영, 류재철, "S/KEY를 개선한 일회용 패스워드 메커니즘 개발", 정보보호학회논문지, 9(2), June 1999
[5] 박중길, 장태주, 박봉주, 류재철, "시간을 이용한 효율적인 일회용 패스워드 알고리즘", 정보처리학회논문지C, 8(4), Aug 2001
[6] D. M' Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen, "HOTP: An HMAC-Baced One-Time Password Algorithm," RFC 4226, IETF, 2005
[7] M. Nystroem, "Cryptographic Token Key Initialization Protocol (CT-KIP)," RFC 4758, IETF, 2006
[8] OATH, http://www.openauthentication.org
[9] RSA, http://www.rsa.com

〈著者紹介〉

최 동 현 (Donghyun Choi)
정회원
2005년 8월 : 성균관대학교 정보통신공학부 공학사
2007년 2월 : 성균관대학교 컴퓨터공학과 석사
2007년 3월~현재 : 성균관대학교 일반대학원 휴대폰학과 박사과정 재학 중
관심분야 : 암호이론, 네트워크 보안, DRM, 모바일 보안

김 승 주 (Seungjoo Kim)
종신회원
1994년 2월-1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월-2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월-현재 : 성균관대학교 정보통신공학부 교수
2001년 1월-현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월-현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 7월-현재 : 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2006년 2월-현재 : 한국우주통신연구소 암호연구회 운영위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won)
종신회원
1976년-1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 : 한국전자통신연구원 전임연구원
1985년-1986년 : 일본 동경공업대 객원연구원
1988년-2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 : 국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
관심분야 : 암호이론, 정보이론, 정보보호