2013년 6월 전자공학회 논문지 제 50 권 제 6 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 6, June 2013 http://dx.doi.org/10.5573/ieek.2013.50.6.167

논문 2012-50-6-19

신원기반의 차량통신망 메시지 인증 스킴에 대한 안전성 분석

(Cryptanalysis of an Identity-Based Message Authentication Scheme in VANETs)

류 은 경*, 이 성 운**, 유 기 영***

(Eun-Kyung Ryu, Sung-Woon Lee, and Kee-Young Yoo©)

요 약

최근 Biswas등은 신원기반의 대리서명을 사용한 차량통신망 메시지 인증 프로토콜을 제안하였다. 저자들은 제안된 인증기법이 대리 서명키에 대한 안전성, 메시지 위조 및 재전송 공격에 대한 안전성, 부인방지 서비스, 대리 서명키 노출에 대한 저항성 등에 대한 안전성을 제공한다고 주장하였다. 본 논문에서는 Biswas등이 제안한 프로토콜에서 위임 받지 않은 임의의 공격자가 원 서명자의 비밀키에 대한 정보 없이 메시지 전달자의 대리 서명키를 계산할 수 있음을 보인다. 이것은 Biswas등이 제안한 메시지 인증 프로토콜은 저자들의 주장과는 달리 안전하지 않음을 의미한다. 또한, 본 논문에서는 이를 해결할 수 있는 개선된 프로토콜을 제시한다.

Abstract

In a paper recently published in the International Journal of Parallel, Emergent and Distributed Systems, Biswas et al. proposed a VANET message authentication scheme which uses an identity-based proxy signature mechanism as an underlying primitive. The authors claimed that their scheme supports various security features including the security of proxy-key, the security against message forgery and the security against replay attack, with non-repudiation and resistance to proxy-key compromise. Here, we show how an active attacker, who has no knowledge of an original message sender's private key, can compute the proxy-signature key of the corresponding message sender, meaning that the scheme is completely insecure. We also suggest an enhanced version of the protocol capable of solving such serious security holes.

Keywords : Message Authentication, Identity-based Proxy Signature, Vehicular Ad-hoc Networks

Ⅰ. 서 론

차량 애드혹 네트워크 (VANET: Vehicular Ad-hoc Network)은 교통정보 서비스, 위치기반 서비스, 자동비용 징수 서비스, 일반 통신 서비스 등의 응용에서 뿐만 아니라, 자동차와 운전자, 그리고 외부환경과의 정보 교환을 통해서 운전자의 안전성 개선을 주요 목표로 하고 있다[2~5,10]. VANET 메시지 인증 프로토콜은 다른 네트워크와는 달리 빠른 이동성과 잦은 네트워크 토폴리지의 변화 등의 특성을 갖는 차량 간 또는 차량과 노변장치(RSU: Road-Side Unit)간에 무선 통신에서 전송되는 정보들을 도청, 위장공격, 재생공격과 같은 다양한 보안 위협들로부터 안전하고 신뢰성 있게 전달할 수 있게 하는 암호학적 기법이다[7~8]. 이와 같은 차량통신망 보안문제는 운전자의 안전성과도 직결된다 할 수 있다.

최근 Biswas 등(BMM)[9]은 신원기반 암호시스템[1]과 대리서명 기법[6]을 암호학적 도구로 사용하는 차량통신

* 정회원, 경북대학교 전자전기컴퓨터학부
(EECS, Kyungpook National University)
** 정회원, 동명대학교 정보보호학과
(Department of Information Security, Tongmyong University)
*** 정회원, 경북대학교 컴퓨터학부
(School of Computer Science and Engineering, Kyungpook National University)
※ 이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음.
© Corresponding Author(E-mail: yook@knu.ac.kr)
접수일자 2013년2월7일, 수정완료일 2013년5월16일

망 메시지 인증 프로토콜을 제안하였으며, 대리 서명키에 대한 안전성, 메시지 위조 및 재전송 공격에 대한 안전성, 부인방지 서비스, 대리 서명키 노출에 대한 저항성 등에 대한 안전성을 제공한다고 주장하였다. 본 논문은 BMM 프로토콜에서 위임받지 않은 공격자가 원 서명자의 비밀키 정보 없이 메시지 전달자의 대리 서명키를 계산할 수 있음을 보인다. 이것은 BMM 프로토콜이 저자의 주장과는 달리 메시지 인증 프로토콜의 기본적인 요구사항을 만족하지 않으며 안전하지 않다는 것을 의미한다. 또한, 본 논문에서는 이를 해결할 수 있는 개선된 프로토콜을 제시한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 BMM 메시지 인증 프로토콜에 대해 간략히 살펴보고 Ⅲ장에서 BMM 프로토콜의 안전성을 분석한다. Ⅳ장에서는 이러한 문제점들을 해결할 수 있는 개선된 프로토콜을 제안하고 제안된 기법에 대한 안전성을 분석한다. 마지막으로, Ⅴ장에서는 결론을 맺는다.

Ⅱ. BMM 메시지 인증 프로토콜

본 장에서는 S. Biswas 등이 제안한 차량 통신망 환경에서 대리서명 기반의 메시지 인증 프로토콜에 대하여 간략하게 기술한다.

1. 키설정

메시지 송신자 CA의 비밀키는 x이고, 이에 대응하는 공개키는 $Q=xP$이다. 송신자 CA의 공개키 Q는 시스템 파라메터로 시스템내의 모든 사용자에게 사전 분배되어 있다고 가정한다. 메시지 송신자 CA는 메시지 m을 전달자 RSU_i들을 통해 메시지 수신자인 각 차량의 OBU에 전송하기 위해 다음 과정을 수행한다.

1) 난수 k_0를 선택하고, $R_0 = k_0 P$를 계산한다.
2) 난수 k_i를 선택하고, $R_i = k_i P$로 정의한다.
3) 메시지 m, 메시지 유효기간 t_m및 메시지 유효범위 a_m를 이용하여 다음 $h_{i,m}$을 계산한다.

$$h_{i,m} = H(ID_i \| ID_0 \| m \| t_m \| a_m).$$

여기서, ID_0는 메시지 송신자 CA의 식별자 ID_i는 메시지 전달자 RSU_i의 위치정보를 나타낸다.

4) 각각의 RSU_i에 대해서 다음의 같이 대리 서명키 $s_{i,m}$를 계산한다.

$$s_{i,m} = (k_i + h_{i,m} x) k_0^{-1} (\mathrm{mod}\, q).$$

5) $(S_{i,m} \| R_0 \| R_i \| m \| t_m \| a_m)$는 안전한 채널로 RSU_i에 전송한다. RSU_i는 CA의 공개키 Q를 사용하여 다음과 같이 $S_{i,m}$를 검증한다.

$$R_i = ? s_{i,m} R_0 - h_{i,m} Q.$$

2. 대리서명 및 메시지 전달

RSU_i는 CA로부터 받은 메시지 m을 전송범위 내의 차량들의 OBU에 전송하기 위해 다음과정을 수행한다.

1) 세션 파라메터 $k_p = H(ID_i \| t)$와 $(x_p, y_p) = k_p R_0$를 생성한다. 여기서 ID_i는 RSU_i의 위치 정보, t는 시스템의 현재시간을 나타낸다.
2) 대리 서명키 $s_{i,m}$을 이용하여 메시지 m에 대한 서명값 $s_{p,i,m}$를 다음과 같이 생성한다.

$$s_{p,i,m} = k_p^{-1} (H(m) + s_{i,m} x_p) (\mathrm{mod}\, q).$$

3) $(s_{p,i,m} \| R_0 \| R_i \| m \| t_m \| a_m)$을 브로드캐스트 한다.

3. 메시지 및 서명값 검증

메시지 수신자 OBU는 수신된 메시지 및 서명값에 대한 검증을 다음과 같이 수행한다.

1) $h_{j,m} = H(ID_j \| ID_0 \| m \| t_m \| a_m)$을 계산한다. 여기서 ID_j는 OBU 자신의 위치정보를 나타내며, OBU가 RSU_i의 전송 유효범위 내에 있다면 ID_j는 RSU_i의 위치정보인 ID_i와 같은 값을 가진다.
2) $k_p = H(ID_j \| t)$와 $(x_p, y_p) = k_p R_0$ 를 계산한다. 다음 식을 통해 메시지 m과 서명값 $s_{p,i,m}$을 검증한다.

$$(x_p, y_p) = ? s_{p,i,m}^{-1} (H(m) R_0 + x_p (R_i + h_{j,m} Q)).$$

Ⅲ. BMM 프로토콜의 보안 취약성

본장에서는 앞서 기술된 BMM 메시지 인증 프로토콜이 프로토콜 설계시 발생된 치명적인 결함 때문에 메시지 인증 프로토콜에 대한 기본 요구사항 만족하지 않음을 보인다.

먼저, BMM 프로토콜의 메시지 인증 메커니즘을 간략히 살펴본다. BMM 프로토콜은 전송 메시지의 원 서명자 CA가 생성한 서명값, 즉 메시지 m에 대응되는 인증 값 $s_{i,m}$이 안전한 채널로 메시지 전달자 RSU_i에게 전달된다. 전달된 $s_{i,m}$는 CA로부터 인증된 RSU_i의 서명키로 사용되며, CA의 메시지 m은 $s_{i,m}$로 서명된 서

1) 난수 k_0를 선택하고, $R_0 = k_0 P$를 계산한다.
2) $h_{i,m} = H(ID_i \| ID_0 \| m \| t_m \| a_m)$를 계산한다. 이때, ID_i는 공격자의 위치정보, ID_0는 메시지 원전송자 CA의 공개된 식별자이고, t_m과 a_m은 메시지의 유효기간 및 유효범위이다.
3) 난수 r_A를 선택한 후, 다음을 만족하는 R_i를 계산한다.

$$R_i = r_A R_0 - h_{i,m} Q.$$

4) 현재시간 t 및 위치정보 ID_i를 사용해서, 세션 파라메터 $k_p = H(ID_i \| t)$와 $(x_p, y_p) = k_p R_0$를 계산한다.
5) 메시지 m에 대한 서명값

$$s_{p,i,m} = k_p^{-1}(H(m) + r_A x_p) \pmod q$$

을 계산한다.
6) $(s_{p,i,m} \| R_0 \| R_i \| m \| t_m \| a_m)$을 브로드캐스트 한다.

그림 1. 공격 - 대리 서명키 계산
Fig. 1. The Attack - Extracting Proxy-Signature Key.

명값 $s_{p,i,m}$와 함께 RSU_i의 브로드캐스트 전송 방식으로 통신범위 내에 있는 OBU들에게 전달된다. 각각의 OBU는 수신한 메시지 m과 서명값 $s_{p,i,m}$에 대해서 CA의 공개키 Q를 사용하여 검증하고, 그 유효성을 판단하게 된다.

그러나, BMM 프로토콜에서는 원 메시지 전송자 CA로부터 위임을 받지 않는 임의의 공격자가 RSU_i의 서명키 $s_{i,m}$에 대응되는 유효한 대리 서명키 값을 생성할 수 있다는 치명적인 결함을 갖는다. 이것은 BMM 프로토콜은 안전하지 않으며 실제 응용에 사용할 수 없음을 의미한다. 그림 1은 BMM 프로토콜에서 임의의 공격자 A가 자신이 선택한 메시지 m에 대응되는 유효한 대리 서명키 r_A과 이에 대응되는 유효한 서명값 $s_{p,i,m}$를 계산할 수 있음을 보인다.

공격자 A의 통신범위 내에 있는 차량들이 공격자의 메시지 및 서명값 $(s_{p,i,m} \| R_0 \| R_i \| m \| t_m \| a_m)$를 수신했을 때 각 차량의 OBU는 프로토콜의 메시지 검증 과정에 따라 수신된 메시지와 그 서명값에 대해서 다음 식을 만족하는지 검증한다.

$$(x_p, y_p) = s_{p,i,m}^{-1}(H(m) R_0 + x_p(R_i + h_{j,m} Q)).$$

이때, $h_{j,m} = H(ID_j \| ID_0 \| m \| t_m \| a_m)$이고, ID_j는 OBU의 위치정보를 나타내며 유효거리 범위 내에 있다면 ID_i와 같은 값을 갖게 된다. 여기서, 우리는 다음과 같이 메시지 인증에 대한 검증식이 만족함을 알 수 있다.

$$\begin{aligned}
&s_{p,i,m}^{-1}(H(m)R_0 + x_p(R_i + h_{j,m}Q)) \\
&= s_{p,i,m}^{-1}(H(m)R_0 + x_p(r_A R_0 - h_{i,m}Q + h_{j,m}Q)) \\
&= s_{p,i,m}^{-1}(H(m)R_0 + x_p r_A R_o \\
&= s_{p,i,m}^{-1}(H(m) + x_p r_A) R_0 \\
&= k_p (H(m) + x_p r_A)^{-1}(H(m) + x_p r_A) R_0 \\
&= k_p R_0 \\
&= (x_p, y_p)
\end{aligned}$$

따라서, 우리는 다음 Theorem 1로 BMM프로토콜에 대한 안전성 분석 결과를 요약할 수 있다.

Theorem 1. [대리 서명키 계산 공격] BMM 프로토콜은 대리 서명키 계산 공격에 대한 안전성을 제공하지 않는다.

상기 Theorem 1은 BMM 프로토콜의 안전성에 총체적인 결함이 있음을 함축한다.

다시 말해서, 대리 서명키 $s_{i,m}$는 CA의 비밀키 x로 서명된 값이며 안전한 채널을 통해 등록된 적법한 RSU_i에게 전달된다. 전달된 $s_{i,m}$는 인증서를 필요치 않는 RSU_i의 인증된 비밀 개인키로 사용된다. 따라서 공격자가 CA의 비밀키 x에 대한 정보 없이 RSU_i의 키 $s_{i,m}$을 계산할 수 있다는 것은 S. Biswas 등이 주장한 바와 달리, BMM 프로토콜은 메시지 위조 및 재전송 공격에 대한 안전성, 부인방지 서비스, 대리 서명키 노출에 대한 저항성, OBU의 메시지 위조공격에 대한 안전성과 같은 부가적인 보안 특성들 역시 지원할 수 없음을 의미한다.

Ⅳ. 개선된 프로토콜

앞서 기술된 BMM 프로토콜의 안전성 문제의 원인은 전송된 메시지 및 서명값 검증에 필요한 R_0 및 R_i에 대한 무결성을 메시지 수신자가 확인 할 수 없기 때문에 야기된다. 본 장에서는 이를 해결할 수 있는 개선된 프로토콜을 제시한다. 프로토콜에서 사용할 표기는 표 1과 같다.

1. 인증 프로토콜

메시지 송신자 CA의 비밀키는 x이고, 이에 대응하는 공개키는 $Q = xP$이다. 송신자 CA의 공개키 Q는 시스템 파라메터로 시스템내의 모든 사용자에게 사전 분배

표 1. 표기
Table 1. Notations.

표 기	설 명
q	160bit 크기의 소수
x	시스템의 마스터 비밀키
P	타원곡선상의 기저 포인트
k_0, k_i	난수
$H()$	암호학적 일방향 해쉬함수
m	메시지
t_m	유효시간
a_m	유효범위
ID_i	RSU$_i$의 식별자
ID_0	CA의 식별자
t	현재시간
$\|$	두 개의 비트열을 연결하는 연산자
-----➔	안전한 채널
——➔	안전하지 않은 채널

되어 있다고 가정한다. 개선된 프로토콜에서 메시지 전달자 RSU$_i$에 대한 대리 서명키 설정 과정은 그림 2와 같다. CA로부터 생성된 RSU$_i$의 서명키 및 관련정보는 안전한 채널로 전달된다.

RSU$_i$는 CA로부터 받은 메시지 m을 자신의 전송 범위 안에 있는 차량들의 각 OBU에 전송하는 과정은 앞서 살펴본 2.2절의 BMM 프로토콜과 같다. 메시지 수신자 OBU에서의 메시지 및 서명값 검증을 통한 메시지 인증 과정은 다음과 같다.

1) $(s_{p,i,m}\|R_0\|R_i\|m\|t_m\|a_m)$를 수신한 각 차량의 OBU는 먼저 $h_{j,m}=H(ID_j\|ID_0\|R_0\|R_i\|m\|t_m\|a_m)$을 계산한다. 여기서 ID_j는 OBU의 위치정보를 나타내며, OBU가 RSU$_i$의 전송 유효범위 내에 있다면 ID_i와 ID_j는 같은 값을 가진다.
2) 각 OBU는 다음식을 통해 메시지 m과 서명값 $s_{p,i,m}$를 검증한다.

$$(x_p, y_p)=?(H(m)R_0+x_p(R_i+h_{j,m}Q))s_{p,i,m}^{-1}.$$

그림 3은 개선된 프로토콜에서의 대리 서명된 메시지 전송 및 검증을 메시지 인증 과정을 나타낸다.

2. 안전성 분석

앞서 기술된 BMM 프로토콜의 안전성 문제는 전송된 메시지 및 서명값 검증에 필요한 R_0 및 R_i의 변조 여부를 수신자가 검증 할 수 없기 때문에 야기된 프로토콜 설계상의 치명적인 오류이다.

이를 해결하기 위해서 개선된 프로토콜에서 브로드캐스트 되는 모든 값들에 대한 변조여부를 확인할 수 있도록 메시지 인증값 $h_{i,m}=H(ID_i\|ID_0\|R_0\|R_i\|m\|t_m\|a_m)$를 이용하여 프로토콜의 안전성을 강화하였다. 다음은 대리 서명키를 사용하는 메시지 인증 프로토콜의 핵심 보안 요구사항인 대리 서명키 계산공격과 메시지 위조공격에 대해서 제안된 프로토콜의 안전성을 분석한다.

가. 대리 서명키 계산공격

제안된 프로토콜에서, 공격자가 자신이 선택한 임의의 메시지 m 및 $R_0=k_0P$, $R_i=k_iP$에 대해서, 유효한 대리 서명키를 생성하기 위한 유일한 방법은 $s_{i,m}=(k_i+h_{i,m}x)k_0^{-1}(\mathrm{mod}\,q)$를 계산해야 한다.

이때, k_i및 k_0는 공격자가 선택한 난수이고, $h_{i,m}=H(ID_i\|ID_0\|R_0\|R_i\|m\|t_m\|a_m)$이다. 이것은 $s_{i,m}$를 계산하기 위해서 공격자는 CA의 공개키 $Q=xP$로부터 x를 계산할 수 있어야 함을 의미한다. 따라서 제안된 프로토콜의 대리 서명키 계산 공격에 대한 안전성은 잘 알려진 암호학적 가정인, 이산대수 가정을 기반으로 한다.

CA (x, Q)		RSU$_i$ (Q)
$k_0, k_i \in Z_q$ $R_0=k_0P$ $R_i=k_iP$ $h_{i,m}=H(ID_i\|ID_0\|R_0\|R_i\|m\|t_m\|a_m)$ $s_{i,m}=(k_i+h_{i,m}x)k_0^{-1}(\mathrm{mod}\,q)$	$s_{i,m}\|R_0\|R_i\|m\|t_m\|a_m$ ----------➔	$h_{i,m}=H(ID_i\|ID_0\|R_0\|R_i\|m\|t_m\|a_m)$ check if $R_i=(s_{i,m}R_0-h_{i,m}Q)$

그림 2. 대리서명 키 생성
Fig 2. Generation of Proxy-Signature Key.

OBU (Q)		RSU$_i$ (Q)
$h_{j,m} = H(ID_j \| ID_0 \| R_0 \| R_i \| m \| t_m \| a_m)$ check if $(x_p, y_p) = (H(m)R_0 + x_p(R_i + h_{j,m}Q))s_{p,i,m}^{-1}$	$\xleftarrow{s_{p,i,m} \| R_0 \| R_i \| m \| t_m \| a_m}$	$k_p = H(ID_i \| t)$ $(x_p,\ y_p) = k_p R_0$ $s_{p,i,m} = k_p^{-1}(H(m) + s_{i,m}x_p) \pmod q$

그림 3. 메시지 인증
Fig 3. Message Authentication.

나. 메시지 위조공격

제안된 프로토콜에서 공격자가 RSU$_i$를 대신하는 메시지 위조 공격에 성공하기 위해서는 자신이 선택한 임의의 메시지 m 및 $R_0 = k_0 P$, $R_i = k_i P$에 대응되는 유효한 서명값 $s_{p,i,m} = k_p^{-1}(H(m) + s_{i,m}x_p) \pmod q$를 계산해야 한다. 이때, $k_p = H(ID_i \| t)$는 위치정보 및 현재시간에 대한 해쉬값으로 세션 파라메터이며, x_p는 $k_p R_0$에 대한 x 좌표 값이다. 즉, CA로부터 m 및 $R_0 = k_0 P$, $R_i = k_i P$에 대응되는 대리 서명키 $s_{i,m}$을 가진 적법한 RSU$_i$ 만이 계산할 수 있음을 의미한다. 따라서 제안된 프로토콜의 메시지 위조공격에 대한 안전성 역시 공개키 Q로부터 x를 계산하는 이산대수 문제로 귀결된다.

V. 결 론

본 논문에서는 Biswas 등이 제안한 신원기반 대리서명 기법을 이용한 차량통신망 메시지 인증 프로토콜에 대한 안전성을 분석하였다. 분석결과, Biswas등이 제안한 프로토콜은 프로토콜 설계시 발생된 치명적인 결함으로 위임받지 않은 임의의 공격자가, 원 메시지 서명자의 비밀키 정보 없이 메시지 전달자의 대리 서명키를 계산할 수 있음을 보였다. 따라서 Biswas등의 프로토콜은 대리 서명키의 안전성을 기반으로 하는 메시지 위조 및 재전송 공격에 대한 안전성, 부인방지 서비스, 대리 서명키 노출에 대한 저항성과 같은 부가적인 안전성을 지원할 수 없는 총체적인 결함이 있어 실제 응용에 사용할 수 없다. 또한, 본 논문에서는 이를 해결할 수 있는 개선방안을 제시하였다.

REFERENCES

[1] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," in Proceedings of CRYPTO 84 on Advances in Cryptology, Springer-Verlag, pp. 47 - 53, 1985.

[2] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication," in Proceedings of the 6th Embedded Security in Cars Workshop (ESCAR), 2008.

[3] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in Proceedings of Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[4] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinm, "Secure and Efficient Beaconing for Vehicular Networks", In Proceeding of 5th ACM VANET, 2008.

[5] M. Raya and J.P. Hubaux, "The Security of Vehicular Ad hoc Networks," in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05), 2005.

[6] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation, in Proceedings of the 3rd ACM Conference on Computer and Communications Security, pp. 48 - 57, 1996.

[7] P. Papadimitratos, V. Gligor, and J. Hubaux, "Securing Vehicular Communications Assumptions, Requirements, and Principles," in Proceedings of Workshop on Embedded Security in Cars (ESCAR), 2006.

[8] P. Papadimitratos, P. Buttyan, T. Holczer, et al, "Secure Vehicular Communications: Design and Architecture Application and Management Services," IEEE Communications Magazine 46(11), pp. 100 - 109, 2008.

[9] S. Biswas, J. Misic, and V. Misic, "An Identity-based Authentication Scheme for Safety Messages in WAVE-enabled VANETs," International Journal of Parallel, Emergent and Distributed Systems, DOI:10.1080/7445760.011.41965, 2012.

[10] IEEE Std 1609.2, IEEE Trial-use Standard for Wireless Access in Vehicular Environments

(WAVE) - Security Services for Applications and Management Messages, IEEE, 2006.

저 자 소 개

류 은 경(정회원)

1995년 경일대학교 컴퓨터공학과 학사 졸업
1999년 계명대학교 정보통신공학 석사 졸업
2005년 경북대학교 컴퓨터공학과 박사 졸업
2005년～2006년 경북대학교 Post-doc
2006년～2007년 (일)函館未來대학 Post-doc
2007년～2010년 경북대학교 초빙교수
2010년～현재 경북대학교 연구원
<주관심분야 : 정보보호, 암호응용, 보안프로토콜 설계/분석, 네트워크 보안>

유 기 영(정회원)

1976년 경북대학교 수학과 학사 졸업
1978년 한국과학기술원 전산학과 석사 졸업
1992년 미국 뉴욕 R.P.I. 컴퓨터과학과 박사 졸업
1978년～현재 경북대학교 컴퓨터학부 교수
1997년～현재 한국정보과학회 영남지부장
1999년～현재 한국 정보과학회 이사
2006년～현재 제12대 한국 정보보호학회 부회장
<주관심분야 : 암호학, 정보보호, 네크워크 보안, 스테가노그라피>

이 성 운(정회원)

1993년 전남대학교 전산통계학과 학사 졸업
1996년 전남대학교 전산통계학과 석사 졸업
2005년 경북대학교 컴퓨터공학과 박사 졸업
1996년～2000년 (주)한국정보시스템
2005년～현재 동명대학교 정보보호학과 부교수
2009년～현재 보안공학연구회 논문지 편집위원
<주관심분야 : 정보보호, 암호 프로토콜, RFID/USN 보안>