TETRA 인증 프로토콜 분석

박용석* · 안재환* · 정창호* · 안정철*

The Analysis of the TETRA Authentication Protocol

Yong Seok Park* · Jae Hwan Ahn* · Chang Ho Jung* · Joung Chul Ahn*

요 약

TETRA 시스템에서는 Challenge-response 프로토콜에 의해 단말기와 인증 센터 간에 사전에 공유된 인증키가 일치하는지를 확인하는 인증 서비스를 제공함으로써 인가된 단말기만 망에 접속하도록 하고 있다. 그러나 TETRA 표준 인증 프로토콜은 단말기 식별자인 ISSI(Individual Short Subscriber Identity)가 복제된 단말기의 망 접속은 차단할 수 있지만, ISSI와 인증키가 모두 복제된 경우 복제단말기의 불법 사용을 막을 수 없는 취약점이 존재한다. 본 논문에서는 TETRA 표준인 ETSI 규격에서 정의하고 있는 인증 프로토콜을 간략히 설명하고 인증 과정에서 사용되는 인증키의 생성/분배/주입 모델을 설명한 후, 인증키가 인증 센터로 전달되는 과정에서 노출되었을 경우 발생할 수 있는 복제단말기의 위협을 분석한다. 마지막으로 ISSI와 인증키가 복제된 단말기의 망 접속을 차단할 수 있는 새로운 인증 프로토콜을 제안한다.

ABSTRACT

TETRA system provides the radio authentication service which permits only authorized radio to access network. Radio authentication is the process which checks the sameness of authentication-key(K) shared between radio and authentication center by challenge-response protocol. TETRA standard authentication protocol can prevent the clone radio to copy ISSI from accessing network, but can't prevent the clone radio to copy ISSI & authentication-key. This paper analyzes authentication-key generation/delivery/injection model in TETRA authentication system and analyzes the threat of clone radio caused by authentication-key exposure. Finally we propose the new authentication protocol which prevent the clone radio to copy ISSI & authentication-key from accessing network.

키워드

TRS, TETRA, 인증, 인증용 비밀키 K, ISSI

Ⅰ. 서 론

주파수 공용통신 시스템(TRS)은 한정된 무선주파수를 다수의 이동가입자가 공유하여 통신을 행할 수 있게 하는 일련의 시스템을 말하며 이동단말기, 기지국, 이동중계국 및 시스템 관리 설비 등으로 구성된다. 국내에서는 국가 긴급재난 발생 시 일원화된 종합지휘 무선통신 체계를 확보하기 위해 유럽형 디지털 TRS 개방형 표준인 TETRA(TErrestrial Trunked RAdio) 방식으로 국가통합지휘 무선통신망 구축 사업을 추진 중에 있다[1].

TETRA는 유럽 전기통신 표준위원회(European Telecommunications Standards Institute : ETSI)가 개인 이동 무

* 국가보안기술연구소

접수일자 : 2006. 5. 26

선 통신(Professional Mobile Radio : PMR)과 공공 접속 이동 통신(Public Access Mobile Radio : PAMR)을 위해 지원하는 세계 유일의 무선 디지털 개방 표준으로서 업무용 이동 무선 통신을 위해 경쟁력이 높은 개방 시장을 형성하고 있으며 세계 각국의 공공안전 및 재난통신망으로 널리 사용되고 있다. 주로 군이나 경찰을 비롯한 재난관리책임기관 사용자들의 지휘/통제 시스템으로 활용되므로 정보보호에 대한 요구 사항이 높기 때문에 TETRA에서는 정보보호 서비스를 위해 별도의 표준을 정의하고 있다[2-4].

TETRA 표준 보안기능은 보안 수준에 따라 인증(Authentication), 무선구간 암호화(Air Interface Encryption : AIE), 종단간 암호화(End-To-End Encryption : E2EE)로 구성된다.

TETRA 표준 인증 프로토콜은 단말기 위치 등록 단계에서 단말기가 위치 업데이트 요구 메시지를 망으로 전송함으로써 시작된다. Challenge-response 프로토콜에 의해 단말기와 인증 센터간에 사전에 공유된 인증키가 일치하는지를 확인함으로써 적법한 단말기인지를 검증한다. 그러나 TETRA 표준 인증 프로토콜은 단말기 식별자인 ISSI(Individual Short Subscriber Identity)가 복제된 단말기의 망 접속은 차단할 수 있지만, ISSI와 인증키가 모두 복제된 경우 복제단말기의 불법 사용을 막을 수 없는 취약점이 존재한다. 즉, 인증키의 불법 복제 위협은 고려하지 않고 있다. 본 논문에서는 TETRA 표준 인증 프로토콜을 설명하고 인증 과정에서 사용되는 인증키의 생성/분배/주입 모델을 설명한 후, 인증키가 인증 센터로 전달되는 과정에서 노출되었을 경우 발생할 수 있는 복제단말기의 위협을 분석한다. 마지막으로 인증키가 노출되어 복제단말기가 만들어진 최악의 상황에서도 복제단말기의 망 접속을 차단할 수 있는 새로운 인증 프로토콜을 제안한다.

II. TETRA 인증 시스템 분석

2.1 단말기 인증 절차

TETRA 인증 서비스의 목적은 인가된(Authorized) 적법한 단말기만이 망에 접속하도록 함으로써 불법 복제단말기에 의한 통화 도용 및 신분 위장 등의 위협 요소를 제거하는데 있다.

TETRA 인증 방법은 비밀키(symmetric key) 방식으로 동일한 인증용 비밀키 K를 공유한 단말기와 인증 센터 양자가 상대방 K의 유효성을 확인하기 위해 Challenge- response 프로토콜을 수행한다. 전체 인증 절차는 그림 1과 같다.

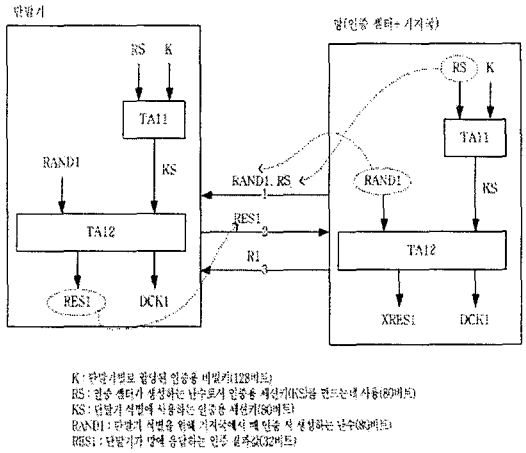
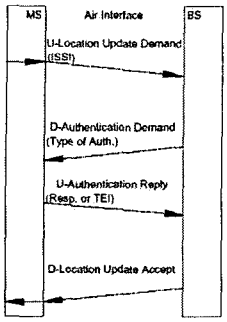


그림 1. 단말기 인증 절차
Fig. 1 Radiuo authentication process

인증키 K와 RS로부터 유도된 인증용 세션키 KS가 단말기와 인증 센터에 의해 계산된다. 기지국은 식별 신청(challenge)을 위한 난수 값으로 RAND1을 생성해 단말기로 전달하고 단말기는 RAND1과 KS로부터 응답값(response)인 RES1을 계산하고 동시에 기지국은 기대되는 응답값인 XRES1을 계산한다. 기지국이 단말기로부터 RES1을 받으면 XRES1과 비교해 동일하면 R1이 "TRUE"로 설정되고 아니면 "FALSE"로 설정이 된다. 인증이 성공한 경우 단말기와 기지국사이에서 교환되는 음성, 데이터, 신호 메시지는 DCK(Derived Cipher Key)를 이용해 암호화된다.

그림 2는 단말기 등록 단계에서 실제 TETRA 단말기가 위치 업데이트 요구 메시지(U-LOCATION UPDATE DEMAND)를 망으로 전송하면서 시작되는 인증 관련 신호 메시지의 교환 과정을 프로토콜 분석기를 이용하여 캡쳐한 화면이다.



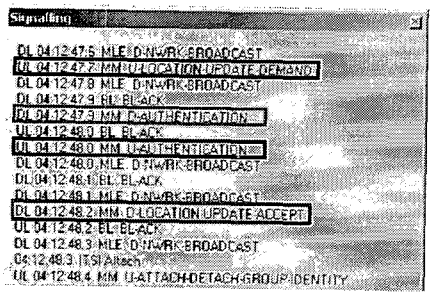


그림 2. 인증 신호 메시지 교환 과정
Fig. 2 Authentication signaling message exchange process

그림 1에서 1번 화살표로 표시된 식별 신청(challenge) 신호는 그림 2의 D-AUTHENTICATION에 해당된다. 실제 프로토콜 분석기가 캡쳐한 D-AUTHENTICATION의 내용은 그림 3과 같다.

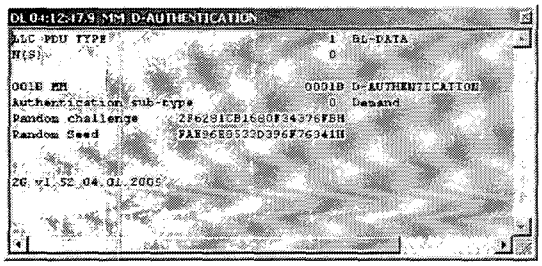


그림 3. D-AUTHENTICATION 메시지 내용
Fig. 3 D-AUTHENTICATION Message

그림 1에서 2번 화살표로 표시된 응답(response) 신호는 그림 2의 U-AUTHENTICATION에 해당된다. 실제 프로토콜 분석기가 캡쳐한 U-AUTHENTICATION의 내용은 그림 4와 같다.

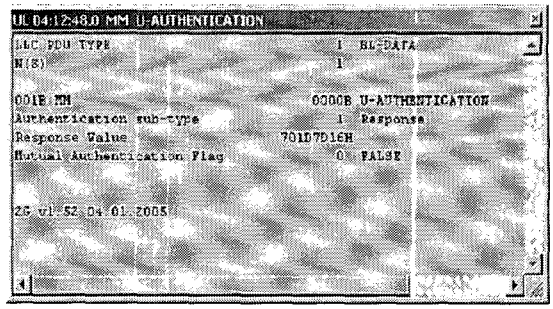


그림 4. U-AUTHENTICATION 메시지 내용
Fig. 4 U-AUTHENTICATION Message

그림 1에서 3번 화살표로 표시된 인증 결과(Result) 신호는 그림 2의 D-LOCATION UPDATE ACCEPT에 해당된다. 실제 프로토콜 분석기가 캡쳐한 D-LOCATION UPDATE ACCEPT의 내용은 그림 5와 같다. 인증이 성공한 경우 Authentication result 필드가 TRUE(1)로 세팅됨을 알 수 있다.

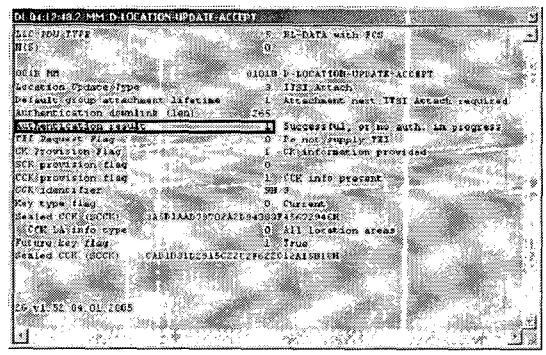


그림 5. D-LOCATION UPDATE ACCEPT 메시지 내용
Fig. 5 D-LOCATION UPDATE ACCEPT Message

2.2 인증키 생성/분배/주입 모델

단말기 인증을 위해서는 사전에 동일한 인증용 비밀키(K)를 개별 단말기와 인증 센터가 공유하고 있어야 한다. 그림 6은 TETRA MoU SFPG 권고안 01.에서 제시하고 있는 인증키 생성/분배/주입 모델을 나타낸다[5].

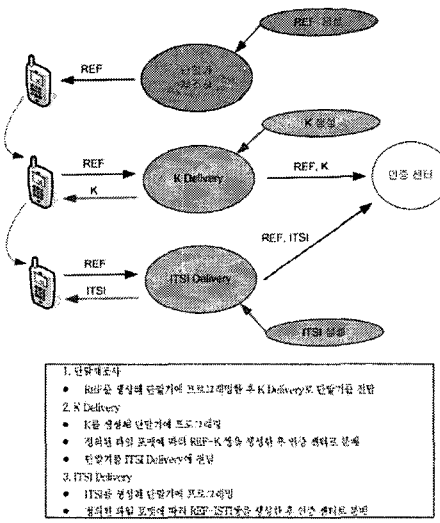


그림 6. TETRA 인증키 생성/분배/주입 모델
Fig. 6 TETRA authentication key generation/distribution/injection model

그림 6에서 알 수 있듯이 인증 센터가 어떠한 단말기에 어떠한 인증키가 주입되어 있는지를 알기 위해서는 REF-K쌍과 REF-ITSI쌍을 인증 센터 데이터베이스에 저장하고 있어야 한다. 여기서 REF(Reference Number)는 단말기 제조사에서 부여한 단말기 일련 번호를 의미하고, ITSI(Individual TETRA Subscriber Identity)는 망 운영자가 부여한 단말기 식별 번호로서 전화번호에 해당한다.

Ⅲ. TETRA 망에서 복제단말기 위협 분석

3.1 단말기 식별 번호인 ISSI를 복제한 경우

ISSI는 48비트 ITSI에서 국가 코드(10비트)와 망 코드(14비트)를 제외한 6 digit의(24비트) 단말기 식별 번호로서 전화번호에 해당한다. 일반적으로 상대방 단말기의 전화번호는 누구나 알 수 있다. 따라서 단말기 프로그래밍 툴을 가지고 있는 사람은 ISSI를 복제한 복제단말기를 쉽게 만들 수 있다. 그러나 대상 단말기의 인증용 비밀키(K)를 모르는 상태에서 단순히 ISSI만 복제한 단말기는 TETRA 표준에서 정의한 단말기 인증 프로토콜에 의해 망 접속이 차단된다. 즉, 정상 단말기를 A라고 했을 경우 A의 ISSI_A를 다른 단말기에 주입하여 복제단말기 B를 만든다. 해커는 정상 단말기 A의 인증용 비밀키인 K_A는 모르는 상태로 A의 ISSI_A만을 이용해 시스템에 대한 접근을 시도한다.

복제단말기 B의 전원을 켜면 (그림 7)과 같은 위치 업데이트 요구 메시지(U-LOCATION UPDATE DEMAND)를 망으로 전송하여 단말기 등록을 시도한다.

Information element	Length
PDU type	4
Location update type	3
Request to append LA	1
Cipher control	1
Ciphering parameters	10
Class of MS	24
Energy saving mode	3
LA information	
SSI	24
Address extension	24
Group identity location demand	
Group report response	
Authentication uplink	
Proprietary	

그림 7. 위치 업데이트 요구 메시지의 내용
Fig. 7 Information of U-LOCATION UPDATE DEMAND Message

망이 위치 업데이트 요구 메시지를 수신하면 메시지 내의 ISSI 값을 읽어 해당 ISSI에 대응되는 인증용 비밀키 K를 인증 센터의 데이터베이스에서 찾아 인증 절차를 시작한다. 이 과정에서 복제단말기 B는 정상 단말기 A의 인증용 비밀키인 K_A를 모르기 때문에 망에서 계산한 XRES1과 동일한 응답값인 RES1을 만들 수 없고 결과적으로 복제단말기 B는 망에 등록이 허용되지 않는다.

3.2 단말기 식별 번호인 ISSI와 인증키 K를 모두 복제한 경우

그림 6에서 REF-K 쌍과 REF-ITSI 쌍은 온/오프라인을 통해 인증 센터로 전달된다. 실제 운용되는 대개의 TETRA 시스템의 경우 REF-K 쌍과 REF-ITSI 쌍을 정의된 파일 포맷에 따라 생성한 후 CD-ROM과 같은 이동성 저장매체에 담아 인증 센터로 전달한다[5]. 키 파일을 인증 센터로 전달하는 과정에서 기밀성 유지를 위한 별도의 표준이 없으므로, 전달 과정에서 키 파일 저장 매체의 분실 등에 의한 인증용 비밀키 값의 유출 위험이 상존한다.

이처럼 인증용 비밀키 K가 분실되어 ISSI와 K가 모두 복제된 경우 TETRA 표준에서 정의한 인증 프로토콜로는 복제단말기의 망 접속을 막을 수 없게 된다. 다음과 같은 시뮬레이션을 통해 ISSI와 K를 복제한 단말기가 인증을 통과하여 망 접속이 되는 문제점을 확인할 수 있다.

1. 시뮬레이션 환경 설정
- 인증과 무선구간 암호가 지원되는 3대의 단말기 A, B, C의 전원을 끈 상태로 둔다.
- 단말기 A는 ISSI_A 및 K_A로 프로그래밍 하고, 단말기 B는 ISSI_B 및 K_B로 프로그래밍 한다.
- 단말기 C에는 단말기 A의 ISSI_A와 K_A를 프로그래밍하여 A의 복제단말기로 만든다.

2. 시뮬레이션
- 단말기 A와 B를 켜고 사이트 1에 정상적으로 등록됨을 확인한다.
- 단말기 프로토콜 분석기를 통해 단말기 A와 B 모두 (그림 5)의 U-LOCATION UPDATE ACCEPT 메시지를 수신하였음을 확인한다. 이것은 단말기가 정상적으로 인증되었으며, 그 결과로 단말기 A와 B가 각각 별개의 DCK를 생성했다는 것을 의미한다. 단말기 A의 현재 생성된 DCK를 DCK_A_1이라고 한다.
- 단말기 A에서 그룹호를 발신한다. 단말기 B가 암호화된 그룹호를 수신함을 확인한다. 단말기 B에서 그룹호를 발신한다. 단말기 A가 암호화된 그룹호를 수신함을 확인한다. 이것은 두 단말기 모두 DCK 및 CCK 키를 이용한 그룹 통신이 가능함을 나타낸다.
- 단말기 A를 사이트 2로 로밍시킨다. 단말기 A는 임목적으로 인증된다. 교환기는 DCK_A_1을 사이트 2로 재공하고 사이트 1에서 DCK_A_1을 제거한다.
- 단말기 A에서 그룹호를 발신한다. 단말기 B가 암호화된 그룹호를 수신함을 확인한다. 단말기 B에서 그룹호를 발신한다. 단말기 A가 암호화된 그룹호를 수신함을 확인한다.
- 복제단말기 C를 켜고 사이트 1에 등록시킨다. 단말기 A의 ISSI와 K를 모두 복제한 단말기 C는 단말기 A와 동일한 것으로 교환기에게 인식되고, 따라서 교환기는 복제단말기 C를 정식적으로 인증한다. 이제 단말기 C는 DCK_A_2를 갖는다. 교환기는 사이트 2에서 DCK_A_1을 제거한다.(단말기 A는 여전히 DCK_A_1을 갖고 있다.)
- 복제단말기 C에서 그룹호를 발신한다. 단말기 B가 암호화된 그룹호를 수신함을 확인한다. 단말기 B에서 그룹호를 발신한다. 복제단말기 C가 암호화된 그룹호를 수신함을 확인한다. 이것은 복제된 단말기가 인증을 통과하여 정상단말기 A인 것처럼 완벽히 사용되는 것을 막을 수 없음을 보여준다.

Ⅳ. 복제단말기의 망 접속을 막기 위한 새로운 인증 프로토콜 제안

앞서 살펴본 바와 같이 ISSI와 K가 모두 복제된 복제단말기의 불법 사용은 현재의 TETRA 표준 인증 프로토콜로는 막을 수 없는 심각한 문제점이 있다. 이러한 문제의 근본적인 원인은 단말기 인증 과정에서 단말기 식별자로 사용되는 일련 번호인 REF값은 망으로 전달되지 않고 ISSI만 전달되므로 - 그림 7의 위치 업데이트 요구 메시지 참조 - 망에서는 ISSI와 K와의 연관성만을 확인하기 때문에 ISSI와 K가 모두 복제된 단말기는 망에서 인지할 수가 없다. 따라서 본 논문에서는 이러한 문제점을 해결하기 위해 그림 8과 같은 새로운 인증 방식을 제시한다.

제안하는 프로토콜은 기존 인증 과정에서는 참조하지 않던 REF를 사용한다. 기존 프로토콜에서 사용하던 80비트 인증용 세션키 KS 대신에 새로운 KS_new를 다음과 같이 생성한다.

해수 함수 SHA1의 입력값으로 KS, REF를 적용한다.

SHA1 출력인 160비트 해쉬값 H의 MSB부터 80비트만 취하는 함수인 T를 적용하여 KS_new를 구한다.

KS 대신에 KS_new를 기존 인증 알고리즘인 TA12의 입력값으로 사용한다.

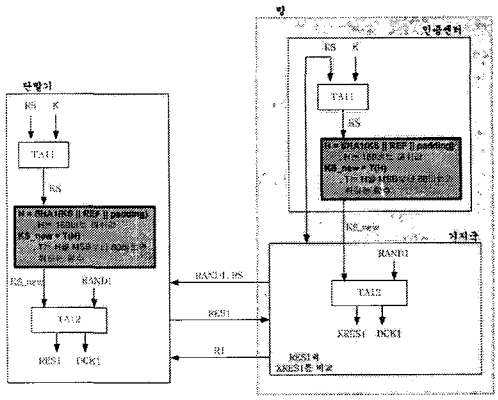


그림 8. 인증키를 복제한 단말기의 불법 접속을 막는 새로운 프로토콜

Fig. 8 New Protocol to prevent clone radio from accessing network

REF는 단말기 제조사에서 생성하여 단말기 출하시부터 영구 보안 식별 메모리에 저장되는 값이므로 외부 프로그래밍 장치로 변경이 불가능하다. 따라서 제안하는 프로토콜은 REF를 확인하는 과정을 추가함으로써 ISSI와 인증용 비밀키 K를 복제한 단말기라 하더라도 REF가 틀릴 경우에는 망에서 계산한 XRES1과 동일한 응답값인 RES1을 만들 수 없고 결과적으로 복제단말기는 망에 등록이 허용되지 않는다.

Ⅴ. 결 론

TETRA 표준에서는 인가된 단말기만이 망에 접속하도록 함으로써 복제단말기에 의한 통화 도용 및 신분 위장 등의 위협 요소를 제거하기 위해 인증 서비스를 제공한다. 그러나 단말기에 주입한 인증용 비밀키 K를 인증 센터로 전달하는 과정에서 키가 노출될 위험이 존재하며 이로 인해 ISSI와 인증키가 모두 복제된 단말기는 망이 인지할 수 없는 프로토콜상의 취약점이 존재한다. 본 논문에서는 TETRA 표준 인증 프로토콜과 인증키의 생성/분배/주입 모델을 설명한 후, 인증키 K의 노출로 인한 복제단말기의 불법 사용은 현재의 TETRA 표준 인증 프로토콜로는 막을 수 없음을 시뮬레이션을 통해 확인하였다. 이러한 문제점을 개선하기 위해 ISSI와 인증키가 복제된 단말기의 등록을 허용하지 않을 목적으로 인증 과정에서 REF를 적용하는 새로운 인증 프로토콜을 제안하였다. 본

논문에서 제안한 인증 프로토콜은 기존의 인증 프레임 워크를 유지하면서 TETRA 표준에서 정의한 인증 관련 신호 메시지 규격의 수정 없이 인증 센터와 단말기의 간단한 소프트웨어 업그레이드만으로 적용이 가능한 장점이 있다.

참고문헌

[1] 소방방재청, "통합지휘무선통신망 구축 시범사업 시방서", 2005.

[2] ETSI EN 300 392-7 V2.2.1, "Terrestrial Trunked Radio(TETRA); Voice plus Data(V+D); Part 7 : Security", September 2004.

[3] ETSI EN 302 109 V1.1.1, "Terrestrial Trunked Radio(TETRA); Security: Synchronization mechanism for end-to-end encryption", October 2004.

[4] TETRA MoU SFPG Recommendation 02 edition 4, "End-to-End Encryption", October 2004.

[5] TETRA MoU SFPG Recommendation 01 edition 4, "TETRA Key Distribution", February 2006.

저자소개

박 용 석(Park Yong Seok)

1995년 경북대학교 전자공학과(공학사)
1997년 경북대학교 대학원 전자공학과(공학석사)
1997년~1999년 LG전자
2000년~현재 국가보안기술연구소
※ 관심분야 : 이동통신 정보보호

안 재 환(Ahn Jae Hwan)

1999년 성균관대학교 전자공학과(공학사)
2002년 광주과학기술원 정보통신공학과(공학석사)
2002년~2004년 삼성전자
2005년~현재 국가보안기술연구소
※ 관심분야 : 유/무선 통신 보안프로토콜

정 창 호(Jung Chang Ho)

2002년 고려대학교 응용생명환경화학학과(이학사)
2004년 9월 고려대학교 정보보호대학원 정보보호학과 (공학석사)
2005년~현재 국가보안기술연구소
※ 관심분야 : 통신보안, 정보은닉

안 정 철(Ahn Joung Chul)

1996년 동경공업대학(공학박사)
1990년~1999년 ETRI
2000년~현재 국가보안기술연구소
※ 관심분야 : 통신정보보호