# IS-95/cdma2000 이동통신 시스템의 취약성과 개선방안

김건우, 홍도원*

*한국전자통신연구원 암호기술연구팀

# Weakness and its Improvement about IS-95/cdma2000 Mobile Communication System

Keon Woo Kim, Do Won Hong*

*Cryptography Research Team, ETRI

**요 약**

최근 ESN과 IMSI 불법복제에 의해 IS-95/cdma2000 이동통신 서비스 정상가입 사용자와 단말의 피해가 확인되고 있다. 이는 정상 가입자의 요금증가, SMS를 통한 휴대폰 결재, 정상단말의 착발신 장애 등의 문제를 일으키고 있다. 이러한 불법복제 단말의 서비스 접근과 정상단말 신원확인을 위해 이동통신 사업자는 파워온 등록, 착신, 발신시에 인증 메커니즘을 적용하지만, 여전히 CDMA/cdma2000 시스템에는 취약점이 존재하는 것으로 분석되고 이의 대응책이 요구된다. 이에 본 논문에서는 파워온 인증, 발신인증, 착신인증이 도입된 이동통신 시스템에서 정상단말과 불법복제 단말이 동일 기지국내에 위치할 때와 서로다른 기지국에 위치할 때, 각각 불법복제 단말에 의해 발생할 수 있는 취약점과 대응방안을 분석하고자 한다.

## I. 서론

우리나라의 CDMA 이동통신 시스템은 2세대 방식인 IS-95-B/C에서 출발해 3세대 방식인 cdma2000와 패킷 데이터 중심의 CDMA2000 1x EV-DO 시스템이 구축되어 있고 현재 서비스가 제공되고 있다.

이를 인증 보안 관점에서 바라보면, IS-95-B/C와 cdma2000 Rev.B 이전 시스템에서는 CAVE(Cellular Authentication and Voice Encryption) 알고리즘[1,2]을 이용한 인증 보안 서비스를 적용하고, cdma2000 Rev.C 이후에서는 CAVE 적용방법과 강화된 가입자 인증방법인 ESA(Enhanced Subscriber Algorithm)[3,4]를 병행해서 사용한다. 하지만, 우리나라 모든 지역에 cdma2000 Rev.C가 구축된것은 아니어서 이동통신 사업자는 CAVE를 이용한 인증보안 서비스를 제공하리라 보여진다. 한편, CDMA2000 1x EV-DO에서는 IS-95 방식과는 달리 무선 인터페이스 계층 구조에 따로 분리된 보안 계층을 이용해서 인증과 암호화 서비스를 제공하는데,[6] 아직 표준화가 완료된 것이 아니기 때문에 사업자가 인증 보안 표준 규격을 적용하지 않았으리라 예상된다.

인증은 기존의 음성 호 처리와는 별도로 수행되므로 시스템의 부하가 증가될수 있다. 이런 이유로 사업자가 인증 서비스 도입을 주저하게 되는 이유가 되기도 한다. 하지만, 최근에는 불법복제 단말기가 음성적으로 유통되고 SMS를 이용한 모바일 결재 등의 휴대폰 불법복제에 의한 피해가 확산되고 있기 때문에, 이런 피해를 최소화하는 하나의 방법으로 인증 서비스 도입이 필요하다. 또한, 인증보안 서비스 적용시 발생가능한 취약점을 분석하고, 그 대응책을 서둘러 시스템에 적용하는 것이 요구된다.

본 논문에서는 보편적으로 사용되는 IS-95/cdma2000 인증에 관한 기술중 CAVE 알고리즘, 각 호에 대한 인증 메커니즘 및 인증서명값 생성, 그리고, VPM(Voice Privacy Mask)

과 CMEA(Cellular Message Encryption Algorithm) 키 생성 등에 관해서는 이미 널리 알려진 사실이기 때문에 자세히 언급하지 않는다. 그래서, 2장은 기본적인 CAVE 인증보안에 관해서 설명하고, SMS에 관해서도 인증보안에 관해 간단히 언급한다. 3장에서는 정상단말과 불법복제 단말이 서로 다른 기지국에 위치하는 경우, 불법복제 단말에 의한 IS-95/cdma2000 이동통신의 취약성을 분석하고 대응책을 제시한다. 마찬가지로 4장에서는 정상단말과 불법복제 단말이 동일한 기지국, 동일한 섹터 내에 위치하는 경우, 불법복제 단말에 의한 IS-95/cdma2000 시스템의 취약성과 대응책을 분석한다. 마지막으로, 5장에서 결론을 내린다.

## II. IS-95/cdma2000 인증 보안 개요

IS-95/cdma2000 이동통신에서의 인증은 단말기를 식별하기 위하여 시스템의 HLR 및 AC에 저장된 가입자 정보와 단말기가 가지고 있는 정보가 일치하는지를 확인하는 절차이다. 인증은 challenge-response 방식으로 등록, 착호, 발호시 단말을 인증하는 Global challenge 방식과 Global challenge 실패의 경우 인증 정책에 따라 SSD(Shared Secret Data) 갱신이나 Unique challenge 등의 인증 보조 절차를 수행한다.

IS-95/cdma2000에서의 인증은 가입자의 발신호나 착신호마다 수행하거나 선택적으로 수행될 수 있다. 인증은 기본적으로 인증알고리즘을 이용하여 수행되며, 보완적으로 호발생시마다 호의 횟수를 이용하는 Count를 관리하여 부가적으로 사용한다. 인증시 RAND, AUTHR 비교는 인증 메커니즘에서 반드시 수행해야 하나, 표준 규격상 Count 비교는 강제사항은 아니다. 이러한 Count 관리는 복제 단말 출현시 복제 단말기 서비스 방지를 하는 중요한 역할을 하기도 한다. [1]

CAVE 알고리즘, 인증서명값 생성, 음성 및 시그널링 메시지 암호화 키 생성에 관해서는 3GPP2의 Common Cryptographic Algorithms 규격[2], Common Security Algorithms 규격[3], 그리고, Enhanced Cryptographic Algorithms 규격[4]을 참고한다.

등록시 단말기는 서비스 지역, 단말기 상태, 단말기 번호, slot cycle 등의 파라미터를 기지국으로 송출하고, 시스템에서는 항상 단말기가 현재 서비스 받고 있는 지역을 인지하고 있어야 하므로 지역을 이동하거나 환경이 변경되면 단말기 등록을 시행해야 한다. 등록기능으로는 Power On Registration, Power Off Registration, Timer Based Registration, Distance Based Registration, Zone Based Registration, Parameter Change Registration, Order Registration, Implicit Registration, Traffic Channel Registration, 그리고, User Zone Registration 이 있다. 이들 각각에 관해서는 [1]에 상세히 기술되어 있다.

등록인증, 그리고 착발신 인증 과정에서 시스템은 RANDC, AUTHR, Count 비교를 통해 인증성공 여부를 판단하고, 결과에 따라 트래픽 채널을 할당하고 Parameter Update를 하거나, 호 거부 또는 SSD 갱신 과정을 선택할수 있다.

한편, SMS/data burst message 인증 및 보안에 관해서 Access 채널에는 인증과 관련된 정보를 담고 있는 필드를 포함하고 Paging 채널에는 인증과 관련된 정보를 담고 있는 필드를 포함하지 않는다.[5] 길이가 짧은 SMS는 Paging이나 Access 채널로, 길이가 긴 경우는 service option을 설정해서 열린 Traffic 채널을 통해서 전송된다. 하지만, SMS 길이에 관계없이 Traffic 채널에서 전송될 수도 있는데, 만약 사업자가 SMS 착발신에 대해서 인증 서비스를 제공한다면 Traffic 채널을 이용하는 것이다.

또한, traffic 채널 data burst message의 ENCRYPTION 필드로 암호화 모드 설정이 가능하므로, SMS에도 VPM 키 등을 이용한 암호화를 적용할수 있다.

## III. 서로다른 기지국에 위치할 때의 취약성 및 해결방안

최근 ESN(Electronic Serial Number) 조회, 복제 프로그램에 의한 ESN, IMSI(International Mobile Subscriber Module) 불법복제 단말의 피해사례가 보고되고 있다. 이에 3장에서는 파

워온 인증, 발신인증, 착신인증이 적용되고, 정상단말과 복제단말 2개의 단말이 서로 다른 기지국에 있다고 가정할 때, 불법복제 단말에 의해 발생할 수 있는 취약점과 대응방안을 분석하고자 한다. 이때, 개인키인 A_Key는 접근이 어려운 메모리 공간에 저장되어 복제되지 않는다고 가정한다.

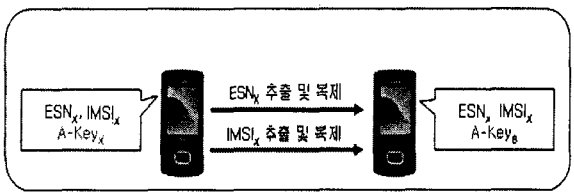


그림 1. ESN, IMSI 복제

하지만, RUIM(Removable User Identity Module)과 같은 스마트카드를 도입하지 않는다면 ESN 복제처럼 A_Key도 불법복제될 개연성은 있다고 보여진다.

IS-95-B/C를 비롯한 cdma2000 등의 CDMA 시스템은 Implicit 등록을 허락한다. 즉, 단말이 IMSI와 ESN을 전송함으로서 시스템에 등록하는데, 단말 부팅후 파워온 인증을 수행하기 전에 긴급호 발신을 시도하면 IMSI와 ESN 전송만으로도 암시적인 등록이 되어서 호가 연결되고 파워온 인증은 무력화 된다.

한편, 이동통신 사업자는 불법복제 단말의 정당한 인증서명값 생성을 불가능하게 함으로서 서비스 이용을 차단한다. 이를 위해 파워온 인증과, 발신인증, 착신인증을 적용한다. 하지만, 이들 세가지 인증만 시행할 때 다음과 같은 문제점이 발생 가능하다.

### 3.1 취약성 분석

Implicit 등록으로 불법복제 단말은 착발신은 불가능하지만 등록 자체는 가능하다. 정상단말의 위치정보가 가장 최근에 등록된 복제단말의 위치정보로 변경되었을때, 기지국 및 교환국 시스템은 정상단말의 위치를 찾지 못하고 복제단말의 위치를 위치등록기에 등록하는 문제점이 발생한다.

이때 복제단말은 정상적인 착발신 인증을 수행하지 못하므로 서비스를 이용할 수는 없다. 하지만, 정상단말조차 위치 등록이 되지 않으므로 서비스를 이용할 수 없게 된다. 이런경우 정상단말을 재부팅하거나 사용자에 의한 민원요청으로 해결될수 있으나, 복제단말 역시 재부팅으로 정상단말의 위치를 잃어버리게 할 수 있다.

### 3.2 해결방안

위에서 제기된 취약성을 해결하기 위해서는 10가지 등록 기능 중 현재 제공하는 파워온 등록인증 외의 다음 2가지 등록기능에 인증 메커니즘을 도입할 필요가 있다.

- Zone Based Registration

Zone Based Registration 인증을 수행함으로써 복제단말의 위치 등록으로 인한 정상 단말의 위치등록 변경을 방지하도록 한다.

- Timer Based Registration

Zone Based Registration 인증기능이 없는 경우, Timer Based Registration 인증을 수행함으로써 변경되어있던 정상단말의 위치정보를 원래의 정보로 다시 갱신하고 추후 복제단말의 Timer Based Registration 인증을 실패하게 함으로서 위치정보 변경을 불가능하게 한다.

## IV. 동일 기지국에 위치할 때의 취약성 분석

4장에서는 파워온 인증, 발신인증, 착신인증이 적용되고 정상단말과 복제단말이 동일한 기지국, 동일한 섹터 내에 존재하는 경우, 불법복제 단말에 의해서 발생가능한 문제점을 분석한다.

### 4.1 단말의 발신시도 시

동일 기지국, 동일 섹터 내의 환경에서 복제단말의 정상적인 등록, 착신, 발신은 근본적으로 불가능하다. 하지만, 긴급호 통화를 이용한 Implicit 등록으로 등록 인증과정을 수행하지 않고 시스템 등록이 가능하다.

- 정상단말의 발신 시도

정상단말은 정상적으로 발신인증 성공하고

Channel Assignment Message를 수신한 후 SA 상태에서 traffic 상태로 전환한다. 한편, 복제단말은 정상단말과 마찬가지로 Channel Assignment Message를 수신할 수는 있으나 idle 상태에서 Channel Assignment Message를 수신하였으므로 상태오류로 인해 기지국으로 Reject Order를 송신하게 되고 기지국은 Call Release 한다. 이때 정상단말의 발신처리가 정상적으로 되지 않을 수 있다.

결과적으로 복제단말에 의한 발신은 이루어질수 없으나, 복제단말로 인해 정상단말의 발신이 안될수도 있다. 이는 이론적인 가능성을 제시한 것으로 실제 동일 기지국내에서 확인이 필요하나 복제단말 제작 자체가 불법이기 때문에 현실적으로 확인이 매우 어렵다.

● 복제단말의 발신 시도

복제단말이 발신을 시도하면 발신인증 실패로 인해 기지국으로부터 새로운 인증요구를 정상단말과 복제단말 둘다 수신하게 된다. 이는 정상단말 조차 시스템 재부팅, 사용자 요구 등에 의해 새로운 인증과정을 거쳐야만 정상 사용가능 상태가 됨을 의미한다.

따라서, Implicit 등록 이후라도 가능한 짧은 시간내에 정상 등록인증 절차를 시행해야지만 복제단말에 의한 피해를 방지할수 있다.

4.2 단말의 착신시도 시

4.1절과 마찬가지로 복제단말은 Implicit 등록을 시도한다.

● 정상단말의 착신 시도

파워온 인증과 착신 인증이 도입된 상태에서 기지국이 착호 Paging 신호를 보냈을때 정상단말이 먼저 Page Message를 수신하면 정상단말은 착신인증 성공하고 기지국에게 Page Response Message를 송신한다.

이때 정상단말이 성공적인 인증 처리후 먼저 발신자와 통화하고 복제단말이 그 다음에 수신을 시도하면, 시스템은 하나의 ESN과 IMSI에 대한 인증이 성공한 것으로 판단하여 복제단말도 발신자와 통화가 가능한 상태가 될 수 있다. 즉, 두 단말 모두 발신자와 통화가능한 보안상의 매우 심각한 문제가 발생한다.

SMS의 경우도 마찬가지이다. 정상단말이 먼저 SMS 착신 인증에 성공하면 두개의 단말 모두다 동일한 SMS 수신이 가능하게 되어 개인정보노출이라는 심각한 결과를 초래하게 된다.

● 복제단말의 착신 시도

전파환경이나 RF 수신능력우월 등의 이유로 복제단말이 정상단말보다 착신을 먼저 시도하는 경우, 복제단말은 Page Message를 수신하지만 착신인증 실패하여 복제단말에서 보낸 메시지는 비정상 처리되며 기지국에서는 이를 오류로 인식하여 착호 처리를 중단한다. 그러면, 복제단말뿐 아니라 정상단말조차 기지국으로부터의 새로운 인증요구에 때문에 단말을 재부팅하기 전까지 서비스 불가능 상태가 될 수 있다.

SMS의 경우도 마찬가지이다. 복제단말이 먼저 SMS 착신 인증을 시도하면 두개의 단말 모두다 새로운 인증요구 절차를 요구받게 된다.

결과적으로 복제단말에 의한 착신과 SMS 수신은 이루어질수 없으나, 복제단말로 인해 정상단말 조차 착신과 SMS 수신이 불가능해 질수도 있다.

이런 문제들은 ESN과 IMSI로 단말을 시스템에 등록하는 CDMA 시스템 특징으로써 복제단말의 Implicit 등록후 발생한다. 따라서, 복제단말로 인한 최소한의 피해를 예방하기 위해서는 Implicit 등록후 짧은 시간내에 정상 등록인증 절차를 수행하여야 한다.

## V. 결 론

본 논문에서는 두가지 상황의 기지국 환경에서 ESN과 IMSI 불법복제에 의한 정상가입 단말의 피해 가능성과 대응책을 살펴보았다.

하지만, 보안을 위한 보다 더 근본적인 대책은 불법복제 자체를 불가능하게 하는 것이다. ESN과 IMSI를 단말에 저장하는한 아무리 접근이 어려운 메모리 영역에 저장하더라도 결국에는 제 3자에 의한 메모리 읽기/쓰기는 가능하게 된다. 뿐만아니라, 인증 메커니즘의 비밀키인 A_Key 복제와 저장은 더욱 심각한 문제이다. 이는 WCDMA 서비스에서 USIM을 도입하는 것처럼, IS-95/cdma2000 서비스에도 RUIM과 같은 스마트카드를 도입하여야 가능하다.

RUIM 도입으로 인증보안 뿐만 아니라 글로벌 로밍, 부가 서비스 제공 관점에서도 많은 장점이 있다. 하지만, 지금까지 보급된 IS-95, cdma2000 시스템 단말과의 호환성, 시스템 성능향상, 카드 발급 및 관리 등의 현실적인 문제가 있어 보다 심도깊은 검토가 요구된다.

## [참고문헌]

[1] TIA-95-B, TIA, Mobile Station-Base Station Compatibility Standard for Wideband Spread Spectrum Cellular Systems, Oct. 2004

[2] 3GPP2 S.S0053, Common Cryptographic Algorithms, Jan. 2002

[3] 3GPP2 S.S0078, Common Security Algorithms, Sep. 2005

[4] 3GPP2 S.S0055, Enhanced Cryptographic Algorithms, Sep. 2005

[5] 3GPP2 C.S0015, Short Message Service

[6] 3GPP2 C.S0039, Enhanced Subscriber Privacy for cdma2000 High Rate Packet Data, Sep. 2002