모바일 네트워크 보안 취약점과 방안

지도교수 : 이 강 호
연 구 자 : 이 승 표

< 목 차 >

요 약

스마트폰은 기존 2G를 사용하는 피처폰의 전화 또는 메시지의 기능을 넘어서 SNS, 네비게이션 등 개인 또는 기업의 편의성을 증대시키며 하나의 소규모 컴퓨터 또는 손안의 PC로 불리면서 점점 발전해 나가고 있다. 그에 따라 통신 기술도 나날이 발전해 나가고 있으며, 이에 따라 개인과 기업에서의 활용도가 높아지면서 이동통신의 취약점에 대한 보안은 항상 이슈가 되고 있다. 기본적으로 스마트폰 무선 통신에는 무선 랜(Wi-Fi)기능으로 무선인터넷 접속이 가능하며 이동통신 기술은 3G부터 근래에는 5G까지의 무선 네트워크 통신망이 탑재 되었으며, 스마트폰이라는 제한된 범위를 넘어서 냉장고, 에어컨과 같은 사물에 통신 기술을 탑재한 IoT가 나오면서 무선 네트워크 통신의 중요성을 더해져 가고 있다.
무선 네트워크 통신의 활용이 늘어감에 따른 취약점도 종류와 범위가 증가하고 있다. 이 논문에서는 각 통신별 취약점과 그에 따른 대응 방안을 알아보았다.

주요어 : IMT-2000, WCDMA, LTE, CN, DDoS,

1. 서론

1.1 무선 네트워크(Wireless NetWork)

스마트폰 무선 네트워크에는 3G, 4G 그리고 최근 나오기 시작한 5G가 있다. 기존의 스마트폰 이전에 사용되었던 피처폰 들은 2세대 이동통신 서비스 즉 2G를 사용했었는데, 2003년부터 보급되기 시작하였으나, 스마트폰이 본격적으로 보급되기 시작한 2011년부터 전화와 문자뿐 아니라 영상통화나 인터넷 등 멀티미디어 통신이 가능한 통신규격인 3세대 이동통신 즉 3G가 주로 사용되기 시작했다.

3G네트워크는 3GPP(3rd Generation Partnership Project)라는 표준화 기구에서 제정한 UMTS (Universal Mobile Telecommunication System) 표준안을 따르는 네트워크로 G는 세대(generation)를 지칭하며, 숫자는 모바일 네트워크의 발전 단계를 나타낸다. 비동기식인 WCDMA(광대역 부호분할 다중접속, Wideband Code Division Multiple Access), 동기식인 IMT-2000(International Mobile Telecommunication-2000)이 있다.

4G는 3G 계열의 뒤를 이은 이동통신 규격으로 IMT-Advanced 규격에 의해 규정되어 있다. 100 + MiB/s와 같은 초광대역 속도의 인터넷 속도, IP 전화, 게임 등 스트리밍 멀티미디어 기능이 사용자에게 제공되며, 고속 이동 중 100Mbps가 지원 되고, 정지 상태에서 1Gbps 지원, 그리고 인터넷 프로토콜과 호환이 되어야한다는 인증 조건이 있다.

5G는 2018년부터 채용된 5세대 이동 통신 정식명칭은 IMT-2020으로 6GHz 이하 주파수 대역인 Sub-6와 초고속 근거리망에 쓰이는 mmWave로 나누어져 있는데, 국내 일반 소비자들에게는 Sub-6만 서비스 되고 있으며, 밀리미터파(mmWave)는 기업용으로만 보급되고 있다. 스마트폰과 같은 제한된 통신 장비를 넘어서 인공지능과 주변 차와 실시간 통신을 하며 주행을 하는 자율주행차 개발이 이루어지고 있으며, VR을 이용한 가상현실. IoT를 이용하여 더 많은 통신기기를 통신망에 접속시킬 수 있는 등 광범위하게 개발 중에 있다.

1.2 무선 랜(Wi-Fi)

무선 랜(Wi-Fi)는 무선 통신 표준 기술 중 하나인 IEEE 802.11에 기반을 둔 서로 다른 장치들 간의 데이터 전송 규약으로 사용하기 위해서는 무선 인터넷 공유기가 필요하다.

표준만 준수하면 스마트폰, 태블릿 컴퓨터, 노트북 등 어떤 장치에도 사용 가능하며, 최신 백색 가전도 Wi-Fi를 지원하고 있다. 2010년 이후 부터는 드론과 같은 무선 조종 컨트롤러에도 쓰이고 있다.

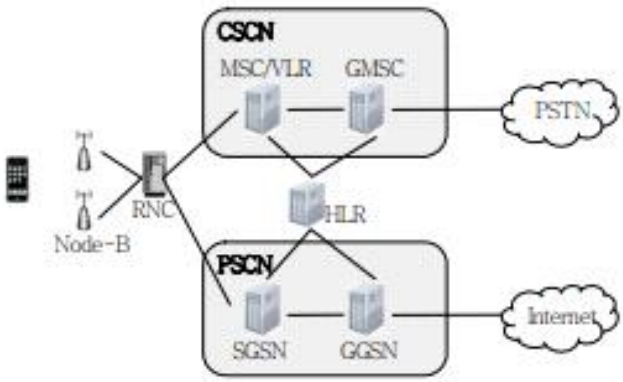
기본적으로 Access Point(Hot Spot)에 기반을 둔 일대다 통신 방식을 사용하며, 연결 장비가 증가하면 전송 속도는 그만큼 느려지게 된다. 근거리 통신을 전제로 제정된 규약이기 때문에 범위가 최대 200m 정도이며, 802.11r이라는 규격을 이용하여 이동 중에도 Wi-Fi를 사용할 수 있다.

2. 무선 네트워크 취약점

한국에서는 대표적인 3G 네트워크로 WCDMA와 EV-DO Rev.A를 사용하고 있다. 먼저 WCDMA 일반적으로 거론되는 TDMA, FDMA, CDMA중에서 기본적으로 각각 사용자가 이용하는 주파수 상의 데이터를 encoding하여 구분 CDMA 방식을 채용하며, 부분적으로 한정된 주파수 자원을 주파수대별로 쪼개서 각각의 사용자들에게 주파수 별로 동시에 쓸 수 있도록 나누어 주는 FDMA와 정해진 시간만큼만 각각의 사용자들이 한정된 전파 자원을 독점해 쓰는 TDMA 방식을 차용하고 있다.

WCDMA는 크게 TDD(Time Division Duplex)와 FDD(Frequency Division Duplex)로 나눌 수 있는데 TDD방식은 CDMA방식에 주파수로 사용자들을 구분하고, TDMA와 같이 통신 자원 사용 시간으로 사용자들을 구분한다. 즉 하나의 주파수에서 데이터를 올리고 받는 일을 같이 처리하는 것이다.

FDD는 코드와 주파수를 기반으로 자원을 분배하는 것은 같지만 통신 자원 사용 시간으로 사용자들을 구분하지 않으며, 데이터를 올리고 받는 일을 주파수 별로 나누어 처리한다.



[사진 1] 단순화된 이동통신 WCDMA 구조도

WCDMA는 NTT DOCOMO에 의해 개발된 3G 네트워크 기술로 <사진 1>에 따르면 무선 접속 네트워크인 Node-B에서 RNC 구간, 코어 네트워크인 SSGN에서 GGSN 구간으로 구성 된다.

코어 네트워크인 CN은 음성 서비스를 위한 Circuit Switched 코어 네트워크(CSCN)와 데이터 서비스를 위한 Packet Switched 코어 네트워크(PSCN)로 나누어지는데, 4G에서의 LTE에서는 하나의 통합된 코어 네트워크를 가지게 된다. 인터넷에서 이동통신 네트워크로 접속을 제공하는 문제 메시지 서비스는 데이터 서비스의 일종이나 CSCN을 통해 제공되고, 그 이후 모든 데이터 서비스는 PSCN을 통해 제공된다.

Node-B는 이동 단말과 이동통신 네트워크를 연결 해주는 Entity로서, 무선 접속 기능을 담당하며 이외의 기능은 최소화되어 RNC에 의해 제어된다.

RNC는 UMTS 무선접속 네트워크의 핵심 Entity로서 Node-B를 제어하고, 무선 리소스 관리, 이동성 관리 등의 기능을 제공한다. 또한, RNC는 이동 단말에서 또는 이동 단말로 데이터를 전송할 경우 암호화되는 포인트이다.

SGSN은 특정 지역 내에서 패킷 데이터의 전송을 담당하는 Entity로서 패킷 라우팅, 데이터 통신을 위한 이동성 관리, 인증 및 과금 관리 등의 기능을 담당한다.

MSC는 음성서비스를 제공하기 위한 서버로서 통화제어, 단말기의 이동성 확보 등의 기능을 제공한다. HLR은 가입자 정보를 관리하는 서버를 말한다. VLR은 VLR 영역 내에 현재 위치한 MS로부터의 요청을 처리하기 위한 정보 등을 제공한다.

WCDMA의 보안 구성은 기본적으로 GSM의 보안 구성을 토대로 구성되어 있으며, GSM 보안의 문제점들을 수정했다. 기본적으로 단말기와 네트워크 간의 상호 인증을 제공하고, 강한 암호화와 무결성 알고리즘을 위한 키 길이가 64비트에서 128비트로 증가 되었으며, 네트워크 구조의 변화를 고려하여 3G에 의해 제공되는 새로운 서비스에 필요한 보안을 제공한다.

GSM에는 네트워크에게 사용자 인증만 제공하고 암호 키들이 네트워크 내에서 평문으로 전달되고, 무결성 알고리즘이 제공되지 않는 문제점이 있었다. 그래서 WCDMA에서 네트워크와 사용자가 서로를 상호 인증하고 무결성 알고리즘에 의해 데이터 무결성이 보장되며, 네트워크 내 그리고 네트워크 사이에 보안이 제공되게 되었다.

WCDMA 보안은 네트워크 접근 보호(Network access security), 네트워크 영역 보호(Provider domain security), 사용자 영역 보호(User domain security), 응용 영역 보호(Application security)로 구성된다.

네트워크 접근 보호는 사용자의 신분 비밀성으로 사용자 위치 추적이 불가능하며, 임시 ID에 의해 신분 확인 또는 방문망이 변경될 때마다 임시 ID의 재할당이 필요하고, 사용자 신분 정보에 관련된 모든 데이터에는 암호화가 필요하다. 사용자와 네트워크에는 인증이 필요하고, 기밀성으로 인증과 키가 일치하는 메커니즘이 필요하며, 무결성으로 데이터 무결성과 데이터 출처가 인증되어야 한다.

네트워크 영역에서는 전송 프로토콜로 IP가 사용되는 경우는 IPSEC으로서 네트워크 계층에서 보호하며, SS7(Signaling System No.7) 기반 전송이 사용되는 네트워크들 사이에서는 응용 계층에서 보호한다. 데이터 무결성 및 출처 확인, 비밀성 제공 등이 필요하다.

사용자 영역에서는 사용자와 USIM 사이의 인증이 필요하다. PIN과 같은 공유 비밀 데이터를 이용하며, USIM과 단말기 사이의 안전하게 저장된 비밀 데이터를 공유한다.

응용 영역에서는 응용 서비스에서 전송되는 메시지를 보호하며, 개체 인증 데이터 무결성 및 출처 인증이 있다.

3G의 대표적인 취약점 공격으로는 애플리케이션 서버 또는 서버군에 대량을 패킷을 전송하여 일반 사용자들에게 서비스 거부를 일으키는 DDOS공격이 있는데, DNS와 같은 네트워크 서비스 엔티티를 공격하는 경우는 드물지만, 이동통신 네트워크에 대한 DDOS 공격은 특정 서버를 대상으로 한 것이 아니라 전체 네트워크 서비스를 대상으로 하기 때문에 공격 방법이 다양하다.

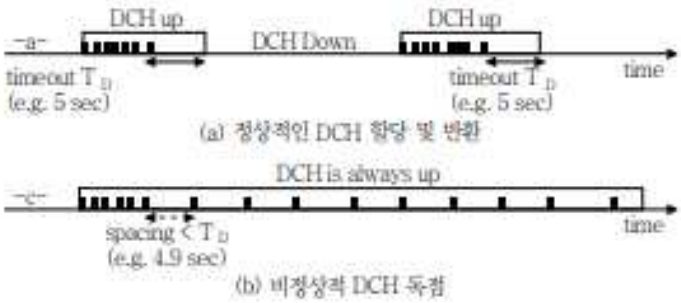
또한, 인터넷 DDOS공격은 수백 Gbps의 트래픽이 사용되지만, 이동 통신 네트워크는 수십 kbps에서 수백 Mbps 정도의 트래픽으로도 공격이 가능하다. 이동 통신 네트워크에 대한 공격은 공격의 대상이 되는 리소스에 따라 네트워크 제어계 공격(Control Plane Attack), 자원 고갈형 공격(Low-rate Flooding Attack), 간접 공격(Indirect Attack)으로 구분할 수 있다.

네트워크 제어계 공격은 공격 트래픽을 이용하여 대상 호스트나 네트워크 자원을 직접 공격하기보다 네트워크 운영을 위한 오버헤드를 증가시켜 서비스 거부를 일으키는 공격 기술이다.

자원 고갈형 공격에는 문자 메시지 공격과, Paging 채널 공격, 데이터 채널 공격으로 나눌 수 있는데, 문자 메시지 공격은 소량의 메시지 전송(SDDCH)의 포화를 위해 초당 360개의 메시지를 수집된 피해자에게 전송함으로써 대도시의 이동통신 네트워크를 마비시킬 수 있다.

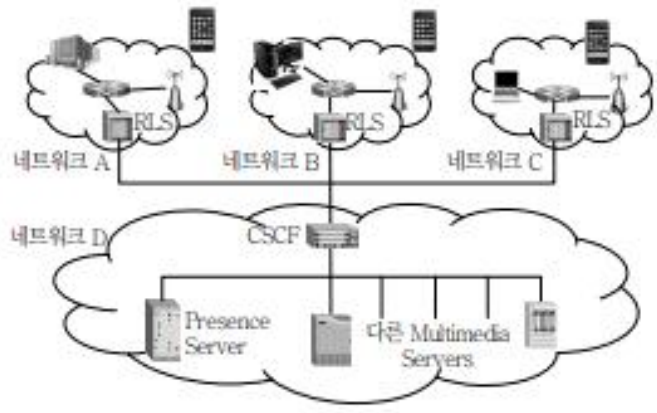
이는 하나의 단말기에 약 10초당 1개의 문자 메시지를 전송하는 공격량으로 인터넷을 대상으로 하는 일반적은 DDOS 기술로는 탐지가 어렵다.

Paging 채널 공격은 이동 단말이 상태를 변화시킬 때 paging 채널을 이용하며, 최소 크기의 UDP 패킷을 주기적으로 전송하여 paging 채널을 고갈 시켜 정상적인 사용자에게 서비스 거부를 일으키게 한다.



[사진 2] DCH/FACH의 채널 할당 비교

데이터 채널 공격은 고속 전송을 지원하는 DCH와 소량의 데이터 전송에 사용되는 FACH간의 채널 할당 및 전환을 이용한 공격으로 최소 모니터링 윈도 동안 전송되는 데이터의 양과 미리 설정된 임계값에 따라 결정되는 FACH에서 DCH 채널의 전환과 반대로 타임아웃 값에 따라 결정되는 DCH에서 FACH 채널로의 전환에서 공격자는 DCH의 효율적인 고갈을 위해 설정된 임계값보다 조금 큰 데이터를 전송하여 DCH를 할당 받고, DCH를 반환하기 직전에 소량을 데이터를 전송함으로써 지속적으로 채널을 사용하는 공격을 한다.



[사진 3] RLS, CSCF, Presence 서버의 연결 구조

간접 공격은 presence service을 기반으로 presence 교환을 위한 RLS(Resource List Server) 방식에서 IMS(Internet Multimedia Subsystem) 서비스 사용자는 다른 사용자의 상태를 확인하기 위해 각각의 사용자와 presence 메시지를 교환하고 RLS에 접속하며 대부분의 IMS에서는 과금과 라우팅을 지원하기 위해 각 RLS들과 CSCF(Call Session Control Function)이 사용된다. 여기서 공격자는 RLS와 CSCF간의 구조적인 문제를 이용하여, 다수의 좀비PC로 RLS에 접속하여,

이용자의 presence 서버에 상태 확인 요청을 하고 그에 의해 정상적인 서비스가 어려워지면서 일반 사용자는 서비스 거부를 경험하게 된다.

presence 서버에 지연이 발생하면, 대다수의 정상적인 사용자들은 재전송 메시지를 보내는데 갑자기 증가하는 재전송요청은 CSCF에 폭주하게 되며, CSCF를 사용하는 다른 서버들의 요청에 서비스 거부를 일으킨다.

예를 들면 1000만 명 이상 사용하는 SNS에 DDOS 공격을 하면 해당 SNS 서버는 서비스 거부를 일으키고 그 서버를 사용하는 단말은 지속적으로 재전송 요청을 하게 되며, 이 요청은 이동 통신 네트워크의 control 채널을 고갈시킬 수 있다.

4G 네트워크에 임프포지티(IMP4GT)라는 새로운 공격 방법이 발견되었는데, 이는 IMPersonation attacks in 4G NeTworks의 줄인 말로, 모바일 기기와 네트워크 간 상호 인증 방법이 보안 측면에서 안정적이지 않다는 것을 입증하고 있다.

현재 LTE망에서의 인증은 제어 영역에서 이루어지지만 사용자 영역에서는 무결성 보호 기능이 없기 때문인데, 이 특성을 활용하는 것이 임프포지티 공격의 핵심이 된다. 이 공격을 성공하게 되면 특정 네트워크 내에서 정상적으로 사용자인 것처럼 위장할 수 있으며, 특정 사용자에게 사용자가 가입한 네트워크 등으로 위장에 접근 할 수도 있게 되며, IP스택 모바일 운영 시스템에 내재된 반사 원리를 남용하여 암호화/복호화 오라클을 구축하고 임의의 패킷을 주입할 수도 있게 된다.

이 공격은 통신사와 사용자 모두에게 영향을 끼칠 수 있는데, 통신사는 사용자로부터 오는 IP 연결 시도를 신뢰할 수 없게 되며, 사용자는 자신이 연결한 LTE망에 대해 신뢰할 수 없게 된다. 잘못된 망 사용 요금이 청구될 수도 있고, 데이터 소진이 빨라지는 일이 생길 수 있다.

또한 사법 기관 수사에도 공격자가 피해자인 것처럼 망에 접속한 후에 경찰이 다른 사람을 추적하도록 할 수도 있다. 이를 위해서는 피해자와 물리적으로 가까운 위치에 있어야 하며, 특수한 하드웨어 장치가 필요하다. 그리고 이는 사용자 영역의 데이터에 다한 무결성 확인 장치 삽입이면 문제 해결이 가능한데, 이는 전송되어야 할 데이터의 양이 추가되면서 통신사들의 비용 부담이 커지게 되는 일이 발생할 수 있다.

5G의 모바일 트래픽은 사용자 단말로부터 무선 엑세스 네트워크와 이동성 관리, 인증, 과금 등을 위한 모바일 네트워킹 기능을 하는 코어 네트워크를 거쳐 IP 서비스 망의 응용 서버로 연결되는데, 5G 디바이스의 가장 큰 보안 위협 요인은 기존의 스마트폰 단말 하나로 제한되었던 기기가 IoT 등 여러 가지 서비스 별 기기로 다양화 되면서 공통된 표준이나 구조 설계가 어려워졌다는 점이다.

특히 사양이 낮은 IoT 기기들은 수준 높은 보안 기능을 탑재하기 위해 취약한 패스워드 및 오래된 보안 취약점을 내포한테 운영되거나 변조에 취약하고 악성 애플리케이션에 의한 부적절한 접근 또는 중간자공격으로 인한 가입자 정보 유출 등의 보안위협에 취약한 환경에 노출될 가능성이 높다.

공격자는 보안이 취약한 IoT 기기의 취약점을 찾고, 많은 IoT기기를 '원격 재부팅'악성코드에 감염시켜 5G RAN을 대상으로 DDOS 공격을 하는 등 활용할 수 있게 된다.

이러한 DDOS 공격은 5G 네트워크에 직접적인 위협이 될 수 있는데, 5G 네트워크는 4G 네트워크보다 20배 빠른 속도로 10배 많은 IoT 기기에 접속할 수 있기 때문에 DDOS 공격 강도도 커질 수 있게 된다.

3. 무선 랜(Wi-Fi) 취약점

보안설정이 되지 않은 무선 랜(Wi-Fi)는 외부인이 무선공유기를 무단으로 사용할 수 있고, 해커가 접속하여 해킹 또는 개인정보 유출 등 다양한 보안 사고를 유발 할 수 있다. 무선 랜 공격에는 도청 및 무선 스캐닝과 서비스 거부 공격이 있다.

도청 및 무선 스캐닝은 암호화 하지 않은 무선 구간의 개인정보, 위치정보와 같은 다양한 정보를 불법적으로 유출하고, 무선 랜 접속과 관련한 정보와, 주변 AP 및 단말의 MAC 주소, 무선네트워크 종류 등을 분석하여 다른 공격을 위한 기반 자료로 이용하는 것을 목적으로 한다.

서비스 거부 공격은 단말과 AP간의 정상적인 통신이 이루어질 수 없도록 무선 랜 프레임을 다량으로 발생하는 형태의 공격으로 물리 계층상의 서비스 거부 공격은 공격의 대상이 되는 AP의 서비스 주파수 대역에 강한 전파를 보내서, 주파수 혼선으로 원활한 서비스가 이루어지지 않도록 하는 공격이다.

와이파이 WPA 보안 프로토콜에 취약점이 있는 것으로 드러났는데, 해커들이 와이파이에 연결된 사용자의 데이터를 볼 수 있는 취약점으로 크랙(KRACK)이라는 이름이 붙여졌다. 이는 특정 제품이나 구현 기술이 아닌 프로토콜 자체에 영향을 미치며, 와이파이를 사용하는 기기라면 크랙의 영향을 받을 수 있다.

크랙은 클라이언트 장치가 보호된 와이파이 네트워크에 연결을 시도할 작동하는 '신호변경(handshake)' 4단계 중 3단계를 표적으로 삼아 그 동안 여러 차례 암호화키를 송신하여 재전송할 때 와이파이 보안을 붕괴시킬 수 있다.

'신호변경' 4단계는 클라이언트가 서버의 통신을 종료하기 위해서 사용되는 것으로 3단계는 서버의 통신이 끝나서 종료할 준비가 되었을 때, 클라이언트에서 FIN 패킷을 전송하는 단계이다. 와이파이 보안이 붕괴되면 공격자는 사용자가 네트워크를 통해 전송하는 트래픽을 엿볼 수 있게 되는데, 하지만 이는 공격자가 사용자 와이파이 네트워크의 도달 범위에 위치해야 공격을 할 수 있다는 점을 이루어 보았을 때, 무선 랜 사용자가 공격을 받게 되는 것은 아니다.

4. 결론

먼저 3G 네트워크 DDOS 공격에 대한 대응 기술로 AQM(Active Queue Management)을 이용한 공격 완화 기술 또는 이상 트래픽 탐지 기술 등이 주를 이루고 있다. 공격 발생 시 효과를 경감시켜주는 기술 또는 WCDMA 네트워크에서의 무선 보안 게이트웨이 형태의 제품이 공격 대응을 위한 상용 제품으로 개발되고 있으며, 트래픽 이상을 탐지하는 보안 기능을 제공한다.

5G 네트워크에서 사용자 트래픽과 서비스를 안전하게 보호하기 위해서는 새로운 보안 기술이 설계되고 솔루션이 개발되어 네트워크에 구축되어 운영되어야 하며, 이를 위해 표준화, 장비 개발, 네트워크 구축 및 운영이 고려되어야 한다.

표준화 단계에서는 국가 간 망의 상호연동을 위한 안전한 통신 프로토콜이 설계되어야 할 것이며, 표준에서 요구하는 보안 기준 및 목표에 맞는 장비가 개발 되어야 하며, 안전한 네트워크 및 서비스 설계와 구축, 그리고 사이버 공격에 대한 탐지 및 모니터링과 사고 대응 관리가 요구된다.

5G의 보안 표준화는 세계적으로 진행 중에 있으며, 2015년부터 보안 아키텍처, RAN 보안 인증 메커니즘, 네트워크 슬라이싱 보안, 가입자 정보보호 표준에 대한 논의가 시작되었고, 2018년 8월에 5G Release 15에서 보안표준(SA3 TS 33.501)이 발표되었다.

이 표준에서는 IMSI(International Mobile Subscriber Identity) 정보 암호화, 로밍 도메인 간 보안 이슈였던 SS7이슈를 해결하고 서로 다른 통신 사업자(Public Land Mobile Network: PLMN) 간 애플리케이션 계층 간의 보안을 구현하기 위한 SEPP(Security Edge Protection Proxy)

기능, 3GPP 액세스와 Non-3GPP 액세스에 대해 동일한 인증방법을 사용할 수 있도록 한 통합 인증 프레임워크 기능이 도입되었다.

장비 개발 및 구축 단계에서는 보안 매커니즘으로 종단 간 보안(End to end security or Horizontal Security), 계층 간 보안(Cross-layer Security or Vertical Security), 멀티 도메인 간 보안(Domain Security), 보안 내재화(Security by design)가 제시되었다.

종단 간 보안에서는 4G 모바일 네트워크와 마찬가지로 사용자 장치로부터 무선 액세스 및 전송 네트워크를 포함하여 코어 네트워크의 종료 지점 간의 수평적 통신 경로에 대한 보안을 유지하는 종단 간 보안 기술이 필요하며, 두 번째 계층 간 보안에서는 5G의 분산되고 유연한 특성으로 인한 수평적 도메인 간의 보안이 어렵다는 점을 들어 서로 다다른 보안 계층의 보안 기술 조정을 위해 수직적인 보안의 통합 프레임 워크가 필요하다.

세 번째 멀티 도메인 간 보안은 네트워크, 서비스 및 장비를 포함한 다양한 도메인의 공존으로 보안 문제가 발생할 수 있는데, 각 도메인별 또는 멀티 도메인에 걸쳐 계층 간 보안이 보장되어야 다른 도메인과 안전하게 작동할 수 있다는 점이다.

네 번째는 보안 내재화로 표준화 단계부터 장비 개발과 네트워크 설계 프로세스의 일부로써 초기에 고려되고 배포되어야 잠재적 보안위협을 최소화할 수 있다.

운영 단계에서의 사이버 공격 방어를 위해서는 첫 번째 분산 사이버 공격에 대비하여 효과적인 사이버 공격 탐지 기능들이 잠재적인 공격 지점과 가까운 위치에 배치되어 대응해야 하며, 유연하고 확장 가능한 보안으로 계층별로 3GPP 표준의 기본적 보안이 제공되어야 한다.

5G 서비스 별로 다양하고 복잡한 요구 사항을 만족시키기 위해 각 서비스 별로 차등화면 보안 기능의 구성과 호출이 유연하게 적용되어야 한다.

사이버 공격의 기술은 점차 현재의 보안기술을 우회하고 정교하고 자동화되고 있기 때문에 수직 계층 간 보안을 관리하고, 각 논리적 계층의 사이버 공격을 모니터링하고 탐지하는 구조가 중요하다.

무선 랜(Wi-Fi)의 보안을 위해서는 일반적으로 무선공유기에 제공되는 보안기술에 입각하여 단말기 설정을 할 필요가 있으며, 신뢰되지 않는 무선 랜 또는 AP에는 가급적 접속하지 않는 것이 바람직하다.

크랙(KRACK) 와이파이 취약점으로부터 보호하기 위서는 기기를 항상 최신 상태로 유지하고 있어야 하며, 만일 비밀번호로 보호된 핫스팟을 포함한 공용 무선 랜을 사용하는 경우에는 HTTPS 암호화를 사용하는 웹 사이트만 이용하는 것이 좋으며, 가상 사설망(VPN)을 사용해 네트워크 트래픽을 감추는 방법도 있다.

시간이 지나고 이동통신 기술이 발전함에 따라 각 이동통신의 취약점이 드러나고 있으며, 해커들은 더 정교하게 그 취약점을 이용하고 있다. 기본적인 네트워크 보안을 위한 개개인의 습관이 필요할 것이며, 무선 이동통신 및 Wi-Fi가 고속, 대용량화되는 시점에서 취약점 탐지 및 그의 따른 대응 기술의 개발이 더 필요할 것이다.