정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

이동통신 보안의 현재와 미래

김 용 대*

요 약

본 고는 필자가 지난 8년 간 다양한 이동통신 취약점 연구를 했던 경험을 바탕으로 5G 이동통신 보안의 미래에 대하여 예측하는 것을 목적으로 한다. 이를 위하여 기존 네트워크 보안과 다른 이동통신 기술의 특수성, 이동통신 보안의 기술적 어려움에 대하여 분석을 하고, 실제로 취약점 분석을 했던 경험을 바탕으로 5G 이동통신 보안의 미래에 대하여 예측하고자 한다.

Ⅰ. 서 론

2019년 4월 한국의 이동통신 3사는 5G 시대를 선언하고 5G 이동통신 서비스를 시작했다. 이와 더불어 국내 이동통신 장비 제조회사들은 화웨이 사건 등으로 부수적인 이득을 얻으며 호황을 누리고 있다. 5G 이동통신은 기존의 통화 및 데이터 통신 뿐 아니라 자율주행, 열차 제어, IoT 등 다양한 응용에 사용될 것으로 기대가 되고 있어, 많은 사람들의 기대를 받고 있다. 그런데 항상 새로운 기술에 대한 기대와 더불어 나타나는 것은 보안에 대한 걱정이다. 본 고에서는 기존에 많이 분석이 되었던 이동통신 기술인 LTE의 보안 취약점들과 이들이 생기게 되었던 문제점들에 대하여 분석을 하고, 이를 통하여 5G 보안의 미래에 대하여 예측해 보고자 한다.

Ⅱ. 이동통신의 특수성 - 네트워크 보안과의 비교 분석

먼저 이동통신망 기술은 TCP 등의 일반적인 인터넷 프로토콜과 달리 평균 10년 주기로 새로운 기술이 등장한다. 따라서, 새로운 기술이 등장할 때 마다 새로운 표준이 만들어 지고 새로운 구현이 나타나기 때문에 새로운 취약점이 존재할 수 있다. 반면 네트워크 보안은 큰 변화를 거치지 않는다. 예를 들어, TCP의 경우, 1981년 처음으로 RFC가 만들어진 이후 작은 변화들이 있어 왔지만 전체적인 설계는 크게 바뀌지 않았다.

두번째로 이동통신망 표준은 많은 변화에도 불구하고 몇 가지 보안 취약점은 제대로 고쳐지지 않고 작은 패치만이 이루어 지고 있다. 통화에 대한 암호화의 부재, 기지국에서 단말기로 브로드캐스트 하는 메세지에 대한 보안의 부재 등이 그 예라고 할 수 있다. 이런 보안 취약점이 계속 존재하는 채로 표준이 바뀌고 있는 것은, 결국 기술이 바뀌더라도 이런 취약점은 계속 이용될 수 있음을 의미한다. 뿐만 아니라 이동통신은 경우에 따라 과거의 기술에 대한 지원, 즉, Backward Compatible하여야 한다. 예를 들어 중국의 경우 매우 취약한 것으로 알려진 2.5G GSM 네트워크를 아직도 지원을 하는 경우가 있다. 참고로 2.5G GSM 네트워크는 암호알고리즘의 취약점이 공개가 되어 현재 무선 구간에서 도청이 가능한 것으로 알려져 있다.

세번째로 세대 전환 중에는 기존의 기술들과 혼재하는 기간이 존재하여 (예를 들어 5G NSA의 경우 LTE의 제어평면을 그대로 사용하고, 5G의 데이터 평면을 이용한다. 비슷한 예로 LTE에 존재했던 CSFB 기술을 들 수 있다.) 이러한 기술들의 혼재와 상호작용으로 인해 새로운 취약점들이 발생할 가능성이 매우 높다. 즉, 5G NSA의 경우, LTE 제어 평면의 보안 취약점, 5G 데이터 평면의 보안 취약점, 그리고 이들을 합치는 기술인

본 연구는 한국연구재단 논문연구과제(95-0100-23-04-3) 지원 및 한국대학교 논문연구소 관리로 수행되었습니다.
본 논문의 요약문은 전자신문 2019년 5월 6일자에 게재된 바 있습니다. [1]
이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00793, 국가기간망 사이버공격 사전 예방을 위한 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술 개발)
* 카이스트 전기및전자공학부 (yongdaek@kaist.ac.kr)

NSA의 보안 취약점이 공존할 가능성이 존재한다. 한 가지 예로 3G와 LTE가 공존했던 CSFB(Circuit Switched Fall Back)의 경우, 많은 취약점과 버그가 존재했었는데, 곧 LTE가 사용될 것이라는 이유로 꽤 오랜 기간 패치가 되지 않았던 적이 있었다.

네번째로 이동통신망은 사업자, 제조사, 지역에 따라 적용된 기술 및 설정이 다르기 때문에 다른 문제점이 나타나고, 따라서 문제를 파악하기 위해서는 지엽적인 분석보다 광범위적인 분석이 요구된다. 예를 들어, Tu 등은 한 네트워크에서의 측정을 통하여 LTE의 설계상의 문제점을 찾았다고 주장했었으나 [4], 이 문제는 다른 네트워크에서는 찾을 수 없는 문제점이라는 것이 밝혀져 [3]. 그 주장이 사실이 아니라는 것이 알려지게 되었다.

마지막으로 이동통신망에서의 문제점 및 보안성 진단은 주로 망을 운영하는 통신사업자 내부적으로 진행하고, 사업상 기밀로 공개하지 않아, 문제의 해결이 독립적으로 이루어지며, 따라서 한 통신사업자에서 패치가 되었더라도 다른 통신사업자에서 동일한 문제가 일어날 가능성이 매우 높다. 예를 들어 2015년 본 연구팀은 5개 이동통신망에 대한 취약점 분석을 통하여 통화에 사용하는 응용 프로그램인 VoLTE의 취약점을 미국 CERT에 제보를 하였으나 [5], 취약점을 찾았던 미국 통신사는 아무도 취약점 유무에 대하여 확인을 해 주지 않았다. [6]

이러한 다섯가지 특수성은 이동통신 보안 문제가 다른 네트워크 보안 문제와 매우 달라지게 하는 특이한 점이다.

Ⅲ. 이동통신 보안의 기술적 어려움

뿐만 아니라, 이동통신 보안은 이동통신을 전공하는 사람은 보안을 몰라 어렵고, 보안은 전공하는 사람은 이동통신을 몰라 어려운, 즉 모두에게 어려운 분야이다. 이외에도 이동통신 보안을 어렵게 하는 다양한 기술적인 한계가 존재한다.

- 논리적 취약점 탐지의 어려움: 이동통신망은 다양한 기술이 복합적으로 적용되며, 프로토콜 및 설계 관련 표준들은 복잡하게 구성되어 있어 논리적 취약점의 탐지가 어렵다. 이동통신 표준은 매우 방대하고 한 가지 기술이라고 할 지라도 여러 문서에 나누어져 작성이 되어 있는 경우가 많기 때문에 모든 문서를 따라 가면서 정확하기 구현을 하는 것이 매우 어렵다. 이 문제는 표준 설계, 구현, 운영에 모두 영향을 끼친다. 먼저 설계하는 관점에서도 다양한 문서에 나누어져 있는 표준은 모든 문서를 따라 가면서 설계하는 것을 어렵게 만든다. 구현하는 사람, 운영하는 사람의 경우도 마찬가지이다. 모든 관련된 문서를 찾아가면서 예외 조항 등에 대해 파악을 하는 것은 매우 어렵다.

- 체계화된 분석의 어려움: 이동통신망 프로토콜 모델의 표준 규격은 정형화되어 있지 않기 때문에 체계화된 문제 진단 및 보안성 분석이 불가능하다. 표준은 자연어로 작성이 되어 있고, 자연어는 개발자나 운영사가 오해를 할 수 있는 부분이 많이 존재한다. 따라서 정형화된 분석 기법을 적용하는 것이 매우 어렵다. 자연어로 된 표준 문서를 오해를 하지 않고 해석을 하는 것은 쉽지 않다. 반면 정형화된 언어로 표현이 된 표준이 존재할 경우, 정형 분석을 통하여 표준 상의 모순 등을 찾아는 것은 어렵지 않을 것이다. 단지, 자연어로 된 인간의 생각을 정형화된 언어로 변환하면서 생기는 인간의 오류 또한 무시하기는 힘들다.

- 프로토콜 구현의 모호성: 표준 규격 상 프로토콜 구현의 높은 자유도와 표현의 모호함으로 인해 동일한 과정에 대해 동작이 달라질 수 있다. 예를 들어, 이동통신 표준은 재전송공격(Replay Attack)을 막는 것을 제조사에 맡기고 있다. 그렇지만 제조사에서 이를 제대로 구현했는지 확인할 수 있는 방법은 존재하지 않고 있다. 제조사에게 혹은 운영사에게 판단을 맡기면서 제대로 구현되었는지 확인할 수 없다는 것은 이동 통신 표준 체계의 큰 허점을 보여준다. 물론 이동통신에는 표준과의 합치성을 테스트할 수 있는 표준은 존재한다. 그렇지만 이 표준은 분명 제대로된 동작을 위해 만들어졌을 뿐 버그를 탐지하기 위하여 만들어지지는 않았다.

- 통합된 프로토콜 동작 모델의 부재: 이동통신망에서는 다양한 프로토콜들이 서로 상호작용하지만 표준에서는 이에 대한 통합된 동작 모델이 없어 분석이 어렵다. 이동통신 시스템의 구성 요소는 SIM 카드,

베이스밴드 칩, 모바일 운영체제, 기지국, MME (Mobility Management Entity), HSS (Home Subscriber Server), P-/S-GW(PDN-/S- Gateway) 등으로 구성이 되며 이러한 기기들이 상호 작용을 해야 제대로 동작을 한다. 표준에서는 이러한 상호 작용을 별도의 문서에서 정의를 하고 있어서, 전체적으로 보았을 때 어떤 문제점이 있는지 파악을 하는 것이 어렵다. 예를 들어, 단말기는 코어망의 다양한 개체들과 통신을 하고 있다. 그런데, 만약 가짜 단말기가 만들어져서 코어망의 개체들에게 다른 상태를 보여준다면 표준 상으로 문제를 일으킬 여지는 많이 남아 있다.

- 수동적 보안성 분석 방식의 비효율성: 보안 위협 상황 재현 및 문제점 분석에 있어 전문가가 손수 설정하는 경우, 시간적, 물질적 비용이 소요된다. 올해 5월 발표된 필자의 연구그룹의 논문을 제외하면 자동적인 취약점 분석 논문은 1-2편만 존재할 뿐이다. [7][8] 뿐만 아니라 이런 취약점 분석 논문 또한 표준의 취약점에 집중을 하고 있다. 앞에서도 언급을 했듯이 상당히 큰 비중의 취약점이 구현과 운영에서 생길 수 있는데, 표준 취약점만 집중을 할 경우, 보안 취약점이 생길 가능성이 매우 크다.

- 기술 발전의 특수성: 이동통신은 평균적으로 10년마다 새로운 표준이 만들어져 기존 기술 분석 방법을 적용하기 힘들며 새롭게 적용되는 기술 분석에 추가적인 비용 발생한다. 예를 들어, 5G 기술이 나왔으나, 새로운 하드웨어와 이동통신 표준을 구현한 새로운 소프트웨어가 나와야 분석이 가능하다. 예를 들어 현재 LTE 네트워크를 분석하는데 주로 사용을 하고 있는 소프트웨어인 srsLTE의 경우아직 5G 버전이 만들어 져 있지 않아, 분석에 어려움을 주고 있다. 뿐만 아니라 신호를 만들어 내는 하드웨어인 USRP의 경우, 6GHz까지 밖에 지원을 하지 않아, 5G에서 새로 사용을 하는 28GHz 이상의 NR(New Radio)를 지원하기 힘들어 새로운 하드웨어가 필요한 실정이다.

Ⅳ. Case Study: LTE 보안 취약점

2018년 말 필자가 속해 있는 연구실은 위의 기술적 어려움을 일부 극복하는 LTEFuzz라는 자동화된 취약점 분석 방식을 개발하여 [2] (http://ltefuzz.syssec.kr) 국내 이동통신망 및 전 세계 단말기를 대상으로 실험한 바 있다. LTEFuzz는 이동통신 제어평면에서 예외 처리가 제대로 되어 있는지 확인하는 것을 목표로 한다. 이를 위해서 먼저 이동통신 제어평면의 각 메세지들에 대하여 안전하게 메시지가 처리되도록 하는 최소한의 요구 조건을 수립하고, 이를 만족하지 않는 (평문, 인증이 되지 않는 메세지, 재전송된 메세지 등) 메세지를 각 제어 평면의 프로토콜에 대하여 생성을 하였다. 이렇게 생성된 메세지를 2개의 통신사와 4개의 단말기에 대하여 시험을 하였다. 이러한 메세지들은 보안상 문제가 있는 메시지 이므로 당연히 무시가 되어야 하는데 실험 결과는 그렇지 않았다. 이 실험을 통하여 본 연구팀은 총 51개의 취약점을 통신사와 단말기에서 찾을 수 있었고, 이중 36개는 신규 취약점, 15개는 기존에 알려진 취약점이 여전히 존재함을 알 수 있었다. 이중에는 14개의 표준 취약점 (즉, 표준 자체에 존재하는 보안 취약점) 또한 존재하였다. 이 실험은 이동통신 시스템의 다양한 문제점을 시사하고 있다.

- 기존의 취약점이 패치가 되고 있지 않은 것은, 통신장비 제조업체와 통신사업자가 학계 및 산업계에서 재기되고 있는 다양한 보안 문제점에 대하여 큰 신경을 쓰고 있지 않은 것으로 보인다. 현재까지 LTE는 200개 이상의 취약점이 학계를 통하여 발견된 것으로 알려져 있다. 그럼에도 불구하고 이동통신 업계의 경우, 학계의 연구 결과에 대해 크게 신경 쓰지 않는 것으로 보안다.

- 표준 취약점들은 당연히 패치하는 것이 힘들다. 그렇지만 끊임없이 재기되고 있는 보안 취약점에 대하여 표준에서 조차 처리를 하고 있지 않은 것은 이동 통신 표준을 선도하고 있는 표준화 기구인 3GPP 및 GSMA에 문제가 있거나, 표준을 만드는 과정에 문제가 있음을 보여준다. 이 문제는 V장에서 좀더 자세히 다루고자 한다.

- 위에서 찾은 보안 취약점들은 이동통신을 하는 사람들이라면 쉽게 찾을 수 있는 예외 상황을 처리하고 있지 않은 것에서 발생한다. 즉, 설계 및 구현 단계에서 당연한 예외 상황들에 대해 정상적인 처리를

하고 있지 않은 것은 이동 통신 장비 설계 및 구현 단계에서 시큐어 코딩이 적용되고 있지 않은 것을 보여준다. 뿐만 아니라 앞에서도 언급을 했듯이, 보안 테스팅을 위한 표준이 존재하지 않는 것이 이 문제의 시발점이라고 생각할 수 밖에 없다.

- 뿐만 아니라 한 통신사의 두 개의 제조업체의 보안 취약점이 다르게 나타나고 있는 것은, 통신사업자가 적합성 테스트에 치중을 하고 있지만, 보안 취약점 테스트 절차는 존재하고 있지 않은 것을 보여준다. 이 논문을 발표한 후에 미국의 T-Mobile, Verizon, Google Project Fi, 독일의 Deutche Telecom, 싱가포르의 Singtel 등은 본 연구팀에 테스팅을 요구해 왔다. 보안 테스팅 표준과 기술이 부재하기 때문에 이러한 요구들이 있는 것으로 생각하고 있다.

- 한 제조업체의 두 개의 통신사의 취약점이 다르게 나타나고 있는 것은, 제조업체 뿐 아니라 통신사가 잘못된 설정을 하는 경우도 있음을 보여주고 있다.

즉, LTEFuzz 연구를 통하여 본 연구팀은 표준, 구현, 운영 등 3가지 측면에서 이동통신 업계는 보안적으로 취약한 요소를 가지고 있음을 입증하였다고 생각할 수 있다. 문제는 이러한 취약점 분석의 대상이 매우 좁았던 것을 들 수 있다. 즉, 전체 LTE 프로토콜 중 NAS와 RRC라는 매우 작은 프로토콜들을 대상으로 하였으며, 여기의 보안 요소들 조차 3-4가지에만 집중하였음에도 51가지나 취약점이 나왔다는 것은 앞으로, 그리고 현재 이동통신 망은 많은 보안 취약점을 내재할 것으로 생각한다.

Ⅴ. Case Study: 안전하지 않은 표준

앞에서도 언급을 했듯이 이동통신 표준에 존재하는 다양한 보안 취약점 중에는 오랫동안 패치가 되고 있지 않은 것들이 있다. 본 장에서는 이러한 표준 보안 문제점에 대하여 정리를 해 보고자 한다.

- 암호화되지 않는 통화, 문자: 이동통신 표준은 통화에 대하여 암호화할 것을 권고한다. 그렇지만 본 연구팀에서 조사한 바에 따르면 전세계 주요 통신사에서 통화를 암호화하는 경우는 거의 없는 것으로 조사되었다. 뿐만 아니라 몇 가지 예외가 있지만 문자도 암호화되지 않고 전달되는 경우가 많이 있다. 암호화를 하지 않는 데는 여러 가지 이유가 있겠으나, 계산상의 복잡도, 합법적인 감청의 편의 등을 가장 중요한 이유로 들 수 있을 것이다.

- SS7: SS7은 이동통신 사용자의 로밍을 지원하기 위한 프로토콜이다. LTE에서는 Diameter, 그리고 5G에서도 새로운 프로토콜이 설계가 되고 있음에도 불구하고 근본적인 보안 문제점은 해결이 되고 있지 않다. 즉, 사용자가 로밍이 된 경우, 통화, 문자, 데이터 등 모든 메시지가 로밍 네트워크로 라우팅이 된다. 문제는 이들이 응용단에서 암호화되지 않을 경우, 로밍 네트워크에 암호화되지 않은 상태로 전달이 되며 로밍 네트워크에서는 이러한 메시지에 대해 자유롭게 도청이 가능하다. SS7의 가장 큰 문제점은 이동통신사는 다른 이동통신사를 신뢰한다는 가정에서 시작되는데, 이러한 문제의식의 근간에는 폐쇄성이 많은 경우, 국가가 이동통신사에 대한 지배력을 가지고 있는 경우가 많다는데 그 문제점을 찾을 수 있다. 즉, 여행자의 경우, 다른 국가에게 아무런 보안 지원이 되지 않는다. 여기에 더 큰 문제는 피해자가 한국에 있더라도 강제로 해외로 옮길 수 있는 보안 문제점은 해외 여행을 하고 있지 않더라도 SS7 공격의 피해자가 될 수 있다는 심각한 문제성을 보여준다.

- 보호되지 않는 브로드캐스트 채널: 브로드캐스트 채널이란 기지국이 단말기에 내려보내는 다양한 메시지들이 브로드캐스트되는 것을 의미하고 있다. 브로드캐스트 채널의 예로는 단말기에 시그날링을 보내는 페이징, 그리고 재난 문자 등 코어망이 단말기에게 필요한 정보를 전달하는 것 등을 들 수 있다. 일반적으로 브로드캐스트 채널에 대한 보안은 전자서명을 사용하는 것이 가장 일반적이나 이동통신 브로드캐스트 채널의 경우 전자서명을 사용하지 않고 있다. 전자서명을 사용하지 않는데에는 몇 가지 이유를 들 수 있는데 코어망의 계산상의 오버헤드, 단말기의 배터리 사용량의 증가 등을 가장 중요한 이유로 들 수 있을 것이다. 단지 5G에서는 SIM 카드에 공개키를 ID의 암호화를 위하여 사용하기 시작했음에도 불구하고 전자서명을 사용하고 있지 않는 것은

매우 실망을 준다. 기존에 보호되지 않는 브로드캐스트 채널에 대한 공격으로는 가짜기지국을 이용하여 단말을 가짜기지국에 접속 시키고 난 후에 재난문자 등 다양한 브로드캐스트 채널 메시지를 보내는 것이 기존의 공격이었다. 올해 필자의 연구팀은 가짜기지국보다 탐지가 힘들고 공격의 효율을 올려주는 SigOver 공격을 발표하여 여전히 브로드캐스트 채널은 전자서명을 통하여 보호를 받아야 한다는 입증을 하였다. [9]

Ⅵ. 5G 보안을 바라보며

5G는 이제 우리의 현실이다. 그렇지만 5G의 보안성은 여전히 물음표이다. 먼저, 5G는 크게 5G NSA(Non Stand Alone)과 5G SA(Stand Alone)으로 나뉜다. 그런데 5G NSA의 경우, LTE 제어평면을 그대로 사용하기 때문에 위에서 언급한 LTE 제어평면의 취약점(표준 및 구현)은 특단의 조치가 있지 않을 경우 그대로 남아 있을 것으로 보인다. 그러면 5G SA의 경우는 어떻게 될까? 현재 개발되고 있는 5G SA 표준을 보면 과거로부터 알려진 취약점을 몇 가지 수정을 하려는 노력은 하고 있으나 원천적으로 안전한 표준을 만들겠다는 설계 철학은 보이지 않고 있다. 이는 핵심적인 표준 문제에 대하여 "땜질식" 설계를 이용하여 패치를 하려는 것으로 부터 쉽게 볼 수 있다. 자율주행차, 철도, 재난안전망 등 인간의 안전과 직접적인 연관이 있는 5G는 LTE와 비교를 하여 더욱 높은 보안성을 요구한다. 필자는 이를 위해서 5G 표준화 및 개발에 다음과 같은 것이 필요할 것으로 생각한다.

- 정형화된 프로토콜 설계 및 분석: 프로토콜 구현의 자유도는 보장을 하되 표현의 모호함을 피하기 위하여 이동통신 표준은 정형화된 언어로 표현되어야 한다. 물론 정형화된 프로토콜에서는 다양한 프로토콜 간의 관계 또한 정형화되어 설명되어야 한다. 이 경우, 기존의 정적 분석 방식을 이용하여 자동화된 논리적 분석이 가능하며 위에서 언급한 것 같은 표준의 문제점을 미리 피할 수 있다.

- 자동화된 구현 취약점 분석 방식의 도입: 인간은 실수를 할 수 밖에 없다. 따라서 다양한 구현 및 운영상의 실수를 탐지하기 위하여 LTEFuzz와 같은 자동화된 분석 방식이 필요하다.

- 통신사업자, 단말기 제조사, 코어망 장비 제조사, 표준 단체, 학계, 보안 산업체 간의 대화의 필요: 현재까지 LTE는 150여가지 취약점이 발견된 것으로 알려져 있다. 표준 및 구현 상의 이런 다양한 취약점들이 계속해서 발견되는 것의 가장 큰 원인으로 필자는 전통적인 이동통신 업계의 폐쇄성을 들고 싶다. 한국의 이동통신 회사들은 그래도 협업이 매우 잘 되고 있으나, 대부분 해외 통신사들은 취약점 제보를 하더라도 긍정도 부정도 하지 않는다. 앞에서 언급을 했듯이, 서로 대화가 부족하기 때문에 한 통신사업자의 취약점이 다른 사업자에게 그대로 나타난다고 생각한다. 따라서 과거의 폐쇄성을 벗어나 이제 이동통신 업계가 적극적으로 대화에 나서야 한다고 생각한다. 취약점을 찾는 학계, 보안 산업체 뿐 아니라, 사업자, 제조사 들간의 대화가 반드시 필요하다고 생각한다.

Ⅶ. 결 론

필자는 보안 문제가 통신사 및 제조사에게 불명예스럽다는 것을 잘 알고 있다. 그렇지만, 반대로 생각을 해보면 우수한 보안 기술로 5G 표준 및 구현을 선도할 수 있다고도 생각한다. 다른 나라에서 잘못 만들어진 표준에 따라갈 것이 아니라 더 안전한 표준을 제안하여 기술을 선도하는 우리나라의 이동통신업계를 기대해 본다.

참 고 문 헌

[1] 김용대, "이동통신 보안의 현재와 미래", 전자신문 2019년 5월 6일

[2] H. Kim, J. Lee, E. Lee, Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane", *Proceedings of the IEEE Symposium on Security & Privacy (SP)*, 2019

[3] B. Hong, S. Park, H. Kim, D. Kim, H. Hong, H. Choi, J-P Seifert, S-J Lee, Y. Kim, "Peeking over the Cellular Walled Gardens – A Method for Closed Network Diagnosis", *IEEE Transactions on Mobile Computing (IEEE*

TMC), Vol. 17, No. 10, 2018

[4] G.-H. Tu, Y. Li, C. Peng, C.-Y. Li, H. Wang, S. Lu, "Control-Plane Protocol Interactions in Cellular Networks," *Proceedings of the 2014 ACM Conference on SIGCOMM*. ACM, 2014

[5] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, Y. Kim, Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations, *ACM Conference on Computer and Communications Security* (ACM CCS '15), 2015

[6] CERT Coordination Center, Voice over LTE implementations contain multiple vulnerabilities - Vulnerability Note VU#943167, https://www.kb.cert.org/vuls/id/943167/

[7] S. Hussain, O. Chowdhury, S. Mehnaz, E. Bertino, LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, NDSS 2018

[8] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, V. Stettler, A Formal Analysis of 5G Authentication, ACM CCS 2018

[9] H. Yang, S. Bae, M. Son, H. Kim, S. Kim, Y. Kim, Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, USENIX Conference on Security Symposium (USENIX Security '19), 2019

〈저자소개〉

김 용 대 (Yongdae Kim)

정회원

1991년 2월 : 연세대학교 수학과 졸업
1993년 2월 : 연세대학교 수학과 석사
2002년 5월 : 미국 Univ. of Southern California 박사
2002년~2012년 : 미국 미네소타대학교 교수
2012년~현재 : 카이스트 전기및전자공학부 교수
2012년~현재 : 카이스트 정보보호대학원 겸임교수
2017년~현재 : 카이스트 사이버보안연구센터 센터장

<관심분야> 정보보호