KR Maritime Cyber Security

News from KOREAN REGISTER

May 2019

Vol. 013

싱가포르 항만청, 해상 사이버보안 운영 센터 개설

● **사이버 공격 조기 발견 및 대응을 위한 해상 사이버보안 운영 센터 개설**

싱가포르 항만청(MPA : Maritime and Port Authority)은 해상 주요 정보 인프라(CII : Critical Information Infrastructure)에 대한 사이버 공격 조기 발견 및 대응을 위한 사이버보안 운영 센터(MSOC : Maritime Cybersecurity Operation Centre)를 개설하였다.

MSOC는 해상 CII에 대한 잠재적인 사이버 공격에 대한 조기 발견, 모니터링, 분석 및 대응을 통해 싱가포르의 해상 사이버 보안 태세를 강화할 것이며, 해상 CII를 보호하고 사이버 보안 위협이나 사건을 조사 할 수 있다. 또한 싱가포르 항만청은 보다 총체적이고 적시에 사이버 사건에 대응하기 위해 MSOC와 항구 운영 통제 센터 간의 주요 데이터 연계를 구축한다.

싱가포르 항만청은 해상 부문의 사이버보안 준비를 강화하기 위한 또 다른 계획을 시행하였다. 해상 요원이 사이버 위협 관리에 대한 지식을 향상시킬 수 있는 “해상 사이버보안 교육 과정(1일)”을 개발하였으며 이 과정은 내년 상반기에 실시될 예정이다.

싱가포르 항만청은 싱가포르 해상 연구소와 해상 사이버보안 연구 프로그램 개발에 착수하였으며, 다른 항구 당국과 정보 공유 네트워크를 통해 사이버 위협 및 사건에 대한 상황 인식을 향상시켜 선상 시스템 보호 및 항만 사이버보안을 강화할 예정이다.

Ref. : https://safety4sea.com/mpa-singapore-opens-maritime-cyber-security-centre/

수백만 대의 IoT 장비에 탑재된 P2P 취약점 발견

● **iLnkP2P를 사용하는 수백만대의 IoT 장비에 심각한 보안 취약점 발견**

보안 엔지니어인 폴 마라페스(Paul Marrapese)에 따르면, iLnkP2P로 구성된 수백만 대의 IoT 장비가 심각한 보안 취약점이 있는 것으로 나타났다. iLnkP2P는 장비 제조업체가 사용하는 P2P 솔루션 중 하나이며 UID로 알려진 특별한 일련 번호를 사용하면 사용자는 모바일 또는 컴퓨터에서 IoT 장비에 즉시 연결할 수 있다. 이 경우 접속하기 위한 포트 전달이나 동적 DNS가 필요하지 않으며 NAT 및 방화벽 시나리오를 극복 할 수 있다.

마라페스가 찾아낸 취약점은 두 가지로, 이 두 가지 취약점을 동시에 사용하면 대규모의 공격을 할 수 있다고 설명한다. (CVE-2019-11220)을 통해 중간자 공격을 실행할 경우 장비 접근권한이 따로 필요하지 않으며, (CVE-2019-11219)를 이용하여 빠르게 많은 장비를 검색할 수 있다.

(CVE-2019-11219) iLnkP2P의 열거 취약점이며, 공격자가 온라인 상태인 장비를 빠르게 검색 할 수 있다. P2P의 특성으로 인해 공격자는 방화벽 제한을 무시하면서 임의의 장치에 직접 연결할 수 있다.

(CVE-2019-11220) iLnkP2P의 인증 취약점으로, 공격자가 장비에 대한 연결을 가로 채고 중간자 공격을 수행 할 수 있게 한다. 공격자는 이 취약점을 이용하여 장비의 암호를 훔쳐 제어 할 수 있다.

● **대응책**

1) 패치가 없으므로 신뢰할 수 있는 공급 업체로부터 새 장비를 구입한다.

2) UDP 포트 32100로 가는 아웃 바운드 트래픽을 차단하여 P2P 기능을 제거한다.

Ref. : https://cyware.com/news/millions-of-iot-devices-affected-by-newly-discovered-p2p-vulnerabilities-d8d92b1c

사이버 해적과 항해 시스템을 대상으로 한 위협

● 러시아 정부 GPS 공격 사례 및 공격 방법 분석

2018년 5월 러시아 크림반도 부근에서 24개 선박의 GPS 시스템들이 이상작동을 보여, 실제 정박된 거리와 약 65키로미터 벗어난 곳을 가리키고 있었다. 미국의 한 연구기관에 의하면, 당시 푸틴 대통령이 행사 차 근처에 있었으며 러시아 정부기관이 의도적으로 GPS를 공격했다고 한다. 현재 러시아 정부는 GPS, 바이두, 글로나스, 갈릴레오 등을 포함한 위성시스템까지 공격대상으로 삼고, 재밍과 스푸핑 공격을 정부 및 군 차원에서 진행하고 있다. 현재까지 파악된 숫자만 보더라도 약 10,000 척에 해당하는 선박이 영향을 받아 피해를 입었다고 보고되고 있다. 추정하는 바로는 러시아가 행하는 대부분의 공격은 주로 크림반도, 흑해, 시리아, 러시아 주변에서 발견되고 있으며, 그 외 국가들을 포함한다면 그 범위와 영향력은 더 커질 것으로 보인다.

이러한 시스템과 네트워크를 재밍, 스푸핑하는 방법은 크게 어렵지 않다. 해킹장비는 핸드폰 크기부터 서류가방 크기까지 다양하며, 민간에서 제작한다고 해도 수십만원 안팎에서 만들 수 있다. 2017년 미국의 한 대학에서는 65미터의 요트를 연구 목적으로 해킹하고 가짜 GPS 데이터를 넣어서 선박 충돌 위험까지 가능함을 입증했다. GPS 스푸핑은 GPS 인공위성에서 송신하는 GPS 신호보다 강한 위조 신호를 송신하여, GPS 수신기가 인공위성의 신호 대신 조작한 GPS 신호를 수신하게 만드는 공격이다. 공격자는 GPS 인공위성처럼 신호를 발신하여 공격 대상의 위치 정보와 시간 정보를 조작할 수 있다. 공격자가 GPS 인공위성인 것처럼 가장하여 정상 경로에서 벗어난 위치를 송신하면 시스템에서는 경로를 이탈했다고 착각하게 된다. 공격 대상은 정상 경로로 복귀하기 위해 수동으로 경로를 조정하게 되고 시스템 상에서는 정상 경로로 돌아온 것으로 보이지만 실제 경로에서는 이탈하게 된다.

선박의 GPS 수신기는 수십 개의 위성에서 위치 정보를 기록한다. 해커는 기존 인공위성의 신호를 복제한 다음 원래 경로에서 이탈하도록 조작한 신호를 발신한다. 신호가 갑자기 실제 경로에서 멀어지면 GPS 기반의 네비게이션 시스템이 이상을 감지할 수 있기 때문에 선박의 GPS 수신기가 조작한 신호를 송신할 때까지 거짓 GPS 신호의 전력을 점차 증가시킨다. 선박의 GPS 수신기가 실제 신호와 공격자에 의해 조작된 신호를 구별할 수 없게 되면, 선박 시스템에서는 경고 없이 공격을 성공시킬 수 있다.

Ref. : https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/

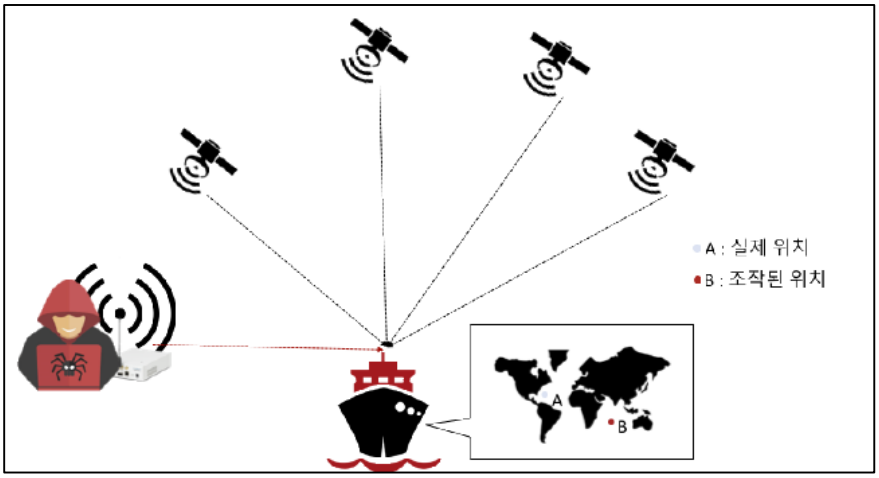


그림 01. NSHC 레드얼럿 연구소 산업 제어 시스템 무선 신호 공격 분석 보고서

연구팀에서는 직접 테스트 진행 시, 위치 정보를 조작하는 신호를 보내기 위해 GPS-SDR-SIM 프로젝트의 오픈 소스를 사용했다. GPS 대역 신호를 생성하고 SDR 장비를 통해 생성한 신호를 공격 대상으로 송신한다. 지원하는 SDR 장치로는 HackRF, BladeRF, USRP가 있다. 또한 전송하는 신호의 노이즈를 줄이기 위해 TCXO 모듈이 필요하다. 이러한 방법들을 가지고 공격을 할 경우 스마트폰을 포함한 모든 GPS 장비들에 대해 최소 100미터부터 오차를 만들 수 있고, GPS 신호를 못 잡도록 할 수 있다.

예전과 달리 요즘은 사이버 해적들이 생겨나고, 오로지 선박과 항만 등을 대상으로 하는 범죄 집단이 늘어나고 있다. 이들 또한 사이버보안 전문가들처럼, 선박 시스템과 구조에 대해 공부를 하고 현 시점에서는 주로 ECDIS와 AIS를 1차 해킹 대상으로 삼고 있다. 위에서 언급한 GPS 재밍, 스푸핑 등의 방법을 쓰며 위성 시스템까지 손을 대어 물리적인 선박 납치가 아닌, 사이버 공격으로 인한 납치를 계획하고 있으며, 해외에서는 이로 인한 금전적인 피해 규모를 조 단위 이상으로 보고 있다. 이를 대비하기 위해서는 장비에만 의존할 수 없고 그 상황에 대처할 수 있는 인력에 대한 훈련과, 일반 침투테스트가 아닌 실제 해킹과 유사한 침투테스트 시행을 통해 다양한 공격 시나리오를 학습하여 대비해야 한다.

Ref. : https://www.businessinsider.com/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4

▪ 본 기사는 (㈜ NSHC & Shield Consulting co.,ltd 이승준 책임 연구원에 의해 작성되었습니다.

NSHC SECURITY는 ICS/SCADA(OT)사이버보안 분야에서 국내 및 아시아에서 유일하게 사이버 침투테스트 수행가능한 회사이며, 랜섬웨어, APT 공격과 같은 악성코드 분석 및 산업용 기기 대상 침투테스트 및 소스코드 진단을 수행하고 있다. SHIELD CONSULTING은 사이버보안에서 요구되는 물리적 보안(CCTV, 외부자 출입, 전자기기 반입 통제, 잠금장치) 컨설팅을 제공하고 있다.

사이버 위협의 이해(OWASP Top 10)

● 사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● 한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● OWASP Top 10

OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 높고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 1월 뉴스레터에 이어 **'A4 : 2017 – XML 외부 개체(XXE)'** 를 분석하고자 한다.

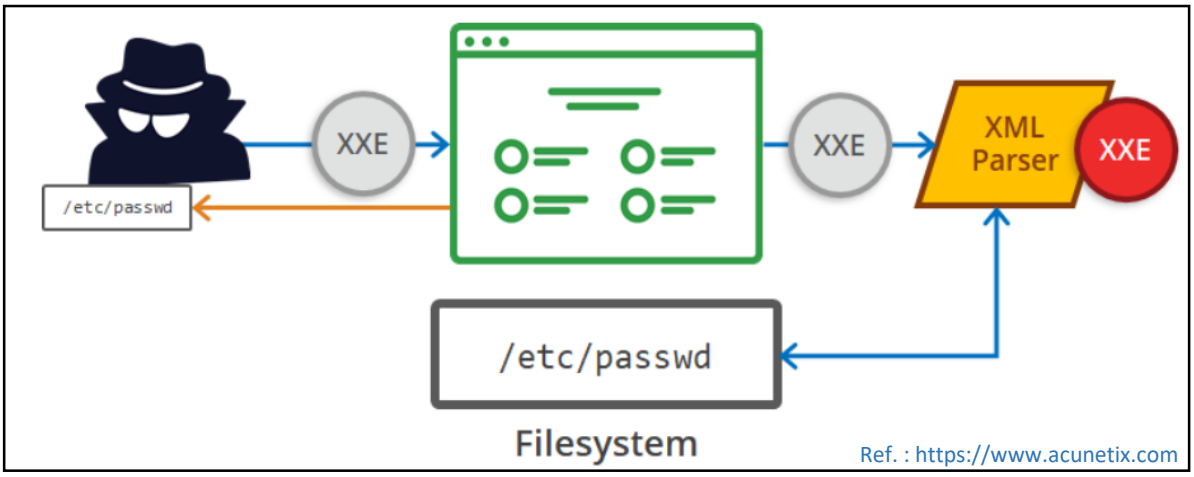
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

Ref. : OWASP Top 10 Project

● **OWASP 10대 위협 'A4 : 2017 – XML 외부 개체(XXE)'**

XML 외부 개체 (XXE) 공격은 SSRF (Server Side Request Forgery)를 기반으로 한다. 공격자는 XXE를 사용하여 DoS (Denial of Service)를 유발 할뿐만 아니라 로컬 및 원격 컨텐츠 및 서비스에 액세스 할 수 있다. XML (Extensible Markup Language)은 매우 보편적인 데이터 형식이다. 웹 서비스 (XML-RPC, SOAP, REST)부터 문서 (XML, HTML, DOCX), 이미지 파일 (SVG, EXIF 데이터)에 이르기까지 모든 분야에서 사용된다. XML 데이터를 해석하려면 응용 프로그램에 XML 구문 분석기 (XML Parser)가 필요하다.

공격자는 오래되거나 설정이 잘못 구성된 XML 구문 분석기를 이용하여, 주요 시스템 파일 접근(LFI), 외부 악의적인 파일 참조(RFI)가 가능하다. 또한 하나의 Entity에 다른 Entity를 계속적으로 참조하여 응용프로그램의 부하를 일으킬 수 있다. 해당 코드는 1KB보다 작지만 최종적으로 참조된 Entity를 XML Parser가 처리할 때 10억(2^9)개의 문자열을 처리해야 하므로 메모리상에서는 3GB를 차지하게 만들 수 있다.



취약점 확인 방법

아래와 같은 애플리케이션, 특히 XML 기반 웹 서비스나 다운스트림을 사용할 경우 공격에 취약할 수 있습니다:

- 애플리케이션이 직접 XML를 입력 받거나 특히 신뢰할 수 없는 곳의 XML를 업로드하거나 XML 문서에 신뢰할 수 없는 데이터를 입력할 경우. 이는 XML 프로세서가 처리합니다.
- 애플리케이션에 있는 XML 프로세서나 웹 서비스 기반의 SOAP에 Document Type Definitions(DTD)이 활성화되어 있을 경우. DTD 처리를 비활성화하는 정확한 방법은 처리기마다 다르기 때문에 OWASP Cheat Sheet 'XXE Prevention'와 같은 문서들을 참조하기를 권장합니다.
- 애플리케이션이 페더레이션 보안이나 싱글 사인온(SSO)의 목적으로 확인 처리를 위해 SAML을 사용할 경우입니다. SAML은 assertio을 확인하기 위해 XML을 사용하며 취약할 수 있습니다.
- 애플리케이션이 1.2이전의 SOAP을 사용하고 있다면 XML 개체들이 SOAP 프레임워크에 넘겨질 경우 XXE 공격에 민감할 수 있습니다.
- XXE 공격에 취약하다는 것은 애플리케이션이 Billion Laughs 공격을 포함하는 서비스 공격에 취약하다는 것을 의미합니다.

보안 대책

개발자에 대한 교육이 완벽하게 XEE을 확인하고 완화시키는데 필수적입니다. 그외에 XXE를 막기 위해서 다음이 필요합니다:

- 가능할 때마다, JSON과 같은 덜 복잡한 데이터 형식을 사용하거나 민감한 데이터를 지양합니다.
- 애플리케이션이나 운영체제에서 사용중인 모든 XML 프로세서와 라이브러리를 패치하거나 업그레이드합니다. 의존성 체커를 사용합니다. SOAP을 SOAP 1.2나 그 이상으로 업그레이드합니다.
- OWASP Cheat Sheet 'XXE Prevention'에 따라 애플리케이션에 있는 모든 XML 파서의 XML 외부 개체와 DTD 처리를 비활성화합니다.
- 서버에서 허용 목록(화이트리스트)을 이용한 입력값 검증, 필터링, 검사를 구현해서 XML 문서, 헤더, 노드에 있는 악의적인 데이터를 막습니다.
- XML이나 XSL 파일 업로드 기능이 XSD 검증기 같은 것을 사용해서 XML이 유효한 내용인지 확인하고 검증합니다.
- 많은 것들이 통합된 크고 복잡한 애플리케이션에서는 수동으로 소스코드 리뷰가 최선의 방법일 수 있으나, SAST는 소스코드에 존재하는 XXE를 탐지하는데 도움이 될 수 있습니다.

위 방법들이 가능하지 않다면 XXE 공격을 확인하고 감시하고 막기 위해 가상 패치, API 보안 게이트웨이, 웹 애플리케이션 방화벽(WAF) 사용을 고려하기 바랍니다.

시스템 운영 보안 수립 가이드라인

● 시스템 운영 보안 수립 필요성

시스템 운영보안 정책의 부재는 심각한 사이버 사고로 이어질 수 있다. 불필요하거나 취약한 서비스가 활성화되어 있는 경우 네트워크 스캐닝을 통해 취약한 서비스를 찾아내, 비인가자 접근, 악성코드 유포 등 해당 서비스를 악용하여 해킹을 할 우려가 있다. 예를 들어 SMB(Server Message Block) 프로토콜을 이용하여, 해당 네트워크 트래픽을 해커가 장악한 SMB 서버 또는 악성 웹사이트로 우회시킬 수 있는 취약점을 이용한다. 이를 통해 해커는 윈도우 PC 사용자들의 해당 로그인 정보를 탈취할 수 있다. 이와 같은 공격에 대한 최선의 보안대책은 TCP 139와 445 포트를 차단하여 SMB 프로토콜 자체를 이용하지 못하도록 하는 것이다. 쇼단(Shodan)과 같은 웹사이트는 IoT, ICS 등과 같은 설비 기반의 IT 인프라에 대해 국가, 기관, 서비스(포트), IP 주소 등의 검색어 입력만으로 어떤 서비스가 활성화되어 있고 인터넷 상으로 접근 가능한지 검색 가능하다. [출처 : 한국인터넷진흥원, 주요정보통신기반시설 기술적 취약성 분석 및 평가 방법 가이드]

● 한국선급 해상 사이버보안 인증 검사항목(CS1)

인터페이스 제한(213.1) : 정보기술 내 승인되지 않은 인터페이스, 포트 또는 서비스가 존재하는지 확인하도록 한다.

보안설정 변경(213.3) : 모든 정보기술 자산 도입 시 최초의 기본 설정값은 회사의 보안정책 또는 변경관리 기준에 따라 보안설정을 변경하여야 하며, 보안설정이 변경되기 전 사용을 금지하여야 한다.

데이터 백업(213.4) : 시스템의 변경 전 장애사항을 대비하여 필요 시 관련 데이터를 백업하여야 한다.

자동 실행 통제(213.6) : 정보자산에 접근하는 모든 소프트웨어는 자동 실행되지 않도록 구성하여야 한다.

변경관리 실행(213.7) : 변경관리 시행 시 사전 테스트를 실시하고 변경관리 기록을 보관 및 관리하여야 한다.

● **변경관리 절차(예시)**

정보자산 변경관리 필요성 제기	→	변경사항 작업 신청	→	보안성 검토 및 작업 사항 승인	→	변경 작업 실시	→	완료 검토

※ 변경관리 절차는 내부 지침(IT보안 지침 등)에 따라 처리되어야 함

● **변경관리 작업 계획서 (예시)**

변경 작업 계획서

	결재	서버 운영 담당자	서버 운영 관리자	전사 정보 보안관리자

등록요청 번호		요청 사유	
제품정보	제조사	제품명	서버명
변경 예정 내역			
작업내용			
보안성 검토의견			

위와 같이 변경 작업을 하고자 하오니 검토 후 조치하여 주시기 바랍니다.

20 . . .

신청인 소속 :

직위 :

성명 : (인)

용어 설명

- **CVE(Common Vulnerabilities and Exposures) :** 공개적으로 알려진 소프트웨어 보안취약점을 체계적으로 관리하기 위해 취약점이 반견된 연도와 순번을 붙여 만들어진 취약점 데이터베이스로 미국의 마이터(MITRE. 비영리 연구기관)에서 운용, 관리하고 있다.

  (예) CVE-2019-0001 : 2019년 1번째로 식별된 취약점

- **P2P(Peer to Peer)** : 동등 계층간 통신망으로 클라이언트나 서버 개념 없이, 오로지 동등한 계층 노드들(peer nodes)이 서로 클라이언트와 서버 역할을 동시에 네트워크 위에서 하게 된다. 오디오나 비디오, 데이터 등 임의의 디지털 형식 파일의 공유는 매우 보편적이다. 또한, 인터넷 전화(VoIP)같은 실시간 데이터 등도 P2P 기술을 통해 서로 전달될 수 있다.

- **SDR(Software Defined Radio)** : 소프트웨어에 기반한 무선 데이터 전송제어기술을 말한다. 안테나, 고주파(RF) 처리 부분, 배터리 등 무선통신을 위해서 필요 최소한의 기능만을 하드웨어로 구성하고 하드웨어를 제외한 나머지 부분은 주파수, 네트워크, 무선통신 방식에 따라 소프트웨어를 로딩시켜 사용하게 한다. 이 기술을 이용하면 소프트웨어를 조작하는 것만으로 하나의 단말기에서 WCDMA·GSM 등 차세대 이동통신 서비스를 즐길 수 있다.

- **SSRF(Server Side Request Forgery)** : CSRF(Cross Site Request Forgery)와 달리 서버가 직접 호출해서 발생하는 문제이다. 이를 통해서 외부에서 내부망에 대해 접근하거나 스캔하고 각종 보안장비들을 피해갈 수 있다. **SSRF**는 사용자 입력을 받아 서버가 직접 다른 웹이나 포트에 직접 접근해서 데이터를 가져오는 기능들에서 주로 발생한다.