보안 테스트 벤치에서 연결된 자동차, IoT 및 모바일 디바이스

사이버 공격의 경우 일반적으로 고정 네트워크를 통해 인터넷과 통신하는 장치에 중점을 둡니다. 그러나 모바일 사용자는 사물 인터넷의 출현으로 인해 점점 더 중요 해지고 있는 위험에 처해 있습니다. 새로운 테스트 솔루션은 이제 무선 장치의 네트워크 활동을 다루며 보안 격차에 대한 중요한 정보를 제공합니다.

사물 인터넷과 보안

현재 사물 인터넷 (IoT)은 현실보다 더 많은 헤드 라인으로 홈 오토메이션, 웨어러블 및 커넥 티드 카 기술을 통해 일상에 스며들 것입니다. 오늘날 스마트 폰 보다 훨씬 큰 영향을 미칩니다. 통합 무선 모듈을 사용하여 데이터를 교환하고 (종종 민감한) 데이터를 측정하고 값을 원격으로 제어하기 위해 점점 더 많은 장치가 설계되고 있습니다. 인터넷을 통해 통신하는"사물"의 수는 향후 몇 년 동안 급격히 증가 할 것으로 예상되며, 5G가 필요한 네트워크 리소스를 제공 할 때 2020 년 이후 급격한 증가가 예상됩니다 (그림 1).

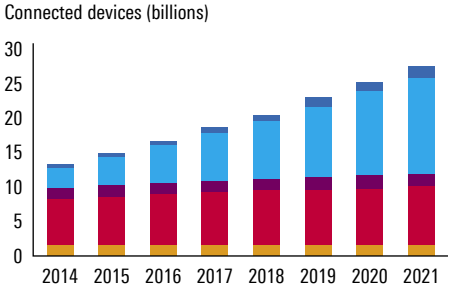
이 개발의 단점은 IT 코어가 있는 모든 무선 장치가 해커에게 잠재적 인 대상이 된다는 것입니다.

WikiLeaks가 최근에 공개 한 사이버 도청 방법으로 인해 이 위협은 유형화되었습니다. 모든 IoT 연결 디바이스는 특히 IoT 구성 요소가 원래 IT 세계 용으로 설계된 제품보다 일반적으로 보호 수준이 낮다는 사실을 고려할 때 잠재적 위험을 나타냅니다. 가격 및 시간 압박에서부터 인식 및 기술 전문 지식 부족에 이르기까지 IT가 2 차 또는 존재하지 않는 역할 (예: 가전 제품)을 수행하는 많은 무선 제품의 보안 기능은 초보적이며 제대로 구현되지 않습니다. 암호화가 없거나 약한 암호화, 개방 포트 (통신 채널) 및 취약한 펌웨어와 함께 설치된 앱은 개발자가 일반적인 IP 연결 보안 표준을 준수하지 않거나 정기적 인 업데이트를 제공하지 않으면 심각한 보안 위험을 나타냅니다. 하나의 약점은 하나 이상의 장치에 대한 무단 액세스를 가능하게 하는 허점을 제공 할 수 있습니다. 광범위하게 손상된 IoT 장치는 네트워크 사업자에게 어려움을 초래할 수 있으며 네트워크 충돌을 일으킬 수도 있습니다.

위험에 처한 회사들

IoT는 아직 초기 단계이지만 고전적인 무선 통신은 전 세계에 있으며 전문 및 개인 환경 모두에서 광범위하게 사용됩니다. 예를 들어 이 두 구체가 서로 섞일 때 회사에게는 문제가 됩니다.(고용주가 "자신의 기기 가져 오기"모토를 따르고 개인 모바일 기기가 업무 목적으로 사용되는 경우) 보호되지 않은 고객 및 회사 정보는 임박한 위험을 초래합니다. 불행히도, 공격자는 모든 보안 격차를 악용하려고 시도해야 합니다. 운영 체제뿐만 아니라 점점 더 많은 앱에 보안 위험이 있습니다. 잘 정리 된 개인 휴대 전화에서 발견되는 수많은 도우미는 잘못 프로그래밍되거나 오래된 앱이 보안 격차를 드러낼 가능성을 높입니다. 최악의 경우 이러한 장치를 통해 전체 회사 네트워크에 액세스 할 수 있습니다. 탈옥 또는 루팅이 운영 체제를 조작하고 기본 보안 기능을 비활성화하면 장치가 위협에 취약 해집니다. 그러나 공격자는 전 세계적으로 2 개의 주요 시스템 만 사용하기 때문에 안전한 원본 운영 체제에서 허점을 찾는 것이 더 나은 대안입니다. 그림 2는 선택된 국가에서 회사 및 정부에서 iOS 및 Android 장치의 비율을 보여줍니다.

IoT devices – expected growth



	15 billion 2015	28 billion 2021	CAGR* 2015–2021
Cellular IoT	0.4	**1.5**	27 %
Non-cellular IoT	4.2	**14.2**	22 %
PC/laptops/tablets	1.7	**1.8**	1 %
Mobile phones	7.1	**8.6**	3 %
Fixed phones	1.3	**1.4**	0 %

* Compound annual growth rate

그림 1 : 사물 인터넷은 곧 "고전적인"인터넷 사용을 능가 할 것입니다.
(출처 : http://blogs-images.forbes.com/louiscolumbus/files/2016/07/Internet-of-Things-Forecast.jpg)

* The article on page 70 presents an alternative solution. BizzTrust from Rohde&Schwarz offers a secure solution for mobile devices that are used for business and personal purposes.

새로운 전력과 테스트 방법이 필요했습니다.

모바일 장치가 위험에 있는지 여부와 설치된 앱이 보안 요구 사항을 충족하는지 여부를 확인해야합니다. 담당 IT 팀의 임무는 회사 환경에서 사용되는 모든 무선 장치가 WLAN을 사용하는지 또는 셀룰러 연결을 사용하는지에 관계없이 데이터를 저장하고 전송하는 데이터의 기밀성과 무결성을 보호하는지 확인하는 것입니다 (악의적 인 두 환경에서 동일하게 작동합니다). 과거에는 장치의 통신 동작을 쉽게 검사 할 수 없었기 때문에이 작업을 수행하는 것보다 설명하기가 더 쉬웠습니다. 인터넷에 연결된 서버, 특히 서버 위치에 대한 분석은 원치 않는 통신에 대한 필수 정보를 제공합니다. 난독 화 기술이 사용되지 않는 한 IP 위치 정보를 사용하여 서버 위치를 식별 할 수 있습니다. 이상이 있는지 더 조사해야하고 필요한 경우 회사 내에서 사용되는 장치에서 소스 앱을 금지해야합니다. 그러나 회사용으로 특별히 개발 된 앱은 특히 보안과 관련하여 예상대로 인증 가능하게 작동해야합니다.

보안 매개 변수가 공개되었습니다.

R&S®CMW500 광대역 무선 통신 테스터는 개발자가 모바일 장치 및 IoT 모듈에 대한 IP 기반 데이터 통신의 보안을 향상시키는 데 크게 도움이됩니다. 새로운 IP 연결 보안 분석보고 모듈 (R & S®CMW-KM052)은 제어 된 테스트 환경에서 실시간 IP 데이터 트래픽 분석을 수행합니다 (그림 3). R&S®CMW500은 또한 모바일 네트워크 또는 WLAN 액세스 포인트를 에뮬레이션합니다. 보안 분석에는 DAU (Data Application Unit)가 필요합니다. DUT에 IP 주소를 제공하고 월드 와이드 웹의 서버와의 연결을 관리합니다.

R & S®CMW-KM052는 데이터 트래픽의 보안 관련 매개 변수를 분석하고 기록합니다. 이를 통해 개발자는 설계 프로세스 초기에 보안 격차를 감지하고 해결할 수 있습니다. IT 직원은 업무용으로 사용되는 모바일 장치가 내부 보안 정책을 준수하는지 확인할 수있는 도구를 제공합니다. 분석 소프트웨어는 사용 된 IP 연결 및 통신 프로토콜에 대한 실시간 통계를 생성합니다.

소프트웨어 모듈을 사용하면 암호 및 장치 IMSI와 같은 사용자 지정 입력을 포함하여 데이터 스트림에서 중요한 정보를 검색 할 수 있습니다. 이 정보가 암호화되지 않은 상태로 전송되면 소프트웨어는 대상 주소, 도메인 이름 및 가능한 경우 소스 앱을 나열합니다.

이 모듈은 SSL / TLS 핸드 셰이크 매개 변수와 서버 위치의 인증서 및 국가 / 도메인 이름도 분석합니다. 클라이언트와 서버가 암호화 방법에 동의하기 위해 사용하는 SSL / TLS 핸드 셰이크는 보안 연결에 필수적이므로 면밀히 검사합니다 (22 페이지의 상자 참조).

R&S® CMW-KM052는 키 설정 및 기타 매개 변수를 포함하여 서버에서 선택한 암호화 제품군뿐만 아니라 통화 설정 중에 클라이언트가 제공하는 암호화 방법 (암호 제품군)을 표시합니다 (그림 4). CMW KM052는 서버가 전송 한 인증서를 분석 할 수도 있습니다.

	Global	France	Germany	Japan	Spain	UK	US	Govt.
iOS	81	50	85	92	33	83	86	82
Android	18	50	14	5	66	16	14	18

그림 2 : 기업 및 정부 기관의 iOS 및 Android 모바일 장치 비율 (출처 : 모바일 보안 및 위험 검토, 2016 년 2 판, MobileIron Security Labs).

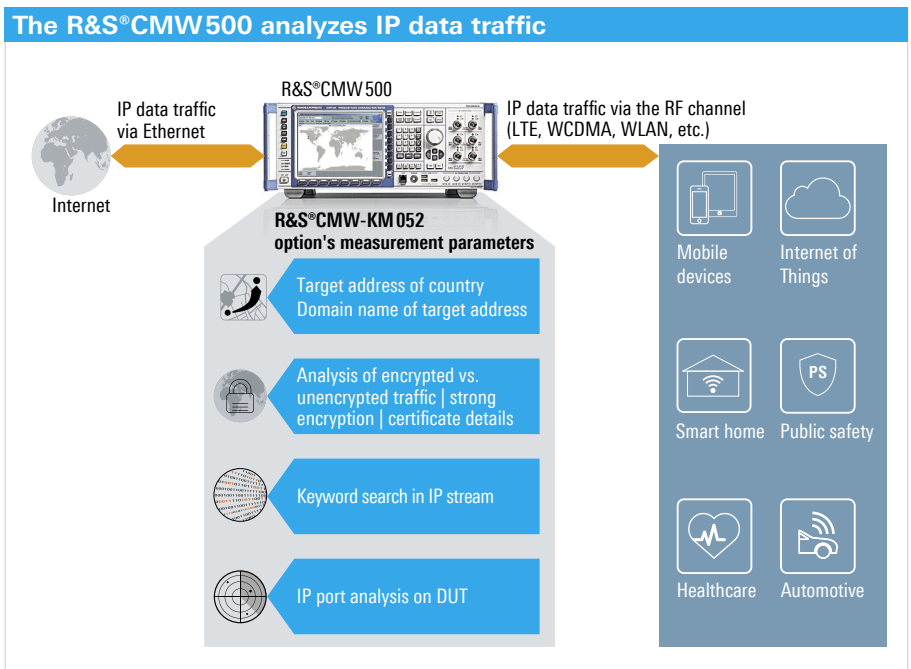
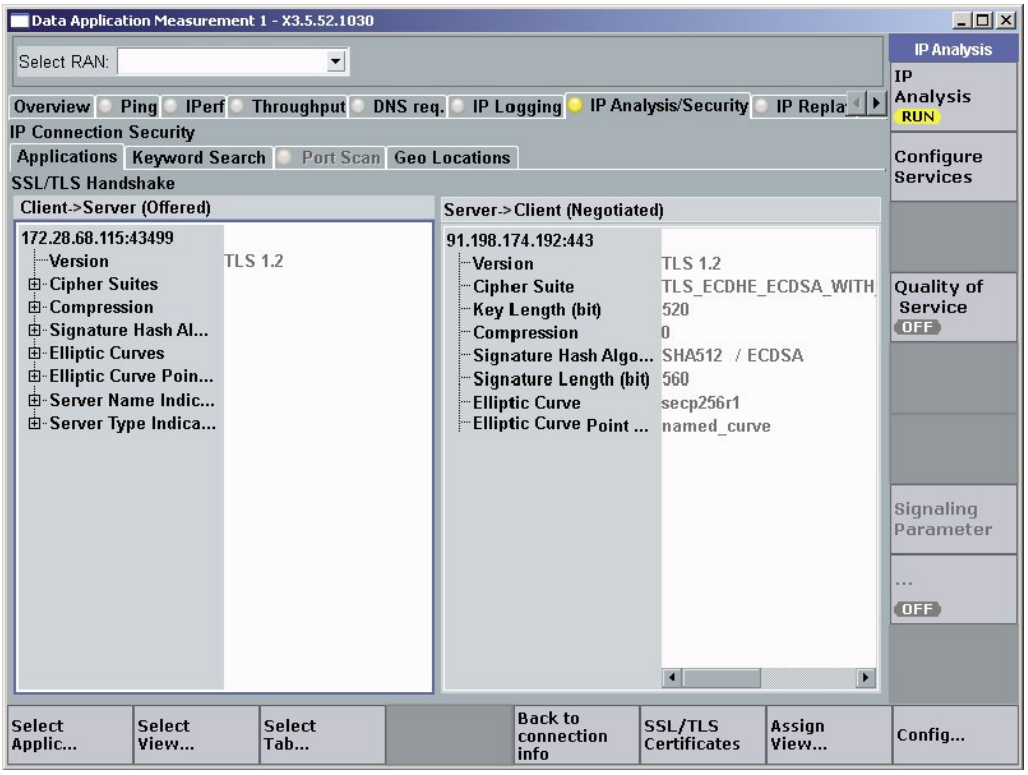


그림 3 : 연결된 모바일 또는 IoT 장치가 송수신하는 데이터에 의해 취해지는“경로”.

R & S®CMW500은 테스트중인 무선 제품과 인터넷 간의 데이터 트래픽을 관리합니다. 방화벽과 유사하게 보안 관련 콘텐츠 (예 : 암호가 암호화되지 않은 상태로 전송되는지 여부

그림 4 : SSL / TLS 핸드 셰이크는 연결 보안을 결정하고 종합적으로 분석됩니다.



소프트웨어 모듈을 사용하면 암호 및 장치 IMSI와 같은 사용자 지정 입력을 포함하여 데이터 스트림에서 중요한 정보를 검색 할 수 있습니다. 이 정보가 암호화되지 않은 상태로 전송되면 소프트웨어는 대상 주소, 도메인 이름 및 가능한 경우 소스 앱을 나열합니다.

이 모듈은 SSL / TLS 핸드 셰이크 매개 변수와 서버 위치의 인증서 및 국가 / 도메인 이름도 분석합니다. 클라이언트와 서버가 암호화 방법에 동의하기 위해 사용하는 SSL / TLS 핸드 셰이크는 보안 연결에 필수적이므로 면밀히 검사합니다 (22 페이지의 상자 참조).

R&S® CMW-KM052는 키 설정 및 기타 매개 변수를 포함하여 서버에서 선택한 암호화 제품군뿐만 아니라 통화 설정 중에 클라이언트가 제공하는 암호화 방법 (암호 제품군)을 표시합니다 (그림 4). CMW KM052는 서버가 전송 한 인증서를 분석 할 수도 있습니다.

통신 동작을 분석 할 때 사용자가 알고 싶어하는 가장 중요한 것 중 하나는 관련 서버의 위치 (국가)입니다. 지리적 위치 (지리적 위치에 따른 IP 주소 할당)를 통해이 정보를 확인할 수 있습니다. IP 도메인은 고유하고 등록되어 있기 때문에 95 ~ 99 %의 현지화가 성공합니다. 도메인 이름은 추가 보안 관련 정보를 제공합니다. 새로운 분석 옵션을 통해 사용자는 보안 문제를 일으킬 수있는 의심스러운 도메인과 원치 않는 국가를 쉽게 탐지 할 수 있습니다 (그림 5).

포트 스캔 기능은 소프트웨어의 또 다른 중요한 보안 기능입니다. 응용 프로그램의 클라이언트와 서버는 포트를 통해 서로 통신합니다. 운영 체제를 통해 네트워크 (서버)에서 서비스를 제공하는 응용 프로그램은 클라이언트가 액세스 할 수있는 포트 (주소)를 엽니 다. 이 포트는 "듣기"상태에서 문의를 기다립니다.

인터넷에 우연히 열려있는 "듣기"상태의 포트는 공격자에게 잠재적 인 게이트웨이입니다. 트로이 목마와 같은 멀웨어는 종종 자유롭게 액세스 가능한 포트를 통해 "백도어"를 엽니 다 (일부 포트는 특정 응용 프로그램 용으로 예약되어 있음). 따라서 R & S®CMW-KM052 옵션으로 측정을 쉽게 구현할 수있는 시스템의 개방 포트를 수시로 검토하는 것이 좋습니다. 분석 도구를 사용하기 위해 DUT에 추가 소프트웨어가 필요하지 않습니다. 테스트는 운영 체제와 무관합니다. 안테나 커넥터가있는 DUT는 케이블을 통해 R&S®CMW500에 연결할 수 있습니다. 커넥터가없는 DUT는로 데슈 바르 즈의 RF 차폐 박스에 수용 할 수 있으며 무선 인터페이스를 통해 R & S®CMW500에 연결할 수 있습니다 (그림 6).

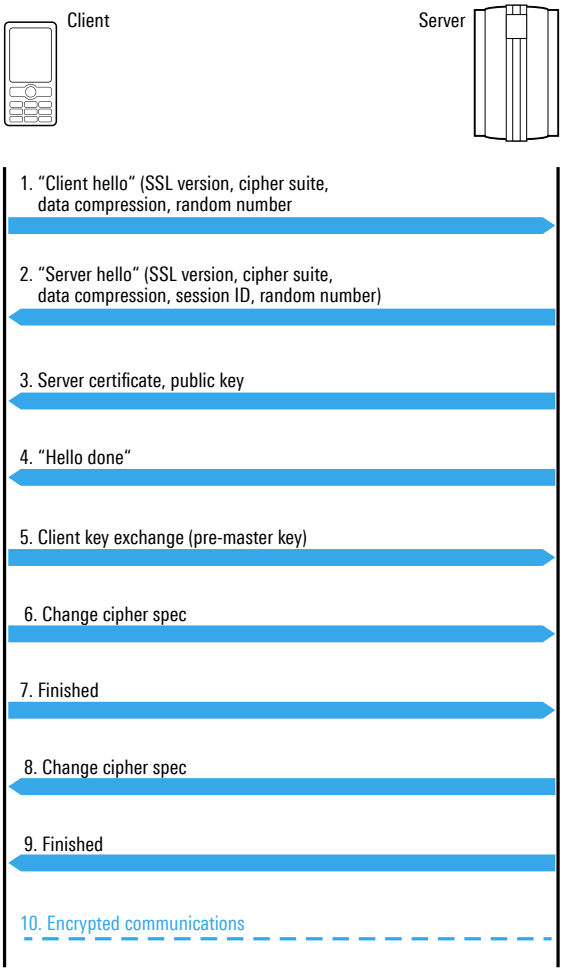
IP 연결 보안

SSL (Secure Sockets Layer)이라고 하는 TLS (Transport Layer Security)는 안전한 온라인 통신에서 중요한 역할을 합니다. SSL 프로토콜의 마지막 버전은 3.0입니다. 그 후, 개발 및 표준화는 버전 1.0부터 새로운 이름 인 TLS로 계속되었습니다.

SSL / TLS는 클라이언트와 서버 간의 통신을 위한 보안 수준을 정의하고 인증서의 신뢰성을 확인하며 세션 키를 협상합니다. 이 모든 것은 SSL 연결 중에 각 연결이 시작될 때 발생합니다.

R&S® CMW-KM052 소프트웨어는 보안 IP 통신 (www.keylength.com에서 제공되는 키 길이 권장 사항)을 위한 강력한 암호화의 중요성 때문에 SSL 핸드 셰이크를 철저히 검사합니다. 명확하게 구성된 매개 변수 목록을 통해 연결이 보안 요구 사항을 충족하는지 쉽게 확인할 수 있습니다 (그림 4).

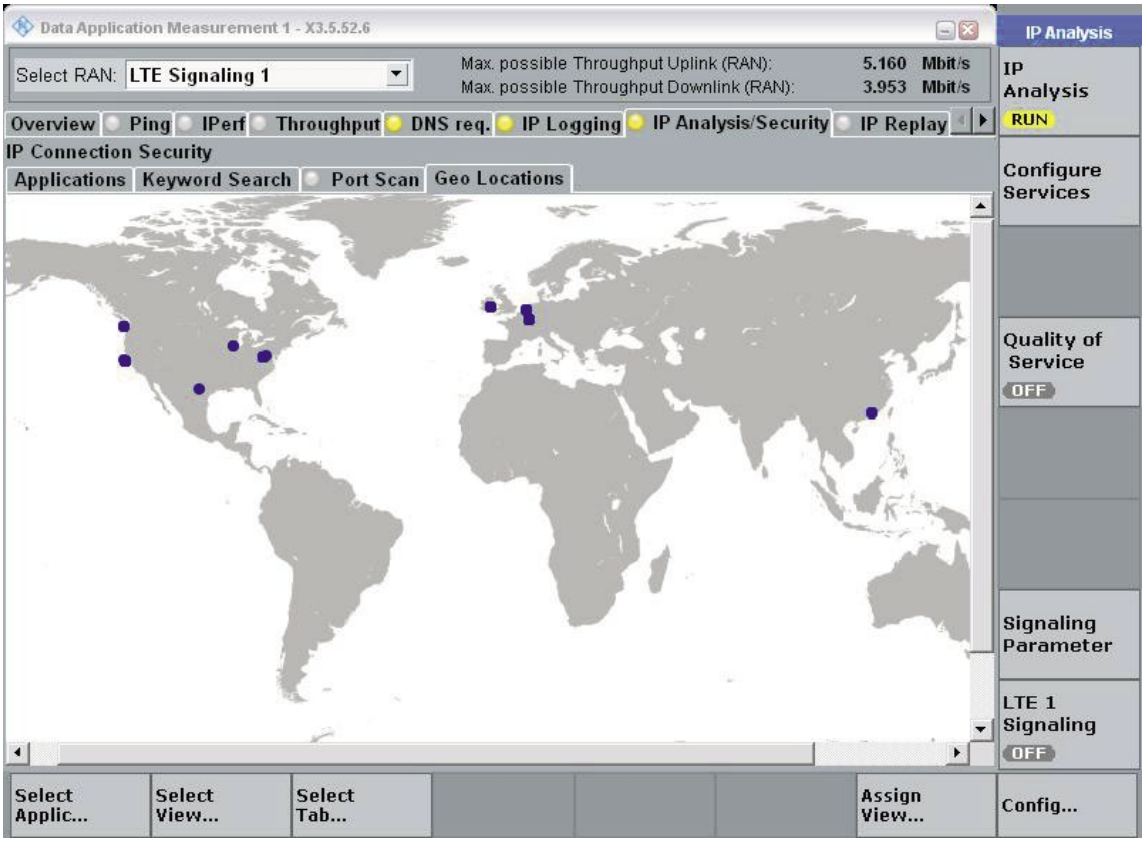
SSL/TLS handshake process



Source: https://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/en_US/HTML/admin231.htm

1. 클라이언트는 SSL 버전, 클라이언트가 지원하는 암호 제품군 및 클라이언트가 지원하는 데이터 압축 방법과 같은 클라이언트의 암호화 기능 (클라이언트 기본 설정 순서로 정렬)을 나열하는 "클라이언트 hello"메시지를 보냅니다. 이 메시지에는 28 바이트 난수도 포함됩니다.
2. 서버는 서버에서 선택한 암호화 방법 (암호 모음) 및 데이터 압축 방법, 세션 ID 및 다른 난수를 포함하는 "서버 헬로"메시지로 응답합니다. 참고 : 클라이언트와 서버가 하나 이상의 공통 암호 스위트를 지원하지 않으면 핸드 셰이크에 실패합니다. 서버는 일반적으로 가장 강력한 공통 암호 제품군을 선택합니다.
3. 서버는 공개 키가 포함된 디지털 인증서를 보냅니다. 클라이언트는 다른 인증서(TrustStore)를 사용하여 이 인증서를 인증합니다.
4. 서버는 "서버 헬로 완료"메시지를 보내고 클라이언트 응답을 기다립니다.
5. 클라이언트는 사전 마스터 시크릿이 포함 된 "클라이언트 키 교환"메시지를 전송하여 서버가 대칭 암호 제품군에 대한 마스터 시크릿을 생성할 수 있도록 합니다. 사전 마스터 비밀은 서버의 공개 키를 사용하여 암호화 되며 이 키로 만 해독 할 수 있습니다.
6. 클라이언트는 또한 마스터 키를 생성하고 키가 변경되었음을 서버에 알리기 위해 "암호 변경 사양"메시지를 보냅니다.
7. 클라이언트는 마스터 키를 사용하여 암호화 된 "완료"메시지를 보냅니다.
8. 서버가 "암호 스펙 변경"메시지로 응답합니다…
9. … 또한 "완료"메시지를 보냅니다.
10. SSL 핸드 셰이크 종료 및 암호화 된 데이터 전송

그림 5 : 특정 IP 주소 및 국가는 데이터 스트림에서 원하지 않을 수 있습니다. 그만큼 R & S®CMW-KM052 옵션은 DUT가 DUT와 접촉하는지 여부를 보여줍니다.



요약

지금까지는 모바일 및 IoT 장치의 데이터 트래픽을 분석하기가 매우 어려웠습니다. 보안 취약점이 오랫동안 발견되지 않을 수 있습니다. R & S®CMW-KM052 분석 옵션이 있는 R&S® CMW500 광대역 무선 통신 테스터가 이 문제를 해결합니다. 사용자는 자유롭게 구성 가능한 제어 무선 환경에서 보안 관련 통신 매개 변수에 대한 자세한 개요를 얻을 수 있으며 장치가 WLAN 및 셀룰러 네트워크에서 다르게 작동하는지 확인할 수 있습니다.

개발자는 설계 프로세스 초기에 보안 격차를 감지 할 수 있습니다. IT 팀은 회사 환경에서 사용되는 스마트 폰, 태블릿 및 앱의 통신 동작을 분석 할 수 있습니다. 자동차 OEM 및 네트워크 운영자는 연결된 자동차 및 IoT 장치가 지정된 연결 보안 표준을 준수하는지 확인할 수 있습니다.

DUT는 준비 할 필요가 없으므로 테스트 순서는 매우 간단합니다. R & S®CMW-KM052 옵션은 강력한 R&S® CMW500 테스트 스위트에 완벽하게 통합됩니다. 단일 T & M 기기를 통해 이제는 셀룰러 및 비 셀룰러 네트워크에서 RF 분석, 프로토콜 테스트 및 IP 애플리케이션 테스트는 물론 IP 데이터 통신을 위한 보안 관련 매개 변수 분석이 가능합니다. 진정으로 독특한 솔루션입니다.

그림 6 : 안테나 커넥터가 없는 DUT를 R&S®CMW-Z10 RF 차폐 상자에 넣고 무선으로 R&S® CMW500에 연결할 수 있습니다.

<크리스천 호프, 로데슈바르즈>

NUBICOM
(주)누비콤

서울본사 서울특별시 영등포구 경인로 775(문래동 3가, 에이스하이테크시티 3동 2층 201호)
TEL: 070-7872-0701 FAX: 02-2167-3801 E-mail: sales@nubicom.co.kr

대전지사 대전광역시 유성구 덕명동로 22번길 10
TEL: 070-7872-0712 FAX: 02-2167-3801 mail: jbkim@nubicom.co.kr