블루투스를 통한 자동차 해킹 위협에 대한 예상과 대응방안에 대한 연구

권구환, 이근호
백석대학교 정보통신학부
e-mail:kwon6594@nate.com, root1004@bu.ac.kr

A Study on the Prediction and Countermeasure of Hacking Threat of Car using Bluetooth

Ku-Hwan Kwon, Keun-Ho Lee
Division of information & communication, Baek-seok University

요 약

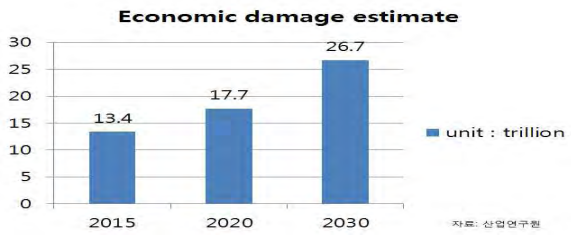
해킹의 범위가 넓어지고 있는 현 시대에는 컴퓨터 통신 장비만을 해킹 하던 과거와 달리 우리가 살고 있는 21세기에는 컴퓨터 시스템에 한정되지 않고 인간이 사용하는 모든 장비에 통신시스템이 설계되면서 해킹이 가능한 장비들의 범주가 증가하고 있고 인간이 사용하는 모든 통신장비를 해킹하는 사례가 증가하는 추세이다. 특히 스마트 자동차가 나오기 시작하면서 스마트 자동차에 대한 해킹의 위험이 높아지고 있는 상황이다. 블루투스에 대한 보안적인 요소들과 보안 취약점 및 대응방안에 대하여 제안하였다.

1. 서론

21세기가 되면서 모든 사물끼리 통신이 연결되어 소통하는 사물인터넷(IoT)이 점차적으로 발달하면서 해킹 등으로 발생하는 피해 규모가 13조 4000억 원에 이를 수 있다는 결과가 나왔다. 국내에 융합보안 피해가 <표 1>의 자료에서 볼 수 있듯이 피해의 규모정도가 점점 커질 것으로 예상된다. 그리고 컴퓨터를 통한 기술이 빠르게 발전하면서 해킹이나 사이버에서 범죄들이 발생하게 되었고, 지능적인 범죄에 영향을 미치고 있다. 사물인터넷과 더불어 자동차도 스마트 자동차가 나오고 있는 시점에서 블루투스를 통한 스마트 자동차의 해킹이 발생하고 있다.

본 논문은 블루투스를 통한 자동차 해킹 위협에 대한 예상과 대응방안에 대한 연구를 분석 평가 하고 그 해킹 공격에 대한 대응방안을 제안한다.

<표 1> 스마트 자동차 등록 대수 증가로 인한 경제적 피해 규모의 증가



2. 관련연구

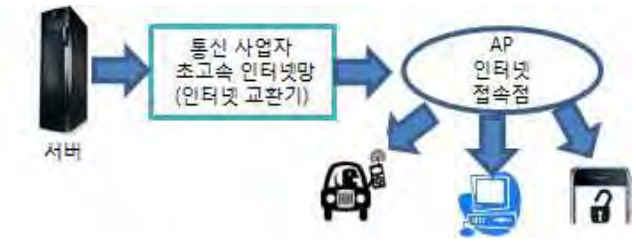
2.1 스마트 자동차 블루투스 해킹 위협

스마트 자동차가 등장하면서 차량 내부에 무선통신망과 텔레매틱스 서비스를 지원하는 차량의 등록 대수가 점점 늘어날 것이며 이로 인해 스마트 자동차의 해킹공격위협도 증가할 것이다. 자동차에서는 블루투스를 이용한 서비스를 사용하는데 블루투스의 경우 통신의 범위가 넓고 빠른 무선 데이터 통신프로토콜을 이용하기 때문에 범죄발생의 빈도와 그 피해가 증가 할 것으로 예상된다.

2.2 블루투스의 원리

블루투스는 주파수 대역이 2.4Ghz 정도이며 다른 시스템들의 간섭을 막기 위해서 사용되었다. 물리적인 케이블의 이용 없이 무선 네트워크를 이용한다. 또한 데이터를 고속으로 송, 수신 할 수 있는 무선 디지털 통신 규격으로 저 전력으로 근거리 무선 통신에 활용되기 위해 제작되었다. 그러나 여러 시스템들과 같은 주파수의 대역을 사용하기 때문에 시스템 간의 전파 충돌이 생길수가 있는데, 이를 예방하기 위해서 블루투스는 많은 수의 채널을 특정한 패턴에 따라서 빠르게 이동하며 패킷을 조금씩 나눠

전송하는 기법인 주파수 호핑 (Frequency Hopping) 방식을 취한다[4].



(그림 1) 블루투스의 원리

3. 블루투스를 이용한 해킹

블루투스의 큰 특징 중에 하나는 기기들의 연결을 위해 사용되는 SDP(Service Discovery Protocol)를 이용하여 서로 연결이 되기 전에 기기간의 이용 가능한 서비스의 가능 여부를 판단하여 알리게 되는데 이것이 취약점이라고 볼 수 있다. 해커들은 이 점을 노리고 통신망에 침투하게 된다. 블루투스는 데이터 교환 시에 정보가 암호화 되지만 정보 암호화의 강도가 약하다. 그리고 제조 시에 PIN 번호가 설정되어 나오는데 이 PIN번호는 공격의 지점으로 형성 되어 있다. 해커들이 랜덤 대입방식을 이용하여 침투할 수 있기 때문이다. 운전자가 시동을 걸게 되면 자동으로 서로 연결하여 작동시키는 페어링 과정으로 들어가게 되는데 그러면서 기본적인 PIN코드 탈취를 통해 사용자의 기기에 연결을 시도 하게 된다. 또한 PIN 번호를 인증 우회의 방식으로 해킹을 시도 한다. 이러한 인증 우회는 스마트폰 해킹처럼 쉬운 방법으로 우회가 가능하다. 사용자들은 해킹을 당하고 있는지도 대상자가 모르기 때문에 사건이 발생하게 되면 매우 위험하다고 볼 수 있다[5].

4. 대응방법

첫째, PIN번호 탈취에 대한 대응방법으로는 그림 2에서 볼 수 있듯이 현재 게임 사이트들이 사용하고 있는 OTP 방식이 있다. 이 프로그램의 경우 사용자가 게임회사의 어플리케이션을 다운받아 가입을 하고 OTP서비스에 가입을 한 후 게임에 접속할 때마다 컴퓨터 모니터 화면에 인증번호가 발생하고 스마트폰의 어플리케이션 안에 인증번호를 입력해야 게임에 접속이 되는 방식을 이용하고 있다.

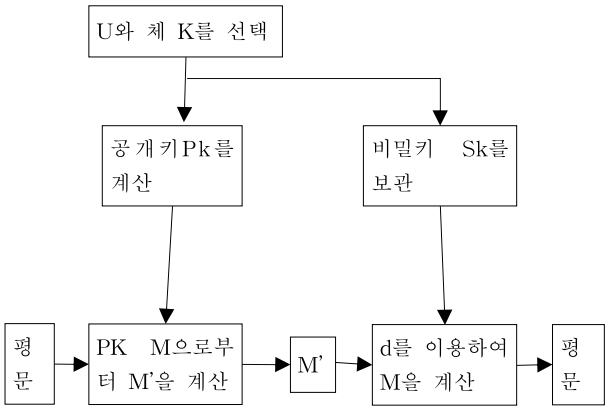
이러한 방식을 활용하여 차량에도 차량사용자가 차량회사가 제작한 통합 어플리케이션을 다운 받아 사용자가 로그인을 하게 되고 어플리케이션 상에서 차량 블루투스 연결이라는 부분을 터치하게 되면 스마트폰 상에 PIN코드의 입력란이 생기고 차량 내부의 LCD 판에 차량 회사의 OTP인증 서버로부터 받은 PIN코드가 나타나게 된다. 회사의 인증 서버를 통해 발급받은 OTP PIN코드를 스마트폰에 입력하게 되면 블루투스와 연동이 되는 방식을 사용

(그림 2) 게임회사에서 사용하고 있는 U-OTP방식

한다. 이렇게 고정된 패스워드 대신에 패스워드가 랜덤하게 생성되는 OTP(One Time Password) 방식을 도입하여 블루투스와 자동차 시스템간의 인증을 할 때 좀 더 안전한 방식의 연동을 대응방안으로 제안하였다.

둘째, 블루투스는 최근까지 사용자의 정보암호화를 위해 알고리즘을 이용하는 4개의 선형 귀환이동 레지스터를 갖고 있는 합산 수열 발생기를 사용해 오고 있다[1]. 즉, 이 수열 발생기 방식은 스트림 암호 방식인데 블루투스에서 사용하는 스트림 암호는 일회용 암호이며 대칭형 암호화의 방식 중에 하나이고 블록 암호화 방식보다 빠르다는 장점을 가지고 있지만 암호화의 강도는 약하다는 단점을 가지고 있다. 반면에 타원곡선 암호화(ECC)방식은 이론상으로는 유한한 시간 안에 복호화 계산이 가능하지만 실제로는 계산이 오래 걸린다는 점을 이용한 암호화 방식이며 공개키 암호 방식인데 짧은 키를 사용하면서도 킷값이 큰 암호체계와 비슷한 수준의 안전성을 제공하고 있다.

그림 3은 ECC의 일반구조를 나타내는 그림인데 먼저 곡선 U와 체 K를 선택하여 공개키(Pk:Public Key)와 비밀키(Sk: Secret Key)를 계산하여 보관하고 공개키를 사용하여 평문과 암호화된 평문(M')를 만들어 전송하여 수신자는 비밀키(Pk)의 역원을 구한 d를 이용하여 복호화 과정을 통해 평문을 구한다.



(그림 3) ECC 암호화의 일반구조

타원곡선 암호는 잉여류 집합 Z_p위에서 정의된 암호로

서 다양한 암호시스템 설계가 용이하고 RSA 암호화 알고리즘에서 1024 비트 수준이 ECC 암호화 알고리즘에서는 160 비트의 짧은 킷값의 효과를 내기 때문에 <표 2>에서 보는 것과 같이 짧은 킷값으로 강력한 암호화 방식을 구현할 수 있는 암호체계라고 볼 수 있다.

<표 2>RSA/DSA와 ECC 암호화 방식의 키 값 차이 분석표

Time to break in MIPS year	RSA/DSA(단위: bits)	ECC (단위: bits)	RSA와 ECC 키 사이즈 비율
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

컴퓨터의 성능이 점점 향상함에 따라 높은 속도로 구현이 가능하게 되었고 메모리의 크기와 비용면에서도 다른 공개키 방식들에 비해서 가장 적게 차지하며 다양한 H/W, S/W로 구현이 용이하다. 또한 공개키를 생성할 시에 1초 이내의 시간이 걸리기 때문에 무선 네트워크와 같은 데이터의 전송량이 상대적으로 열악한 환경에 적합하다. ECC암호는 다양한 타원곡선을 활용하여 암호시스템의 설계가 가능하기 때문에 블루투스에서 전송되는 데이터를 암호화하는데 있어서 응용이 가능할 것으로 보인다.

타원곡선 위에서 ElGamal 암호체계를 적용하여 블루투스 암호화 방식에 적용한다면 더 복잡한 복호화 방식이 필요할 것이다. 암호화와 복호화를 적용하는 과정을 보면 먼저, 타원곡선 U위의 점 P를 선택하고 사용자들이 임의의 정수 e를 선택하고 개인키를 보관하고 eP를 계산하여 공개한다. 수신기 B는 e_B를 선택하여 비밀키를 만들고 $e_B \cdot Q$를 공개한다. 송신기 A가 수신기 B에게 메시지 M을 보내려 한다면 송신기 A는 임의의 정수 k를 선택하여 점들의 순서쌍 $(kP, M+k(e_BP))$를 보낸다. B는 kP에 e_B를 곱하여 e_BkP를 구하고 이를 이용하여 메시지 $M+ke_BP-e_BKP=M$를 얻는다. 이러한 방식으로 암호화 방식을 적용하게 된다면 공격자가 kP와 ka_BP를 도청했더라도 a_B를 계산해야 암호문을 복호화 할 수 있다. 그렇기 때문에 블루투스에서는 타원곡선 암호와ElGAmal 암호화를 적용한 방식을 사용하여 암호화의 강도를 높여야 한다는 대응방안을 제안하였다.

5. 결론

21세기에는 IoT시대가 도래하면서 사회는 많은 변화가 일어났다. 스마트폰, 스마트 자동차 등의 인간 편의를 도모하는 장치들이 나오면서 새로운 문화가 생겨났다. 그러나 새로운 장치와 기술이 나오게 되면 항상 그 속에는 해킹 범죄가 발생하고 그에 대한 공격기법은 점차 지능화되고 있다. 아직까지는 스마트자동차를 해킹하여 문제를 일으킨 사건이 거의 찾아보기 힘들지만 시간이 지날수록 해킹에 의한 피해의 사례는 확대될 것으로 보인다.

본 논문에서는 블루투스에 대한 내용만 다뤘지만 공격루트는 다양할 것으로 보인다. 그렇기 때문에 피해를 입기 전에 대응방안을 철저하게 만들어내고 점검하여 미연에 방지해야한다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)

참고문헌

[1] Hyeong-rak Kim, Hun-jae Lee, Sang-jae Mun “NSG : A Security Enhancement of the E 0 Cipher Using Nonlinear Algorithm in Bluetooth System” The KIPS transactions, 2009

[2] Pyeong-hyeon Cho “A major information and communications infrastructure for a study on the improvement of security vulnerability: Traffic signal control systems, focusing on” M.s dissertation Korea University 2012

[3] 강동호 , 백강호 , 김기영 , “블루투스 보안 기술 ” 정보통신진흥연구원 주간기술동향, 2009

[4] 이인범, 류대현 “블루투스의 보안 취약성과 공격” 한국해양정보통신학회 학술지, 2011

[5] 이민섭 , 정수론과 암호학, 에이콘 출판사, 2007

[6] 육군사관학교 수학과, 암호학 개론, 경문사, 2000