논문 17-42-01-29 The Journal of Korean Institute of Communications and Information Sciences '17-01 Vol.42 No.01
https://doi.org/10.7840/kics.2017.42.1.233

2.4 GHz AES 무선 키보드 공격 시스템 구축에 관한 연구

이 지 우•, 심 보 연*, 박 애 선**, 한 동 국°

A Study on Development of Attack System on the 2.4 GHz AES Wireless Keyboard

Ji-Woo Lee•, Bo-Yeon Sim*, Aesun Park**, Dong-Guk Han°

요 약

최근 무선 키보드, 무선 마우스의 사용이 증가하는 추세에 따라 무선 통신 과정에서의 물리적 취약성을 이용하여 사용자의 입력 정보를 탈취하거나 원격으로 컴퓨터를 제어하는 공격들이 보고되고 있다. 특히 바스틸 네트워크에서 발표한 MouseJack 공격은 각 제조사별 수신기의 취약성을 이용하여 2.4 GHz 무선 키보드 및 마우스를 공격하였다. MouseJack 공격은 기존에 공개된 공격들과는 달리 AES 암호화가 적용된 무선 키보드를 대상으로 공격이 가능하다는 특징이 있다. 하지만 공격에 대한 개요만 설명할 뿐 공격 방법에 대한 구체적인 정보를 제공하지 않는다. 따라서 본 논문에서는 마이크로소프트 2.4 GHz 무선 마우스 패킷 구조를 분석하고 무선 마우스로 가장한 글쇠 주입 공격이 가능한 마우스 패킷 설정 방법을 제안한다. 또한 제안된 패킷을 이용하여 2.4 GHz AES 무선 키보드 글쇠 주입 공격 시스템을 구성하고, 실제 이를 통해 키보드 글쇠 주입이 가능함을 실험을 통해 보인다.

Key Words : AES wireless keyboard, wireless mouse, MouseJack, HID Packet Injection, USB receiver

ABSTRACT

Due to a recent rise in use of a wireless keyboard and mouse, attacks which take user's input information or control user's computer remotely exploiting the physical vulnerability in the wireless communication have been reported. Especially, MouseJack, announced by Bastille Network, attacks 2.4 GHz wireless keyboards and mice through exploiting vulnerability of each manufacturer's receiver. Unlike other attacks that have been revealed, this allows to attack AES wireless keyboards. Nonetheless, there is only a brief overview of the attack but no detailed information on this attacking method. Therefore, in this paper we will analyze the Microsoft 2.4 GHz wireless mouse packet and propose a way to set the packet configuration for HID packet injection simulating a wireless mouse. We also develop a system with 2.4 GHz AES wireless keyboard HID packet injection using the proposed packet and demonstrate via experiment that HID packet injection is possible through the system we built.

Ⅰ. 서 론

최근 휴대성, 편리성 등의 이유로 PC나 노트북에서 무선 키보드, 무선 마우스의 사용이 증가하고 있으며, 특히 2.4 GHz 무선 주파수 통신 기반의 장비는 기존의 저주파수 장비에 비해 반응속도 및 수신 거리가 길

※ 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2013R1A1A2A10062137)
• First Author : Kookmin University Department of Mathematics, jiwoo0412@kookmin.ac.kr, 학생회원
° Corresponding Author : Kookmin University Department of Mathematics, christa@kookmin.ac.kr, 정회원
* Kookmin University Department of Mathematics, qjdusla@kookmin.ac.kr
** Kookmin University Department of Financial Information Security, aesons@kookmin.ac.kr
논문번호 : KICS2016-11-334, Received November 1, 2016; Revised December 6, 2016; Accepted December 6, 2016

어 많이 사용되고 있다. 27 MHz 또는 2.4 GHz ISM 밴드에서 동작하는 프로토콜을 사용하는 무선 키보드는 블루투스(bluetooth)와 달리 산업 표준을 따르지 않고 제품을 생산하는 제조사마다 제품에 사용할 프로토콜을 직접 구현하여 사용한다. 특히 대부분의 제조사는 2.4 GHz 무선 통신을 위해 Nordic사의 nRF24L01 모듈을 이용하며, 사용자가 정의할 수 있는 통신 패킷 내부 영역을 제조사별 프로토콜에 따른 패킷 구조로 변형하여 사용한다. 하지만 인증 절차 없이 통신을 위해 필요한 MAC 주소로 XOR하는 것과 같은 취약한 프로토콜을 사용하기 때문에 이러한 취약점을 이용해 2009년부터 27 MHz 무선 키보드 및 nRF24L01 칩을 사용하는 2.4 GHz 무선 키보드의 물리적 취약성 연구가 활발히 진행되고 있을 뿐만 아니라 무선 키보드의 물리적 취약성 이용하여 사용자의 입력 정보를 탈취하거나 원격으로 컴퓨터를 제어하는 공격들이 계속 보고되고 있다[1-5,9-12]. 이러한 취약성 발표에 따라 최근에는 강력한 암호 알고리즘인 AES(Advanced Encryption Standard)[7]를 사용한 키보드가 개발되어 많은 사용자들이 사용하고 있다.

하지만 아직까지도 취약한 프로토콜을 사용하는 제품들이 많으며, 최근 미국의 보안업체인 바스틸 네트워크(Bastille Network)에서는 시중에 판매되고 있는 다양한 제조사의 무선 키보드 및 마우스의 취약성을 이용한 공격을 발표했다[6]. 바스틸 네트워크에서 발표한 공격은 MouseJack, KeyJack, KeySniffer로 분류되어 있고, MouseJack과 KeyJack은 AES와 같은 강력한 암호화가 적용되어 있는 무선 키보드에 글쇠 주입이 가능한 공격이다. MouseJack 공격 방법에는 공격자가 임의로 구성한 마우스 패킷 신호를 이용하여 키보드 신호를 주입하는 공격이 존재한다. 즉, 공격자는 임의의 글쇠 신호를 무선 마우스 신호로 가장하여 사용자 컴퓨터에 주입함으로써 사용자의 컴퓨터를 악의적으로 원격 제어할 수 있다. 본 공격은 키보드 신호와 달리 마우스 신호는 강력한 암호 알고리즘을 사용하여 암호화되지 않는다는 점과 수신기가 수신된 패킷이 마우스로부터 전송된 것인지 키보드로부터 전송된 것인지 인증하지 않는다는 취약점을 이용한다. 본 공격은 사용자가 AES와 같은 강력한 암호화가 적용된 무선 키보드를 사용하는 환경에서도 공격이 가능하다는 특징이 있다. 하지만 바스틸 네트워크는 임의의 글쇠 정보를 주입하기 위한 무선 마우스 패킷 구성 방법뿐만 아니라 무선 마우스 신호의 패킷 구조 등 실제 공격에 필요한 정보를 공개하지 않는다. 따라서 지금까지 공개된 정보만을 이용해 무선 마우스로 가장한 글쇠 주입 시스템 구성이 불가능하기 때문에 AES 무선 키보드 공격 시스템 구축에 많은 어려움이 존재한다. 또한 지금까지 취약성이 검증된 무선 키보드 및 마우스 모두 해외 제조사 제품으로 국내 제조사 제품에 대한 취약성 검증은 이루어지지 않았다. 뿐만 아니라, 아직 국내 무선 키보드 및 마우스 취약성 평가 기술력은 국외에 비해 미비한 실정이다. 따라서 바스틸 네트워크에서 발표한 취약점을 기반으로 공격 시스템을 구축함으로써 국내 무선 키보드 및 마우스의 취약성 평가 기술력 확보가 필요하다. 앞서 언급했듯이, 대부분의 제조사는 2.4 GHz 무선통신을 위해 Nordic사의 nRF24L01 제품군을 사용하여 통신 패킷 내부 영역을 제조사별로 구현하여 사용한다. 따라서 무선 키보드에 임의로 글쇠를 주입하기 위해서는 공격 대상 제품별 패킷 구조에 대한 자세한 분석이 필요하다. 하지만 여러 연구를 통해 공개된 키보드 패킷 구조와 달리 마우스 패킷 구조에 대한 정보는 아직 보고된 바 없다.

이에 본 논문에서는 마이크로소프트 2.4 GHz 무선 마우스 패킷 구조를 분석하고, 무선 마우스로 가장한 글쇠 주입 공격이 가능한 마우스 패킷 설정 방법을 제안한다. 또한 제안된 패킷을 이용하여 2.4 GHz AES 무선 키보드 글쇠 주입 공격 시스템을 구성하고 실제 이를 통해 키보드 글쇠 주입이 가능함을 실험을 통해 보인다. 본 실험은 공격자가 무선 키보드의 암호키를 모르더라도 사용자의 컴퓨터를 제어할 수 있는 매우 강력한 공격으로, 재전송 공격 대응기법도 적용되어 있는 마이크로소프트 2.4 GHz AES 무선 키보드를 무력화 시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 2.4 GHz 무선 키보드 및 마우스 공격 동향을 소개하고, 3장에서 마이크로소프트 2.4 GHz AES 무선 키보드 및 마우스 패킷 구조 분석 결과와 무선 마우스로 가장한 글쇠 주입 공격 방법을 제안한다. 4장에서는 3장의 공격 방법을 이용하여 실제 환경에서 무선 마우스를 통해 키보드 신호 주입이 가능함을 실험을 통해 보인다. 이후 5장에서 본 논문의 결론으로 마무리 짓는다.

Ⅱ. 2.4 GHz 무선 키보드 및 마우스 공격 동향

지금까지 보고된 2.4 GHz 무선 키보드 물리적 취약성에 대한 대표적인 연구로는 'KeyKeriki v2'[1], 'NHB12'[3], 그리고 'KeySweeper'[4]가 있다. 'KeyKeriki v2'는 2010년 2.4 GHz 무선 키보드의 물리적 취약성을 최초로 발표한 연구로 서로 다른 두 개의 모듈을

공격에 사용했다. 이후 하나의 모듈을 사용하여 신호를 송·수신할 수 있도록 구성된 'NHB12'가 발표되었다. 'KeySweeper'는 앞의 두 공격 수행 시 PC와 공격 장비를 항상 연결해야 한다는 단점을 보완하여 PC와 공격 장비를 연결하지 않고도 원거리에서 신호를 수신할 수 있는 장비를 구성했다. 더하여 'KeySweeper'와 유사하지만 안드로이드 스마트폰을 사용함으로써 신호를 원격으로 송·수신할 수 있는 시스템도 발표되었다[11]. 하지만 지금까지 보고된 연구 모두 장비의 MAC 주소 값으로 XOR하는 약한 암호화 기법이 적용된 마이크로소프트 무선 키보드만을 공격 대상으로 한다는 제한점이 존재한다.

최근 미국의 보안 업체 바스틸 네트워크에서 발표한 MouseJack, KeyJack, KeySniffer 공격[6]은 다양한 제조사의 무선 키보드에 대한 공격이 가능하다. 특히 MouseJack은 AES와 같은 강력한 암호화가 적용되어 있는 무선 키보드에 키보드 신호 주입 공격이 가능하다.

본 장에서는 바스틸 네트워크에서 발표한 MouseJack 공격을 간략히 설명한다.

1) 무선 마우스로 가장한 글쇠 주입 공격

무선 마우스가 키보드 신호를 전달하는 것과 같은 비정상적인 환경을 고려하지 않는 일부 수신기는 전달된 신호가 무선 키보드에서 전달된 것인지 무선 마우스에서 전달된 것인지 확인하지 않는다. 즉, 신호를 전송한 기기 유형과 전달된 신호 유형을 확인하지 않기 때문에 공격자는 키보드 신호를 무선 마우스 신호로 가장하여 사용자의 컴퓨터에 키보드 글쇠 주입이 가능하다.

2) 암호화 무선 키보드 글쇠 주입 공격

최근 무선 키보드의 보안성에 대한 문제가 제기되면서 송·수신 신호에 AES와 같은 강력한 암호화를 적용한 무선 키보드가 증가하고 있다. 이들은 암호화를 적용하여 수신기에 전달하고 수신기에서 복호화를 진행하여 신호를 송·수신하는 방식으로 이루어진다. 하지만 일부 수신기에서는 암호화가 적용된 키보드와 연결되었음에도 불구하고 암호화가 적용되지 않은 일반 키보드의 신호도 받아들이는 취약점이 발견되었다. 이에 공격자는 무선 키보드의 암호화 방식과 암호키를 모르더라도 일반 키보드 신호를 주입하여 사용자의 컴퓨터를 제어할 수 있다.

3) 강제 페어링

무선 키보드 혹은 무선 마우스는 제조사에서 만들어 질 때 페어링 된 수신기만 통신 가능하다. 하지만 일부 제조사에서는 수신기를 잃어버렸을 때 사용자가 또 다른 세트를 구입할 필요 없이 새로운 수신기와 페어링 할 수 있는 시스템을 제공한다. 제조사에서는 임의의 무선 키보드 혹은 무선 마우스가 페어링 되는 것을 막기 위해 '페어링 모드'를 만들었다. 따라서 새로운 기기는 사용자가 페어링 모드를 설정하였을 때만 페어링 될 수 있다. 하지만 일부 수신기에서 페어링 모드를 설정하지 않고도 새로운 기기를 페어링 할 수 있는 취약점이 발견되었다. 이에 공격자는 임의의 무선 키보드를 연결하여 사용자의 컴퓨터를 제어할 수 있다.

하지만 다양한 무선 키보드 및 마우스 공격 방법에 대한 개요만 설명할 뿐, 실제 공격 방법에 대해서는 공개하지 않았다. 따라서 지금까지 공개된 정보만을 이용해 무선 키보드 및 마우스 취약성 검증 수행에 많은 어려움이 있다. 특히 무선 마우스로 가장한 글쇠 주입 공격은 사용자가 AES 암호화 무선 키보드를 사용하는 환경에서도 공격이 가능하다. 따라서 이에 대한 대책을 마련하기 위해서는 공격 방법을 구성하고 실험을 통해 가능성 여부를 확인 후 취약성 대응 방안에 대한 연구가 필요하다.

Ⅲ. 제안하는 2.4 GHz AES 무선 키보드 공격 시스템

본 장에서는 마이크로소프트 2.4 GHz 무선 마우스 패킷을 분석하고, 2장에서 언급된 무선 마우스로 가장한 글쇠 주입 공격 방법을 이용하기 위한 마우스 패킷을 설계하여, 이를 기반으로 2.4 GHz AES 무선 키보드 공격 시스템 구축 방법을 제안한다.

3.1 마이크로소프트 2.4 GHz AES 무선 키보드 및 마우스 패킷 분석

무선 마우스로 가장한 글쇠 주입 공격을 수행하기 위해서는 공격하려는 AES 무선 키보드 및 마우스의 패킷 분석 연구가 선행되어야 한다. 하지만 지금까지 마이크로소프트 2.4 GHz 무선 키보드 분석 연구를 통해 일반 무선 키보드 패킷 구조는 보고된 바 있지만 AES 무선 키보드 및 마우스 패킷 구조는 공개된 자료가 없다. 이에 본 절에서는 마이크로소프트 2.4 GHz AES 무선 키보드 및 마우스 패킷 분석 결과를 소개한다.

3.1.1 패킷 분석 환경

무선 마우스 패킷 분석은 KeySweeper와 유사하게 Arduino 보드와 nRF24L01+ 칩을 기반으로 구성한 실험 장비를 사용하였다. 이때 위 장비로 확인이 어려운 PREAMBLE, CHECKSUM, CRC 값을 확인하기

위해 추가적으로 USRP(Universal Software Radio Peripheral)와 GNU Radio를 기반으로 구축한 SDR(Software Defined Radio) 시스템을 이용하였다.

3.1.2 패킷 분석 결과

마이크로소프트 2.4 GHz 무선 마우스 패킷 구조는 그림 1.과 같고 암호화가 적용되어 있지 않다.

앞서 언급한 바와 같이, 마이크로소프트 2.4 GHz 무선 키보드 및 마우스는 2.4 GHz 무선통신을 위해 Nordic사의 nRF24L01 제품군을 사용한다. 따라서 전체적인 패킷 구조는 일반 무선 키보드의 패킷 구조[1]와 같지만 제조사에서 제어할 수 있는 PAYLOAD 구성 방법이 다르다. 그림 2.는 마이크로소프트에서 제조된 일반 무선 키보드, AES 무선 키보드 및 두 종류의 무선 마우스 PAYLOAD 구성의 차이를 보여주고 있다. PAYLOAD의 길이는 HEADER부터 CHECKSUM까지의 길이를 의미하며, 일반 무선 키보드의 경우 16 바이트, AES 무선 키보드는 20 바이트, 무선 마우스는 19 바이트로 표현된다. AES 무선 키보드는 HEADER 영역을 제외한 16 바이트가 AES 암호화된다. 이 과정에서 임의의 데이터가 추가되어 그림 3.과 같이 'a' 글쇠를 연속적으로 네 번 입력한

PACKET :

1 Byte	5 Bytes	9 Bits	19 Bytes	2 Bytes
PREAMBLE	MAC ADDRESS	PACKET CONTROL	PAYLOAD	CRC

PACKET CONTROL :

6 Bits	2 Bits	1 Bit
PAYLOAD LENGTH	PACKET ID	DISABLE AUTO ACK

PAYLOAD :

4 Byte	2 Bytes	2 Bytes	10 Bytes	1 Byte
HEADER	SEQUENCE ID	META FLAGS	DATA	CHECKSUM

HEADER :

1 Byte	1 Byte	1 Byte	1 Byte
DEVICE TYPE ID	PACKET TYPE ID	MODEL ID	UNKNOWN

그림 1. 마이크로소프트 2.4 GHz 무선 마우스 패킷 구조
Fig. 1. Microsoft 2.4 GHz wireless mouse packet format

	HEADER	128-Bit AES Encryption	
	4 Bytes	16 Bytes	
20:	09 98 8E 01	BC 5B DB 03 D4 36 1F 44 27 8C A4 7F 49 93 FC 9D	①
20:	09 98 8E 01	BC 5B DB 03 D4 36 1F 44 27 8C A4 7F 49 93 FC 9D	
20:	09 98 8E 01	58 46 9D 4F 1C 6B DD 3A 45 C5 00 A7 D5 A8 38 7C	②
20:	09 98 8E 01	58 46 9D 4F 1C 6B DD 3A 45 C5 00 A7 D5 A8 38 7C	
20:	09 98 8E 01	37 5A D5 C5 C3 38 19 07 D7 48 91 DE BB 96 F1 46	③
20:	09 98 8E 01	37 5A D5 C5 C3 38 19 07 D7 48 91 DE BB 96 F1 46	
20:	09 98 8E 01	F4 3A B8 63 0A 12 A2 32 49 25 50 69 91 3A 95 13	④
20:	09 98 8E 01	F4 3A B8 63 0A 12 A2 32 49 25 50 69 91 3A 95 13	

그림 3. AES 무선 키보드 'a' 글쇠 PAYLOAD 변화
Fig. 3. The PAYLOAD change of the 'a' keystroke on AES wireless keyboard

경우 20 바이트 중 HEADER 4 바이트를 제외한 16 바이트가 매번 다른 값으로 표현된다. 따라서 마이크로소프트 2.4 GHz AES 무선 키보드는 재전송 공격이 불가능하다.

HEADER 영역은 기기에 대한 정보를 포함하고 있으며, HEADER 영역의 각 바이트에 대한 값의 의미는 그림 4.에서 확인할 수 있다. 첫 번째 바이트는 암호화 알고리즘 및 적용 여부를 나타내며, 두 번째 바이트를 통해 PAYLOAD의 총 길이를 알 수 있다. 세 번째 바이트인 MODEL ID는 제품 종류에 따라 변하는 값이며, 마지막 바이트의 의미는 확인되지 않았다. SEQUENCE ID는 패킷이 전송될 때마다 하나씩 증가하며, META FLAGS 영역은 일반 무선 키보드의 경우 Ctrl, Alt, Shift 등의 메타 글쇠가 눌릴 때마다 값이 변경되고 그 외에는 0x4300이다. 무선 마우스의 경우 META FLAGS는 신호의 종류와 상관없이 0x4000이다.

그림 5.는 무선 마우스 1의 DATA 영역을 나타내고 있다. 오른쪽, 왼쪽 이동의 경우 이동 거리에 따라 두 번째 바이트의 값이 변경되며, 위쪽, 아래쪽 이동의 경우 또한 이동 거리에 따라 네 번째 바이트의 값이 변경된다. 대각선 이동의 경우 두 가지 동작이 합

	PAYLOAD															
	HEADER				SEQUENCE ID	META FLAGS	DATA									CHECKSUM
	4 Bytes				2 Bytes	2 Bytes	1	2	3	4	5	6	7	8	9	10	11	1 Byte
Normal Wireless Keyboard	0A	78	–	01	XOR Encryption by MAC Address													Type 1
					#	43 00	00 HID 00 00 00 00 00										·	
AES Wireless Keyboard	09	98	–	01	128-Bit AES Encryption													
Wireless Mouse 1	08	90	–	01	#	40 00	클릭 / 좌우 이동 / 상하 이동 / 휠 00 00 01										·	Type 2
Wireless Mouse 2	0A	90	–	01	XOR Encryption by MAC Address													Type 3
					#	40 00	클릭 / 좌우 이동 / 상하 이동 / 휠 00 00 10										·	

그림 2. 마이크로소프트 일반 무선 키보드, AES 무선 키보드, 무선 마우스 PAYLOAD 비교
Fig. 2. PAYLOADs comparison

1st Byte of HEADER	0x0A : XOR Encryption
	0x09 : AES Encryption
	0x08 : Not encrypt
2nd Byte of HEADER	0x38 : 8 bytes PAYLOAD
	0x78 : 16 bytes PAYLOAD
	0x98 : 20 bytes PAYLOAD
	0x90 : 19 bytes PAYLOAD
3rd Byte of HEADER	Products
4th of HEADER	Unknown

그림 4. HEADER 영역 의미
Fig. 4. The meaning of HEADER

	DATA									
	1st Byte	2nd Byte	3rd Byte	4th Byte	5th Byte	6th Byte	7th Byte	8th Byte	9th Byte	10th Byte
Left click	01	00	00	00	00	00	00	00	00	01
Right click	02	00	00	00	00	00	00	00	00	01
Right movement	00	01	00	00	00	00	00	00	00	01
Left movement	00	FF	FF	00	00	00	00	00	00	01
Movement down	00	00	00	01	00	00	00	00	00	01
Movement up	00	00	00	FF	FF	00	00	00	00	01
Wheel up	00	00	00	00	00	01	00	00	00	01
Wheel down	00	00	00	00	00	FF	FF	00	00	01
Diagonal movement	00	01	00	FF	FF	00	00	00	00	01

그림 5. 마이크로소프트 2.4 GHz 무선 마우스 DATA 패킷
Fig. 5. The DATA packet of Microsoft 2.4 GHz wireless mouse

쳐져 표현되며, 이 또한 이동 거리에 따라 두 번째 바이트와 네 번째 바이트의 값이 변경된다. 무선 마우스 2의 DATA 영역은 무선 마우스 1과 거의 유사하나 마지막 열 번째 바이트가 0x10으로 표현되며, PAYLOAD중 SEQUENCE ID부터 DATA까지의 영역에는 MAC 주소와 배타적 논리합(exclusive OR)을 계산한 값이 저장된다.

무선 키보드의 CHECKSUM 계산법은 기존에 보

Type 1	(⊕ *each byte of PAYLOAD*) ⊕ (*reverse of the 2nd MAC Address*) Ex) MAC ADDRESS CD 1E 1C 37 A8 PAYLOAD 0A 78 09 01 ED 04 43 00 00 04 00 00 00 00 00 CHECKSUM (0A ^ 78 ^ 09 ^ 01 ^ ED ^ 04 ^ 43 ^ 04) ^ E1 = 35
Type 2	(⊕ *each byte of PAYLOAD*) ⊕ *0xFF* Ex) PAYLOAD 08 90 03 01 1F B1 40 00 01 00 00 00 00 00 00 00 00 01 CHECKSUM (08 ^ 90 ^ 03 ^ 01 ^ 1F ^ B1 ^ 40 ^ 01 ^ 01) ^ FF = 8B
Type 3	(⊕ *each byte of PAYLOAD*) ⊕ *0x56* Ex) PAYLOAD 0A 90 88 01 63 06 40 00 01 00 00 00 00 00 00 00 00 10 CHECKSUM (0A ^ 90 ^ 88 ^ 01 ^ 63 ^ 06 ^ 40 ^ 01 ^ 10) ^ 56 = 71

그림 6. 마이크로소프트 2.4 GHz 무선 키보드 및 마우스 CHECKSUM 계산
Fig. 6. CHECKSUM calculation of Microsoft 2.4 GHz wireless keyboard and mouse

고된 바 있지만 무선 마우스의 CHECKSUM 계산법은 공개된 자료가 없다. 이는 전송된 신호의 오류를 탐지하는 영역으로, 계산된 CHECKSUM 값과 전송된 CHECKSUM 값이 동일하지 않을 경우 수신기는 신호를 수신하지 않는다. 따라서 본 논문에서는 수신된 신호 분석을 통해 그림 6.과 같이 무선 마우스의 CHECKSUM 계산법을 찾아 수신기가 정상적으로 신호를 수신할 수 있게 구성하였다.

3.2 무선 마우스로 가장한 글쇠 주입 공격 방법

본 절에서는 본 논문에서 제안하는 무선 마우스 패킷 구성을 통해 무선 마우스로 가장한 글쇠 주입 공격 방법에 대해 설명한다.

3.2.1 실험 환경

실험 환경은 그림 7.과 같이 구성하였으며 USRP와 GNU Radio를 기반으로 구축한 SDR 시스템을 이용하여 수행하였다.

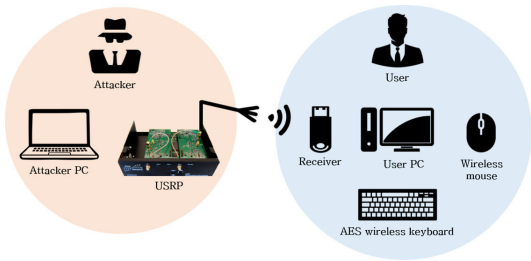


그림 7. 공격 시스템
Fig. 7. Attack system

3.2.2 제안하는 무선 마우스 패킷 구성

본 항에서는 무선 마우스로 가장한 글쇠 주입 공격을 위한 무선 마우스 패킷 구성 방법을 설명한다. 본 논문에서는 무선 마우스로 가장한 글쇠 주입 공격을 위해 무선 마우스 1의 패킷을 그림 8.과 같이 구성하였다. 무선 마우스의 HEADER 영역은 그대로 사용하고 META FLAGS 영역은 그림 9.와 같이 무선 키보드의 META FLAGS 값으로 변형하여 구성한다. 또한 DATA 영역에서 앞의 7 바이트는 무선 키보드의 DATA로 구성하고 마지막 세 바이트는 0으로 채웠다. 이때 마지막 세 바이트는 실험을 통해 키보드 주입 신호와 관련이 없음을 확인하였으며 0이 아닌 랜덤 값으로 채워도 무관하다.

실험 대상 무선 마우스 1은 패킷을 송·수신할 때 암호화를 적용하지 않기 때문에 그림 8.과 같이 패킷을 구성하여 신호를 보내면 수신기는 무선 마우스의

HEADER	SEQUENCE ID	META FLAGS	DATA	CHECKSUM
08 90 – 01	–	43 00		–

1 byte	1 byte	5 bytes	3 bytes
00	HID CODE	00 00 00 00 00	00 00 00

그림 8. 무선 마우스로 가장한 글쇠 주입 공격을 위한 패킷 구성
Fig. 8. Packet configuration for HID packet injection as a pretend wireless mouse

Ctrl	0x4301
Shift	0x4302
Alt	0x4304
Window	0x4308
Ctrl – Alt	0x4305

그림 9. 무선 키보드 META FLAGS 값
Fig. 9. META FLAGS of wireless keyboard

신호로 인식하여 DATA에 포함된 모든 HID CODE[8]을 수신한다. PAYLOAD 영역에 XOR 암호화가 적용되어 있는 실험 대상 무선 마우스 2의 경우도 SEQUENCE ID부터 DATA 영역까지 MAC 주소와 배타적 논리합을 계산하여 패킷을 구성한 후 신호를 보내면 모든 HID CODE 송신이 가능하다. 따라서 암호화가 적용된 무선 키보드와 페어링 된 수신기라도 무선 마우스로 가장한 글쇠 주입 공격에 의해 임의의 글쇠 주입이 가능하다. 특히 공격자는 사용자가 AES 암호화 무선 키보드를 사용하는 환경에서도 임의의 글쇠 주입 공격을 수행할 수 있다.

Ⅳ. 실제 환경에서의 공격 사례

본 장에서는 실제 2.4 GHz AES 무선 키보드를 사용하는 환경에서 구축한 시스템을 통하여 무선 마우스로 가장한 글쇠 주입 공격이 가능함을 실험을 통해 보인다.

공격 장비는 무선 키보드 및 마우스를 사용하는 사용자와 통신이 가능한 범위 안에 존재하고, 사용자는 세트로 구성된 마이크로소프트 2.4 GHz AES 무선 키보드와 무선 마우스를 사용한다고 가정한다. 본 논문의 실험은 그림 7.의 실험 환경과 같이 공격 시스템을 이용하여 공격자가 임의의 프로그램을 인터넷을 통해 사용자의 컴퓨터에 다운로드 및 설치하는 공격을 수행한다.

사용자의 컴퓨터에서 그림 10과 같이 인터넷을 실

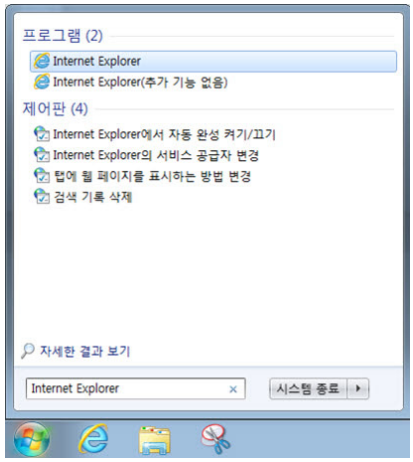


그림 10. Internet Explorer 실행
Fig. 10. Run Internet Explorer

그림 11. 파일 다운로드 링크 주소 값 주입 결과
Fig. 11. The result of file download link address injection

행시키기 위해 'Window' 글쇠 신호를 전송한 후 'Internet Explorer'에 대한 글쇠를 순차적으로 주입하고 'Enter' 글쇠 신호를 전송한다. 이후 인터넷이 실행되면 주소창으로 포인터를 옮겨주는 'F6' 글쇠 신호를 전송하고 프로그램을 내려 받을 수 있는 사이트의 주소를 입력한다. 본 논문에서는 그림 11과 같이 'AhnLab V3 Internet Security 9.0' 설치 파일을 내려 받을 수 있도록 구성한 링크 주소에 대한 글쇠를 순차적으로 주입하고 'Enter' 글쇠 신호를 전송하였다. 이후 설치 파일을 실행하기 위하여 'Alt+r' 신호를 주입하면 프로그램이 설치된다.

이와 같이 실험을 통해 사용자 컴퓨터에 임의의 글쇠를 주입하여 임의의 프로그램을 다운로드 및 설치할 수 있음을 확인하였다. 이에 공격자는 사용자의 컴퓨터를 랜섬웨어와 같은 악성코드에 감염시키는 등 심각한 피해를 입힐 수 있다.

Ⅴ. 결 론

본 논문에서는 무선 마우스로 가장한 글쇠 주입 공격 기반 2.4 GHz AES 무선 키보드 공격 시스템을 구축하였다. 분석 대상으로는 마이크로소프트 2.4 GHz

AES 무선 키보드 및 마우스를 선정하였고 공격에 앞서 무선 마우스의 송·수신 신호를 분석하였다. 이후 무선 마우스 패킷을 임의로 구성하여 무선 마우스를 통해 AES 무선 키보드를 사용하는 환경에 글쇠를 주입 할 수 있는 위협이 존재하는 것을 확인하였다.

마이크로소프트 AES 무선 키보드는 무선 키보드 신호에 임의의 데이터를 추가하여 재전송 공격에 대응할 수 있도록 구성되어 있다. 따라서 암호키를 모르는 공격자는 키보드 신호 송·수신 공격을 수행할 수 없었다. 하지만 바스틸 네트워크에서 발표한 취약점을 기반으로 본 논문에서 공격 환경을 구성한 결과 무선 마우스로 가장한 글쇠 주입 공격은 AES와 같은 강력한 암호화가 적용된 무선 키보드도 무력화 시킬 수 있음을 확인하였다. 이에 공격자는 사용자의 컴퓨터에 랜섬웨어와 같은 악성코드를 주입하는 등 심각한 피해를 입힐 수 있다. 하지만 본 논문의 공격 방법은 현재 마이크로소프트사의 일부 AES 암호화 무선 키보드에 한정되어있고 무선 마우스만을 사용하는 환경에의 적용이 어렵다. 따라서 향후 모든 AES 암호화 무선 키보드 또는 무선 마우스만 사용하는 환경에서도 공격이 가능할 수 있도록 일반화하는 연구를 진행할 계획이다.

또한 현재 취약성이 검증된 무선 키보드 및 마우스는 모두 해외 제품으로 국내 제품에 대한 취약성 검증은 이루어지지 않고 있다. 따라서 이러한 실험 결과를 기반으로 국내 무선 키보드 및 마우스의 취약성 평가 기술력 또한 확보할 수 있음이 기대된다.

References

[1] T. Schröder and M. Moser, *KeyKeriki v2.0 – 2.4 GHz*(2010), Retrieved Oct., 28, 2016, from http://www.remote-exploit.org/articles/keykeriki_v2_0__8211_2_4ghz/.

[2] T. Schröder and M. Moser, *KeyKeriki v1.0 – 27 MHz*(2009), Retrieved Oct., 28, 2016, from http://www.remote-exploit.org/articles/keykeriki_v1_0_-_27mhz/.

[3] Travis Goodspeed, *Promiscuity is the nRF24L01+'s Duty*(2011), Retrieved Oct., 28, 2016, from http://travisgoodspeed.blogspot.kr/2011/02/promiscuity-is-nrf24l01s-duty.html.

[4] S. Kamkar, *KeySweeper*(2015), Retrieved Oct., 28, 2016, from http://samy.pl/keysweeper/

[5] S. J. Lee, "Study about vulnerability to 2.4GHz wireless keyboard with Arduino," M.S. Thesis, Kookmin university, 2015.

[6] Bastille Network, *MouseJack*(2016), Retrieved Oct., 28, 2016, from https://www.bastille.net/technical-details.

[7] NIST, "Announcing the Advanced Encryption Standard(AES)," FIPS PUB-197, Nov. 2002.

[8] Universal Serial Bus, *HID Usage Tables*, Oct. 2004.

[9] H. Y. Kim, "Study on the electromagnetic signal analysis of 27MHz wireless keyboards," M.S. Thesis, Kookmin university, 2014.

[10] H. Y. Kim, B. Y. Sim, A. S. Park, and D. G. Han, "Analysis of 27MHz wireless keyboard electromagnetic signal using USRP and GNU radio," *J. Korea Inst. Inf. Security and Cryptol.*, vol. 26, no. 1, pp. 81-91, Feb. 2016.

[11] S. J. Lee, A. S. Park, B. Y. Sim, S. S. Kim, S. S. Oh, and D. G. Han, "Building of remote control attack system for 2.4 ㎓ wireless keyboard using an android smart phone," *J. Korea Inst. Inf. Security and Cryptol.*, vol. 26, no. 4, pp. 871-883, Aug. 2016.

[12] M. F$\ddot{a}$hnle and M. Hauff, "Analysis of unencrypted and encrypted wireless keyboard transmission implemented in GNU radio based software-defined radio," *Univ. of Appl. Sci. Inst. Commun. Technol.*, *Hochschul Ulm,* 2011.

이 지 우 (Ji-Woo Lee)

2013년 2월~현재 : 국민대학교 수학과

<관심분야> 부채널 분석 및 대응법, IoT 정보보호 기술

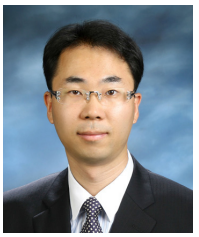
심 보 연 (Bo-Yeon Sim)

2013년 2월 : 국민대학교 수학과 졸업
2015년 2월 : 국민대학교 금융정보보안학과 석사
2016년 3월~현재 : 국민대학교 수학과 박사과정
<관심분야> 공개키 암호 시스템, 부채널 분석 및 대응기법 설계, 경량 ·저전력 정보보호 기술

박 애 선 (Aesun Park)

2011년 2월 : 국민대학교 수학과 졸업
2013년 2월 : 국민대학교 수학과 석사
2014년 3월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 부채널 분석 및 대응법, 신호처리, 스마트 카드 평가, Post-quantum cryptography

한 동 국 (Dong-Guk Han)



1992년 2월 : 고려대학교 수학과 졸업
2002년 2월 : 고려대학교 수학과 석사
2005년 2월 : 고려대학교 정보보호대학원 박사
2004년 4월~2005년 4월 : 일본 Kyushu Univ. 방문연구원
2005년 4월~2006년 4월 : 일본 Future Univ. -Hakodate. Post.Doc.
2006년 6월~2009년 2월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재 : 국민대학교 수학과 부교수
<관심분야> 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술