임베디드 시스템의 RDP¹⁾와 ARP 취약점 분석 및 해결방안

정이원*, 허태겸* *대구대학교 정보보호영재교육워

RDP and ARP Vulnerabilities on Embedded Systems

Yi Won Chung*, Tae Gyeom Heo*
*Information Security Institute for the Gifted, Daegu University

요 약

본 연구에서는 임베디드 시스템을 이용함에 있어서 ARP와 RDP Bluekeep 취약점을 분석하고 가상 임베디드 머신에 대한 모의 해킹으로 관련 시스템의 취약점이 미치는 부정적인 파급효과를 규명하였다. 또한, 본 연구결과는 RDP Bluekeep 취약점을 통해 관리자 권한을 쉽게 탈취할 수 있다는 점 그리고 ARP Spoofing 기법을 통해 클라이언트의 각종 프로토콜로 진행되는 통신의 내용을 유출할 수 있다는 점을 실증적으로 보여준다. 이러한 취약점에 대한 분석을 통해 해결방안을 제시하고자 하였다.

ABSTRACT

This study examines the ARP and RDP Bluekeep vulnerabilities on using Embedded Systems and identifies the possible implications of such vulnerabilities by performing penetration testing on virtualized embedded machines. Furthermore, this study elaborates on that the Administrative privileges can be easily taken away through the RDP Bluekeep vulnerability, and that all packets containing communication information of various protocols could be severely leaked by the ARP Spoofing method. The result of this study presents the solutions for these vulnerabilities.

I. 서론

본 연구에서는 기업체, 교육 및 공공 기관에서 사용하는 임베디드 시스템의 여러가지 취약점을 분석하고 이를 악용할 수있는 가능성과 해결방안에 대해 살펴보고자 한다.

Bluekeep 취약점 (CVE-2019-0708)을 통해 Use After Free 메모리 공격 기법을 이용 하여 관리자 권한에 접근하는 것과 ARP Spoofing을 이용하여 실제 라우터를 가장함 으로써 클라이언트의 모든 패킷을 탈취하 는 중간자 공격을 통한 직접적 정보 탈취 등의 공격 방법이 이를 뒷받침한다.

이러한 기초적인 공격으로 쉽게 개인정보 및 사생활 유출이 발생할 수 있는데 이는 곧 기업 또는 법인에 금전적 손실을 초래 할 수 있고 사회적으로 큰 타격을 입힐 수 있다. 따라서 이러한 손실과 타격을 입히는 행위에 대하여 대응할 수 있는 대책을 모 색하기 위해 최대한 비슷한 형태로 구성한 가상 머신을 토대로 본 연구를 진행하였다.

¹⁾ Remote Desktop Protocol: 원격 데스크톱 프로토콜

Ⅱ. 배경 지식

2.1. 임베디드 시스템

임베디드 시스템은 기계나 기타 제어가 필요한 시스템에 대해, 제어를 위한 특정 기능을 수행하는 컴퓨터 시스템으로 장치 내에 존재하는 전자 시스템이다. 대표적인 임베디드 시스템으로는 은행 ATM, 자동차 내비게이션, 슈퍼마켓의 결제용 컴퓨터 또 는 공공기관의 안내용 키오스크가 있다. 임 베디드 시스템의 안정성을 추구하는 특성 상 윈도우 7과 그 이전의 운영체제를 사용 하고 있는 기기들이 매우 많다.

2.2. ARP Spoofing

ARP Spoofing은 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 이 공격은 데이터 링크 상의 프로토콜인 ARP를 이용하므로 근거리 통신에서만 사용할 수있는 공격이다.

2.2. Use After Free 취약점

메모리의 heap 영역에서 할당된 공간을 비우고 다시 사용할 때 일어날 수 있는 취 약점이다. 메모리 블록이 비할당되고 난 뒤 그에 상응하는 포인터가 NULL 값으로 설 정되지 않고 다음에 그 메모리 블록이 사 용되려는 그 순간 메모리의 코드를 수정하 면 원하는 코드를 실행하게 할 수 있다.

2.3. RDP

RDP (Remote Desktop Protocol)은 원격 접속용으로 개발된 프로토콜로, 다른 컴퓨터에 세션 할당 방식으로 GUI (그래픽 사용자 인터페이스를) 제공하는 프로토콜이다. TeamViewer의 원격 데스크톱과 같이 로그인된 상태에서 화면을 공유하는 것이 아닌자체의 세션 기반이므로 다른 컴퓨터에서 대상 컴퓨터로 로그인을 하면 대상 컴퓨터의 계정은 자동으로 로그아웃이 되는 특징이 있다.

2.4. NAC

네트워크 접근 제어(Network Access

Control)는 바이러스 백신, 호스트 침투 방지, 취약점 분석과 같은 보안 기술, 사용자 또는 시스템 인증, 그리고 네트워크 보안을하나로 묶으려는 시도를 의미한다. 본 연구에서는 여러 세트의 프로토콜을 이용하여보안정책을 정의하고 실행하고자 한다.

III. 본론

3.1. 네트워크 모델링

본 논문에서는 임베디드 시스템을 원격 조종으로 관리하는 컴퓨터로 정의한다. 이 러한 네트워크는 이를 운용 목적의 특성상 보안 장비에 높은 비중의 투자가 이뤄지지 않는 것이 일반적 특징이다.

3.2. 취약점 분석

(1) ARP Spoofing으로 패킷 감청

특정 패킷이 telnet이나 SSL을 사용하지 않는 웹 같은 데이터가 암호화되지 않는 프로토콜은 사용해서 전송될 경우 패킷을 얻을 수 있으면 무단 정보 탈취가 손쉽게 이루어진다. 단순히 단일 클라이언트에 프록시 서버를 설치하여 패킷을 감청하는 것도 가능한 것에서 같은 네트워크망 내에 있으면 이루어질 수 있는 ARP Spoofing, Router Hijacking을 통해서 공격할 수 있다.

다음 실험은 ARP Spoofing의 시연을 통하여 공격 대상 컴퓨터의 패킷을 탈취해오는 중간자 공격을 요약해 제시한 것이다. 실험하는데 이용한 컴퓨터는 두 대이며, 공격자인 Kali Linux와 공격 대상의 Windows 10의 운영체제가 각각 설치되어 있다.

첫 번째 절차는 두 컴퓨터의 IP를 파악하는 것이다. 공격 대상은 (192.168.1.105), 공격자는 (192.168.1.103)인 것을 확인한다.

<그림 1 - 공격자의 IP와 MAC Address²)>



<그릮 2 - 공격 대상의 IP>

다음으로 게이트웨이인 (192.168.1.1)의 MAC Address를 파악한다.

____ 인터페이스: 192.168.1.105 --- 0x3 인터넷 주소 물리적 주소 192.168.1.1 e8-94-f6-e2-e4-d0

<그림 3 - 라우터의 실제 MAC Address>

공격자에서 라우터 에뮬레이터인 fragrouter 를 통해 가상 라우터를 생성한다.

root@kali:~# fragrouter -B1
fragrouter: base-1: normal IP forwarding

<그림 4 - fragrouter 가상 라우터 생성>

공격 대상에게 공격자가 라우터로 가장하기 위해 ARP Reply를 전송한다.

root@kali:~# arpspoof -i eth0 -t 192.168.1.105 192.168.1.1 0:c:29:ba:51:bl 98:83:89:85:65:2c 0806 42: arp reply 192.16 :51:bl 0:c:29:ba:51:bl 98:83:89:85:65:2c 0806 42: arp reply 192.16 :51:bl

<그림 5 - arpspoof로 공격 대상을 스푸핑>

그런데 공격 대상의 모든 패킷이 공격자로 전달하게 되면 패킷들이 진짜 라우터에 도달하지 않아 공격 대상의 인터넷 연결이 끊어지게 되므로 진짜 라우터에 패킷을 전달하기 위해 똑같이 공격자가 공격 대상을 가장하여 ARP Reply Packet을 전송한다.

root@kali:~# arpspoof -i eth0 -t 192.168.1.1 192.168.1.105
0:c:29:ba:51:b1 e8:94:f6:e2:e4:d0 0806 42: arp reply 192.10
ba:51:b1
0:c:29:ba:51:b1 e8:94:f6:e2:e4:d0 0806 42: arp reply 192.10
ba:51:b1

<그림 6 - 실제 라우터를 스푸핑>

라우터의 IP 주소에 할당된 MAC Address가 공격자의 것임을 확인할 수 있다.

인터페이스: 192.168.1.105 --- 0x3 인터넷 주소 물리적 주소 192.168.1.1 00-0c-29-ba-51-b1

<그림 7 - 변조된 MAC Address>

2) Media Access Control Address: 데이터 링크 계층에 소속된 인터페이스에 할당되는 주소 이제 공격 대상의 모든 패킷이 공격자의 컴퓨터로 전송되므로 공격자가 Wireshark 패킷 캡처 프로그램을 실행하여 패킷을 캡 처하고 공격 대상 컴퓨터에서 (https://www. google.com/)에 접속하면 다음과 같이 공격 대상의 IP 주소에서 전송되는 패킷이 나타 나는 것을 확인할 수 있다.

192.168.1.105 172.217.27.78 TCF

<그림 8 - 전달되는 공격 대상의 패킷>

(2) RDP Bluekeep

최근에 발견된 BlueKeep 취약점(CVE-2019-0708)의 경우 패치 권고안에 따르면 공격자는 인증 없이도 서버에 코드 실행이 가능해진다. 보안업체 Errata Security 조사(2019)에 의하면 약 95만대의 윈도우 시스템이 해당 취약점에 노출되어 있는 것으로 조사되었다. RDP는 연결 과정에서 클라이언트가 서버에 정적 채널을 요청하면 서버는 요청된 채널에 대하여 채널 번호를 할당하고 해당 채널을 통해 통신하게 된다.

Microsoft에서 배포한 보안 패치를 Hexrays의 IDA Pro 프로그램을 이용하여 분석해보면 채널 번호와 객체를 바인딩하는 "_IcaBindChannel" 함수가 변경된 것을 확인할 수 있다. "_IcaBindChannel" 함수 호출전에 "MS_T120" 문자열이 존재할 경우 세번째 인자가 강제로 31로 변경되도록 패치되었다.

<그림 8 - 패치된 _IcaBindChannel>

취약점에 노출된 "MS_T120" 채널은 일반적으로 요청되는 채널이 아니고 이미 할당되어 있다. 그런데 사용자가 명시적으로 "MS_T120" 채널을 요청할 경우 임의의 번호와 "MS_T120" 객체가 바인딩 된다. 이렇게 하나의 객체에 두 개의 채널 번호가 할

당되면 마지막에 해당 채널이 두 번이나 비할당되면서 메모리 오류가 발생하여 Use After Free(UAF) 취약점을 사용할 수 있다.

해당 함수의 라이브러리를 분석해보면 "_IcaCopyDataToUserBuffer"를 호출하는 함수와 "_MCSPortData" 함수를 찾을 수 있는데 전자의 함수는 아래의 일정량의 데이터를 EAX 레지스터로 전송할 수 있게 한다.

<그림 9 - 전송 문자열의 일부가 EAX에 할당>

후자의 함수는 CPU의 EAX 레지스터값이 2일 경우 "_MCSChannelClose" 함수를 호출하며 해당 채널 객체를 비할당 한다. Microsoft에서 배포한 RDP 패킷 매뉴얼과 위에 HGFE 문자열이 할당된 것을 토대로 다음과 같은 패킷을 전송하면 시스템이 크래시 된다.

#모든 채널 비할당 요청

#TPKT Header "\x03\x00\x00\x09"

PER encoded PDU "\x02\xf0\x80"

shutdownRequestPduData " $\times 21 \times 80$ "

<표 1 - 시스템 크래시 RDP 패킷>

위 패킷에서 "모든 채널 비할당 요청" 대 신 다른 요청을 하여 관리자 권한을 탈취 할 수도 있다.

IV. 결론

본 연구에서는 임베디드 시스템의 네트워크에 대한 여러 가지 취약점을 분석하고 ARP Spoofing 공격 기법과 RDP Bluekeep취약점을 이용하여 가상 머신에 대한 모의

해킹을 하였다. 이를 통해서 위험성을 검증하였으며 통합 보안관리 솔루션의 필요성을 시사하였다.

ARP Spoofing의 경우 네트워크 스위치별로 MAC 주소를 동적 형태가 되어 실시간으로 Gateway를 찾는 방식이 아닌 고정형태로 설정이 되어야 하고 스파이웨어 같은 경우 관리자에 의해서 검증이 된 프로그램만 설치해야 한다. RDP 취약점의 경우에는 RDP 프로토콜을 최대한 내부에서만사용해야 하고 사용이 불가피할 때에는 고급수준의 네트워크 인증 절차를 도입함과더불어 RDP의 개발사인 Microsoft 사에서정기적으로 긴급하게 배포되는 보안 패치를 신속하게 설치하는 것, 그리고 Snort와같은 네트워크 침입 감지 및 방지 시스템을 통해 "MS_T120" 문자열을 필터링함으로써 문제를 방지할 수 있다.

이를 기반으로 통합적으로 관리할 수 있는 NAC 솔루션이 충분히 개발될 수 있을 것이며 상용화가 되면 효용성이 뛰어나 이 익창출의 가능성이 클 것으로 예상된다.

향후 연구과제로는 Snapshot 형식으로 배포할 수 있어 관리가 쉬운 클라우드 컴퓨팅이라고 할 수 있다. 그래서 클라우드 컴퓨팅을 상용화하는데 비용을 절감하는 방법과 빠른 속도를 유지하여 효율성을 높일수 있는 프로토콜과 임베디드 시스템용 Zero Client(클라우드 서버 접속 전용 운영체게 탑재 기기)에 대한 연구를 이어 나가야 할 것이다.

[참고문헌]

- [1] 황현욱, 박은신, 박종백 (2001). ARP Spoofing 공격과 대응방법에 관한 연구. 한국통신학회학술대회논문집, (), 1821-1824.
- [2] "CVE-2019-0708", 이글루 시큐리티 블로그, 2019년 7월 3일 수정, 2019년10월23일 접속, http://www.igloosec.co.kr/BLOG_BlueKeep%20(CVE-2019-0708)
- [3] "CVE-2019-0708 Proof of Concept", GitHub, 2019년 5월 31일 수정, 2019년11월16일 접 속, https://github.com/n1xbyte/CVE-2019-0708