단위취약성 분석을 통한 무선랜 취약점 분석 방법

김동현, 고경희, 김형종, 신동훈*
*한국정보보호진흥원
e-mail:dhkim@kisa.or.kr

WLAN Vulnerabilities Analysis by AV analysis

Dong-Hyun Kim, Kyoung-Hee Ko,
Hyung-Jong Kim, Dong-Hoon Shin*
*Korea Information Security Agency

요 약

최근 무선 네트워크의 이용이 증가하고 있다. 일반적으로 무선 네트워크 환경은 유선 네트워크 환경보다 취약한 것으로 알려져있다. 본 논문에서는 무선랜 취약점과 이동 단말 운영체제 취약점 분석에 단위 취약성과 복합 취약성을 이용한 취약점 분석 방법을 적용하여본다. 단위 취약성 분석 방법은 Bishop의 가설을 바탕으로 보안 취약성 평가를 위한 시뮬레이션에 적용할 수 있도록 구체화한 것이다. 이를 통하여 단위 취약성 분석방법이 무선 환경까지 적용가능한지를 알아보고, 그 특성을 알아본다.

1. 서론

최근 무선 네트워크의 성능이 향상되고, 사용자의 요구가 이동성을 추구하는 방향으로 진행되어 감에 따라 무선 환경에서의 인터넷 서비스가 증가하고 있다. 3세대 이동통신 서비스인 IMT-2000 서비스가 개시되었으며, 무선 랜 서비스 지역도 점차 확대되고 있다. 일반적으로 무선 환경은 유선환경보다 취약한 것으로 알려져 있다. 서비스 구조가 무선환경으로 확대됨에 따라 무선 네트워크 환경의 취약점에 대한 보안 권고 및 분석의 필요성이 증대되고 있다.

무선랜은 무선 네트워크 중에서 가장 널리 사용되고 있으나, 다양한 취약점을 내재하고 있다. 현재 무선랜 관련한 취약점 보고는 각종 취약성 데이터베이스에 두드러지게 나타나고 있지는 않고, 논문이나 기사를 통하여 위험성이 강조되고 있다. 이동 단말기 운영체제 취약성 역시 최근 PDA의 사용자가 급격하게 증가함에 따라 취약성 분석의 필요성이 증대되고 있다. 본 논문에서는 단위취약성과 복합취약성 개념을 무선 랜의 취약점과 이동단말 운영체제 취약점 분석에 적용한다. 이를 통하여, 기존의 유선환경에서의 취약성 분석에 사용하였던 단위 취약성 분석 방법이 무선 환경에서의 취약성까지 적용 가능한지를 검증하고, 그 특성을 분석한다.

2. 단위취약성 분석 방법

2.1 Bishop의 취약점 분석[1]

Bishop은 모든 취약점은 취약점의 기본 특징 집합(basic characteristic set)인 최소 크기의 unique하고, Sound한 특징 집합을 가지고 있다는 가설을 세웠다.

Bishop의 가설

- 어떤 취약점에 대해서 기본 특징 집합(basic charact-eristic set)을 정의할 수 있다.
- 여러 취약점 집합의 특징 집합을 정의할 수 있다.
- 어떤 시스템의 complete 특징 집합의 크기는 전체 취약점의 그것보다 작다.
- 각 특징들은 시스템이나 프로그램을 분석하기 위한 툴의 개발에 사용될 수 있다.

2.2 단위 취약점과 복합 취약점을 이용한 취약점 분석

단위 취약점과 복합 취약점을 이용한 취약점 분석은 Bishop의 취약점 분석 가설을 취약성 평가를 시뮬레이션에 적용할 수 있도록 구체화하고 개선한 것이다.[2] AV를 이용해서 분석한 취약점 데이터는 시뮬레이션에서 보안관점에서 중요한 상태와 상태전이 함수로 활용된다.

본 논문에서 취약점이라고 할 때, 이것은 일반적인 취약성 DB에서 식별번호를 부여하여 다루고 있는 하나의 토픽이며, CVE 코드 하나에 대응되는 것이다. 취약점이란 보안 정책에 위배를 가져오는 결함이며 이를 복합 취약점(CV, Compound Vulnerability)라고 칭한다. 특별한 언급이 없는 경우 취약점은 복합취약점을 말한다. 그리고 이 CV가 악용 가능한 세부 원인을 단위 취약점(AV, Atomic Vulnerability)라 한다.

시뮬레이션에서 사용하는 단위 취약점은 Name, Type, Category, 상태 전이 함수, 상태집합, 공격입력의 6 가지 요소로 이루어진다. 본 논문에서는 단위 취약점의 요소 중 각 단위 취약점을 구분할 수 있는 요소만을 고려하여 사용한다. 복합 취약점은 단위 취약점을 이용하여 분석한다. 단위 취약점들은 4 가지의 이항 연산자를 이용하여 하나의 복합 취약점을 표현한다.

- AND : 두 AV 모두가 참인 경우에만 악용되는 취약점을 표현할 때 사용
- OR : 두 AV 중 하나라도 참인 경우 악용될 수 있는 취약점을 표현할 때 사용
- POR(Probabilitic OR) : 두 AV 중 하나라도 참인 경우 악용될 수 있는 취약점을 표현할 때 사용. 이 경우에는 두 AV에 가중치가 존재하는데 여기서 가중치란 단위 취약점에 대해 시스템이 어느 정도 취약한지를 정량화한 것이다.
- SAND(Sequential AND) : 두 AV가 순서적으로 악용되어야 하는 취약점을 표현할 때 사용

위 4가지의 관계가 복합된 형태로 사용될 수 있다. 연산자의 우선 순위는 SAND>AND>OR,POR의 순이며 괄호를 사용하여 표현식이 계산되는 순서를 지정할 수 있다.

3. 무선랜 취약점 분석

ICAT Metabase에 무선랜 관련 취약점은 각 다양한 벤더들이 제공하는 무선랜 관련 제품에 대한 취약점으로, 무선랜이 기본적으로 그리고 잠재적으로 지니고 있는 취약점에 대해서는 포함하고 있지 않다. 특이할 사항은 지금까지 분석해왔던 소프트웨어 취약점들이 대부분 운영체제와 응용프로그램이었던데 반해, 무선 랜 제품들에 대한 취약점들은 펌웨어나 디바이스 드라이버 수준의 소프트웨어에 해당한다. 이러한 펌웨어나 디바이스 드라이버의 경우 하드웨어에 종속적인, 즉 무선 랜 관련 제품에 상당히 의존적이기 때문에 여러 제품에서 한 취약점이 공통적으로 나타나는 경우가 적으며, 취약점이 해당되는 버전의 범위도 작다는 특징을 보인다.

3.1 CVE-2001-0888 - Atmel SNMP public Community or Unknown OID Denial of Service Vulnerability

Atmel Firmware는 네트워크 관리를 위한 SNMP 프로토콜을 지원한다. Atmel Firmware가 설치된 장치를 서비스 거부 상태에 빠지게 할 수 있는 취약점이며, 장치를 다시 시작해야 서비스가 가능해진다.

이 취약점은 SNMP 기능을 사용할 때 발생한다. SNMP read request를 받은 Atmel Firmware는 응답을 하게된다. 만약, SNMP read request가 'public'이 아닌 community name으로 구성된 community string이거나 알려지지 않은 OID'을 포함하고 있다면, Atmel Firmware는 서비스 거부 상태에 빠지게 된다. 심지어 응답에서 에러 코드가 ok'일지라도 서비스 거부 상태에 빠진다. 이 취약점의 AV는 두 가지 종류의 입력에 대해서 나타나므로 각각 AV를 구성한다. community name에 대한 AV는 'IncorrectHandling_CommunityName_SNMPreadrequest', 알려지지 않은 'OID'에 대한 AV는 'IncorrectHandling_UnknownOID_SNMPreadrequest'이다. 두 개의 AV를 악용하기 위한 방법도 다르므로 취약점을 이용하기 위한 AV도 두 개로 구성되고, 해당하는 AV와 and' 연산으로 묶을 수 있다. 묶인 AV들은 다시 or' 연산으로 묶어 하나의 취약점을 표현하게 된다. 공격 결과에 대한 AV는 DenyService_AP'이며, 묶인 두 AV들에 대해서 결과는 같다.

Ato1: IncorrectHandling_CommunityName_SNMPreadrequest

Ato2: IncorrectHandling_UnknownOID_SNMPreadrequest
Ato3: SNMPreadrequest_with_notPublicCommunityName
Ato4 : SNMPreadrequest_with_UnknownOID
Ato5 : DenyService_AP
Vul_Expression : (Ato1 and Ato3 and Ato5)
or (Ato2 and Ato4 and Ato5)

3.2 트래픽 감시와 가로채기

트래픽의 감시와 가로채기는 무선 환경에서 가장 쉽게 이루어질 수 있는 공격이다. 트래픽의 감시는 단순히 공격자가 원하는 Access Point(이하 AP)의 서비스 범위 안으로 들어가기만 하면 된다. 이때, AP가 WEP key를 사용하지 않거나, 모든 무선 클라이언트에 대해서 서비스를 제공하도록 설정되어 있다면, 공격자는 쉽게 서비스를 이용할 수도 있고 트래픽을 도청할 수 있다. 이 취약점에 대해서 가장 기본적인 문제점은 AP의 서비스 범위, 즉 전송매체의 관리가 불가능하다는 것이다. 유선 랜과 같은 경우 관리자가 직접 전송매체(ex. UTP 케이블)을 제어할 수 있지만, 무선 랜의 경우 2.4GHz 주파수를 관리자가 혹은 AP가 원하는 클라이언트에게만 제공할 수 없다. 방사형으로 퍼지는 무선 주파수의 특징으로 각 클라이언트에 대한 주파수의 접근을 제어할 수 없고,WEP key와 같은 방법을 사용해서 클라이언트의 서비스 접근을 제어한다. 이 취약점은 'UnableControl_Transmission_Media' AV로 표현할 수 있을 것이다. 공격자의 공격하는 방법에 대한 AV는 'Join_in_AP_ServiceArea', 결과는 'Monitoring_WirelessTraffic'으로 표현한다.

Ato1 : UnableControl_Transmission_Media'
Ato2 : Join_in_AP_ServiceArea
Ato3 : Monitoring_WirelessTraffic
Vul_Expression : Ato1 and Ato2 and Ato3

4. 이동 단말 운영체제 취약점 분석

이동 단말 운영체제로써 Palm OS와 Window CE가 가장 널리 사용되고 있다. 이 운영체제들의 CVE에 등록된 취약점은 10건 이하로 아직 소수이며, 알려진 악성코드들도 많지 않다. 이런 OS의 종류가 다양하고, 각 모바일 디바이스에 적재될 때 customization되며 데이터의 교환이 비대칭적(데스크탑 PC->PDA)이기 때문이다.

4.1 CAN-2000-1008 - weak encryption에 의한 password crack 가능성

HotSync process 동안 Palm OS(Palm OS 3.5.2 이하)는 인증을 위해 HotSync Manager 또는 HotSync Network Server로 인코딩된 패스워드를 보낸다. 인코딩된 패스워드 블록은 Palm 디바이스 상에 'Unsaved Preferences' 데이터베이스에 저장되어 있다. 그런데 weak encryption scheme 때문에 이 패스워드 블록이 ASCII 형태로 decrypt될 수 있다.

취약점의 exploit 결과는 루트 권한 획득(GainRootAccess)이 되며 디자인 에러로 발생한 것이다. 따라서 Fact 타입 AV는 WeakEncryption (Palm-password) 이다.

이 취약점을 exploit 하기 위해서는 먼저 팜 디바이스에 물리적으로 접근이 가능해야 한다. 'Unsaved Preferences' 데이터베이스에서 직접 패스워드 블록을 retrieve할 수도 있고 initial HotSync negotiation sequence를 흉내내어 encoded password block(32 바이트)을 포함하는 특정 SLP 패킷을 획득할 수 있다.

Ato1 : WeakEncryption(Palm-password)
Ato2 : EnableDecodePassword(Palm-password)
Vul_Expression : Ato1 and Ato2

4.2 CAN-2002-0116 - TCP/IP stack implementation 에러에 의한 시스템 crash

Palm OS 3.5h를 탑재한 Handspring Visor는 많은 TCP connect() request을 수신 받았을 때 unstable해진다. 종종 crash를 가져오면 정상적으로 작동하기 위해서는 reset을 해야한다. 취약점의 exploit 결과는 서비스 거부(DoS)이며 TCP 스택 디자인 에러로 발생한 것이다. 따라서 Fact 타입 AV는 'SystemDesignError'이다. 이 취약점을 exploit 하기 위해서는 네트워크를 통해 접근이 가능하면 된다. nmap 스캐닝 툴을 사용하여 victim이 되는 대상 Visor의 IP 어드레스를 알면 된다.

Ato1 : SystemDesignError
Ato2 : Crash(Palm)
Vul_Expression : Ato1 and Ato2

5. 결론

본 논문에서는 단위 취약성 방법으로 무선 네트

워크 중에서 가장 이용이 활발한 무선랜 취약점과 이동 단말 운영체제 취약점을 분석하여 보았다. 무선랜 취약점은 기존의 운영체제나 응용프로그램 수준의 취약점이 아니라, 하드웨어에 의존적인 펌웨어나 디바이스 드라이버의 취약점으로 나타난다. 또한, 무선 환경에서의 단말기의 특징인 이동성 때문에 물리적 보안을 고려해야 하며, 공격자의 위치는 논리적 위치에서 물리적 위치까지 포함해야한다. 무선랜의 경우 공격자가 AP의 서비스 영역 안에 존재하는지, 밖에 존재하는 지에 따라 취약함의 정도에 차이가 있다. 이동 단말기는 클라이언트의 역할을 하므로 기존의 능동적인 공격에 대한 분석뿐만 아니라, 수동적인 공격까지 고려되어야 한다.

참고문헌

[1] M. Bishop, Vulnerabilities Analysis Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection, Sep. 1999, pp. 125-136

[2] HyungJong Kim, Vulnerability Assessment Simulation for Information Infrastructure Protection , InfraSec 2002, Oct. 2002, pp. 145-161

[3] ICAT Metabase, http://icat.nist.gov

[4] Security Focus, http://www.securityfocus.com

[5] Internet Security Systems, http://xforce.iss.net

[6] T. Aslam, A Taxonomy of Security Faults in the UNIX Operating System, Master of Science thesis, Department of Computer Sciences, Purdue University, West Lafayette, IN 47907 (1995).

[7] M. Bishop, A Taxonomy of UNIX System and Network Vulnerabilities, Technical Report 95-10, Department of Computer Science, University of California at Davis, Davis, CA (1995).

[8] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, A Taxonomy of Computer Program Security Flaws, *Computing Surveys* 26(3) pp. 211255 (Sep. 1994).