정 보 보 호 학 회 지
제 29 권 제6호, 2019. 12

IoT 기기 취약점 및 익스플로잇 수집을 통한 IoT 공격 유형 연구

김 미 주*, 고 웅*, 오 성 택*, 이 재 혁*, 김 홍 근*, 박 순 태*

요 약

IoT 기술을 이용한 다양한 제품과 서비스의 출시로 국내·외 IoT 산업의 급성장 및 초연결사회로의 진입이 가속화되고 있는 가운데, 보안에 취약한 IoT 기기를 공격 목표 및 도구로 악용하여 다양한 침해사고가 발생되고 있다. 이와 같은 상황은 IoT 기기 보급 활성화와 더불어 더욱 증가할 것으로 전망되고 있으며, 피해의 범위 및 정도에 있어서 막대한 사회적·경제적 손실을 유발하게 될 것으로 우려되고 있다. IoT 기기를 대상으로 하는 침해사고는 주로 디폴트 계정이나 추측하기 쉬운 패스워드를 사용하는 등 관리적 미흡 혹은 기기 자체의 취약점을 악용하여 발생하는 공격으로 인하여 발생되고 있다. 이에 정부 및 산업체에서는 IoT 기기의 보안 내재화, 기기 소유자의 보안인식 제고 등 IoT 기기의 보안성 강화를 위한 다양한 활동을 진행하고 있다. 하지만 IoT 기기 및 사용 환경의 특징 상 모든 IoT 기기를 안전하게 배포하여 관리하는 데에는 한계가 존재하기 때문에, 침해사고 예방 및 대응의 관점에서 공격에 노출되기 쉬운 취약한 기기를 파악하여 사전에 조치하는 노력이 필요하다. 이와 관련하여 본 논문에서는 IoT 기기 취약점을 악용하여 발생하는 공격 대응을 위해, 다양한 채널을 통해 IoT 기기 취약점 및 익스플로잇 정보를 수집하여 IoT 기기 취약점 악용 공격의 유형을 분석하고 대응의 일례를 제시함으로써 IoT 위협 탐지 및 대응 전략 수립을 위한 기초정보를 제공하고자 한다.

Ⅰ. 서 론

IoT(Internet of Things) 기술의 발전과 더불어 IoT 기기의 보급 및 서비스의 활성화로 스마트시티, 스마트홈, 스마트빌딩, 스마트팩토리 등 전 산업영역 및 일상생활에 큰 변화와 편리함을 가져다주고 있다. Gartner[1] 및 IHS 마킷[2]의 보고서에 따르면, 2020년까지 IoT 기기의 수가 204억 개에 이르고, 2030년까지는 1,250억 개에 이를 것으로 전망되고 있어 IoT 기기의 보급 증가 및 관련 시장의 지속적인 성장을 예측할 수 있다.

하지만 보안에 취약한 IoT 기기를 공격의 대상 및 도구로 악용하여 다양한 침해사고를 발생되고 있다. 2014년 11월 73천여 개의 CCTV가 해킹되어 실시간 화면이 인터넷(Insecam)에 노출되고, 2016년 10월 IoT 기기들이 미라이(Mirai) 악성코드에 감염되어 CNN 등 1,000여개 웹사이트에 장애를 발생시키는 등 IoT 기기에 대한 침해사고가 지속적으로 발생되고 있다. KT 경제경영연구소[3]는 IoT를 포함한 융합보안 분야의 사이버 위협으로 인한 피해액이 급증하여 2020년에는 17조 7,000억 원, 2030년에는 26조 7,000억 원에 달할 것이라고 전망하고 있다.

하지만 고성능·고가용성의 PC 및 모바일 기기를 사용하고 ISP·보안업체·이용자(개인 및 조직)가 별도의 보안장비나 SW 등을 사용하여 사이버공격을 예방 및 대응한 기존의 ICT 환경과는 달리, IoT 환경에서는 IoT 기기의 다양화 및 저사양 기기의 증가로 기기 자체에 대한 보안 내재화에 한계가 있으며 전문 지식이 부족한 IoT 기기 소유자는 침해사고의 발생여부조차 인지하기 어려운 특징을 가진다. 또한 IoT 기기를 대상으로 하는 침해사고는 주로 디폴트 계정이나 추측하기 쉬운 패스워드를 사용하는 등 관리적 미흡 혹은 기기 자체의 취약점을 악용하여 발생되고 있다. 따라서 안전한 IoT 환경을 보장하기 위해서는 IoT의 환경적 특성

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00232, 클라우드 기반 IoT 위협 자율 분석 및 대응 기술개발)

* 한국인터넷진흥원 정보보호R&D기술공유센터 보안위협대응R&D팀 ({mijoo.kim, wgo, angelrick, jaehyuk, kimhg, stpark12}@kisa.or.kr)

및 공격의 특징을 고려한 위협 탐지 및 대응 전략 수립이 필요하다.

이와 관련하여 본 논문에서는 IoT 기기 취약점을 악용하여 발생하는 공격 대응을 위해 다양한 채널을 통해 IoT 기기 취약점 및 익스플로잇(Exploit) 정보를 수집하여 IoT 기기 취약점 악용 공격의 유형을 분석하고 대응의 일례를 제시함으로써 IoT 위협 탐지 및 대응 전략 수립을 위한 기초정보를 제공하고자 한다.

Ⅱ. 관련연구

본 절에서는 IoT 기기 취약점 및 공격 유형 연구를 위한 취약점 및 익스플로잇 수집을 위해 활용되는 다양한 수집채널에 대해 기술한다.

2.1. IoT 기기 정보 수집채널

IoT 기기 취약점 및 익스플로잇 정보 수집 범위 설정을 위해 IoT 기기 제조사 및 제품명에 대한 수집이 선행되어야 한다. 본 논문에서는 IoT 기기 정보 수집을 위해 Wikidevi 웹사이트[4] 및 Nmap(Network mapper)의 OS(Operating System) 데이터베이스[5]를 활용하고자 한다. Wikidevi는 사용자 주도의 디바이스 정보 데이터베이스로 13,000여개의 유무선 임베디드 시스템, 어댑터, 모바일 디바이스 등에 대한 방대한 자료를 보유하고 있다. 네트워크 스캐너로 유명한 Nmap은 자체 보유한 OS 데이터베이스 정보와의 매핑을 통해 스캐닝 대상 기기의 OS 핑거프린팅 정보를 제공하고 있어 많은 기기에 대한 정보를 보유하고 있다.

2.2. 취약점 정보 수집채널

IoT 기기와 관련된 취약점 정보를 수집하는 채널에는 제조사, 커뮤니티, 블로그, 버그바운티 등 다양하지만 취약점 정보 보유량 및 데이터 신뢰성 등을 고려하여 미국 국립표준연구소인 NIST에서 운영 중인 NVD(National Vulnerability Database)[6]의 CVE(Common Vulnerabilities and Exposures) 취약점 정보를 활용하고자 한다. CVE는 미국 정보보호 연구기관 Mitre에서 소프트웨어, 펌웨어 등에 존재하는 취약점들을 파악 및 공유하여 기업 등에서 보안성 강화를 위해 활용할 수 있도록 하는 취약점 식별 및 교환을 위한 표준화된 방법으로 취약점 정보에 대한 가장 방대한 데이터를 보유하고 있고 취약점 점검 및 위험도 측정의 지표가 되기도 한다.

2.3. 익스플로잇 정보 수집채널

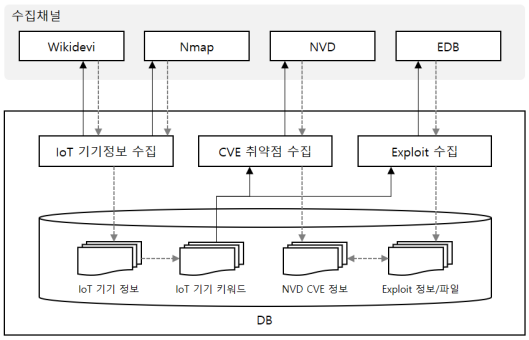
IoT 기기 대상 익스플로잇 수집채널을 선정하기 위하여 121개 정보채널을 통해 자동 탐색 방식으로 소프트웨어 취약점 정보를 수집하는 방식으로 운영되는 Vulners[7] 플랫폼의 통계 정보 및 수집채널 운영 정보에 대한 분석을 통하여 가장 많은 양의 데이터를 보유하고 있으며 안정적인 운영으로 신뢰할 수 있다고 판단한 EDB(Exploit DB)[8]를 익스플로잇 정보 수집채널로 활용하고자 한다. 다만, EDB로부터 수집된 익스플로잇이 어떤 제조사 및 제품의 버전에 영향을 주는지 파악을 위해서는 NVD CVE 정보와 매핑하는 과정이 추가적으로 필요할 수도 있다.

Ⅲ. IoT 기기 취약점 및 익스플로잇 수집

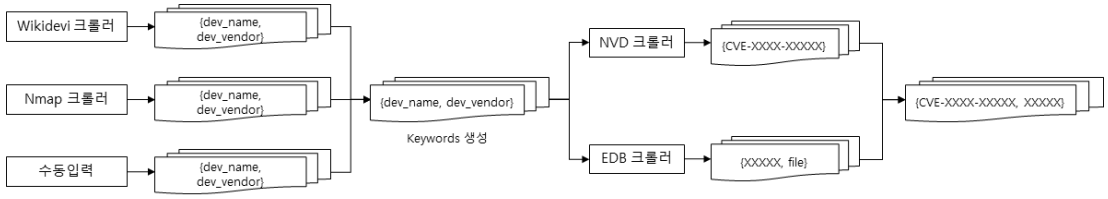
본 절에서는 IoT 기기 정보에 기반하여 취약점 및 익스플로잇 정보를 자동으로 수집하는 시스템에 대한 설계 및 구현사항을 기술한다.

3.1. 수집 시스템 설계 및 구현

IoT 기기 정보와 관련 CVE 취약점 및 익스플로잇 정보 수집을 위해 [그림 1]과 같이 구성된 시스템을 설계 및 구현하였다. Wikidevi 및 Nmap OS 데이터베이스에서 유·무선 임베디드 시스템 및 무선 어댑터 기기에 대한 제조사 및 제품명 등을 수집하고, 수집된 데이



(그림 1) IoT 기기 취약점 및 Exploit 수집 시스템 구성



(그림 2) IoT 기기 정보 기반 취약점·익스플로잇 수집 데이터 항목 및 처리 흐름도

터를 기반으로 비-IoT 기기 및 중복 등을 제거하여 CVE 취약점 및 익스플로잇 수집을 위한 IoT 기기 키워드를 추출하였다. 해당 키워드를 기반으로 NVD 및 EDB를 대상으로 CVE 취약점 및 익스플로잇 정보(파일)을 수집하고, 익스플로잇 정보가 누락된 CVE에 대해서는 해당 정보를 기입하도록 한다. 각각의 수집 단계에 따른 데이터 항목 및 처리 흐름도는 [그림 2]와 같다.

3.2. 수집 결과

IoT 기기 취약점 및 익스플로잇 정보 수집의 결과, 843개의 제조사에 해당하는 6,238개의 제품 정보가 수집되었고, 해당 기기 정보 키워드를 기반으로 NVD 및 EDB 대상 수집 결과, 4,390개의 CVE 취약점 및 1,001개의 익스플로잇이 수집되었다. 이는 EDB에 등록된 41,000여 개의 익스플로잇 중 IoT 관련 익스플로잇이 천여 개에 달함을 의미한다.

Ⅳ. IoT 기기 취약점 및 공격 유형 분류

본 절에서는 수집된 IoT 기기 취약점 및 익스플로잇 정보를 바탕으로 IoT 위협 대응을 위한 공격 유형을 분석하고 분류하고자 한다.

4.1. CWE 기반 분류

수집된 익스플로잇 중 CVE 매핑되는 410개 대상으로 CWE(Common Weakness Enumeration) 취약점 유형 32개 기반 공격 유형 15종을 [표 1]과 같이 분류하였다.

〔표 1〕 CWE 기반 IoT 기기 공격 유형 분류

No	CWE 분류	CWEs
1	Authentication Bypass	CWE-22, CWE-77, CWE-200, CWE-254, CWE-255, CWE-264, CWE-284, CWE-285, CWE-287, CWE-310, CWE-327, CWE-384, CWE-434, CWE-640, CWE-798
2	Denial of Service	CWE-16, CWE-19, CWE-20, CWE-119, CWE-264, CWE-284, CWE-287, CWE-399, CWE-400, CWE-415
3	Command Injection	CWE-20, CWE-77, CWE-78, CWE-94, CWE-255, CWE-264, CWE-284, CWE-287, CWE-352, CWE-943
4	Information Leak	CWE-20, CWE-22, CWE-200, CWE-255, CWE-264, CWE-275, CWE-284, CWE-310, CWE-320
5	Cross-Site Request Forgery	CWE-264, CWE-352
6	Cross-Site Scripting	CWE-79
7	Buffer Overflow	CWE-20, CWE-119
8	Path Traversal	CWE-20, CWE-22
9	SQL Injection	CWE-89
10	File Upload	CWE-434
11	CRLF Injection	CWE-20
12	Security Bypass	CWE-20, CWE-264, CWE-441
13	Code Injection	CWE-94
14	Privilege Escalation	CWE-264, CWE-284
15	URL Redirect	CWE-17

4.2. 익스플로잇 페이로드 기반 분류

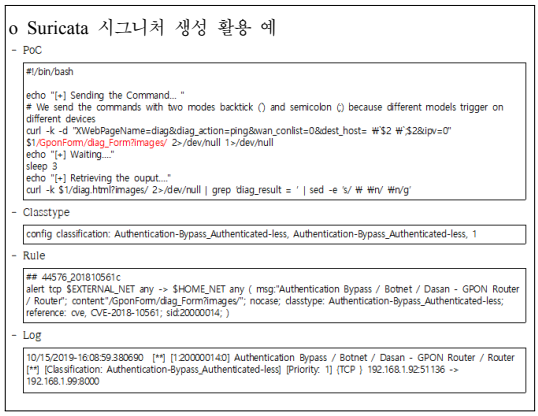
CWE 취약점 유형으로 공격 유형을 분류하는 경우 CWE의 범위가 너무 크거나 같은 공격유형으로 중복되는 경우가 있어 익스플로잇 페이로드의 특징적인 유사성을 토대로 99종의 공격 유형을 [표 2]와 같이 분류하였다.

〔표 2〕 익스플로잇 페이로드 기반 IoT 공격 유형 분류

No	CWE 분류	익스플로잇 페이로드 분류	No	CWE 분류	익스플로잇 페이로드 분류
1	Authentication Bypass	Authenticated-less	51	Information Leak	Config File
2		Hardcoded Credentials	52		Credentials - Clear Text HTML
3		Crafted GET Request	53		Credentials - Clear Text Respone
4		Crafted Cookie	54		LFI
5		Crafted POST Request	55		System Info
6		Predictable Credentials	56		Encoded Credential
7		Session Handling (Stealing)	57		Credentials - Clear Text BackupFile
8		Set Admin Password	58		Credentials - Clear Text XML
9		Crafted SNMP Request	59		Credentials - Clear Text Storage
10		Crafted Soap Request	60		Device Memory
11		Hidden cmd	61		RTSP Stream
12		Brute Force	62		Credentials - Telnet
13		Crafted NFS Request	63		Eavesdrop
14		Simultaneous Connections	64		RSA Key / Certificate
15	Denial of Service	Buffer Overflow	65		User Enumeration
16		Crafted GET Request	66		Web Root Path
17		Crafted POST Request	67	Cross-Site Request Forgery	HTML POST
18		Crafted SIP Messages	68		GET Request
19		ICMP Flooding	69		DHCP Request
20		SYN Flooding	70		XML POST
21		Crafted UDP Packet	71	Cross-Site Scripting	Reflected Base
22		Invalid URL Path	72		Stored Base
23		Repeat Service Request	73		Reflected / Stored Base
24		Crafted TCP Packet	74	Buffer Overflow	ROP
25		ARP Flooding	75		Jmp to Reg
26		Crafted FTP Request	76		system()
27		Null Packet	77		'() {:;};'
28		SNMP Community String	78		popen()
29		UDP Flooding	79	Path Traversal	Relative Path (..)
30		ACK Flooding	80		Escaped Character
31		Crafted CLI Commands	81		Absolute Path
32		Crafted IOCTLs	82	SQL Injection	Boolean Base
33		Crafted IRC Request	83		SQL Command
34		FingerPrinting	84		Union Base
35		Input Qfull	85		Blind Base
36		Invalid SSH Connection	86	File Upload	Improper File Extension
37		RST Flooding	87		Direct Request
38	Command Injection	';'	88		FTP Default Account
39		'`'	89		Fully Qualified Path
40		'() {:;};'	90		Unrestricted Upload
41		'&'	91	CRLF Injection	Crafted Parameter
42		System Parameter	92	Security Bypass	Firewall & NAT
43		'|'	93		URL Filter
44		'$()'	94	Code Injection	Crafted DLM
45		system()	95		Crafted GET Request
46		Crafted UDP Packet	96		RFI
47		Hidden Web Shell	97	Privilege Escalation	Local Root Jailbreak
48		PJL Commands	98		Group Manipulation
49		'ls' Control Characters	99	URL Redirect	Crafted GET Request
50		Crafted GET Request			

4.3. IoT 기기 공격 대응 예

IoT 기기 공격 유형 분류 활용의 예로 오픈소스 IDS 시스템으로 대표적인 Suricata[9]를 활용하여 IoT 기기 공격 대응 시그니처를 생성하여 검증하는 활용 예시를 보여준다.



(그림 3) IoT 기기 공격 유형 기반 IDS 기반 대응 예

V. 결 론

IoT 기기의 보급 및 서비스의 증가로 편리하고 윤택한 삶을 누리게 되었지만, 이는 해커로 하여금 더 많은 공격의 기회를 제공하여 침해사고 등 보안사고를 유발하는 위협요소의 증가를 의미하기도 한다.

본 논문에서는 IoT 기기 정보를 기반으로 공개된 취약점 및 공격 패턴을 수집하여 IoT 기기 취약점 악용 공격 유형을 분석하고, 대응방안의 일례로 네트워크 기반 IDS를 활용하여 IoT 기기 공격을 탐지하는 방법에 대해서 기술하였다. 본 논문을 통해 수집 및 분석된 IoT 기기 취약점 및 공격 유형에 대한 연구가 IoT 위협 탐지 및 대응 등 안전한 IoT 환경 제공을 위한 전략 수립 등 다양한 활동에서 유익하게 활용되기를 기대해 본다.

참 고 문 헌

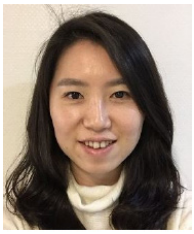
[1] Gartner, https://www.gartner.com/
[2] IHS Markit, https://ihsmarkit.com/
[3] KT 경제경영연구소, “보안시장에서의 새로운 기회”, 2016.11
[4] Wikidevi 웹사이트, https://wikidevi.com/
[5] Nmap OS 데이터베이스, https://svn.nmap.org/nmap/nmap-os-db
[6] NVD(National Vulnerability Database), https://nvd.nist.gov/
[7] Vulners 웹사이트, https://vulners.com/
[8] Exploit-DB, https://www.exploit-db.com/
[9] Suricata 웹사이트, https://suricata-ids.org/

〔별첨〕 IoT 공격 유형 분류에 따른 설명

No	CWE 분류	익스플로잇 페이로드 분류	설명
1	Authentication Bypass	Authenticated-less	인증 기능 부재
2		Hardcoded Credentials	하드코딩된 계정정보(백도어)를 통한 접근
3		Crafted GET Request	조작된 파라미터 값을 통한 우회 (GET Method)
4		Crafted Cookie	조작된 쿠키를 통한 인증 우회
5		Crafted POST Request	조작된 파라미터 값을 통한 인증 우회 (POST Method)
6		Predictable Credentials	쉽게 추측 가능한 계정 정보를 통한 접근
7		Session Handling (Stealing)	조작된 세션을 통한 인증 우회
8		Set Admin Password	관리자 패스워드 재설정을 통한 인증 우회
9		Crafted SNMP Request	조작된 SNMP 패킷 요청을 통한 인증 우회
10		Crafted Soap Request	조작된 Soap 요청을 통한 인증 우회
11		Hidden cmd	숨겨진 명령어를 통한 인증 우회
12		Brute Force	무차별 대입을 통한 인증 우회
13		Crafted NFS Request	조작된 NFS 요청을 통한 인증 우회
14		Simultaneous Connections	동시 연결을 통한 인증 우회
15	Denial of Service	Buffer Overflow	버퍼 오버플로우를 통한 서비스 거부 공격
16		Crafted GET Request	조작된 파라미터 값, 잘못된 서비스, 잘못된 URL 요청을 통한 서비스 거부 공격
17		Crafted POST Request	조작된 파라미터 값, 조작된 헤더를 통한 서비스 거부 공격
18		Crafted SIP Messages	조작된 SIP 요청을 통한 서비스 거부 공격
19		ICMP Flooding	ICMP Flooding (Ping of Death)
20		SYN Flooding	SYN Flooding
21		Crafted UDP Packet	특정 포트에 대한 UDP 패킷 전송 및 서비스 거부를 유발하는 페이로드 전송
22		Invalid URL Path	부적절한 URL 요청을 통한 서비스 거부 공격
23		Repeat Service Request	반복된 서비스 요청을 통한 서비스 거부 공격
24		Crafted TCP Packet	조작된 TCP 플래그를 통한 서비스 거부 공격
25		ARP Flooding	ARP Flooding
26		Crafted FTP Request	조작된 FTP 패킷 요청을 통한 서비스 거부 공격
27		Null Packet	특정 포트로 empty 패킷 요청을 통한 서비스 거부 공격
28		SNMP Community String	조작된 SNMP 패킷 요청을 통한 서비스 거부 공격
29		UDP Flooding	UDP Flooding
30		ACK Flooding	ACK Flooding
31		Crafted CLI Commands	특정 CLI 명령어를 통한 서비스 거부 공격
32		Crafted IOCTLs	특정 IOCTL 요청을 통한 서비스 거부 공격
33		Crafted IRC Request	조작된 IRC 패킷 요청을 통한 서비스 거부 공격
34		FingerPrinting	FingerPrinting 옵션을 통한 서비스 거부 공격
35		Input Qfull	조작된 패킷을 통해 Input 큐를 Full 상태로 설정하여 서비스 거부 공격 유발
36		Invalid SSH Connection	잘못된 SSH 요청을 통한 서비스 거부 공격
37		RST Flooding	RST Flooding
38	Command Injection	';'	쉘 메타 문자 'Semi colon' 을 통한 임의의 명령 실행
39		'`'	쉘 메타 문자 'Back qoute' 를 통한 임의의 명령 실행
40		'() {:;};'	쉘 쇼크 공격을 통한 임의의 명령 실행
41		'&'	쉘 메타 문자 'Ampersand' 를 통한 임의의 명령 실행
42		System Parameter	Systen 권한으로 작동하는 파라미터 값을 조작하여 임의의 명령 실행
43		'|'	쉘 메타 문자 'Pipe' 를 통한 임의의 명령 실행
44		'$()'	쉘 메타 문자 'Dollar' 를 통한 임의의 명령 실행
45		system()	system 함수를 통한 임의의 명령 실행
46		Crafted UDP Packet	조작된 UDP 패킷 요청을 통한 임의의 명령 실행
47		Hidden Web Shell	숨겨진 웹 쉘을 통한 임의의 명령 실행
48		PJL Commands	조작된 PJL 명령어를 통한 임의의 명령 실행
49		'ls' Control Characters	ls 명령어를 악용하여 제어 문자가 포함된 임의의 명령 실행
50		Crafted GET Request	URL에 높은 액세스 수준을 지정하여 로컬 권한 부여를 사용하는 경우 인증을 무시하고 임의의 명령을 실행

No	CWE 분류	익스플로잇 페이로드 분류	설명
51	Information Leak	Config File	다중 정보 노출 취약점으로 id, pw, 및 기타 텍스트 값 접근 및 조작
52		Credentials-Clear Text HTML	일반 텍스트로 저장된 자격증명 접근
53		Credentials-Clear Text Respone	GET 요청을 통한 일반 텍스트로 저장된 자격증명 접근
54		LFI	디렉토리 탐색 취약점을 이용한 자격증명 접근
55		System Info	조작된 패킷을 통해 소프트웨어 및 펌웨어 버전, MAC 등과 같은 시스템 정보 노출
56		Encoded Credential	알려진 방법으로 인코딩된 디코딩을 통한 자격증명 접근
57		Credentials-Clear Text BackupFile	백업 파일 내에서 일반 텍스트의 장치에 대한 중요 정보 접근
58		Credentials-Clear Text XML	사용자 계정 접근 시 XML로 표시되는 관리자 암호로 권한 획득
59		Credentials-Clear Text Storage	일반 텍스트 비밀번호 저장소 접근으로 자격 증명 획득
60		Device Memory	장치 메모리 접근으로 중요 정보 획득
61		RTSP Stream	인증되지 않은 실시간 RTSP 스트림 접근 허용
62		Credentials - Telnet	Telnet 연결을 통해 사용자 정보 접근으로 유효한 모든 자격증명 노출
63		Eavesdrop	오디오 스트림 메시지를 통해 대화 도청
64		RSA Key / Certificate	장치 펌웨어 내부 접근을 통한 개인 RSA 키 및 인증서 획득
65		User Enumeration	정보 노출 취약점으로 유효한 사용자 이름 열거 허용
66		Web Root Path	실패한 오류 메시지의 경로 메시지 노출을 통한 중요 정보 접근
67	Cross-Site Request Forgery	HTML POST	위조된 HTML 스크립트 코드를 사용하여 시스템 정보 접근 및 손상
68		GET Request	위조된 GET 요청을 통한 시스템 정보 접근 및 손상
69		DHCP Request	DHCP 관리 및 로그 페이지에 악성 스크립트 삽입으로 시스템 정보 접근 및 손상
70		XML POST	SOAP 기반 XML 웹서비스 무단 접근
71	Cross-Site Scripting	Reflected Base	악의적인 링크, 이메일 등을 통해 피해자가 서버로 요청하도록 유도, XSS 페이로드 실행
72		Stored Base	악성 스크립트를 응용프로그램에 주입
73		Reflected / Stored Base	다중 XSS 취약성으로 서버/웹 사이트 필터에 악성 스크립트 주입
74	Buffer Overflow	ROP	Bof 취약점으로 시스템 함수 주소를 만들기 위한 바이트 조각의 재조합을 통해 임의 코드 실행
75		Jmp to Reg	Bof 취약점으로 스크립트 주소를 가진 레지스터 주소 실행 후 임의 코드 실행
76		system()	Bof 취약점으로 system() 함수 실행 후 임의 코드 실행
77		'() {:;};'	원격 공격자가 GNU Bash 개별 함수 취약점으로 서비스 거부 공격
78		popen()	Bof 취약점으로 매개 변수의 긴 문자열을 통해 임의 코드 실행
79	Path Traversal	Relative Path (..)	URL에 상대경로 매개 변수를 통해 임의 페이지 접근
80		Escaped Character	URL에 간단한 이스케이프 문자 삽입으로 관리자 페이지 접근
81		Absolute Path	URL에 절대경로 매개 변수를 통해 임의 페이지 접근
82	SQL Injection	Boolean Base	SQL 쿼리를 데이터베이스에 전송하여 쿼리가 참 또는 거짓 결과를 반환 여부 확인
83		SQL Command	SQL 주입 취약점을 통해 원격 공격자는 임의의 SQL 명령 실행
84		Union Base	SQL 주입 취약점을 통해 UNION 키워드를 사용하여 데이터베이스 내의 다른 테이블에서 데이터를 검색
85		Blind Base	SQL 쿼리를 데이터베이스에 전송하여 참 또는 거짓 결과를 반환 여부로 데이터 접근
86	File Upload	Improper File Extension	실행 파일 확장자를 가진 파일을 업로드하여 임의 코드 실행
87		Direct Request	임의의 파일 경로를 찾은 다음 그 파일에 대한 직접 요청을 통해 파일 접근
88		FTP Default Account	웹 루드 디렉토리에 파일을 업로드한 다음 요청을 통해 임의 코드 실행
89		Fully Qualified Path	dev 인수없이 HTTP 요청 수행하여 'path' 매개 변수에 완전한 경로 노출
90		Unrestricted Upload	무제한 파일 업로드 취약점으로 임의 코드 실행
91	CRLF Injection	Crafted Parameter	CRLF를 애플리케이션에 제출할 HTTP 매개변수 또는 URL 수정으로 악성코드 주입
92	Security Bypass	Firewall & NAT	사용자 정의 네트워크 요청 실행으로 라우터 방화벽, 일반적 네트워크 스캐닝 활동 우회
93		URL Filter	긴 URL 웹 요청을 제대로 필터링하지 않으므로 원격 공격자가 웹 제한 필터를 우회
94	Code Injection	Crafted DLM	수정된 DLM(Dynamic Loadable Module) 제공하여 루트 권한으로 임의의 명령을 실행
95		Crafted GET Request	"forgot"과 관련된 조작된 요청을 통해 임의의 Perl 코드를 실행
96		RFI	name 매개 변수의 URL을 통해 임의의 PHP 코드를 실행
97	Privilege Escalation	Local Root Jailbreak	네트워크 파일 공유 결함을 통한 로컬 루트 탈옥
98		Group Manipulation	"스토리지 사용자"의 그룹 설정 조작 및 장치의 서비스 엑세스 권한 정의 수정
99	URL Redirect	Crafted GET request	임의의 웹 사이트로 리디렉션하고 URL을 통해 피싱 공격을 수행

〈저자소개〉



김 미 주 (Mijoo Kim)
정회원
2006년 2월 : 순천향대학교 정보보호학과 졸업
2008년 2월 : 순천향대학교 정보보호학과 석사
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2008년 4월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 정보보호, IoT 및 모바일 보안, 융합보안

고 웅 (Woong Go)
정회원
2010년 2월 : 순천향대학교 정보보호학과 석사
2013년 8월 : 순천향대학교 정보보호학과 박사
2014년 1월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 책임연구원
<관심분야> IoT, 기계학습, 정보보호

오 성 택 (Sungtaek Oh)
정회원
2013년 2월 : 아주대학교 정보컴퓨터공학부 졸업
2016년 2월 : 아주대학교 컴퓨터공학과 석사
2015년 2월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 선임연구원
<관심분야> 머신러닝, 침입탐지, 정보보호

이 재 혁 (Jaehyuk Lee)
학생회원
2014년 2월 : 학점은행제 정보보호학사
2018년 2월 : 고려대학교 정보보호석사
2017년 4월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 주임연구원
<관심분야> 빅데이터, AI, 정보보호

김 홍 근 (Kim Hong-Geun)
종신회원
1985년 2월 : 서울대학교 전자계산기공학과 졸업
1987년 2월 : 서울대학교 전자계산기공학과 석사
1994년 2월 : 서울대학교 컴퓨터공학과 박사
1994년 5월~현재 : 한국인터넷진흥원 연구위원
<관심분야> 병렬알고리즘, 사이버보안, 컴퓨터보안

박 순 태 (SoonTai Park)
정회원
1992년 2월 : 단국대학교 전자계산학과 졸업
1998년 8월 : 국민대학교 정보과학대학원 정보통신학과 석사
2010년 8월 : 전남대학교 대학원 정보보안협동과정 박사
2000년 4월~현재 : 한국인터넷진흥원 팀장
<관심분야> IT보안성 평가, 정보보호 인력 양성, 정보통신기반보호, 조직 정보보안/개인정보보호 실무, 정보보호 R&D