2025 7.23 swing 내부세미나 SSR 발표

33기 방은진

IoT (사물인터넷)

IoT란 무엇이고, 어떻게 보호되어야 하는가

목차

Table of Contents

1. 주제 선정 이유

C언어의 특징

- 하드웨어에 가까운 저수준 접근이 가능
- 실행 속도가 빠르고 메모리를 효과적으로 사용
  -> 기계어 수준의 효율성
- 이식성이 뛰어남

임베디드 시스템

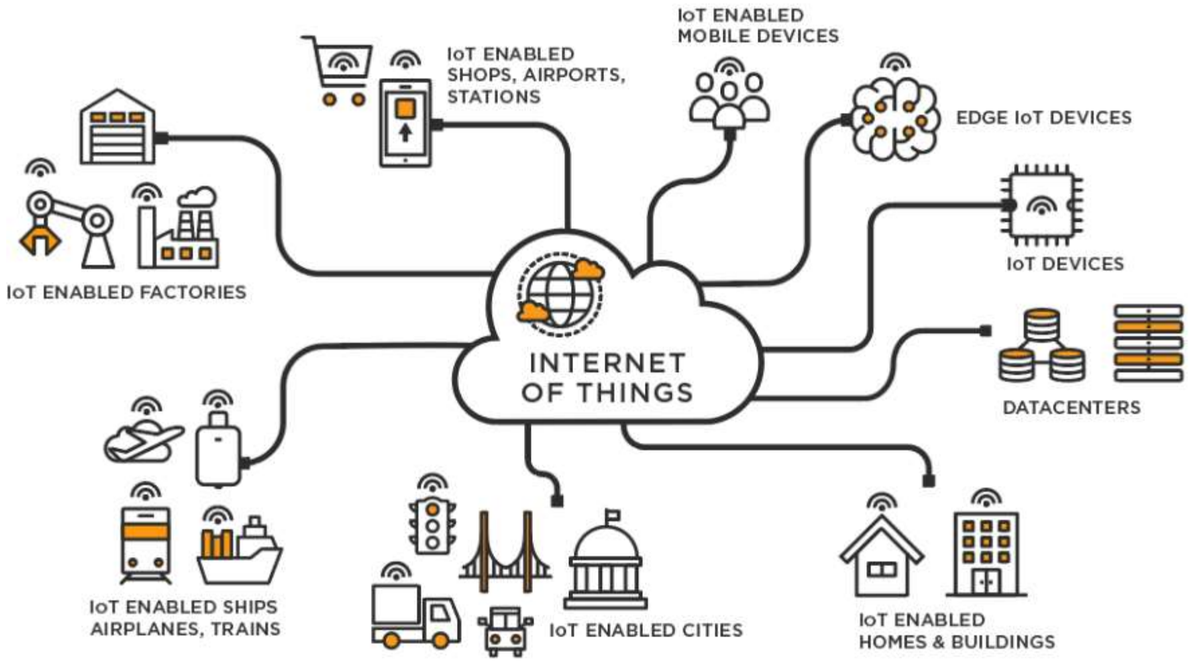
- 전용 동작을 수행하거나 특정 임베디드 소프트웨어 응용 프로그램과 함께 사용되도록 디자인된 특정 컴퓨터 시스템 또는 컴퓨팅 장치
- 제한적 기능을 수행하므로 C언어가 적합

IoT는 임베디드 시스템의 네트워크화된 형태로서, 임베디드 시스템의 확장된 개념

2. IoT 정의

Internet Of Things

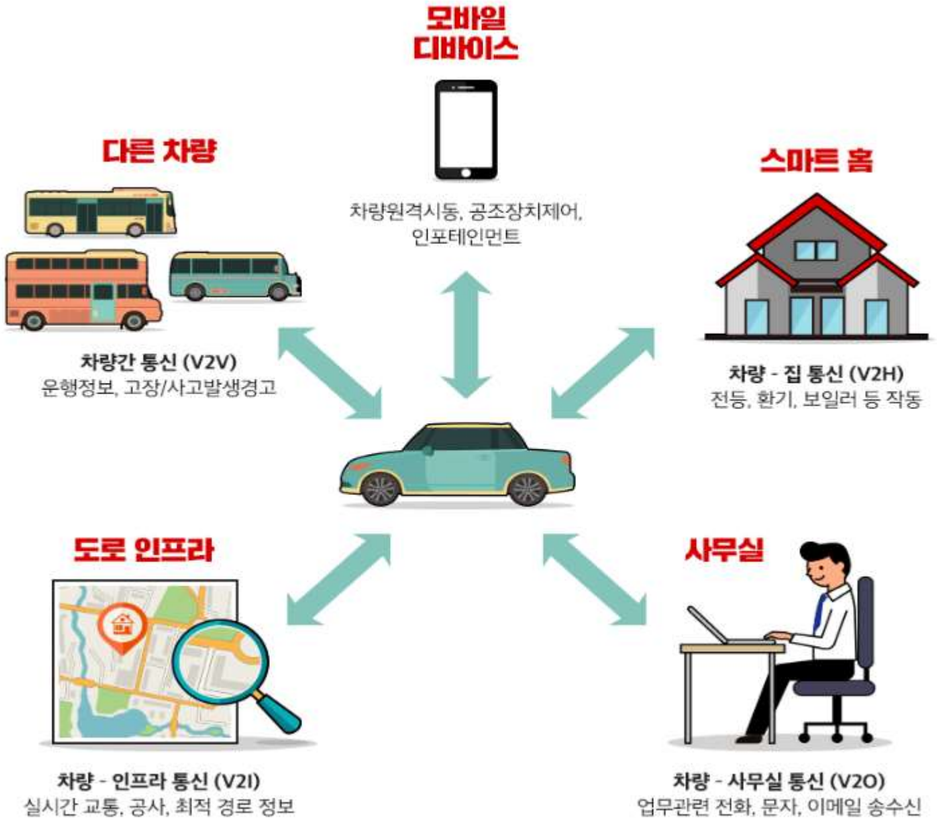
- 다양한 임베디드 시스템을 일컫는 사물(Things)에
  센서와 통신 기능을 내장하여 인터넷에 연결하는 무선 통신 기술을 활용해 각종 사물을 연결하는 기술



2. IoT 적용 분야

●스마트홈

●커넥티드 카



2. IoT 의 보안 위협과 보안 방안

보안 위협

1. 여러 기기의 유기적 결합에 의한 노출

2. 센서·디바이스의 컴퓨팅 성능 및 메모리 용량의 제약

3. REDCAP 5G 기술 : 저전력·저비용 장치의 대량 연결 가능
-> 저전력·저비용 보안 설계 : 해킹에 취약
-> 대량 연결 기기 : 하나의 감염된 장치로 전체 시스템 위험

보안 방안

1. 저전력 암호화 모듈의 적용 필요

2. 게이트웨이에서의 보안솔루션 적용
-> VPN, IPS 강화

3. 철저한 보안 인증
-> 네트워크 다중 인증(MFA)

3. IoT 펌웨어에 대하여 - 펌웨어의 중요성

펌웨어(firmware)

- 하드웨어 장치에 포함된 소프트웨어,
  하드웨어의 기본적인 동작을 제어

- 다른 소프트웨어보다 우선적으로 하드웨어를
  제어할 수 있는 소프트웨어로,
  영구적인 명령어와 데이터로 이루어져 있다.

IoT 펌웨어 보안 취약성 : "잊힌 분야"

- 지속성 : 쉽게 제거되지 X
- 은밀성 : 장기간 탐지되지 X
- 권한 장악 : 루트 권한에 접근 가능

3. IoT 펌웨어에 대하여 - ipTIME 공유기 펌웨어 분석 실습

실습 목적

- ipTIME 공유기 펌웨어에서 CVE-2020-7848 커맨드 인젝션 의심 부분 분석
- system() 함수 호출 유무를 통해 취약점 존재 여부 판단

분석 대상 펌웨어

- ipTIME C200 공유기
- 분석 파일: c200_1_012.bin
- 해당 버전은 CVE-2020-7848 취약점이 패치되기 이전 버전

사용 툴

- 우분투 환경
- binwalk
  : 펌웨어 바이너리 분석 및 파일시스템 추출 도구

사전 준비

1. ipTIME 펌웨어 다운로드 : CVE 취약점이 패치되기 이전 버전을 다운로드

CVE 취약점이 패치되기 이전 버전

CVE 취약점이 패치된 이후 버전

사전 준비

2. binwalk 명령어

: 펌웨어 파일의 구조를 분석하고 파일 시그니처를 사용해서 어떤 데이터가 들어있는지 확인해준다.

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~$ sudo apt install binwalk
[sudo] password for bangeunjin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

binwalk 설치

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
bangeunjin@bangeunjin-VMware-Virtual-Platform:~$ cd Downloads
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads$ binwalk /home/bangeunjin/Downloads/c200_1_012.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
88            0x58            uImage header, header size: 64 bytes, header CRC: 0x68DA56E0, created: 2020-04-08 06:24:37, image size: 2022965
bytes, Data Address: 0x805F2B70, Entry Point: 0x805F2B70, data CRC: 0xE646F319, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression
 type: none, image name: "linux_3.10"
4504          0x1198          LZMA compressed data, properties: 0x5D, dictionary size: 67108864 bytes, uncompressed size: -1 bytes
3145728       0x300000        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 8189792 bytes, 1027 inodes, blocksize: 13
1072 bytes, created: 2020-06-23 03:32:25
```

binwalk [타겟 파일명] : 파일에 보관된 시그니처를 알려준다.

2. binwalk 명령어

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads$ binwalk -e c200_1_012.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
88            0x58            uImage header, header size: 64 bytes, header CRC: 0x68DA56E0, created: 2020-04-08 06:24:37, image size: 2022965
bytes, Data Address: 0x805F2B70, Entry Point: 0x805F2B70, data CRC: 0xE646F319, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression
 type: none, image name: "linux_3.10"
4504          0x1198          LZMA compressed data, properties: 0x5D, dictionary size: 67108864 bytes, uncompressed size: -1 bytes

WARNING: Symlink points outside of the extraction directory: /home/bangeunjin/Downloads/_c200_1_012.bin.extracted/squashfs-root/tmp -> /var/tm
p; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/bangeunjin/Downloads/_c200_1_012.bin.extracted/squashfs-root/init -> /usr/b
in/busybox; changing link target to /dev/null for security purposes.
```

binwalk -e [타겟 파일명] : 펌웨어 파일을 추출하는 옵션으로 [펌웨어 파일명]으로 디렉토리가 만들어진다

※ WARNING 은 무엇일까?

펌웨어 안에 심볼릭 링크 존재

-> 그 링크의 대상 경로가 루트 시스템의 /usr/bin/ 같은 펌웨어 외부 경로를 참조하고 있음

=> 보안을 위해 binwalk가 해당 링크를 실제 경로가 아닌 /dev/null로 강제로 바꿔버림

사전 준비 🔍 2. binwalk 명령어

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads$ ls
be19000_ml_15_092.bin             c200_1_012.bin
_be19000_ml_15_092.bin.extracted  _c200_1_012.bin.extracted
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads$ cd _c200_1_012.bin.extracted
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads/_c200_1_012.bin.extracted$ ls
1198  1198.7z  300000.squashfs  squashfs-root
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads/_c200_1_012.bin.extracted$ cd squashfs-root
```

추출된 펌웨어 루트 파일 시스템(squashfs-root) 으로 이동한다.

※ 펌웨어 다운로드 vs 펌웨어 추출

- 펌웨어 다운로드 : ipTIME 공식 사이트 등에서 .bin 형식의 펌웨어 파일을 내려받는 것
  예: C200_1.018.bin
- 펌웨어 추출 : 펌웨어 파일을 내부 구조(루트 파일시스템, 실행 파일 등)로 분해·추출하는 작업. 압축된 루트 파일 시스템(squashfs 등) 자동 감지, 내부 디렉토리 구조 (/etc, /cgi-bin, /bin, ...)를 꺼내줌

※ CVE - 2020-7848 이란?

- EFM ipTIME C200 IP 카메라는 /login.cgi?logout=1 스크립트의 명령 주입 취약점에 취약하며,
  공격자는 GET 요청을 통해 승인되지 않은 OS 명령을 실행할 수 있다.

- login.cgi?logout=1 란 무엇인가?
  [파일명] ? [파라미터명] = [값] 형태
  login.cgi: 웹서버에 있는 CGI 스크립트 파일(로그인 관련)
  logout=1: "logout"이라는 이름의 파라미터(parameter)를 1로 전달한다.

  http://192.168.0.101/cgi-bin/login.cgi?logout=1
  이런 식으로 웹 브라우저 주소창에서 확인 가능

  http://192.168.0.101/cgi-bin/login.cgi?logout=1;id
  ;id 는 리눅스 명령어(사용자 정보 출력)
  그러면 서버는 진짜로 id 명령어를 실행해버림 = 커맨드인젝션(commend injection) 공격

그러므로 /login.cgi?logout=1 스크립트의 명령 주입 취약점에 취약

=> 따라서 login.cgi 를 찾는다

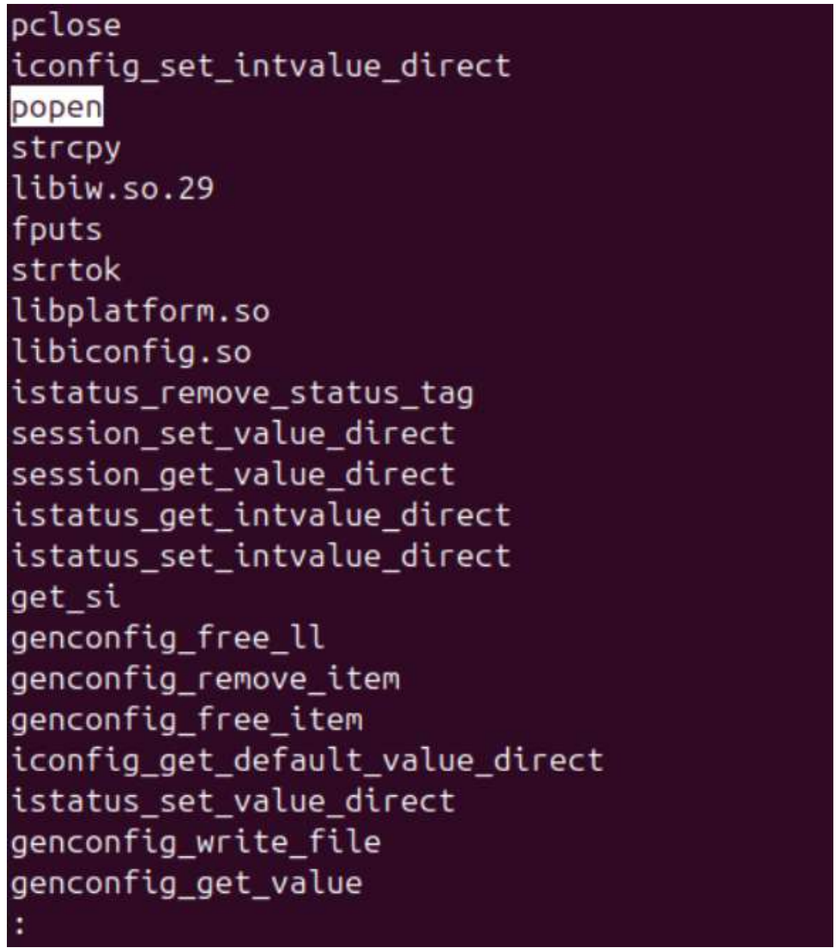
- find . -type f -name "*.cgi" : 현재 디렉토리 이하에서 .cgi 확장자를 가진 모든 파일 경로를 출력

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads/_c200_1_012.bin.extracted/squashfs-root$ find . -type f -name "*.cgi"
./usr/www/nav.cgi
./usr/www/main.cgi
./usr/www/login_handler.cgi
./usr/www/captcha.cgi
./usr/www/login.cgi
./usr/www/cgi/iux_set.cgi
./usr/www/cgi/iux_get.cgi
```

- strings ./usr/www/login.cgi | less : 바이너리(실행 파일 등) 안에서 사람이 읽을 수 있는 문자열만 출력

```
bangeunjin@bangeunjin-VMware-Virtual-Platform:~/Downloads/_c200_1_012.bin.extracted/squashfs-root$ strings ./usr/www/login.cgi | less
```

커멘드 인젝션 공격이 가능하려면 웹 애플리케이션에서 사용자 입력을 기반으로 system(), exec(), os.system() 등과 같은 시스템 호출 함수를 사용해야 한다.



즉, 웹서버가 사용자의 입력값을 검증 없이 system() 등에 넘기면
→ 사용자가 시스템 명령어를 주입해서 실행시킬 수 있게 되는 것이다.

4. IoT 펌웨어 업데이트에 대하여 - 펌웨어 업데이트를 해야하는 이유

- radare2 (리버싱 툴) 을 이용해 system()함수가 실행되는지 확인

패치 이전 버전(c200_1_012.bin)

```
[0x00401080]> ii~system
20  0x00401164 GLOBAL FUNC       system
```

- system() 함수가 존재

```
[0x00401080]> axt 0x00401164
fcn.0040121c 0x401144 [CODE] beqz a1, sym.imp.system
fcn.0040121c 0x401154 [CODE] beqz t9, sym.imp.system
```

- system() 함수가 호출되는 부분이 있음
  = 명령어 실행

패치 이후 버전(c200_1_020.bin)

```
[0x00401040]> ii~system
20  0x00401130 GLOBAL FUNC       system
```

```
[0x00401040]> axt 0x00401130
```

- system() 함수가 호출되는 부분 X
  = 명령어 실행 X

느낀점

제 발표를 들어주셔서 감사합니다.