해킹시연을 통한 스마트기기의 위험성 진단과 대응방안

정구홍@GrayHash

2013-11-19

발표자 소개

- 정구홍 (몽이, 멍멍이)
- GrayHash 수석 연구원
- 해커스쿨(hackerschool.org) 운영자
- 미래부 지원/KITRI 주관 BoB 보안 교육사업 멘토
- cybermong@grayhash.com
- http://facebook.com/goohong.jung

발표 개요

- 우리 주변의 수 많은 스마트 기기들이 해킹에 매우 취약함을 시연을 통해 보임
- 해커들이 다양한 스마트 기기들을 어떤 식으로 공격하고 악용하는지를 설명
- 해커들이 스마트기기의 취약점을 찾는 과정 설명
- 이를 통해 보안인식 제고와 경각심을 높임

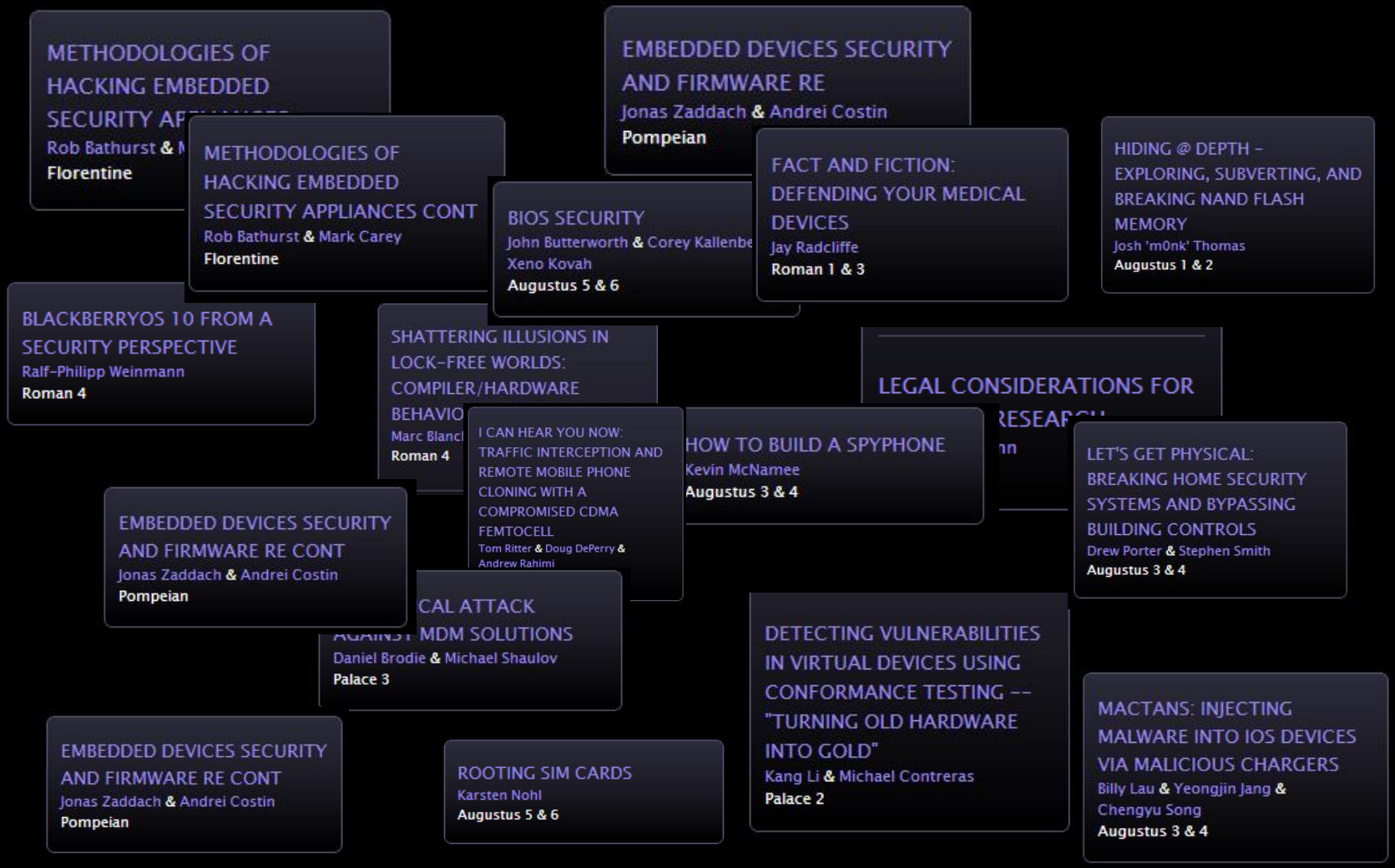
발표 목차

- 스마트기기 해킹에 대하여..
- 스마트기기 해킹 사례들 소개 & 시연
- 스마트기기 취약점 탐지 과정 설명
- 스마트기기 해킹 대응방안 제시

스마트기기 해킹에 대하여

스마트 기기 해킹(?)

하드웨어 해킹 발표(블랙햇2013)



스마트 기기 해킹의 발전

- 스마트폰의 폭발적인 인기
- 다양한 공격 대상(먹잇감) 출현
  - 스마트카드, 스마트TV, 스마트카 …
- 스마트기기로부터 얻을 것이 많아짐
  - 금융거래, 개인 정보, 사내 기밀 정보
- 기존 공격 대상들(Windows/Linux)의 보안성 강화
  - ASLR/DEP, Security Cookie
- 분석툴의 발달
  - IDA/Hex-Rays(x86, ARM)
  - MIPS Decompiler (http://decompiler.fit.vutbr.cz/)

스마트 기기의 기준

- 인터넷에 연결이 되어있는가?
  ex> 스마트폰
- 사용자에게 편리한 기능을 제공하는가?
  ex> 레시피를 제공하는 냉장고
- 기능 확장이 가능한가?
  ex> 스마트 TV
- 사람이 해야 할 일을 자동화 해주는가?
  ex> 자동 제어 에어컨

스마트 기기 해킹의 특징

- 금전적인 피해 유발
- 도청/감시 등 사생활 노출의 피해
- 대상을 장기간 장악 가능
- 물리적인 피해 유발
- 인명 사상 피해 유발

스마트기기 해킹 사례들

그리고 실제 해킹 시연

스마트 기기 해킹 사례들

스마트폰

스마트 카드

스마트카

CCTV

인터넷폰

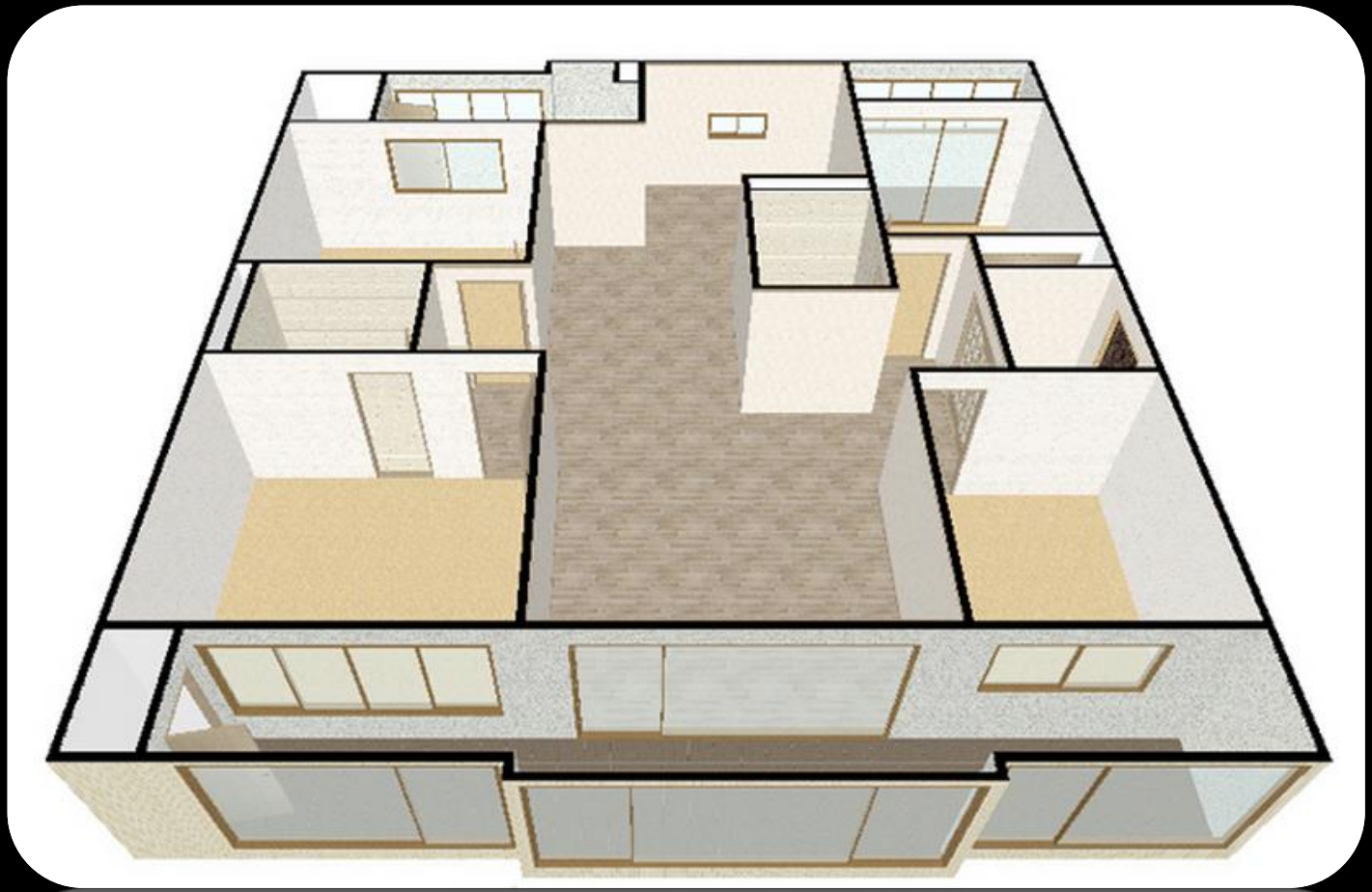
로봇청소기

가전기기

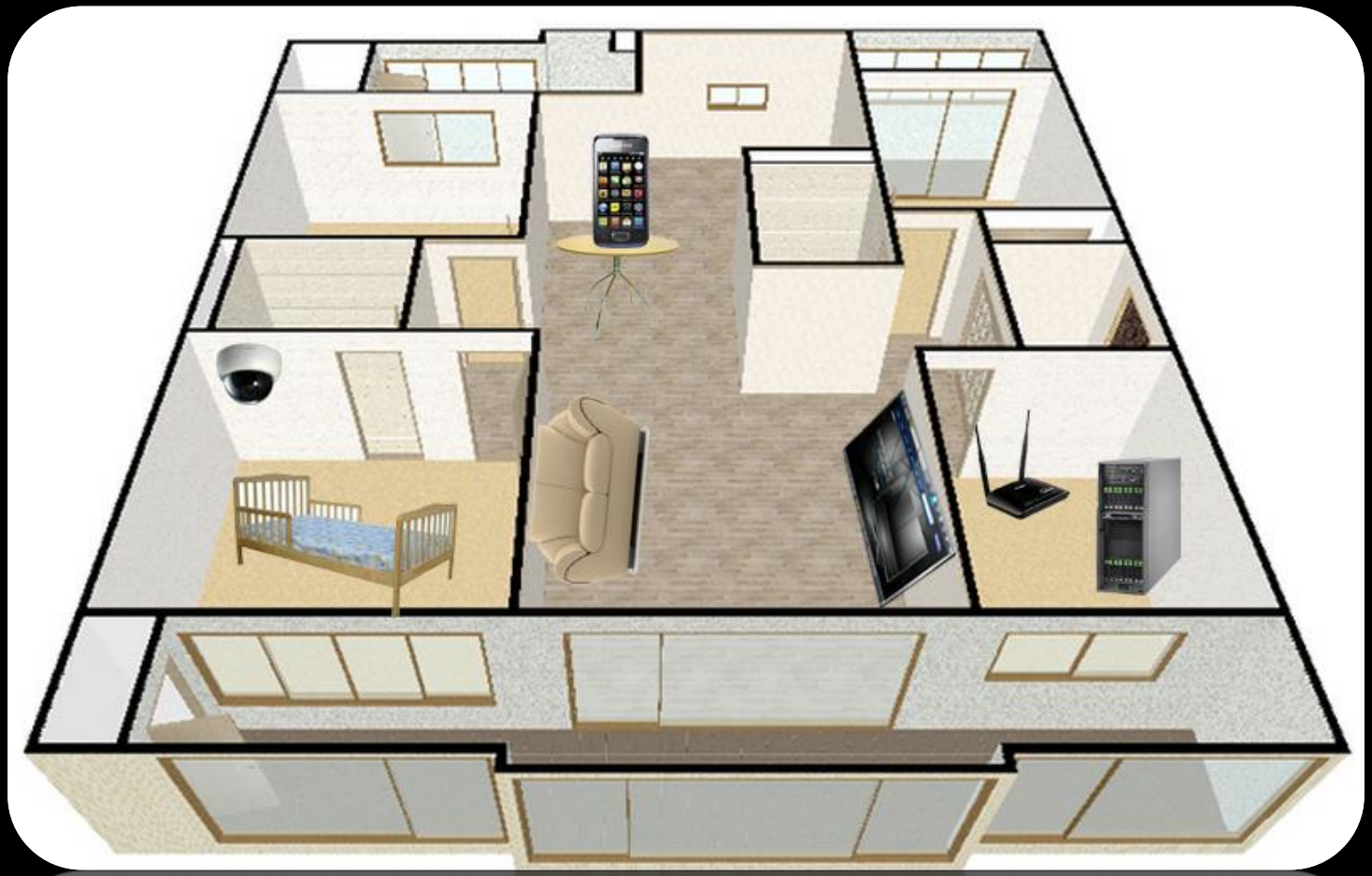
현금인출기

스마트 기기 해킹 사례들

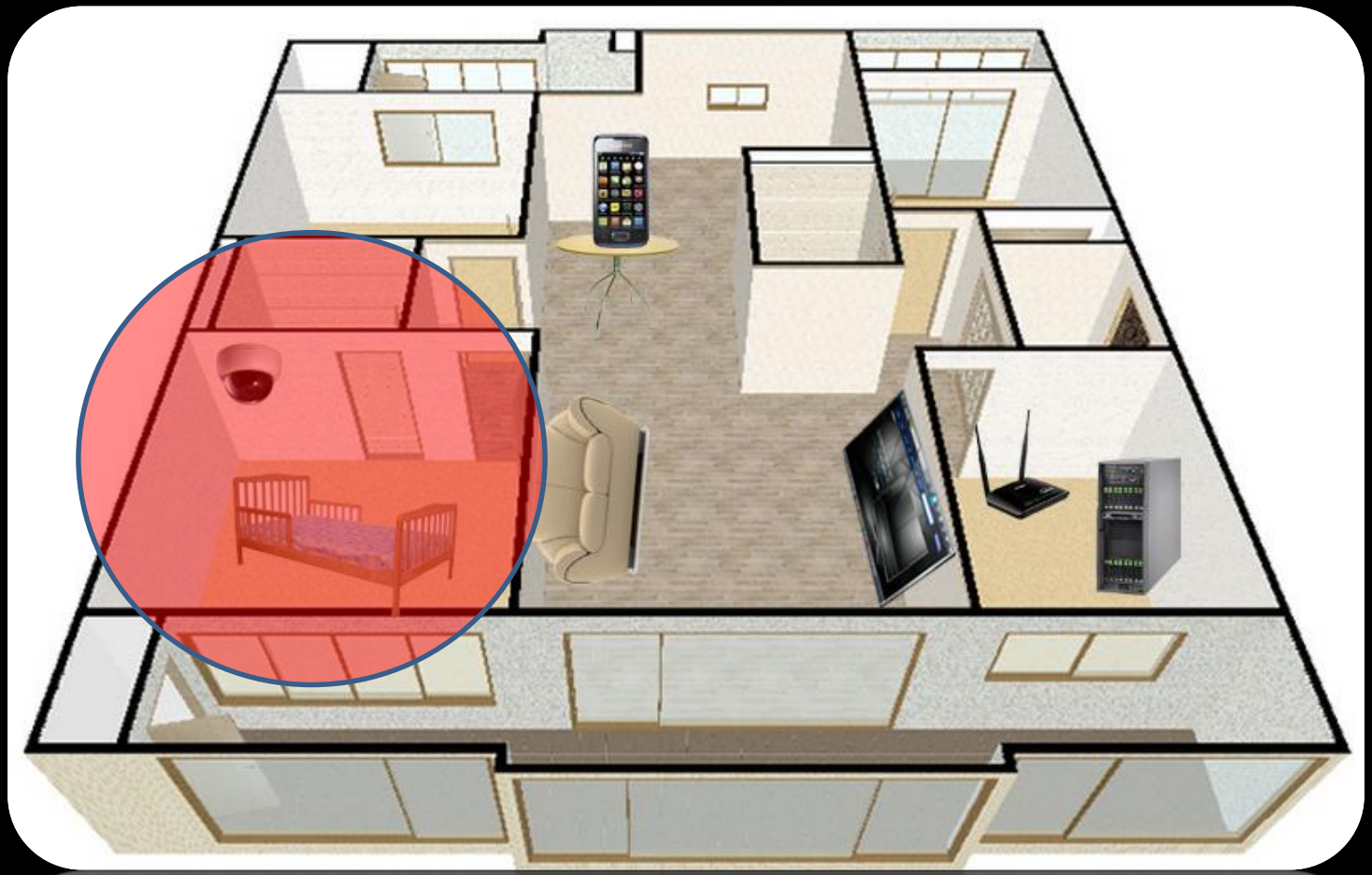
시연 환경



가정용 CCTV(IP 카메라)



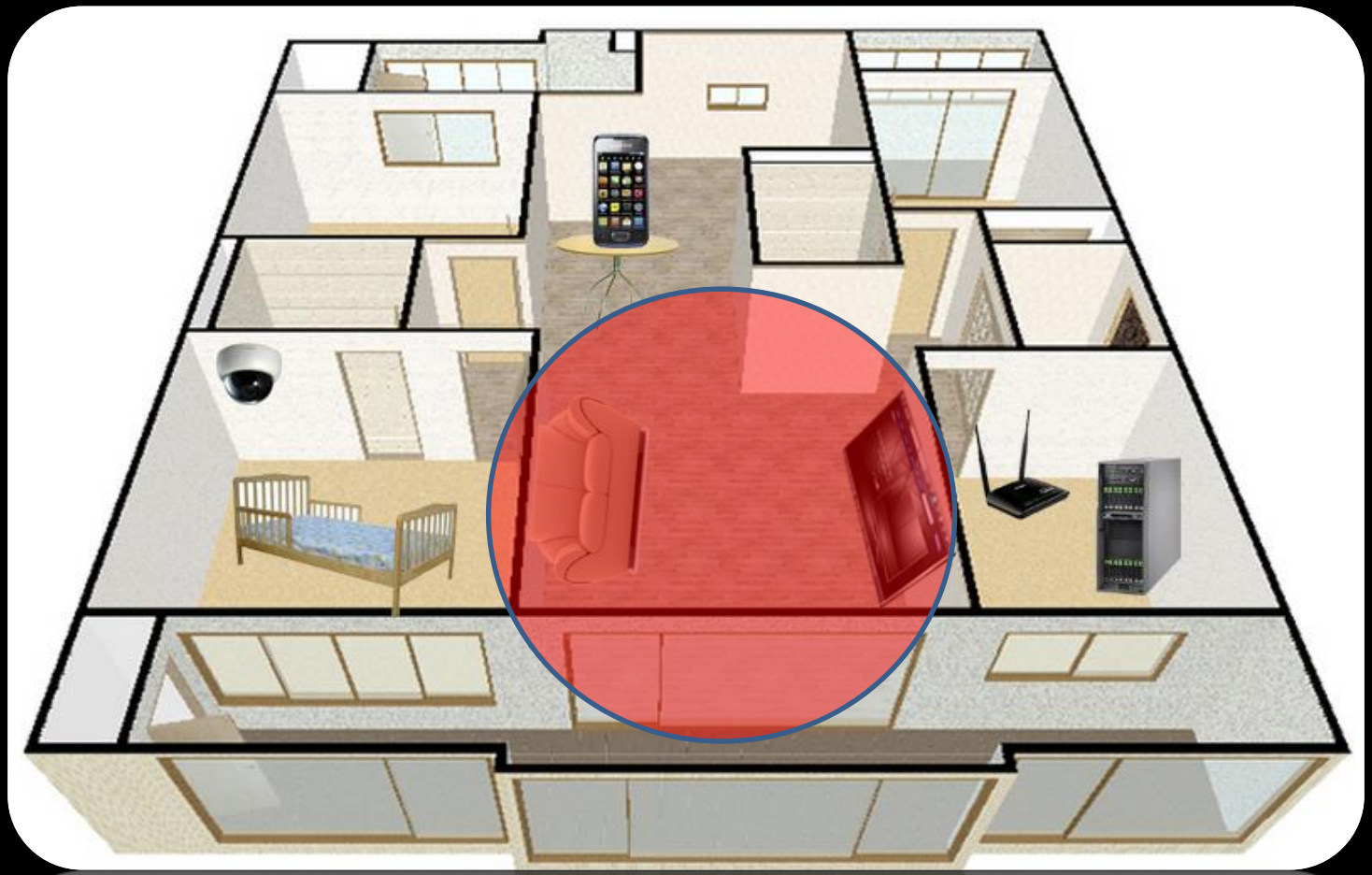
가정용 CCTV(IP 카메라)



가정용 CCTV(IP 카메라)

가정용 CCTV(IP 카메라)

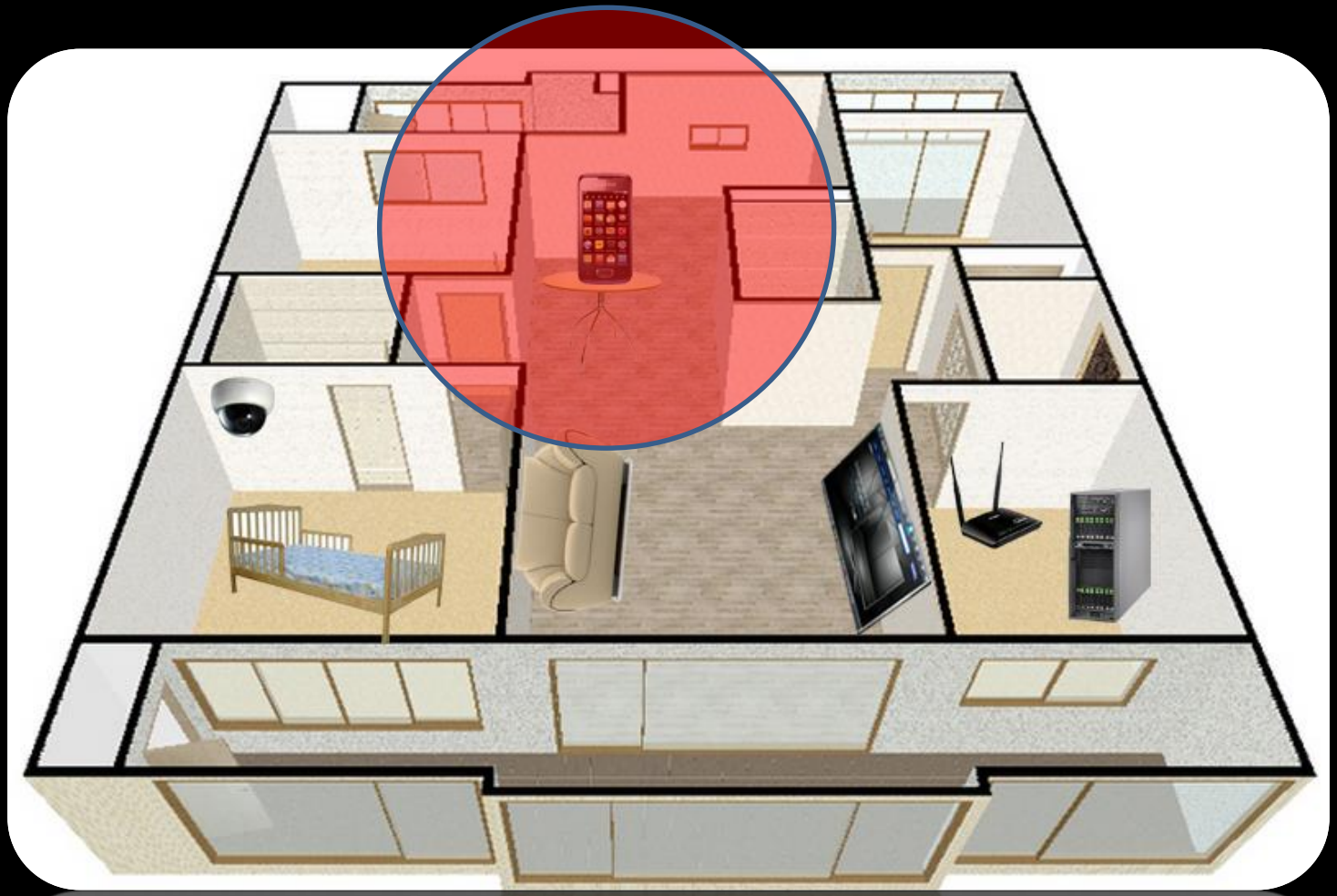
스마트 TV



스마트 TV

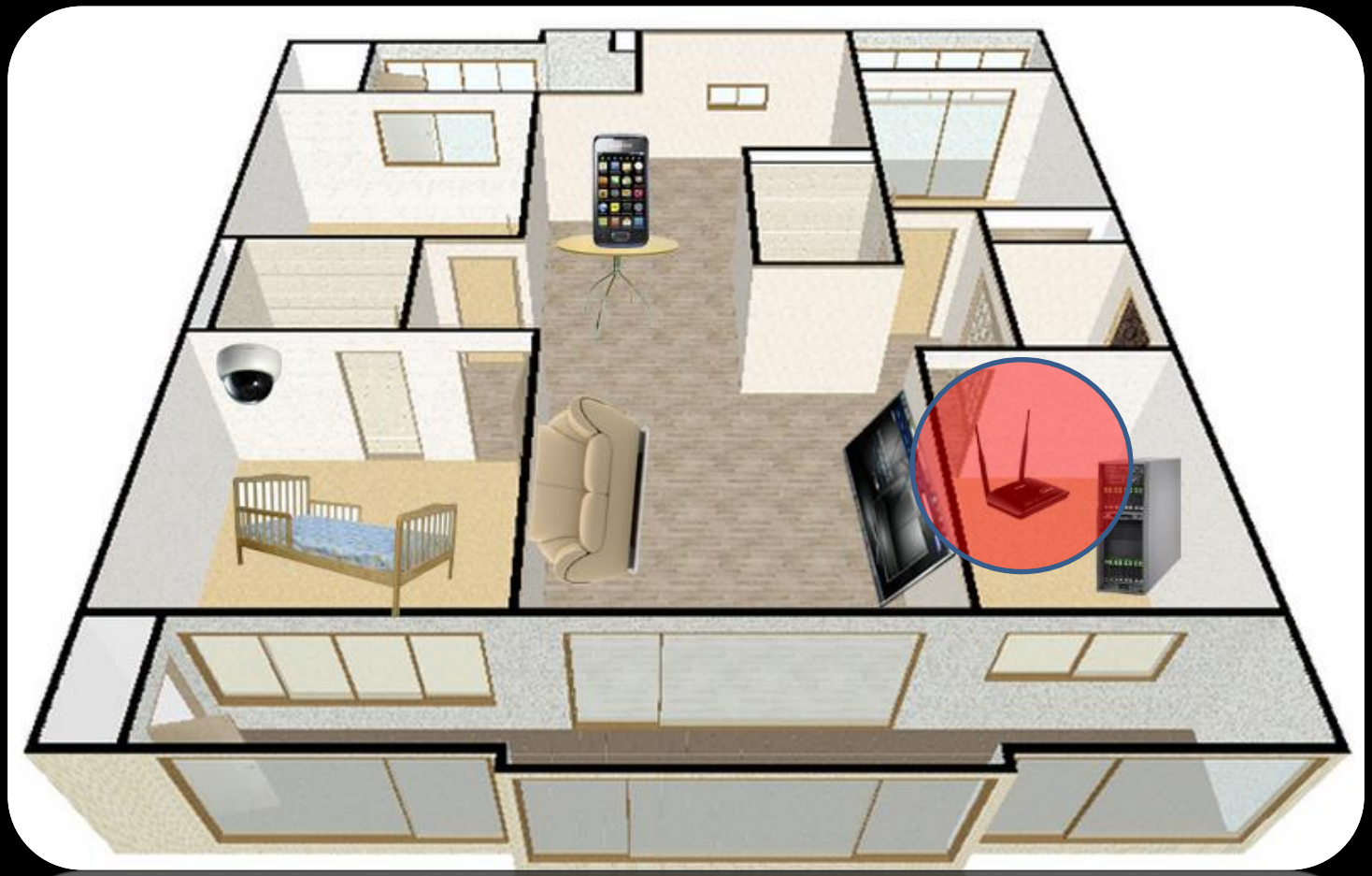
스마트 TV

스마트폰

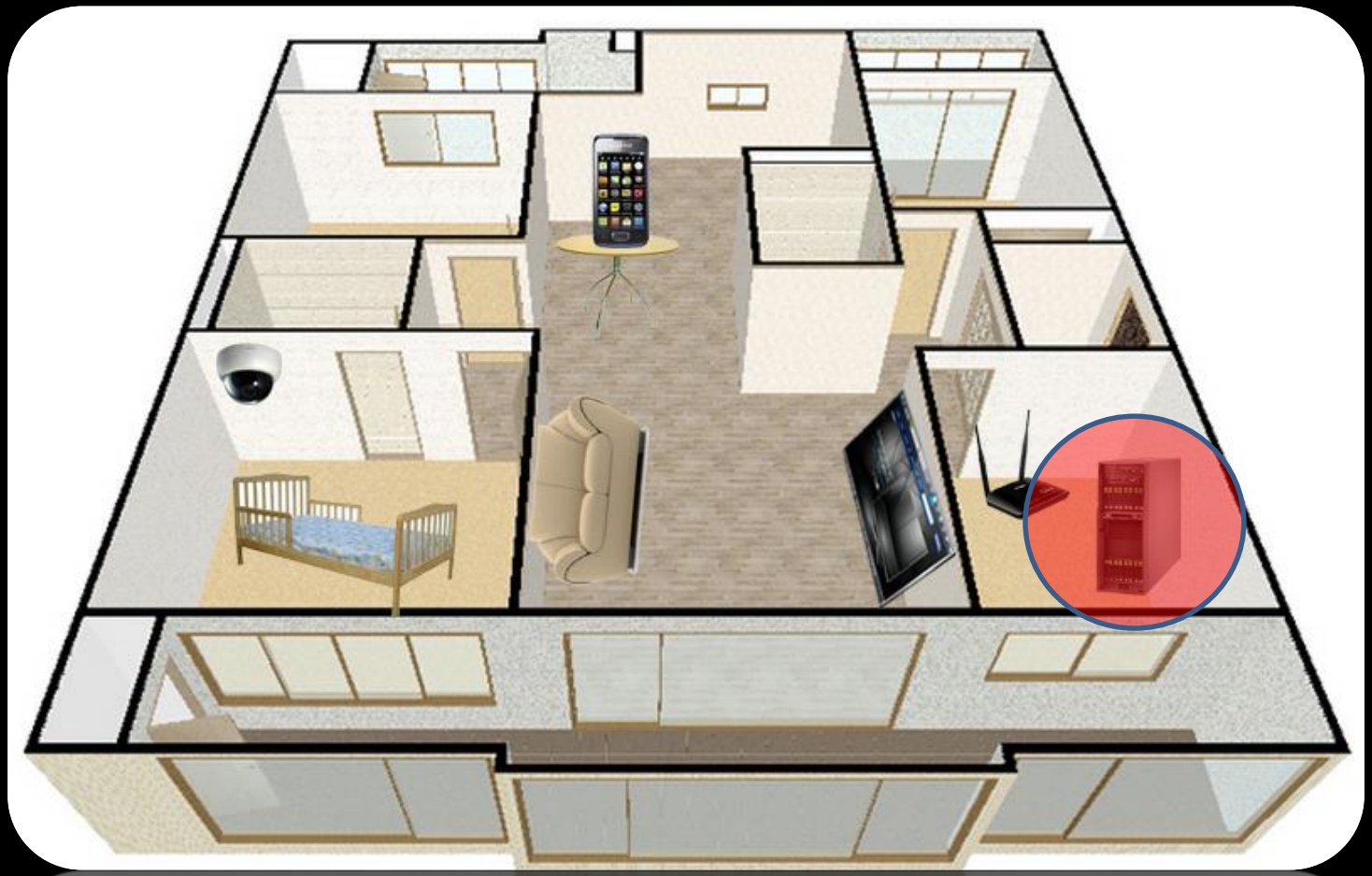


스마트폰

유무선 공유기

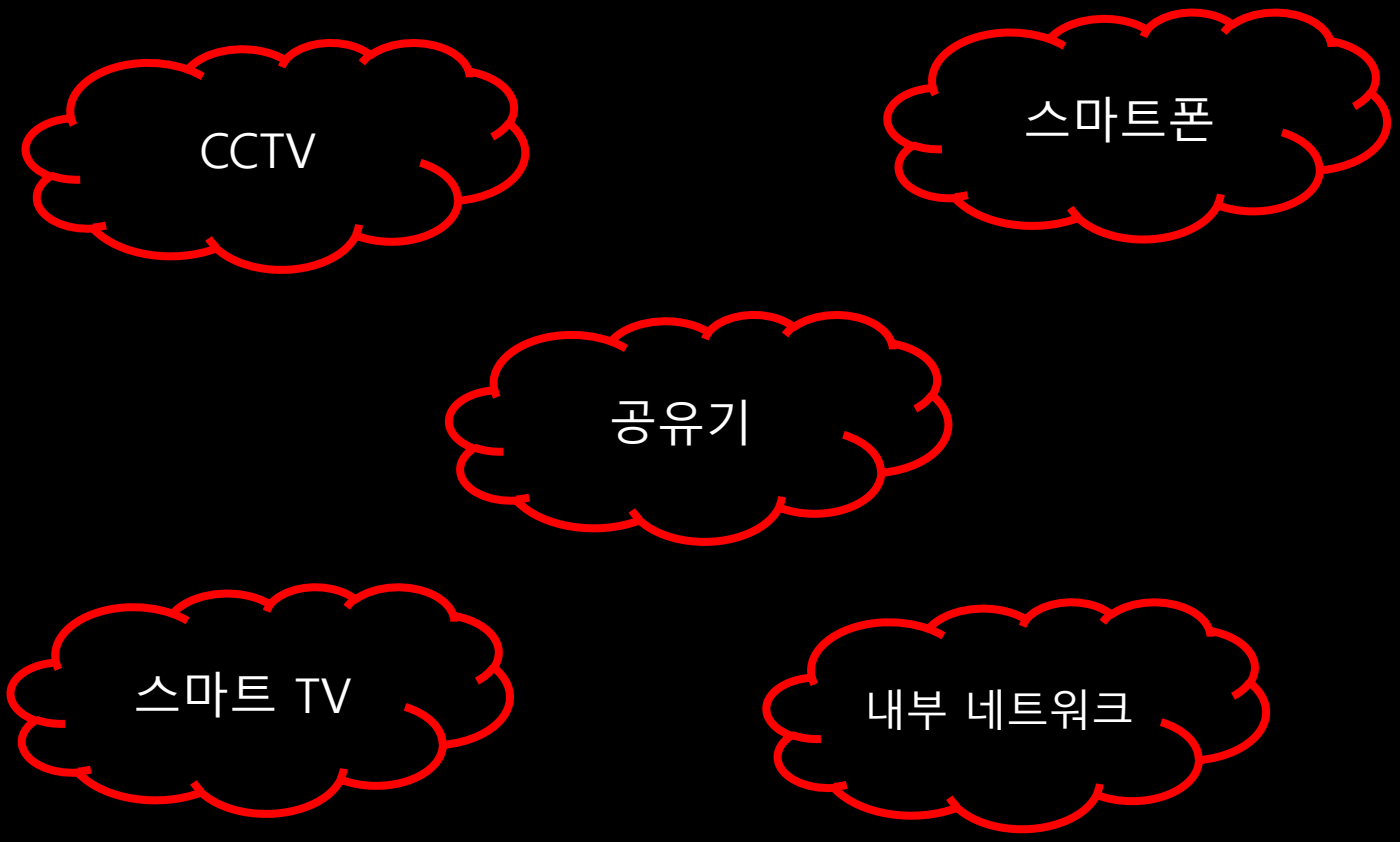


내부 네트워크



공유기 & 홈 서버

스마트 기기 해킹 시연 대상

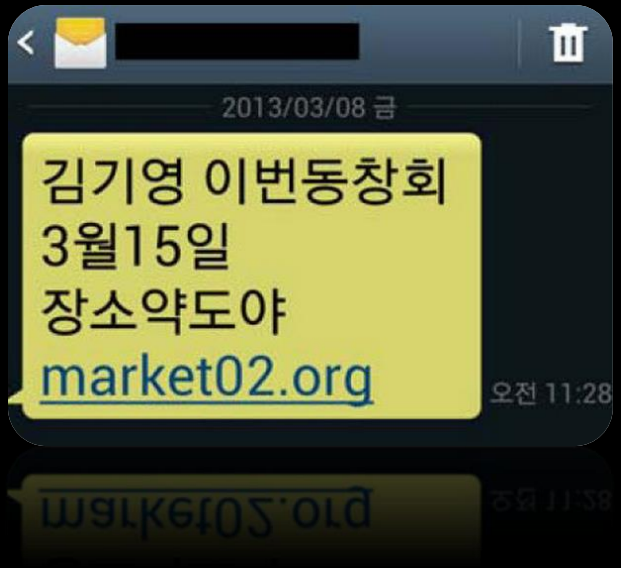


해킹 사례 소개 시작

스마트폰 해킹

스마트폰 해킹

- 요약
  - 가장 대표적인 스마트기기 해킹
  - 스마트폰 해킹의 범람 시대 (올해 피해액 40억 이상)
- 공격 방식
  - SMISHING 공격
    - 악성 앱 설치 유도
  - 웹 브라우저 공격
  - 문서 파일 이용 공격
  - NFC 공격
- 공격의 피해
  - 소액 결제, 인증서 유출
  - 사진, 연락처, SMS 유출
  - 도청, 사생활 감시



스마트폰 해킹 시연

스마트폰 NFC 해킹

- Near Field Communication
- 새로운 스마트폰 해킹 방식
- 스마트폰 근처에 접근하는 것만으로 해킹 가능
- http://www.youtube.com/watch?v=eAe0-J2v7_I

스마트 카드 해킹

- 개요
  - 스마트 카드를 복제하거나 무제한 충전 가능
  - 해킹장비가 50만원에 거래된 사례
- 공격 방식
  - 스마트 카드 프로토콜 조작
  - 스마트 카드 복제
- 공격의 피해
  - 현금 인출
  - 인증 무력화
- 관련 자료
  - http://www.yonhapnews.co.kr/economy/2012/07/13/0303000000AKR20120713038900065.HTML
  - http://www.breaknews.com/sub_read.html?uid=125806&section=sc2

스마트카 해킹

스마트카 해킹

- 요약
  - 스마트카를 원격에서 장악하여 마음대로 제어 가능
- 공격 방식
  - ECU(Electric Control Unit) 프로토콜 제어
  - 네트워크(블루투스, 위성통신) 해킹
  - 스마트폰 앱 해킹
- 공격의 피해
  - 물리적, 금전적 피해
  - 인명 사상 피해
- 관련 정보
  - http://illmatics.com/car_hacking.pdf
  - http://blog.naver.com/nl123456?Redirect=Log&logNo=60193184491
  - http://www.newspim.com/view.jsp?newsId=20130729000191
  - http://article.joins.com/news/article/article.asp?total_id=12578514&cloc=olink|article|default
  - http://news.mk.co.kr/newsRead.php?year=2013&no=637963

시연 영상

- http://www.youtube.com/watch?v=oqe6S6m73Zw

인터넷 전화기

인터넷 전화기

- 요약
  - 인터넷 전화기 해킹을 통해 도청 및 과금 가능
- 공격 방식
  - 내부 네트워크 침투 후 도청
    - ARP Spoofing
    - VoIP 패킷 스니핑
  - 전화 시스템 장악
    - 무단 통화 : 2700만원
- 관련 자료
  - http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1001238275
  - http://powerofcommunity.net/poc2008/gilgil.pdf

CCTV 해킹


SBS
8 NEWS
해킹되는 방범용 CCTV
경제 <원·달러 환율> 1,071.40 (-1.10원)

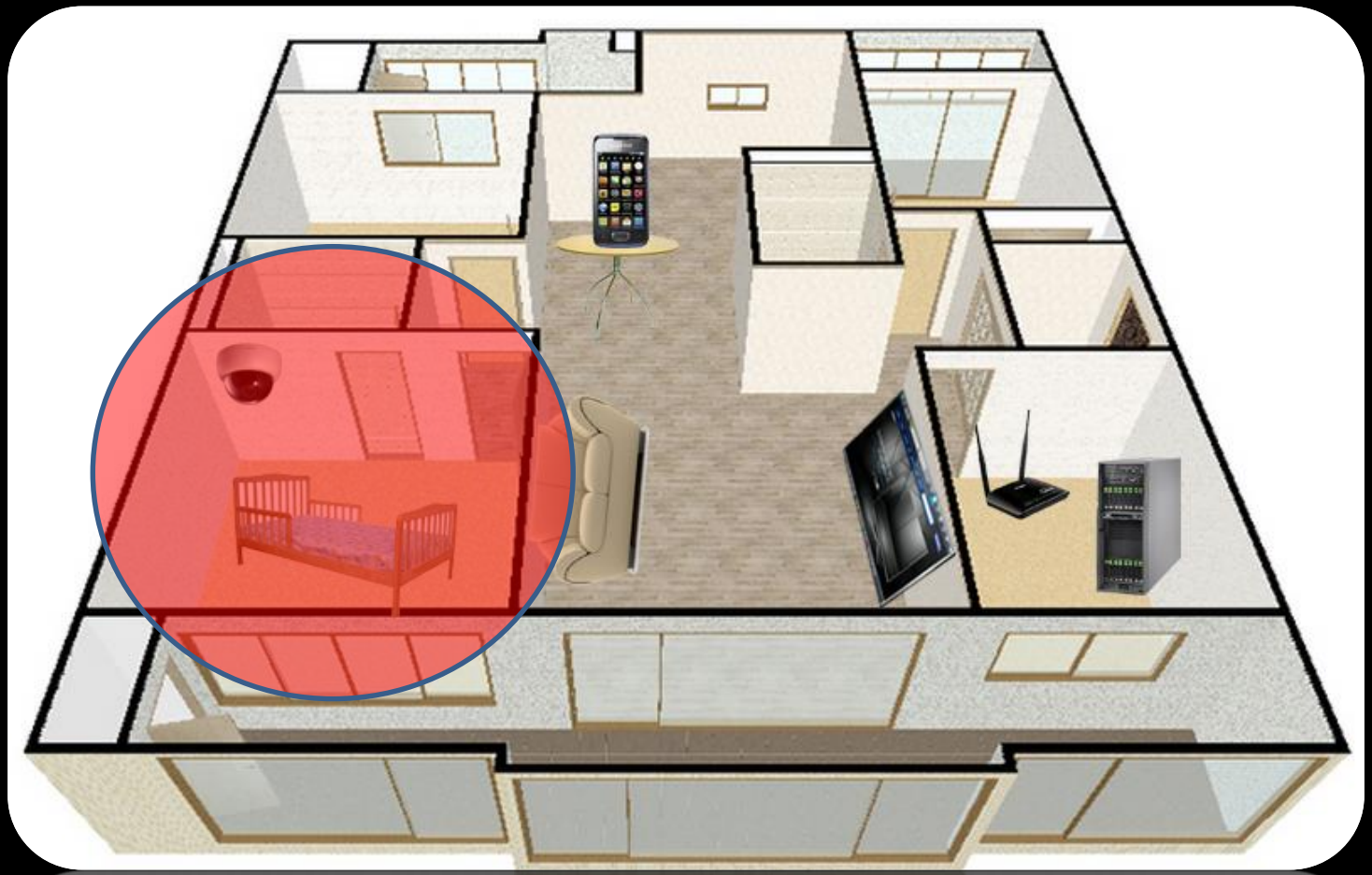

SBS
8 NEWS
사회 사립초 학부모, 영어 몰입교육 허용 요구 기자회견 개최

CCTV 해킹

- 요약
  - 인터넷에 연결된 CCTV를 해커가 훔쳐볼 수 있음
- 공격 방식
  - 공장출하 상태의 관리자 패스워드 이용
  - 쉬운 패스워드 (Password Cracking)
  - 관리자 페이지 웹 해킹
  - CCTV를 찾아내는 원리
    - 제조사별 고유의 URL 이용
      - Ex> inurl:/view/index.shtml
    - 광대역 자동 스캐닝
    - IP 추적 (ex. 이메일, SNS 등)
- 공격의 피해
  - 사생활 감시
- 관련자료
  - http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1002077186
  - http://dailysecu.com/news_view.php?article_id=2014
  - http://www.boannews.com/media/view.asp?idx=31392

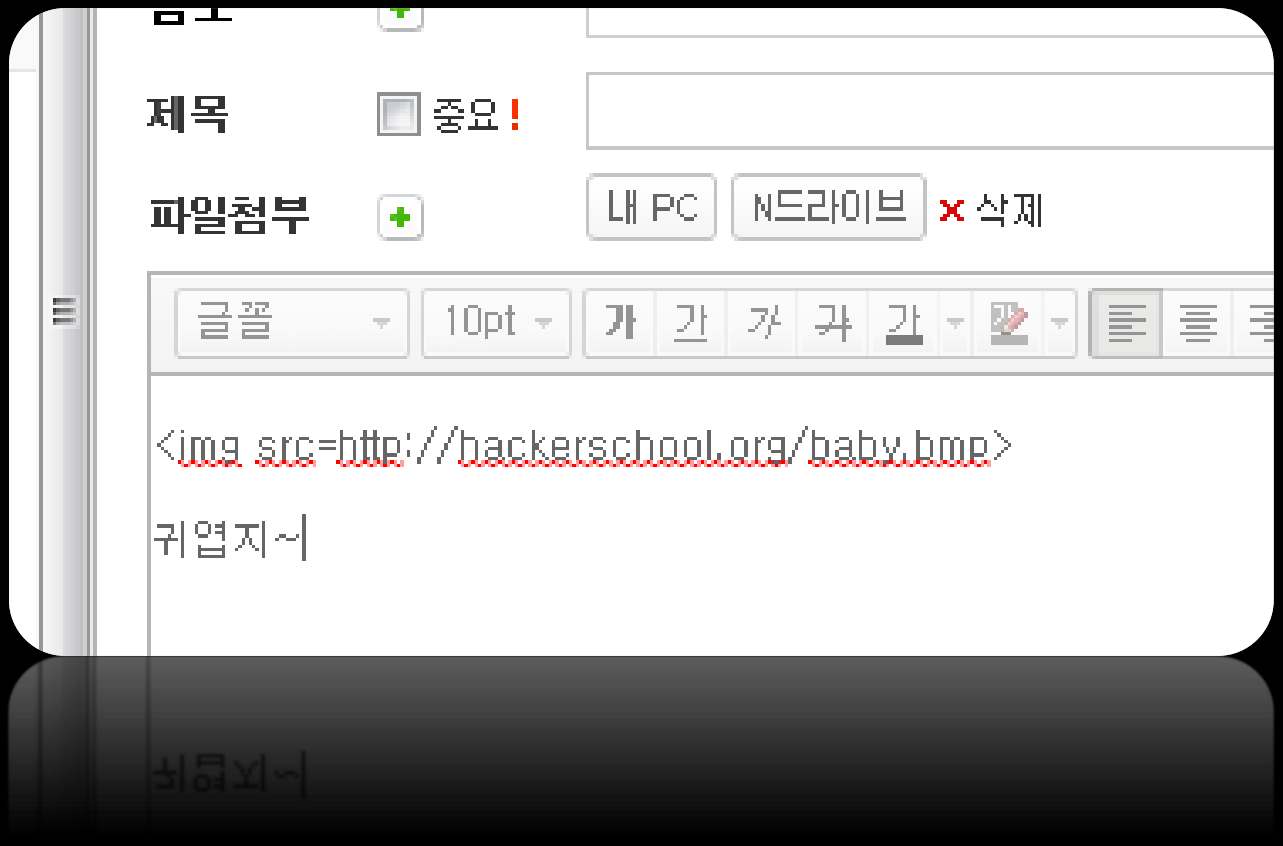
CCTV 해킹 시연

시연 환경



해커가 대상의 IP를 획득하는 방법

- E-Mail
- SNS
- SMS
- 메신저
- 등등



55.13.115.135 - - [19/Nov/2013:00:21:49 +0900] "GET /baby.bmp HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36" 439 151

CCTV 정보

모델명	포트 번호	식별 방법	기본 암호
?????	TCP 8020	Server: Reecam IP Camera	admin/(NULL)

로봇 청소기 해킹

* 상기 이미지는 해킹 사례와 무관함

로봇 청소기 해킹

- 요약
  - 아직 공개된 취약점은 없으나 곳곳에서 연구 중
- 공격 방식
  - 전용 프로그램 혹은 스마트폰이 로봇 청소기와 통신
  - 명령을 REPLAY하여 제어
- 공격 피해
  - 도청 및 감시

로봇 청소기 해킹

- 로봇 청소기의 자살(?) 사건
- 그렇다면 물리적인 해킹도 가능하지 않을까?

- 관련 자료
  - http://www.dailian.co.kr/news/view/403956

가전기기 해킹

- 스마트 냉장고
- 스마트 오븐
- 스마트 세탁기
- …

다리미 해킹

다리미 해킹

- 요약
  - 중국 업체에서 제작한 다리미 안에서 특이한 부품이 발견되어 조사해 본 결과 마이크와 주변 네트워크에 침투하거나 악성코드를 전파하는 Wi-Fi 기반의 해킹툴이 발견됨 (2013-10-30)
- 공격 방식
  - 백도어 심기
- 공격 피해
  - 주변 네트워크 장악 및 정보 유출
- 관련 기사
  - http://www.youtube.com/watch?v=hkiqenPy8zY
  - http://www.kbench.com/hardware/?no=125636&sc=1
  - http://www.etnews.com/news/international/2854994_1496.html

다리미 해킹

주전자 해킹

주전자 해킹

- 요약
  - 앞서 다리미에서 발견된 것과 동일한 해킹칩이 주전자에서 발견됨
  - 이후 다양한 가전기기에서 해킹칩이 발견 됨

- 관련기사
  - http://www.etnews.com/news/international/2855957_1496.html
  - http://nownews.seoul.co.kr/news/newsView.php?id=20131103601002

비데 해킹

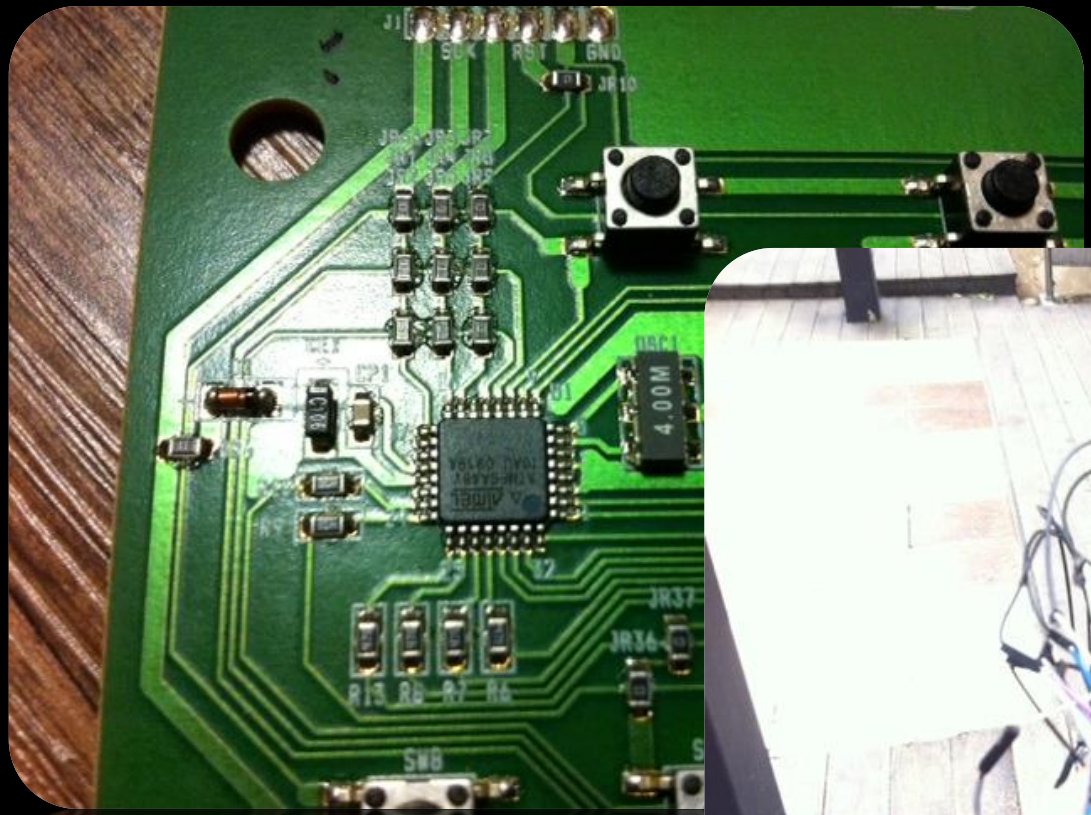
비데 해킹

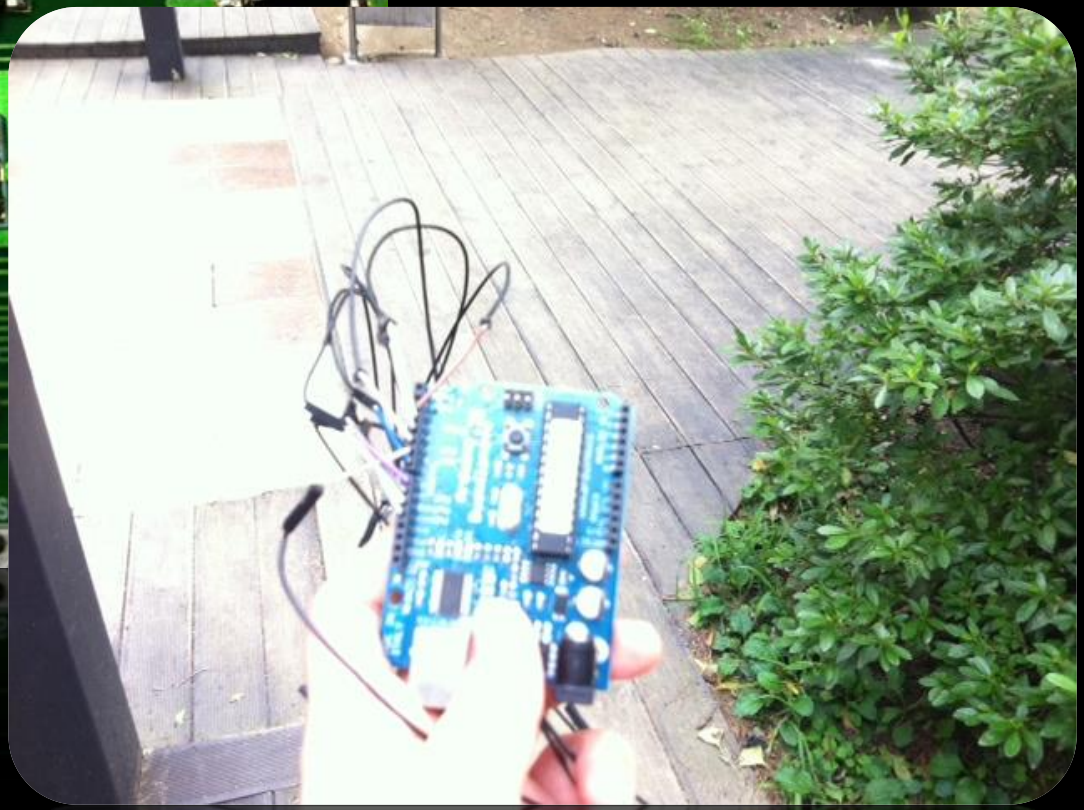
- 요약
  - 스마트 비데를 원격 제어 가능 (2013-08)
- 공격 원리
  - 정상 리모컨과 동일한 RF 신호 전송
- 공격의 피해
  - ???
- 관련 자료
  - http://www.segye.com/content/html/2013/08/06/20130806004230.html?OutUrl=naver

비데 리모트 컨트롤러

비데가 있는 화장실에 들어가는 대상

복제한 컨트롤러^.^





복제한 컨트롤러^.^

^。^。。
〃


SUPREME

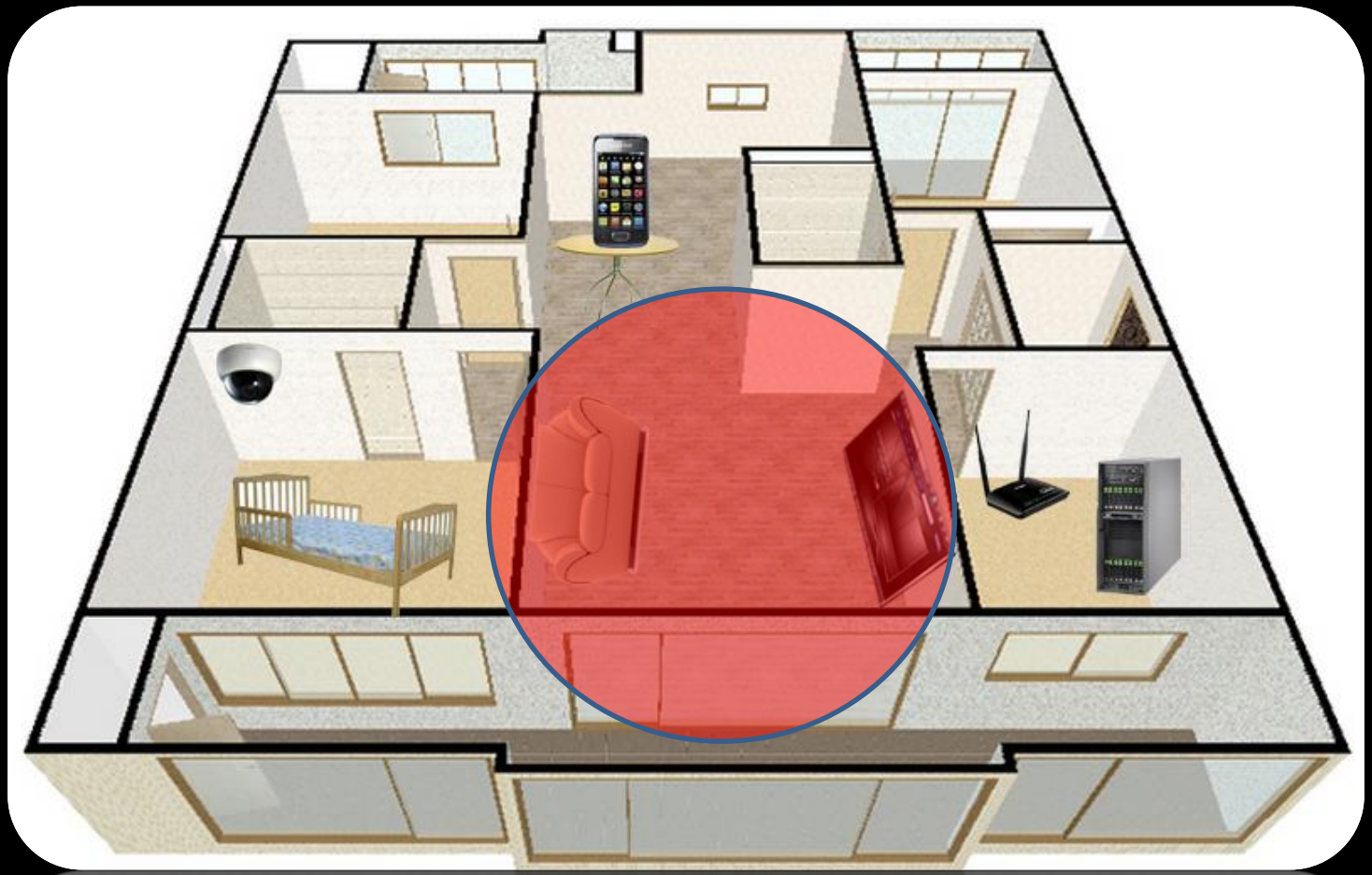

HTML

스마트 TV 해킹

- 개요
  - 스마트 TV에 장착된 카메라/마이크를 통해 24시간 감시 가능
  - 해적 방송 송출 가능
- 공격 방식
  - 원격 서비스 공격
  - 악성 앱 배포 (불특정 다수 공격 가능)
  - 웹 브라우저 공격
- 관련 자료
  - http://www.ddaily.co.kr/news/news_view.php?uid=107675
  - http://news.kbs.co.kr/news/NewsView.do?SEARCH_NEWS_CODE=2726354&ref=A
  - https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf
  - http://www.boannews.com/media/view.asp?idx=34069

스마트 TV 해킹 시연

스마트 TV



스마트 TV

해적 방송 시연

현금인출기(ATM)

- 요약
  - ATM의 취약점을 해킹하여 현금 인출 성공 (2010-10)
- 공격 원리
  - 13456 포트로 작동하는 원격 서비스 해킹
  - 악성 프로그램 업로드
  - ATM 작동 조작
- 관련자료
  - http://www.youtube.com/watch?v=Ss_RWctTARU

시연 영상

- http://www.youtube.com/watch?v=fS3Z8Xv-vUc

디지털 도어락 해킹

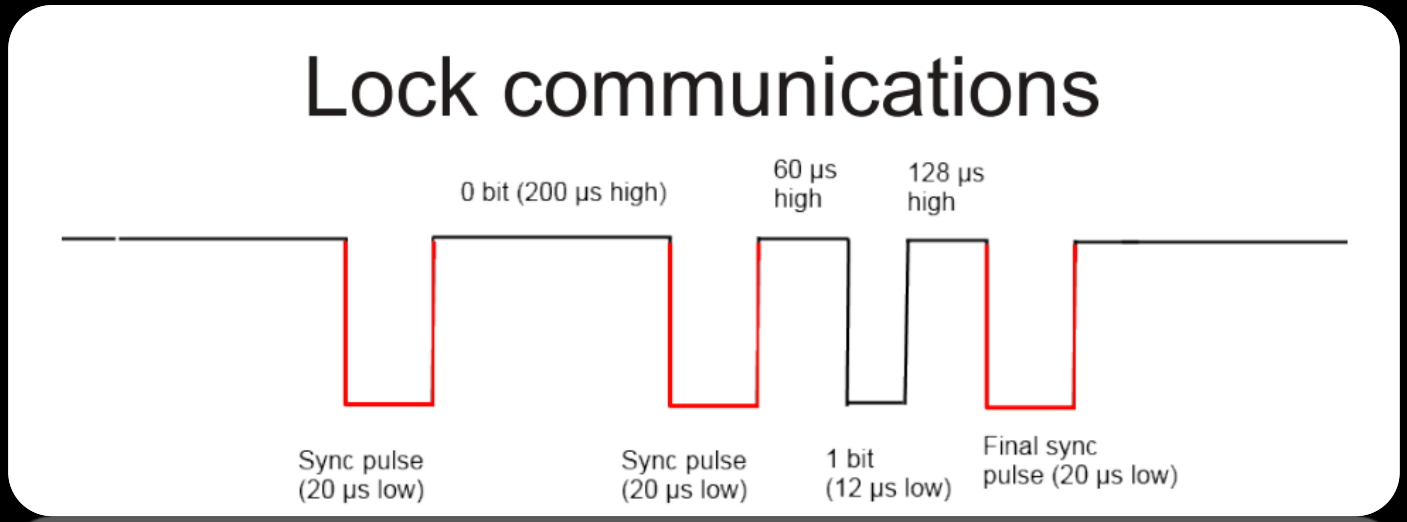
디지털 도어락

- 요약
  - 호텔 등에 설치된 디지털 도어락을 1초도 안돼 열 수 있음을 시연 (2012-10)

- 관련 자료
  - http://blogs.computerworld.com/security/20745/black-hat-hotel-keycard-lock-picking-less-time-it-takes-blink
  - http://demoseen.com/bhtalk2.pdf
  - https://media.blackhat.com/bh-us-12/Briefings/Brocious/BH_US_12_Brocious_Hotel_Key_Slides.pdf
  - http://www.youtube.com/watch?v=t5ca-e4xUVs

디지털 도어락

- 공격 원리
  - 마스터(portable programmer)와 도어락 사이의 신호 분석



  - sitecodes(일종의 비밀키)를 읽는 방법 분석
  - 비밀키와 함께 open command 전송

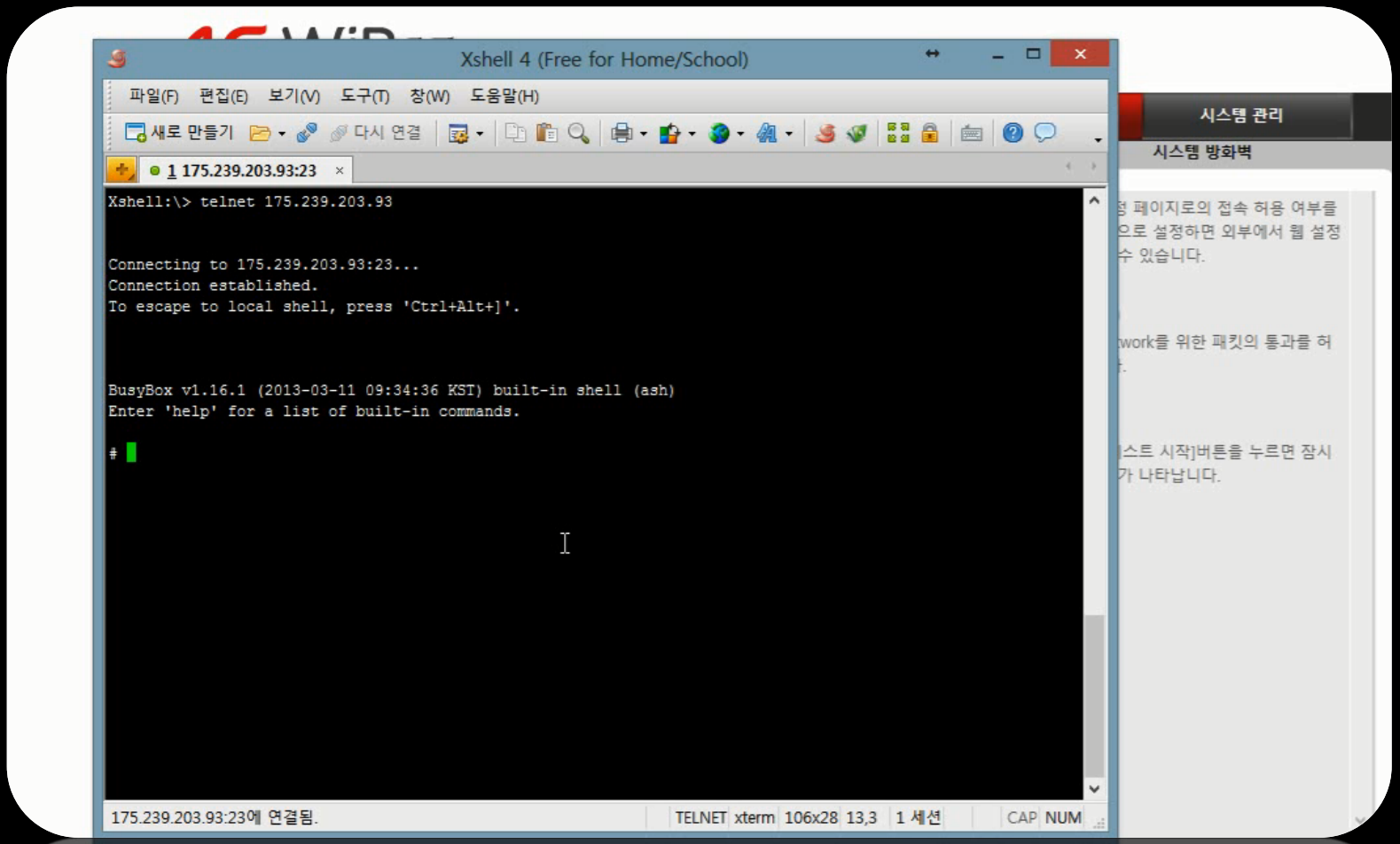
시연 영상

- http://www.youtube.com/watch?v=t5ca-e4xUVs

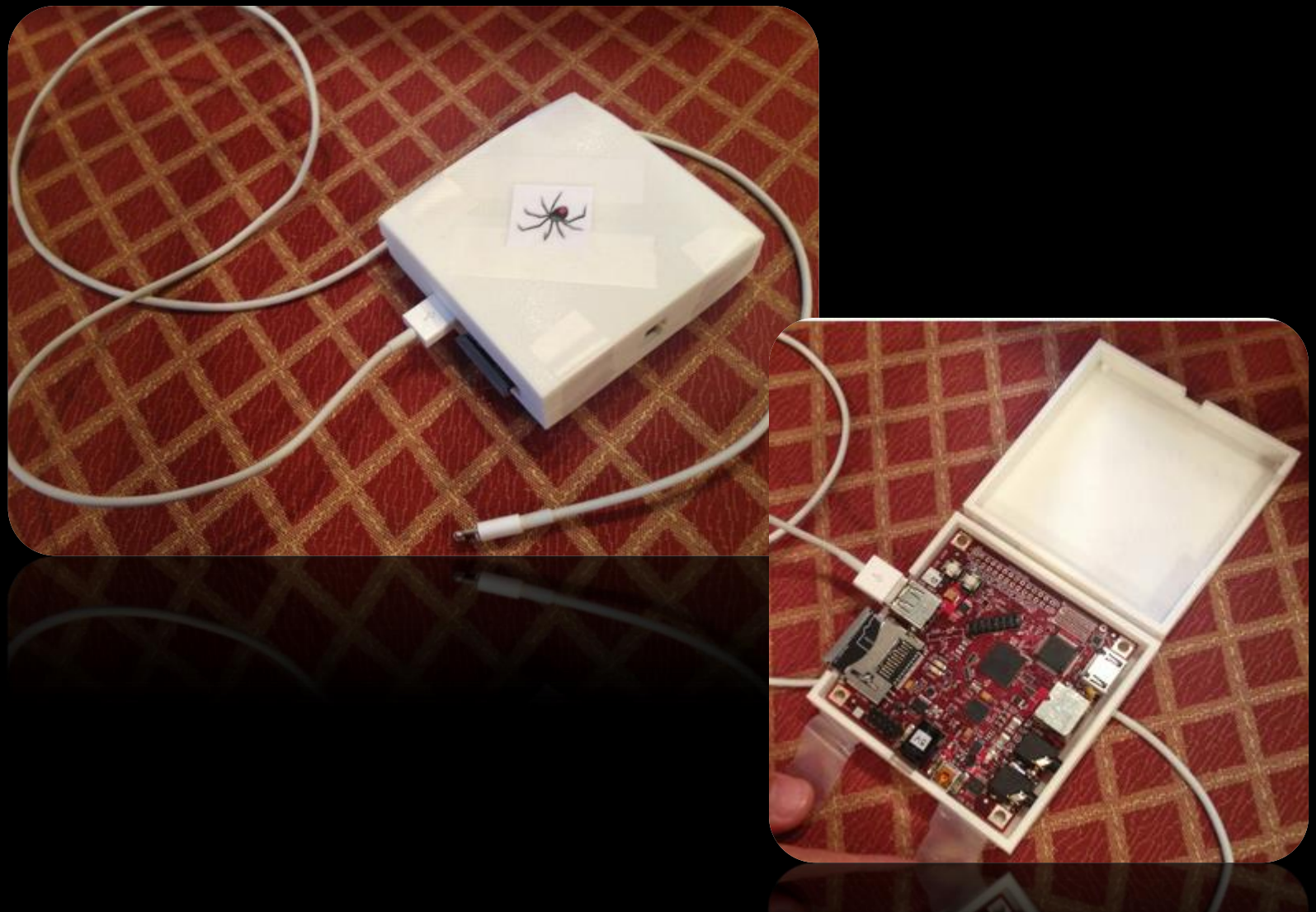
와이브로 EGG

- 개요
  - 무선 인터넷 사용을 가능하게 해주는 장비
  - 와이브로 EGG에 원격 침투 취약점 존재
- 공격 방식
  - 관리자 페이지 노출
  - 웹해킹 취약점 존재
- 공격 피해
  - DNS Spoofing
  - Packet Sniffing

시연 영상


Xshell 4 (Free for Home/School)
파일(F) 편집(E) 보기(V) 도구(T) 창(W) 도움말(H)
새로 만들기
다시 연결
1 175.239.203.93:23
Xshell:\> telnet 175.239.203.93
Connecting to 175.239.203.93:23...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
BusyBox v1.16.1 (2013-03-11 09:34:36 KST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
#
175.239.203.93:23에 연결됨.
TELNET xterm 106x28 13,3 1 세션
CAP NUM
시스템 관리
시스템 방화벽

휴대전화 충전기 해킹



휴대전화 충전기 해킹

- 요약
  - 충전기로 위장된 해킹장치에 아이폰 연결 시 악성 앱 자동 설치 (2013-08)
- 공격 방식
  - 프로토콜을 분석하여 재전송
- 공격 피해
  - 충전기 연결 시 악성코드 감염
- 참고자료
  - https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
  - https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-Slides.pdf
  - http://www.3ders.org/articles/20130804-3d-printed-modified-mactans-charger-could-hack-iphone-in-minutes.html

유무선 공유기 해킹

유무선 공유기 해킹

- 개요
  - 네트워크 구성을 위한 필수 장비
  - 원격 쉘 획득 취약점 발견 (2012-10)
- 공격 방식
  - 관리자 페이지 접근 허용 취약점
  - 관리자 페이지 웹 해킹 취약점
  - 원격 서비스의 취약점 (upnpd, ftpd, vpn, ftpd…)
- 공격 피해
  - Packet Sniffing
  - HOST 변조 (파밍)
  - MiTM Attack
- 관련 자료
  - http://www.powerofcommunity.net/poc2012/re&si.pdf
  - http://www.hackerschool.org/Sub_Html/HS_Posting/?uid=32

유무선 공유기 해킹 시연

내부 네트워크 침투 시연

내부 네트워크 구조

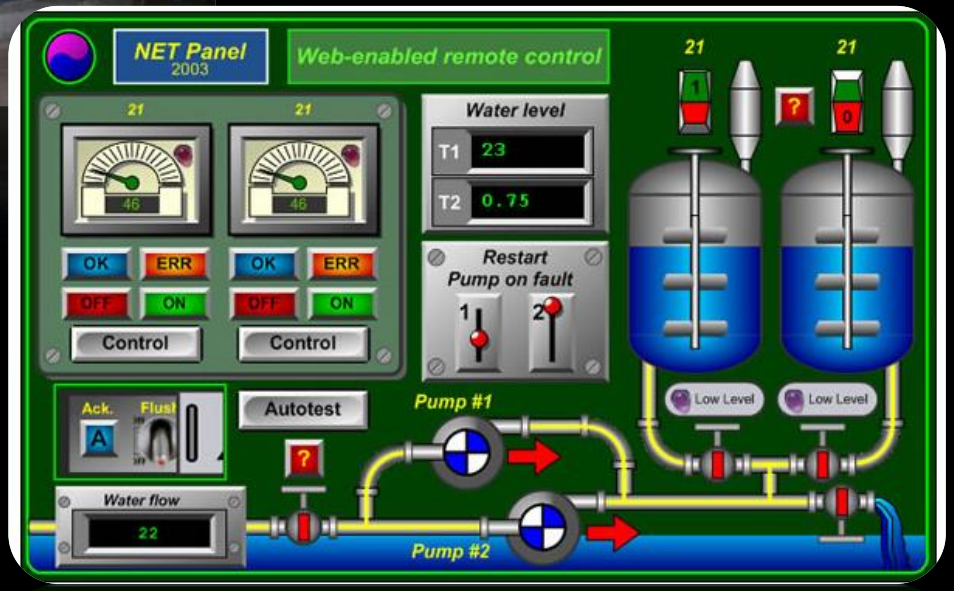
외부 : 121.13.14.15
내부 : 192.168.0.1

내부에서만
접속 가능!!

개발자
내부 : 192.168.0.77

개발서버
내부 : 192.168.0.9

스카다 시스템


NET Panel
2003
Web-enabled remote control
21
21
Water level
T1
23
T2
0.75
OK
ERR
OFF
ON
Control
Restart
Pump on fault
1
2
Ack.
Flush
A
Autotest
Pump #1
Low Level
Low Level
Water flow
22
Pump #2

스카다 시스템

- 개요
  - 사회기반시설에 대한 통합제어시스템
  - 수력발전소, 원자력발전소 등
- 공격 방식
  - 스카다와 연결된 PC 해킹 후 침투
- 공격의 피해
  - 발전소 작동 중단, 파괴
  - Stuxnet
    - 이란 핵시설 공격 (원심분리기 100여기 파괴)
  - 미 일리노이 수자원 펌프 파괴
- 관련자료
  - http://www.powerofcommunity.net/images/pdf.gif
  - http://dailysecu.com/news_view.php?article_id=992
  - http://blog.daum.net/windada11/8756610
  - http://blog.daum.net/sgshwan/15951121
  - http://www.youtube.com/watch?v=3EICf4ztfyM
  - http://www.itworld.co.kr/news/72861

스카다 시스템 해킹

스카다 시스템 해킹

- http://www.youtube.com/watch?v=fJyWngDco3g

의료기기 해킹

의료기기 해킹

- 심장박동기 해킹 (2012)
  - 과전압 발생
- 인슐린 펌프 해킹 (2012)
  - 과다 약물 투여

- 특수 제작된 안테나를 이용하여 약 90m 밖에서도 공격 가능
- 관련 자료
  - http://www.youtube.com/watch?v=THpcAd2nWJ8

기타

- 네비게이션 해킹
- 블랙박스 해킹
- 구글 글래스 해킹
- 스마트 시계
- UAV(무인항공기) 해킹
- 스마트 카메라
- POS(판매시점관리)
- MP3 Player
- 디지털 프린터
- 가정용 게임기
- 배터리 해킹
- 항공기, 선박 해킹

스마트기기 취약점 발견 과정 요약

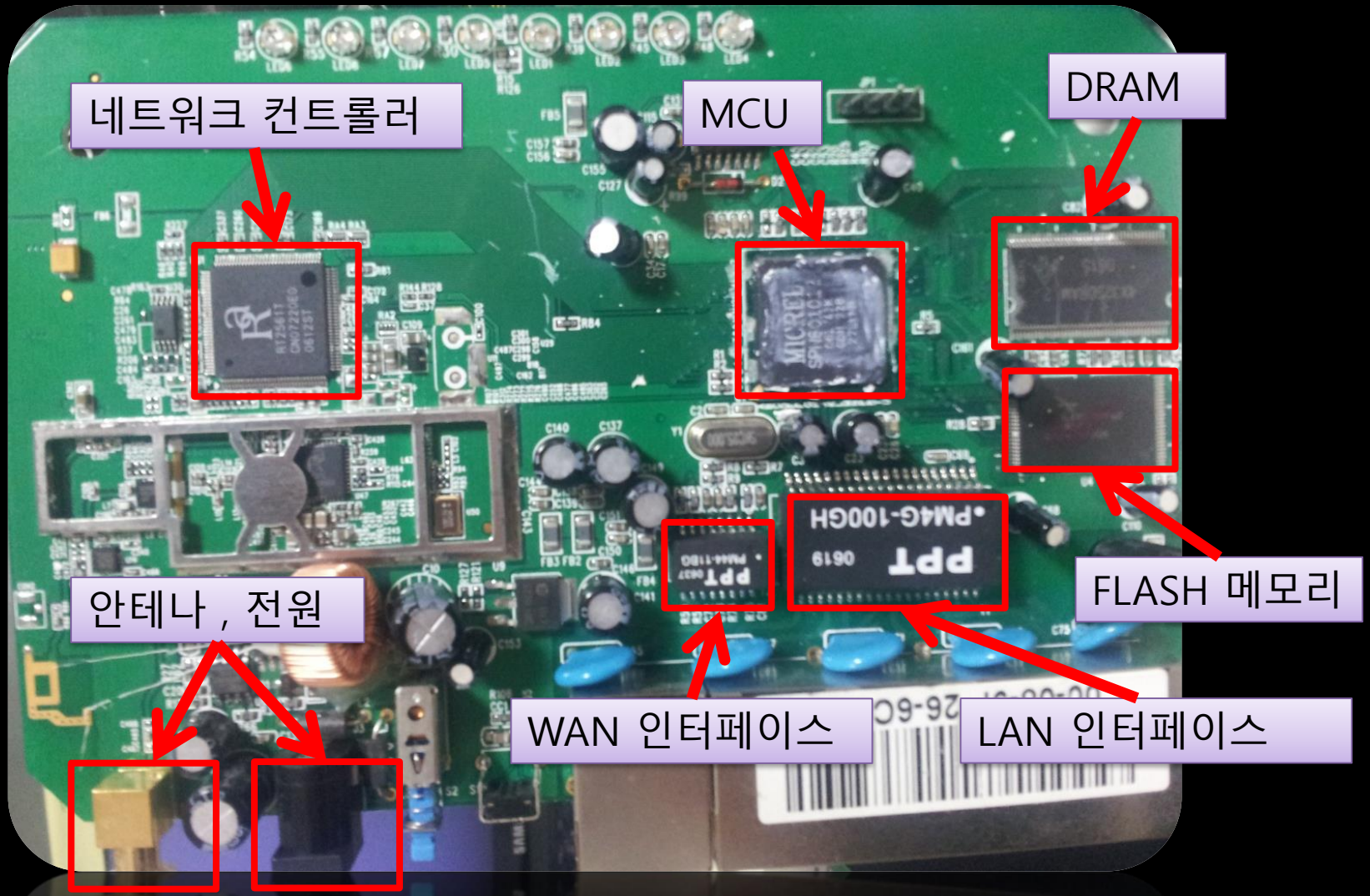
스마트 기기 취약점 분석 절차

- 대상 선정
- 펌웨어 획득
- 파일의 구성 이해
- 사용자 입력 가능 바이너리 탐색
- 바이너리 분석 및 취약점 탐지
- Debugging
- Exploit 개발

스마트 기기의 구조

- 하드웨어
  - CPU
  - 네트워크 컨트롤러
  - RAM
  - Flash ROM
  - GPU, Camera, MIC …
- 소프트웨어
  - 운영체제
  - 파일시스템

하드웨저적인 구조 예(공유기)



Firmware 획득 방법

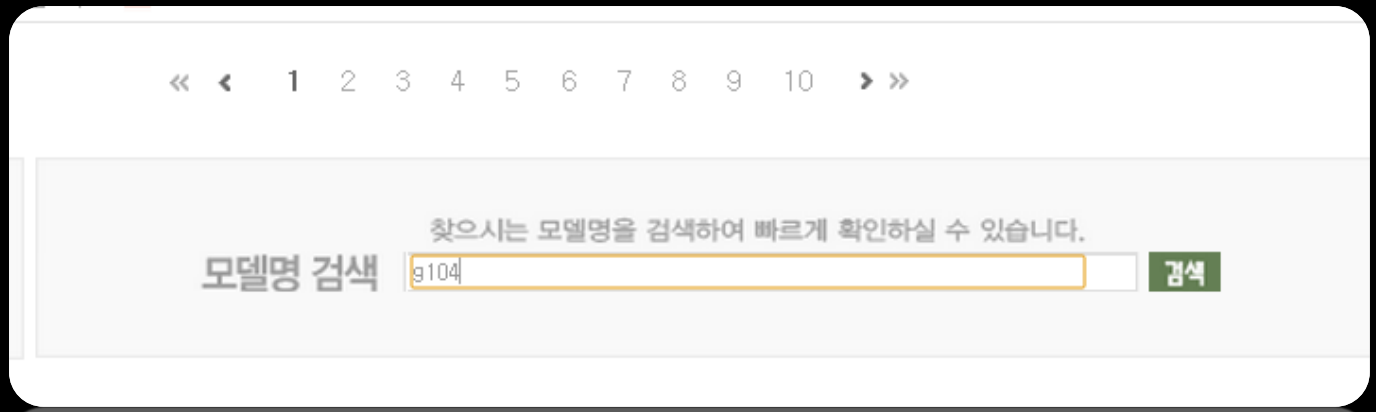
- 제조사에서 제공하는 Update 파일로부터 추출
- 논리적 취약점을 이용하여 Shell 접근 권한 획득 후 추출 (partition dump)
- UART, JTAG 포트를 이용하여 추출
- Flash Memory Dumping

Firmware만 획득하면..

- 그 다음은..

기존의 Software Hacking과
크게 다르지 않다!

업데이트 파일 다운받기



번호	제목	날짜	조회
123	ipTIME **g104** 펌웨어 버전 8.46	2012-11-14	10896
122	ipTIME **g104** 펌웨어 버전 8.44	2012-11-07	2666
121	ipTIME **g104**i 펌웨어 버전 8.38	2012-09-06	1993
120	ipTIME **g104**M 펌웨어 버전 8.38	2012-09-06	6006
119	ipTIME **g104**BE 펌웨어 버전 8.38	2012-09-06	4293
118	ipTIME **g104**A 펌웨어 버전 8.38	2012-09-05	2098
117	ipTIME **g104**A 펌웨어 버전 8.32	2012-07-18	1069
116	ipTIME **g104**A 펌웨어 버전 8.30 (ipTIME 모바일 앱 지원)	2012-07-05	892

업데이트 파일의 구성

- Boot-loader
- Kernel
- Ram Disk (initrd)
- Root File System

- 위와 같은 파일들이 하나의 파일로 덩어리져있다.
- 업데이트 파일의 성격에 따라 구성이 다를 수 있다.

펌웨어 구성 자동 분석 툴

- Binwalk
  - Firmware Analysis Tool
  - 펌웨어 파일의 구성 분석
  - https://code.google.com/p/binwalk/

- FMK
  - Firmware Mod Kit
  - 펌웨어 파일 내에서 각종 파일 추출
    - 펌웨어 추출의 원리
      - Signature 탐색
      - Ex> squashfs == "hsqs"
  - 혹은 수정된 파일을 기반으로 새 펌웨어 빌드
  - https://code.google.com/p/firmware-mod-kit/

UART를 이용한 정보 획득

- Universal asynchronous receiver/transmitter
- 하드웨어 통신 규약의 한 종류
- 기기간 통신에 범용적으로 사용
- 시리얼 통신
  - 데이터 송신/수신 시 각각 하나의 선만 이용
- "프로토콜이 매우 간단함"
- 디버깅 정보, 쉘, 펌웨어 획득 가능

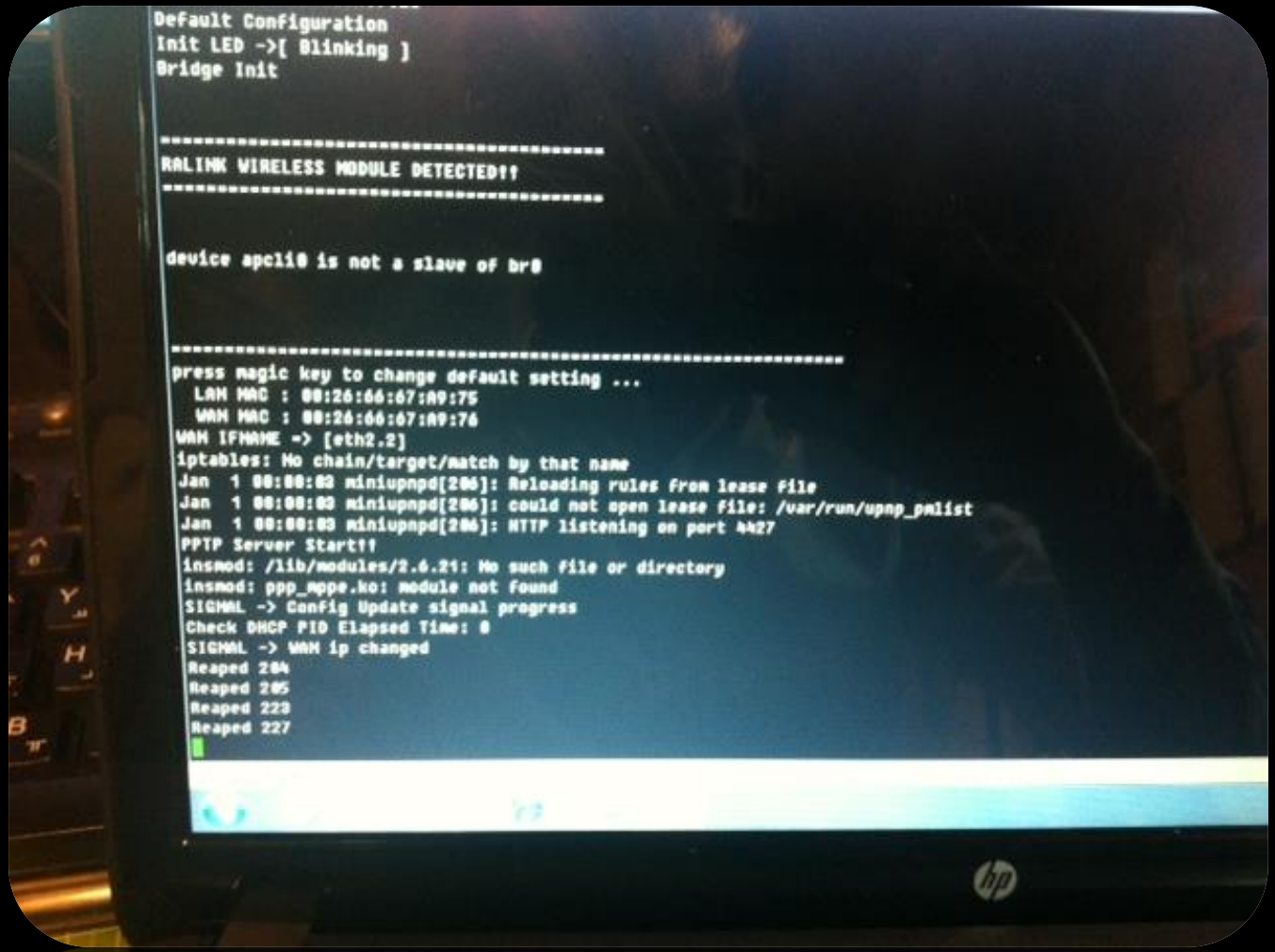
UART 장비 <-> PC 연결

- USB-UART, USB-RS232, USB-SERIAL
  - USB 기반 UART 통신 장비
  - 장치관리자 -> 포트 ->com?으로 연결 됨
  - 다음 장비 추천 (AVR Writer로도 사용 가능)

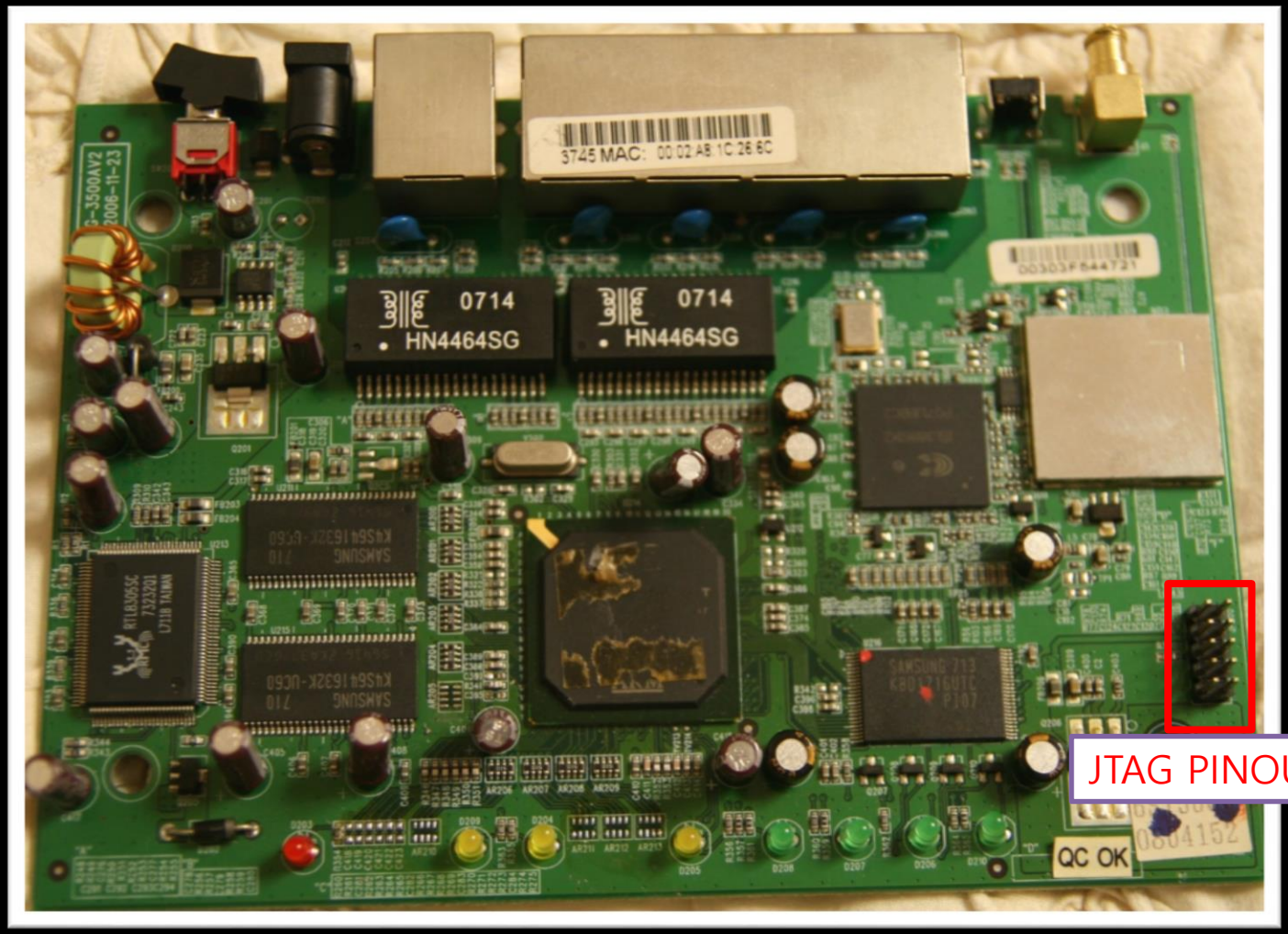
공유기 UART 연결 예제

공유기 UART 연결 예제

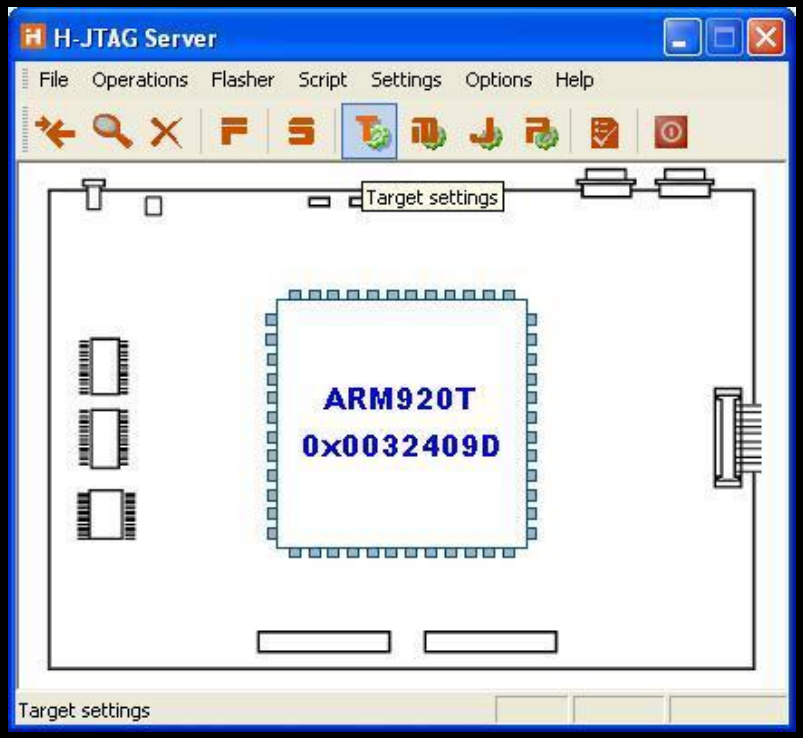
공유기 UART 연결 예제

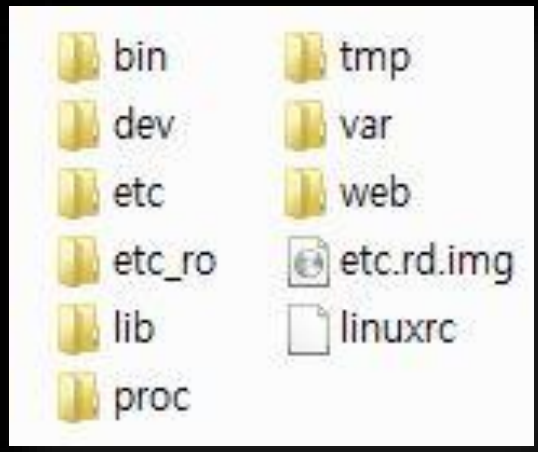


JTAG 포트를 이용한 Firmware 덤프



JTAG 포트를 이용한 Firmware 덤프



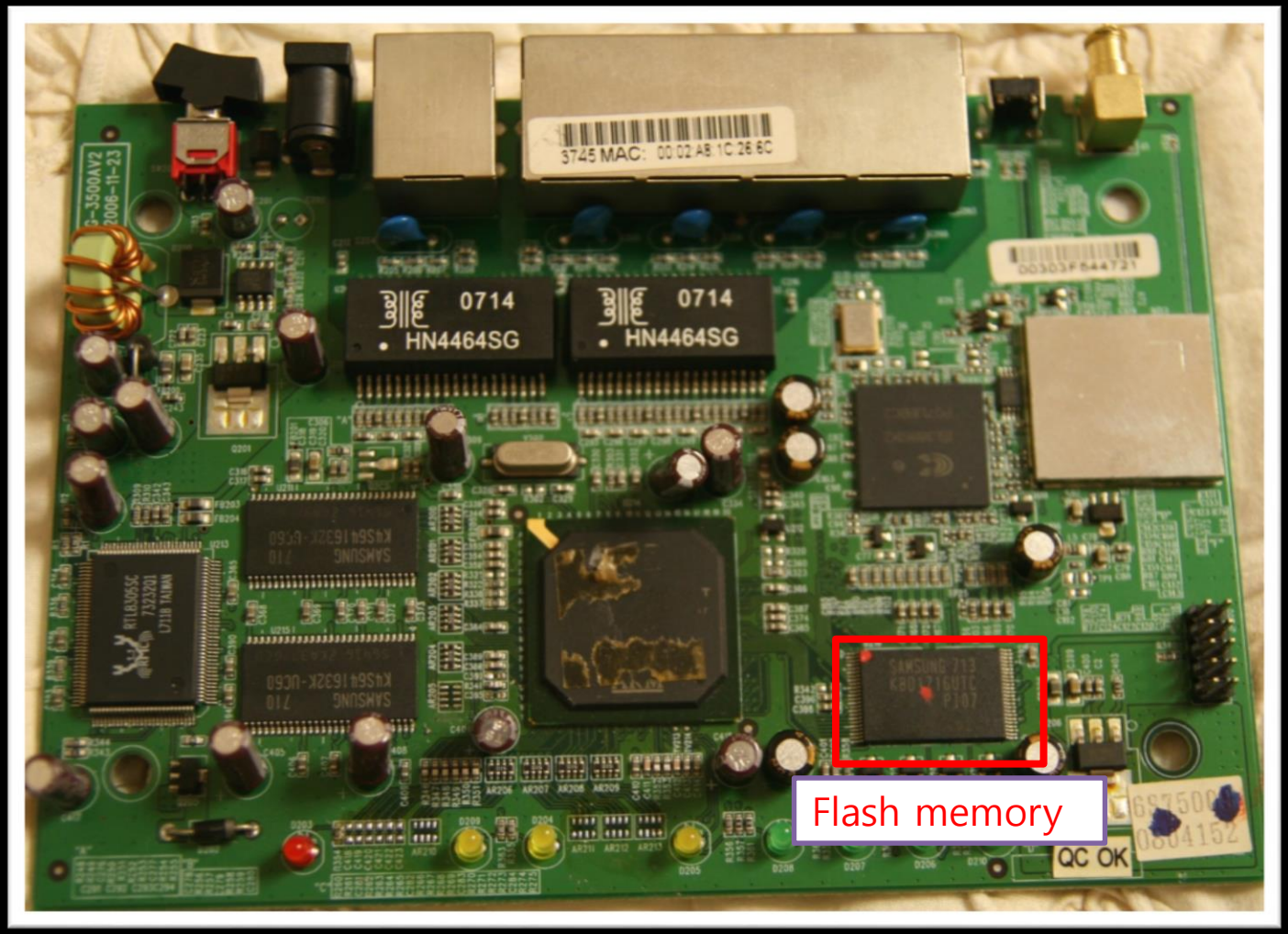


Root filesystem 추출

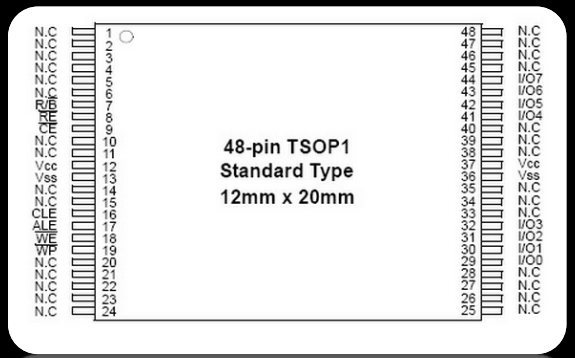
JTAG 전용 장비 필요
http://devicemart.co.kr/goods/view.php?seq=15635

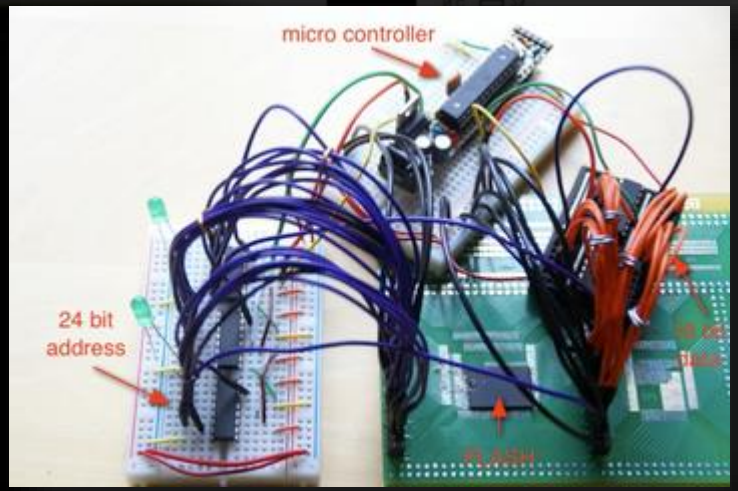
JTAG PIN SCANNER
http://deadhacker.com/2010/02/03/jtag-enumeration/

Flash 메모리 DUMP를 통한 Firmware 추출



Flash 메모리 DUMP를 통한 Firmware 추출





공개 Flash dump 도구 이용

http://github.com/cyphunk/ParallelFLASHDumper

http://events.ccc.de/congress/2010/wiki/Embedded_Analysis#DePCB_Analysis

취약점 탐지 전략

- 디렉토리 구성 파악
- 사용자의 입력을 받는 대상 파악
- 주요 취약점 존재여부 분석
  - 논리적 취약점
  - 버퍼 오버플로우
  - 포맷 스트링
  - …
- Debugging
- Exploit!

디렉토리 구성 파악

```
/ # ls -al
lrwxrwxrwx    1 0        0              11 usr -> /cramfs/usr
lrwxrwxrwx    1 0        0              13 ndbin -> /cramfs/ndbin
lrwxrwxrwx    1 0        0              11 bin -> /cramfs/bin
lrwxrwxrwx    1 0        0              12 sbin -> /cramfs/sbin
lrwxrwxrwx    1 0        0              11 lib -> /cramfs/lib
drwxr-xr-x    7 510      504          1024 var
drwxr-xr-x    2 510      504          1024 upgrade-bin
drwxr-xr-x    1 0        0               0 tmp
drwxr-xr-x    2 0        0            1024 save
dr-xr-xr-x   32 0        0               0 proc
drwxr-xr-x    3 510      504          1024 home
drwxr-xr-x    5 510      504          1024 etc
drwxr-xr-x    3 510      504          1024 dev
drwxr-xr-x   10 0        0              83 cramfs
drwxr-xr-x   11 0        0            1024 ..
drwxr-xr-x   11 0        0            1024 .
/ #
```

프로세스 목록 파악

```
/var # ps
  PID TTY      Uid        Size State Command
    1          root       768   S    init
    2          root         0   S    [keventd]
    3          root         0   S    [ksoftirqd_CPU0]
    4          root         0   S    [kswapd]
    5          root         0   S    [bdflush]
    6          root         0   S    [kupdated]
    7          root         0   S    [mtdblockd]
   30          root         0   S    [polling]
  103          root         0   D    [insmod]
  254          root       588   S    upnpd
  269          root       760   S    httpd
  271          root       564   S    /sbin/dhcpd
  276          root       496   S    /sbin/pptpd -b br0
  278          root       736   S    apcpd
  280          root       736   S    /sbin/iptables-q
  282          root       544   S    /sbin/dhclient -i eth1 -p dhclient.eth1
  700          root       492   R    ps
/var #
```

취약점 조사

- Main(entry point)을 시작으로 추적
- Cross Reference 기반 취약점 탐색
  - Dangerous Functions
    - strcpy
    - strcat
    - sprintf
    - system
    - execl
    - getenv
    - …

취약점 공격

- Debugging
- Shellcode 제작
- 최종 Exploit 제작
- 보안권고문 작성
- 개발사/KISA/보안언론을 통해 공개

스마트기기 해킹에 대한 대책

- 개발 업체들의 보안 마인드 변화 필요
- Secure Coding 적용
- ASLR/DEP 등 보안성 강화 정책 적용
- 해킹 당했을 경우 이상징후를 물리적으로 파악할 수 있도록 함
  – LED 점등
- 스마트 기기 보안성 평가 제도 마련
- 취약점을 찾는 능력이 있는 화이트 해커 양성&지원

스마트기기 해킹에 대한 대책

- 최신 보안 패치
- 의심스러운 파일/웹 사이트 접근 금지
- 모든 암호는 어렵게 (특수문자 조합)
- 공유기 uPnP 서비스 비활성화

결론

- 우리 생활에 편리함을 주는 스마트기기들, 보안이 뒷받침되지 않는다면 오히려 독이 될 수 있다.
- 스마트기기 해킹은 기존의 해킹보다 더 큰 피해를 유발한다.
- 개발 업체 및 개인은 보안에 많은 신경을 써야한다!

질문/답변

감사합니다!