하드웨어 해킹 Warming Up

정구홍(mongii)
BoB 취약점 트랙 멘토
GRAYHASH 수석연구원

cybermong@grayhash.com
https://www.facebook.com/goohong.jung

발표자 소개

- BoB 취약점 트랙 프로그램 멘토
- 정보보안업체 GRAYHASH 수석 연구원
- 보안 커뮤니티 해커스쿨 운영자
- 준우 아빠

- 발표 내용
  - 다양한 하드웨어 해킹 기술들을 단계별로 정리
  - 하드웨어 해킹 공부 방법 소개

Hardware Hacking을 공부하게 된 계기

- 2011 Recon(Reverse Engineering Conference)
- Montreal, Canada

Recon 2011의 발표 주제들

- Abusing Hardware Defined Radios
- RFID Hacking
- How to develop a rootkit for Broadcom NetExtreme network cards
- Sticky Fingers & KBC Custom Shop
- Ghetto Tools for Embedded Analysis
- Hardware Stuff for Software People
- …

Recon 2011의 발표 주제들

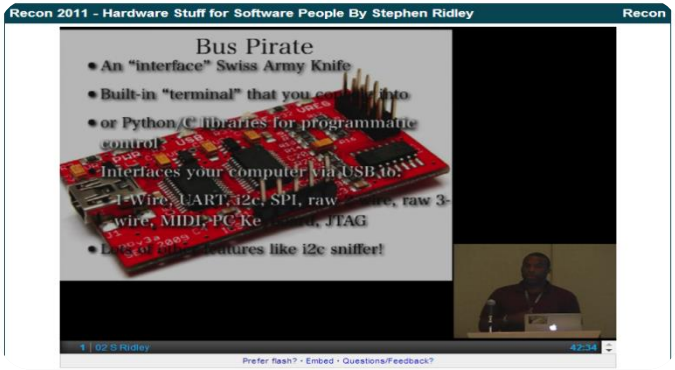
- Abus
- RFID
- How ork cards
- Sticky
- Ghett
- Hardy
- …

After that…

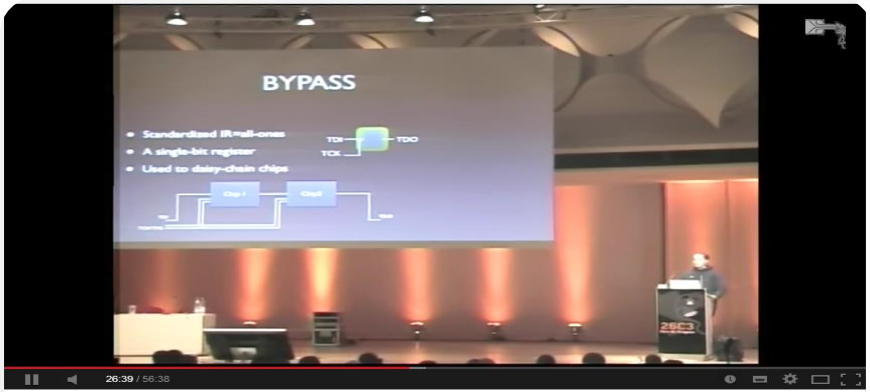
- 하드웨어 그룹스터디 진행

- 하드웨어 기초
  - 납땜부터..
- AVR Programming
- RC Car 제작 실습
- MP3 player 제작 실습

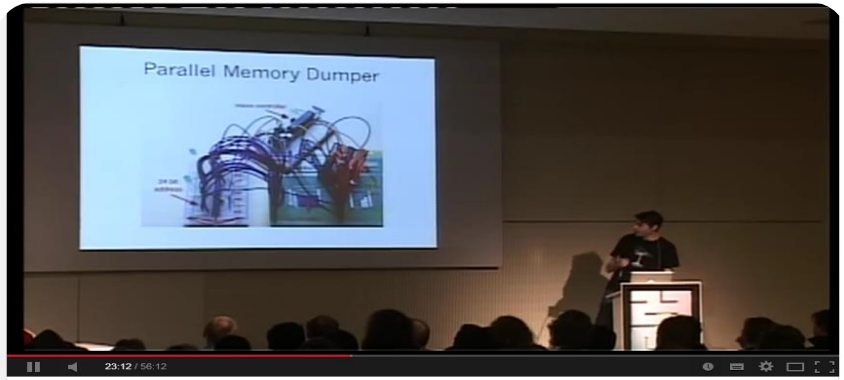
After that…



외국의 하드웨어 해킹 자료들을
열심히 열심히 공부



Blackbox JTAG Reverse Engineering [26C3]



[27C3] (en) JTAG/Serial/FLASH/PCB Embedded Reverse Engineering Tools and Techniques

After that…

- 유무선 공유기(IPTIME) 해킹
- 스마트폰 UART/JTAG 해킹
- 스마트 TV 해킹
- CCTV 해킹
- 프린터 해킹
- 홈 네트워크 해킹
- 무선 해킹
- 도어락 해킹
- 로봇 해킹
- 자동차 해킹
- …

하드웨어 해킹의 발전

- 다양한 공격 대상(먹잇감) 출현
  - 스마트폰, 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/)

하드웨어 해킹의 특징

- 도청/감시 등 사생활 노출의 피해
  - 스마트폰, 스마트TV, 인공지능 스피커
- 대상을 장기간 장악 가능
  - No Format!
- 물리적인 피해 유발
  - Doorlock Open, 화재 유발
- 인명 사상 피해 유발
  - 자동차, 심장박동기 해킹

하드웨어 해킹 레벨 분류

하드웨어 해킹 레벨 분류

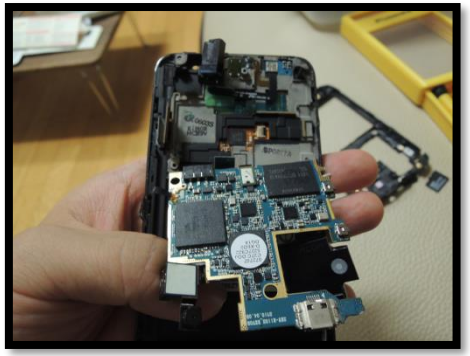
- Level-1 : 용기를 가지고 분해해 보기
- Level-2 : Datasheet를 읽어 보기
- Level-3 : Debug Port에 연결해 보기
- Level-4 : 전기 신호 분석해 보기
- Level-5 : Desoldering
- Level-6 : Side Channel Attack
- Level-7 : Decapping & Imaging
- Level-8 : Glitching Attack
- Level-9 : FIB(Focused Ion Beam) Attack
- Level-10 : IC Chip Reversing

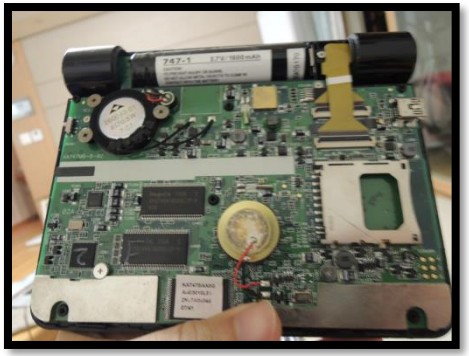
* 주관적인 견해에 따라 분류되었습니다.

LEVEL-1 : 용기를 가지고 분해해 보기

- 주변의 전자장비들을 무작정 뜯어본다!
- 다양한 IC칩들의 모델명을 구글에서 검색해 본다.
  - 특히 CPU, Flash, RAM이 무엇인지 찾아본다.
- 연결이 가능해 보이는 포트들을 찾아본다.
  - USB, UART, JTAG, ISP …
- 분해하고 살펴보는 과정에서 고장이 날 수도 있다.
  - 뒷 수습은 고장이 난 다음에 생각한다.

일단 무조건 뜯어 본다.



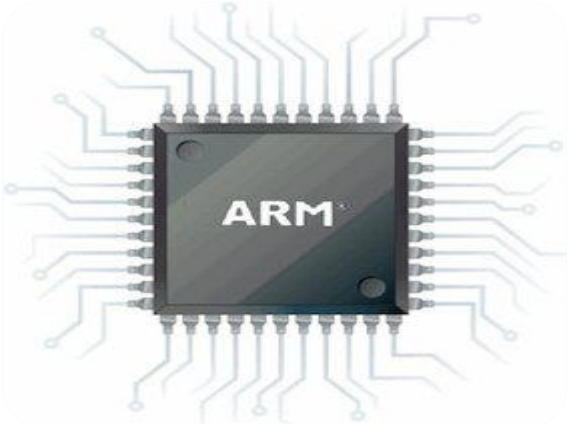


주요 IC칩들

- 당신이 무언가를 분해했을 때...

주요 IC칩들

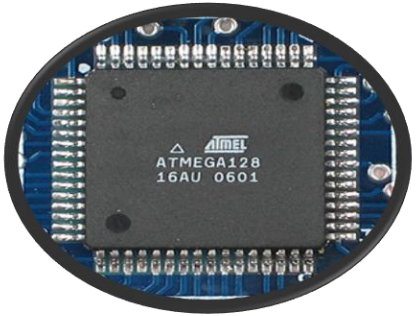
- 당신이 무언가를 분해했을 때...

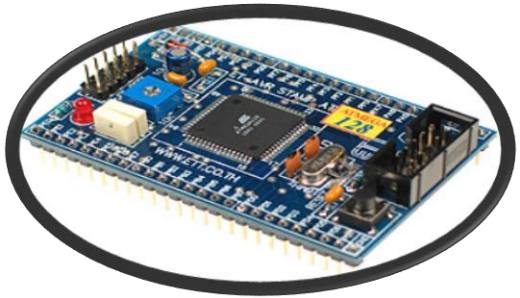


CPU

CPU(MCU) 설명

- 소형 CPU, 저가, 저전력
- AVR, 8051, PPC, ARM, MIPS…
- 거의 모든 전자장비들에 들어있다





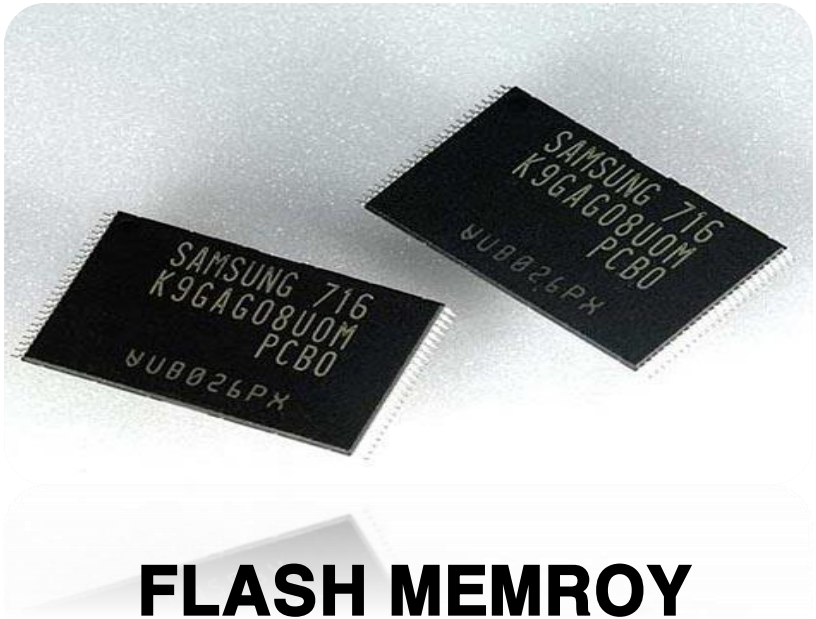
주요 IC칩들

- 당신이 무언가를 분해했을 때...

RAM

주요 IC칩들

- 당신이 무언가를 분해했을 때...



주요 IC칩들

- 당신이 무언가를 분해했을 때...

EEPOM

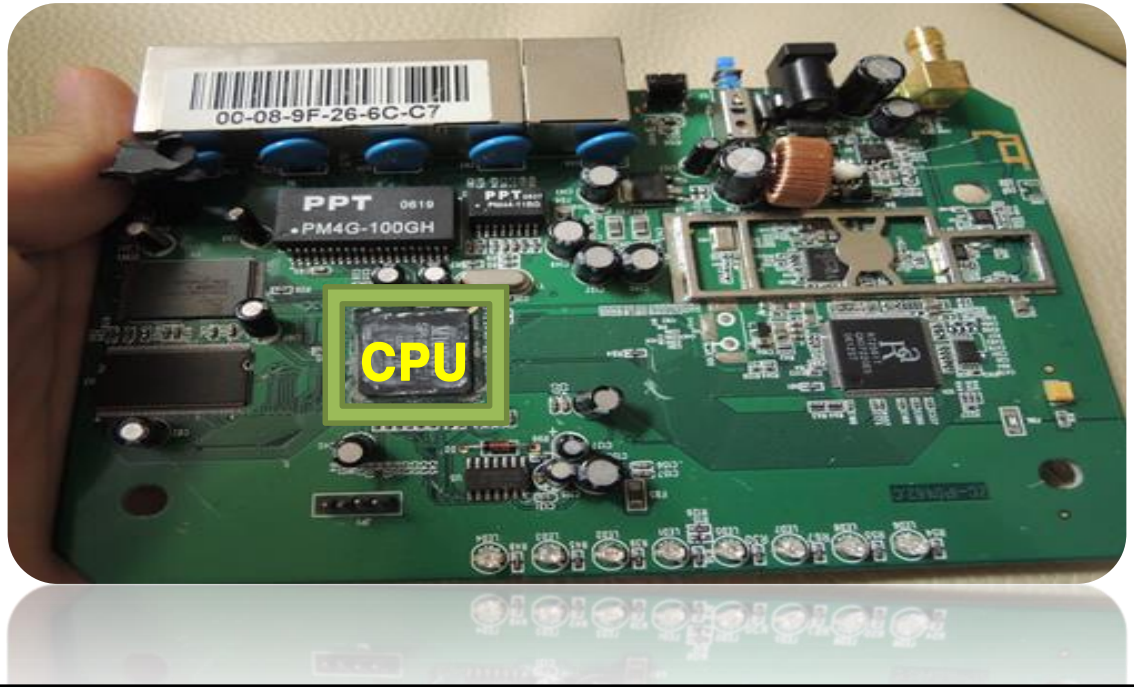
장비 내 주요 부품들

1. CPU(MCU)
   - ARM, MIPS, AVR, …
2. 외부 메모리
   - SRAM, DRAM, DDR RAM …
3. 플래시 메모리
   - 운영체제 및 응용 프로그램 저장공간
4. EEPROM
   - config 값 등의 저장 공간
5. 그 외 무선 칩, 오디오 코덱, 각종 센서들

공유기 분해하기

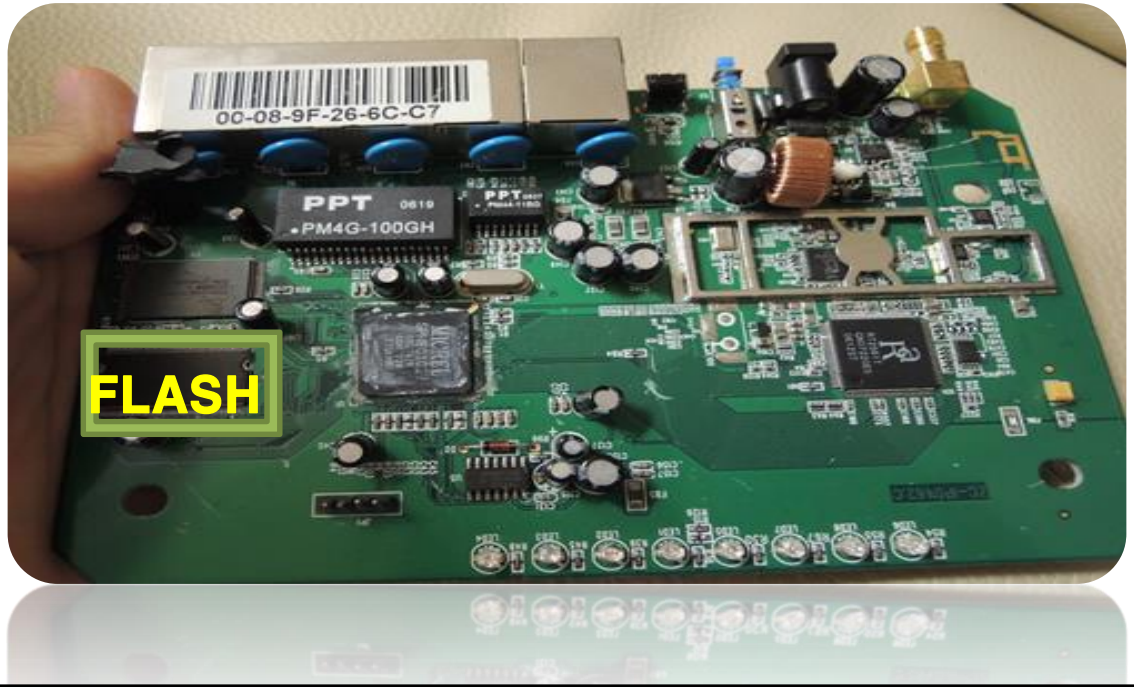
공유기 분해하기

공유기 분해하기



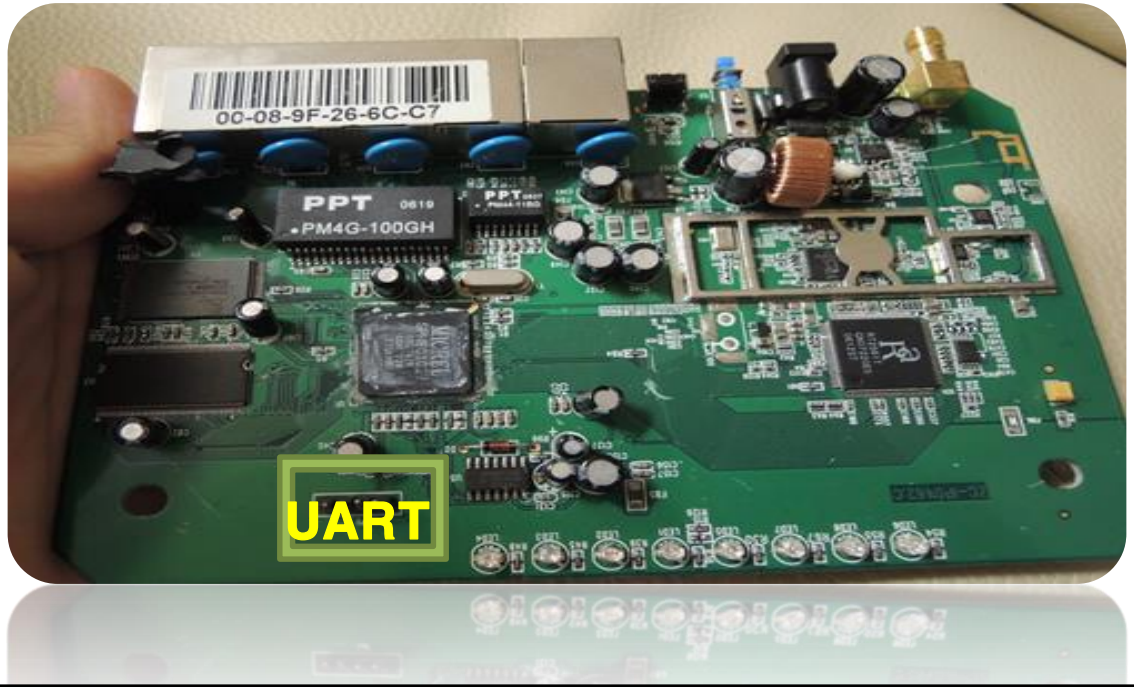
공유기 분해하기

공유기 분해하기

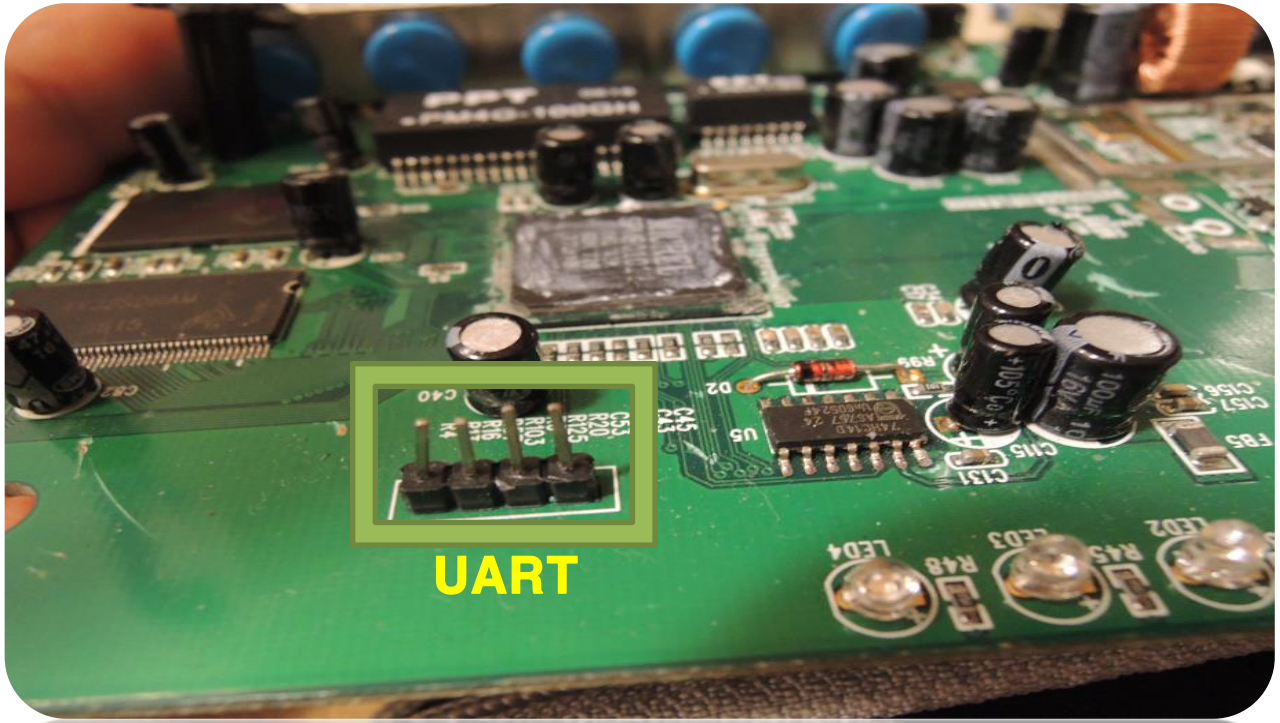


공유기 분해하기

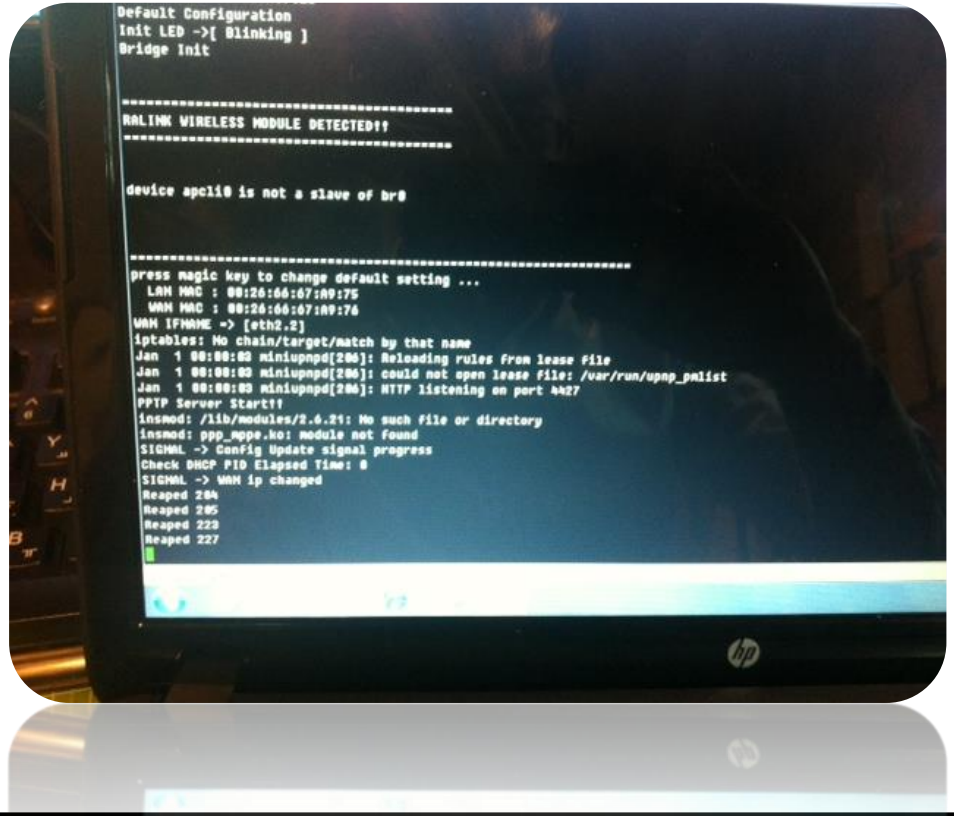
공유기 분해하기



공유기 분해하기

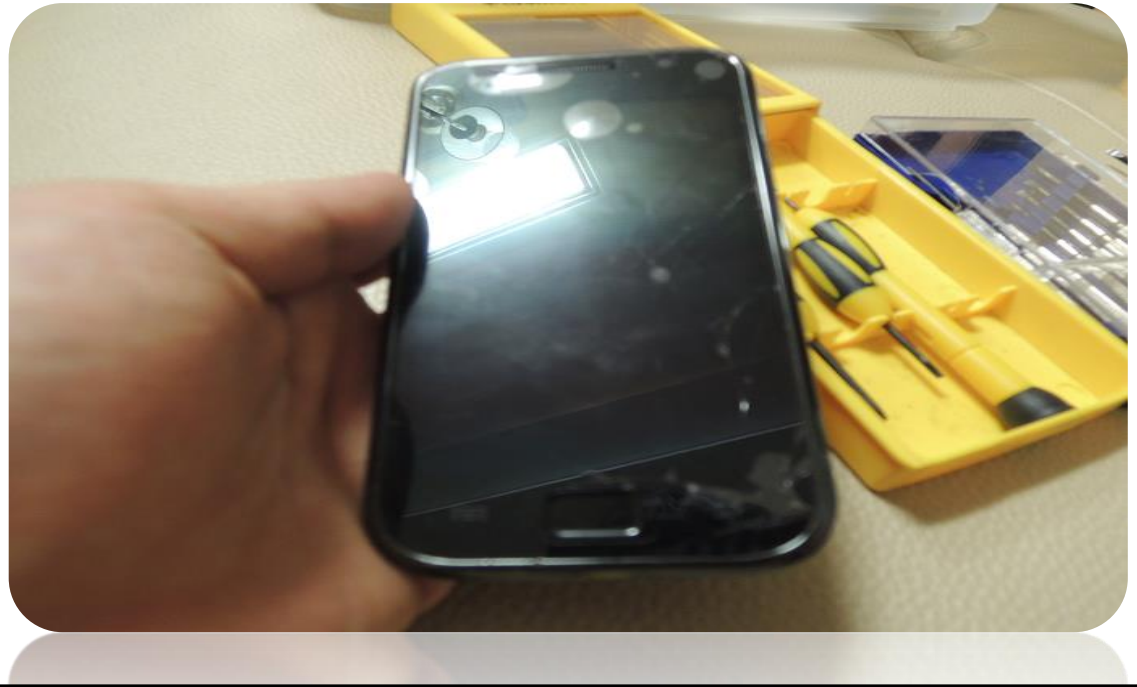


공유기 분해하기


Default Configuration
Init LED ->[Blinking]
Bridge Init
RALINK WIRELESS MODULE DETECTED!!
device apcli0 is not a slave of br0
press magic key to change default setting ...
LAN MAC : 00:26:66:67:A9:75
WAN MAC : 00:26:66:67:A9:76
WAN IFNAME -> [eth2.2]
iptables: No chain/target/match by that name
Jan 1 00:00:03 miniupnpd[206]: Reloading rules from lease file
Jan 1 00:00:03 miniupnpd[206]: could not open lease file: /var/run/upnp_pmlist
Jan 1 00:00:03 miniupnpd[206]: HTTP listening on port 4427
PPTP Server Start!!
insmod: /lib/modules/2.6.21: No such file or directory
insmod: ppp_mppe.ko: module not found
SIGHUL -> Config Update signal progress
Check DHCP PID Elapsed Time: 0
SIGHUL -> WAN ip changed
Reaped 204
Reaped 205
Reaped 223
Reaped 227

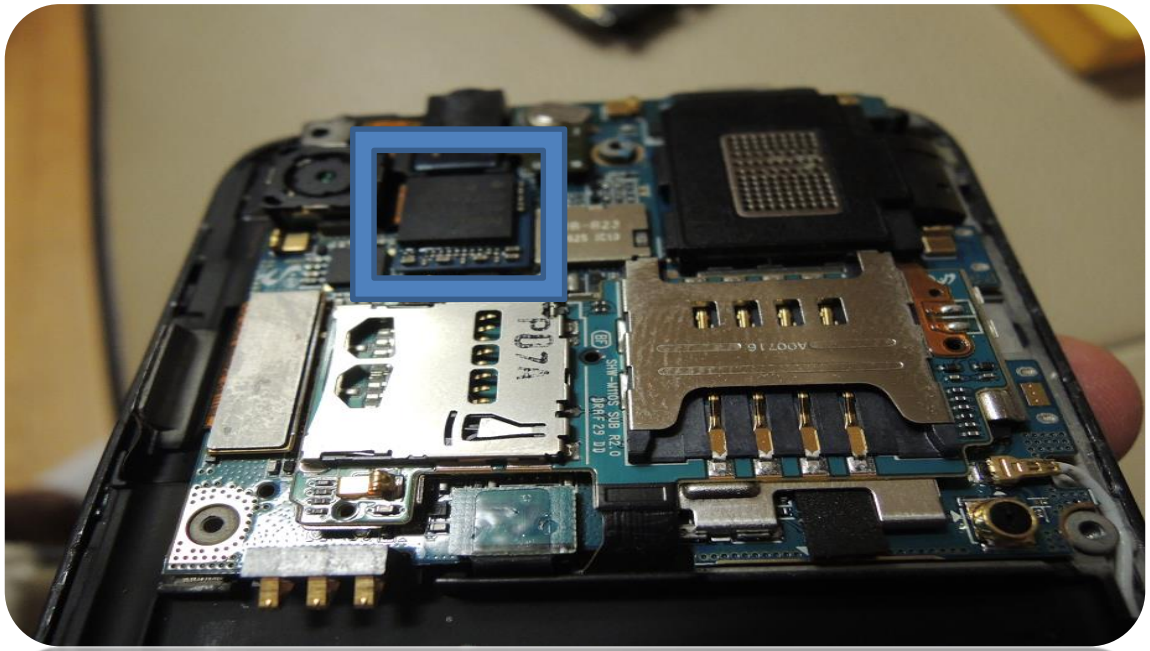
스마트폰 분해하기

- 갤럭시 S1



스마트폰 분해하기

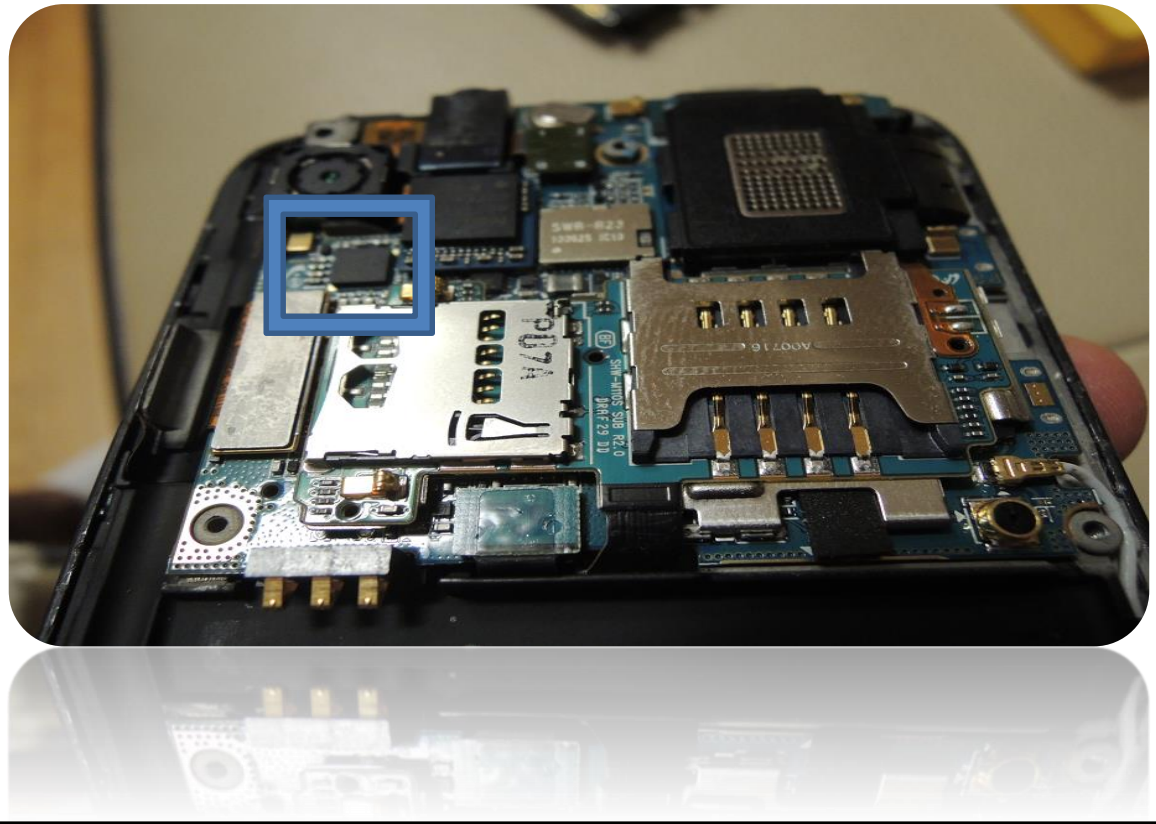
스마트폰 분해하기



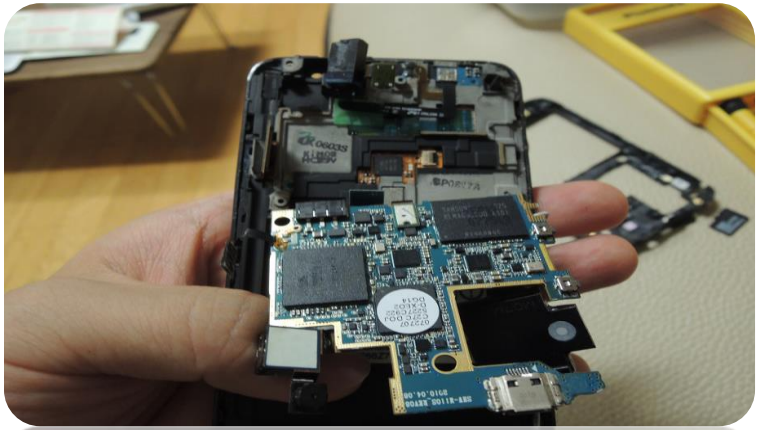
카메라 모듈 (500만화소)

블루투스+와이파이(SWB-B23)

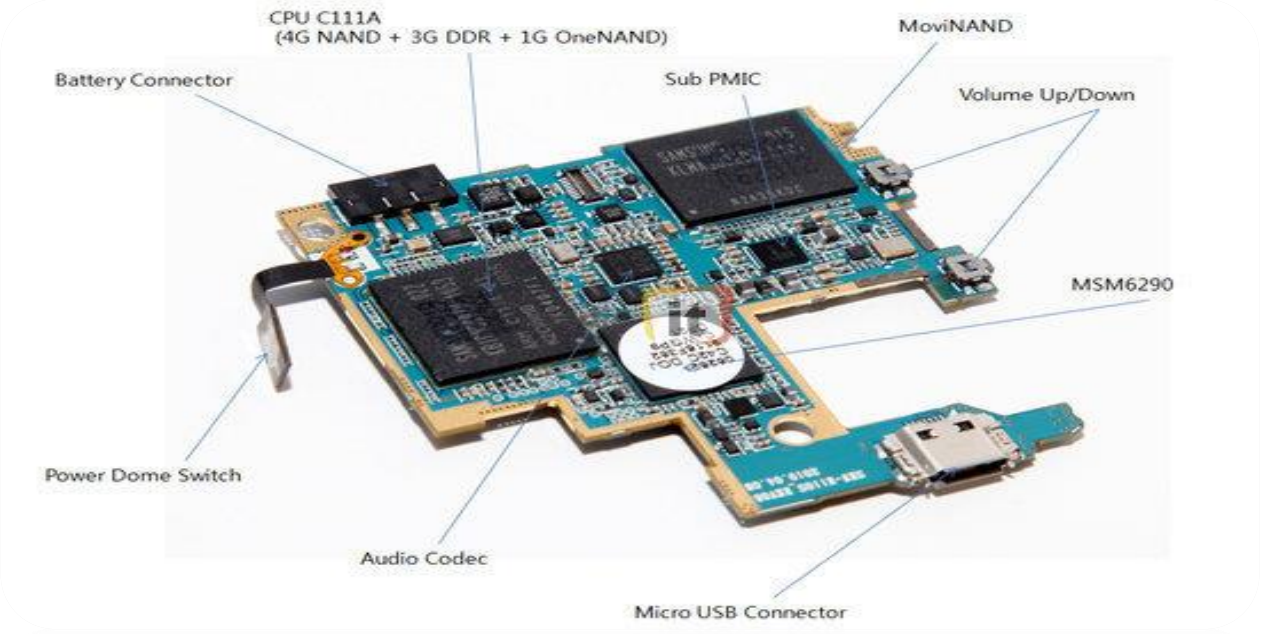
DMB(T3700)



CPU가 어딨지?



PCB 뒷면


CPU C111A
(4G NAND + 3G DDR + 1G OneNAND)
MoviNAND
Battery Connector
Sub PMIC
Volume Up/Down
MSM6290
Power Dome Switch
Audio Codec
Micro USB Connector

그래서, 얻을 수 있는 것은?

- 하드웨어 장비의 구조에 대한 이해
- 각종 값비싼 부품들 $.$
  - CPU(MCU)
  - 500만 화소 카메라
  - DMB
  - RAM
  - Super AMOLED Display
  - 각종 센서들 (근접,GPS,기울기,터치,…)
  - …

초소형 GPS 데이터 수신기 모듈(NR-GPSM)

초소형 사이즈 로서 GPS데이터의 수신이 가능한 안테나 포함 모듈 입니다 . 고감도의 수신성능(-165dBm)과 66개의 위성데이터 수신이

큰이미지 보기

- 상품코드 33761
- 판매가격 45,000원 (부가세 미포함가)
- 제조사 네오틱스
- 적립금 0원
- 브랜드 네오틱스 [브랜드몰바로가기]
- 수량 1

바로구매 장바구니 관심상품

,00만화소(2592x1944) CMOS 화상카메라 모듈

500만화소 , 최대 해상도 2592X1944 픽셀 COMS 카메라 모듈, 10Bit 디지탈 RGB 로우(raw) 데이타 출력 , Full : 2592 x 1944 , sxga : 1 x 480 의 다양한 해상도를 지원합니다.

큰이미지 보기

- 상품코드 **30505**
- 판매가격 **75,000**원 (부가세 미포함가)
- 제조사 한진데이타
- 적립금 0원
- 브랜드 한진데이타 [브랜드몰바로가기]
- 수량 1

바로구매 장바구니 관심상품

갤럭시 S1의 중고 가격은?

게시글 전체 ▾ 최신순 ▾ | 제목만 보기 ▾ | 15개씩 ▾

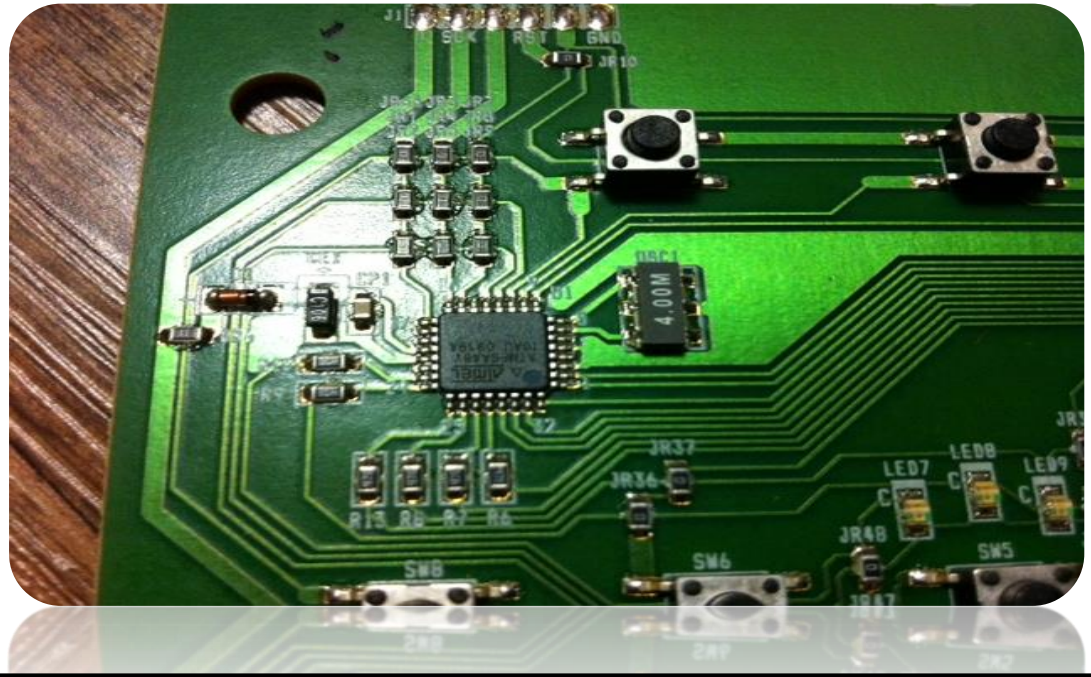
	제목	작성자	작성일	조회	좋아요
399850630	[서울 송파] **갤럭시 S1**~S5, 노트1~노트4, A5, 팝, 그랜드2, 알파, U, 넥서스S 등 공기계 저렴하게 판매합니다	whiz001	10:31	18	0
399846559	[서울 송파] **갤럭시 S1**~S5, 노트1~노트4, A5, 팝, 그랜드2, 알파, U, 넥서스S 등 공기계 저렴하게 판매합니다 판매	whiz001	10:17	58	0
398137173	**갤럭시 s1** 2만원에 팝니다 완료	미송송이	2017.07.30.	42	0
392193326	추억의 **갤럭시 S1**(SHW-M110S) 블랙 단독 1만 5천원 판매합니다. 완료 [1]	JIRRARD	2017.07.04.	50	0
381309379	**갤럭시 S1** 공기계 1만원에 팝니다~ 완료	중고나라애용자9	2017.05.16.	103	0
380685874	(판매완료)**갤럭시 S1**~풀박스 3만원/ 보조배터리 10000m Ah [1]	쵸코	2017.05.13.	42	0
380603334	**갤럭시 S1** / 번인 , 잔상 없음 / 택배 2만 완료	공허의 유산	2017.05.12.	32	0
379439080	[공식앱] **갤럭시 s1** 배터리및거치대 새제품	수빈성민	2017.05.07.	16	0
377930416	SKT **갤럭시 S1**(SHW-M110S) 블랙 완료 [2]	joonyj1128	2017.04.29.	141	0
373569272	skt **갤럭시 s1** 판매합니다 완료 [4]	흑인노예	2017.04.08.	76	0
373010610	[공식앱] **갤럭시 s1**팝니다 [3]	Cake	2017.04.05.	29	0
372206860	**갤럭시 s1** 갤s1 팔아여~ 판매	qkrcognsqkqh123	2017.04.02.	41	0
372088654	**갤럭시 s1** 갤s1 팔아여~ 완료	qkrcognsqkqh123	2017.04.01.	23	0
371417424	[공식앱] **갤럭시 s1**팝니다	Cake	2017.03.29.	11	0
369213010	**갤럭시 s1** 판매합니다. 완료	별난사람	2017.03.18.	101	0

?? What? ??

비데 컨트롤러 분해하기

비데 컨트롤러 분해하기

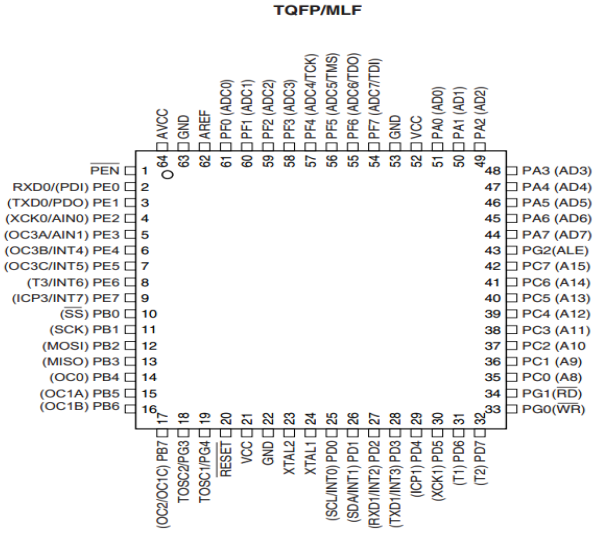
- CPU : ATmega64L



Datasheet(설계도) 찾기

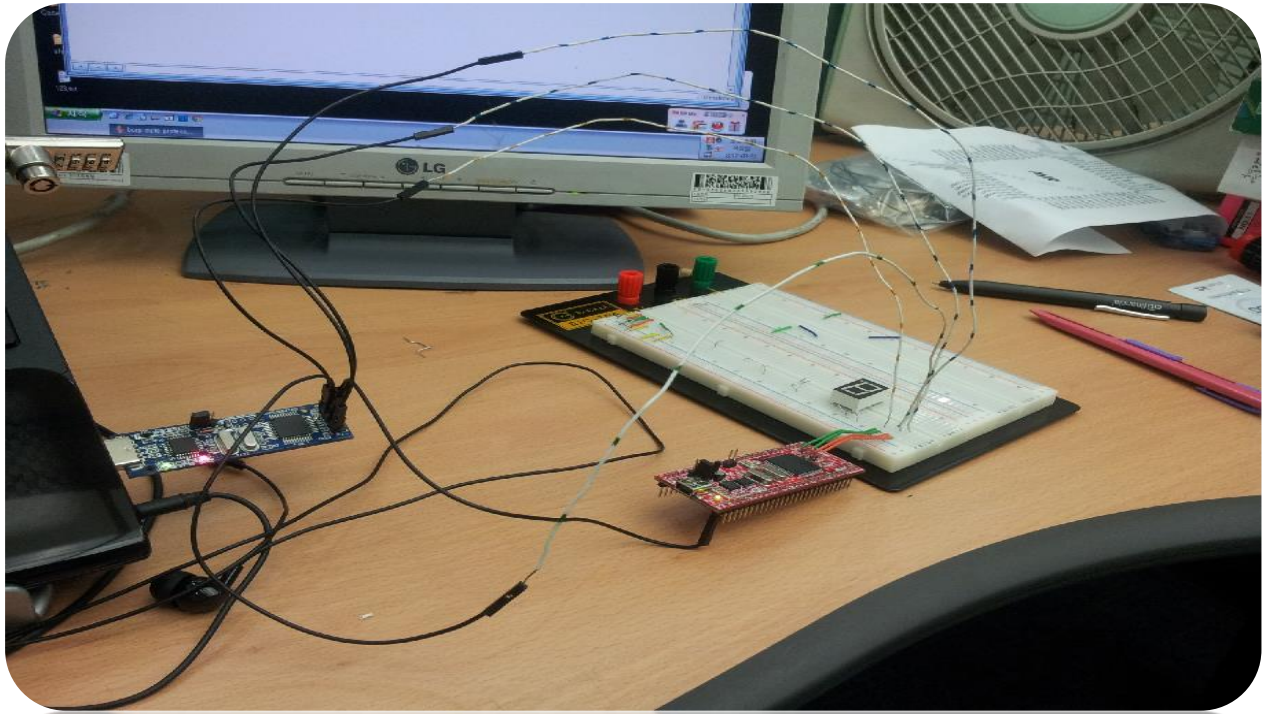
Pin Configuration

Figure 1. Pinout ATmega64



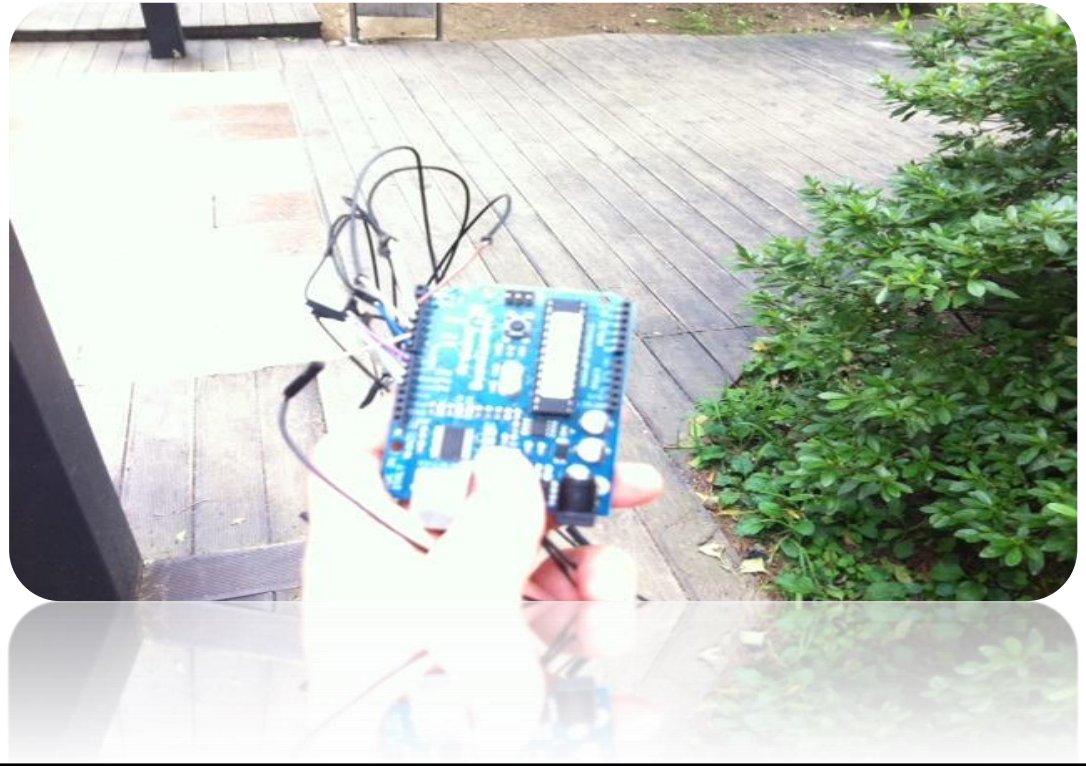
Note: The bottom pad under the QFN/MLF package should be soldered to ground.

Datasheet(설계도) 찾기

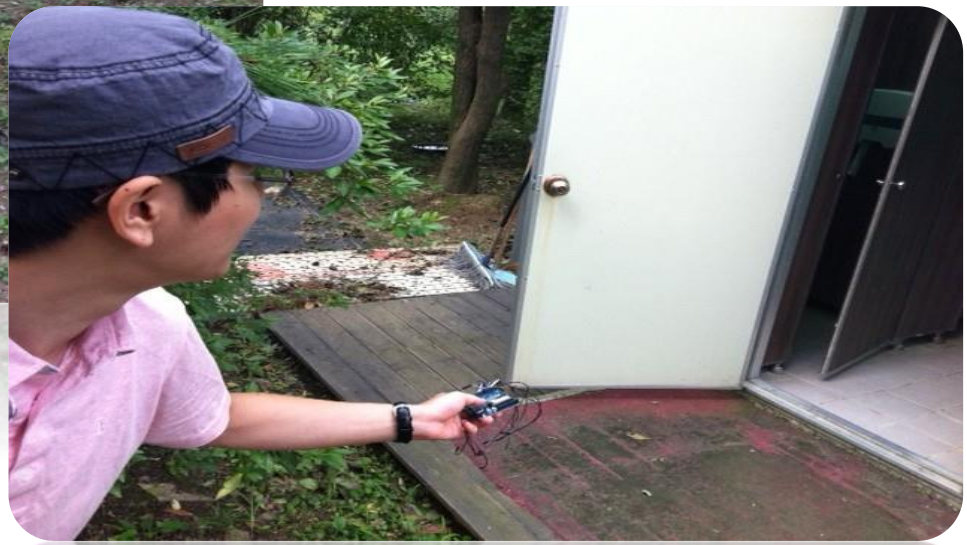


아 쉬야마렵다

복제한 컨트롤러 ㅋㅋ

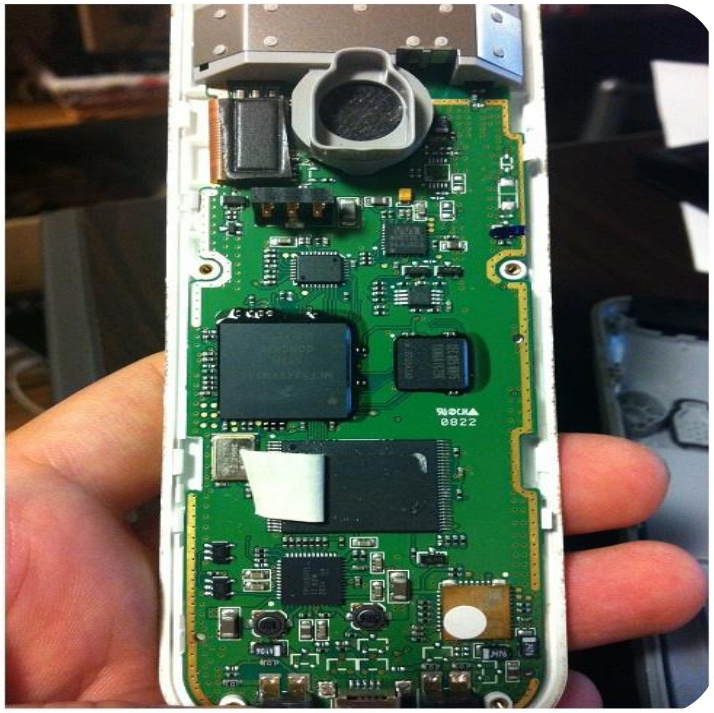


요래요래 ㅋㅋㅋㅋ

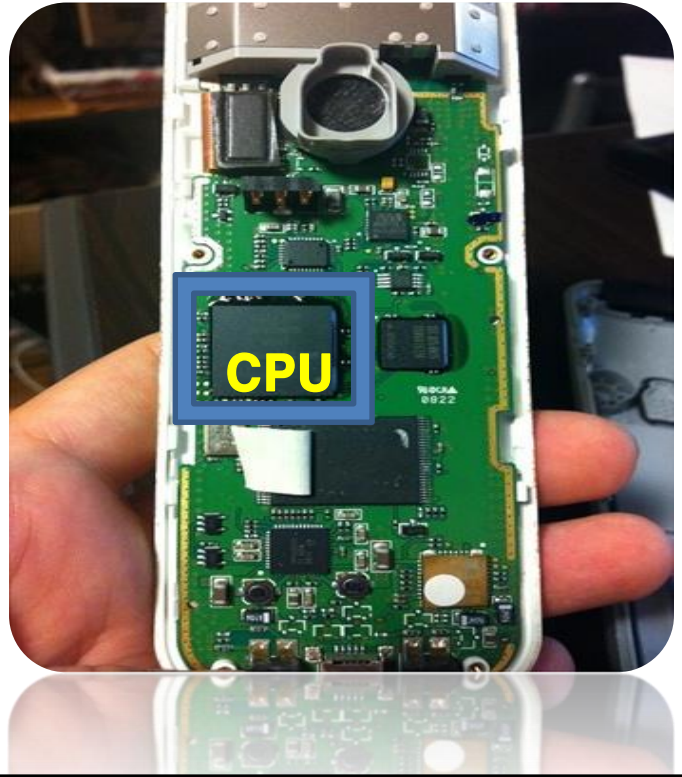


으잉 머지 ㅋㅋㅋㅋㅋㅋ

인터넷 전화 분해하기



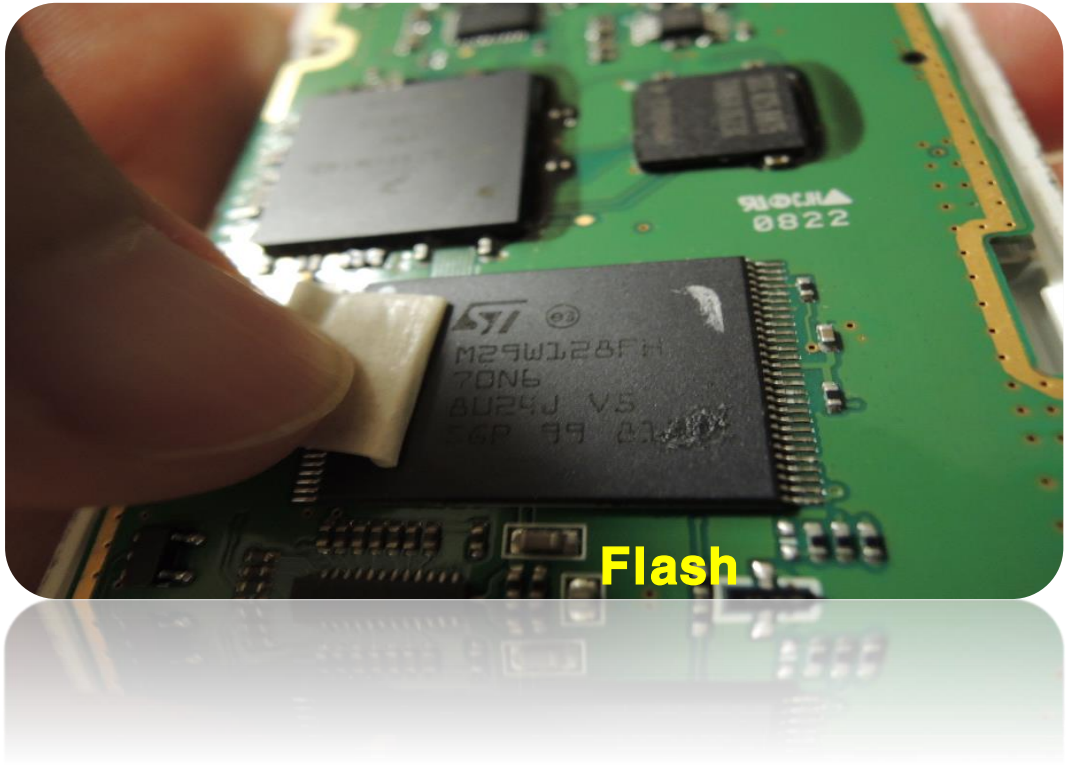
MCF5249VM140
Freescale계열, 140Mhz



Audio：WM8731L

Flash Memory
M29W128FH, 8MB

Flash Memory M29W128FH, 8MB

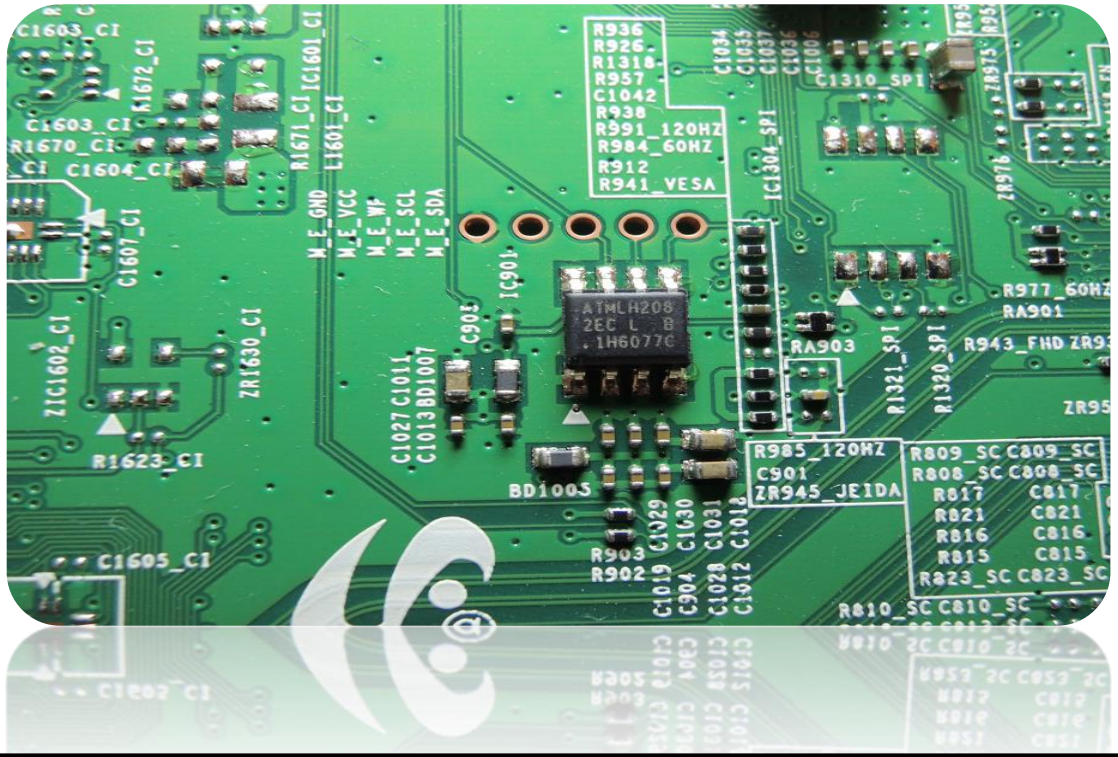


TV 분해하기

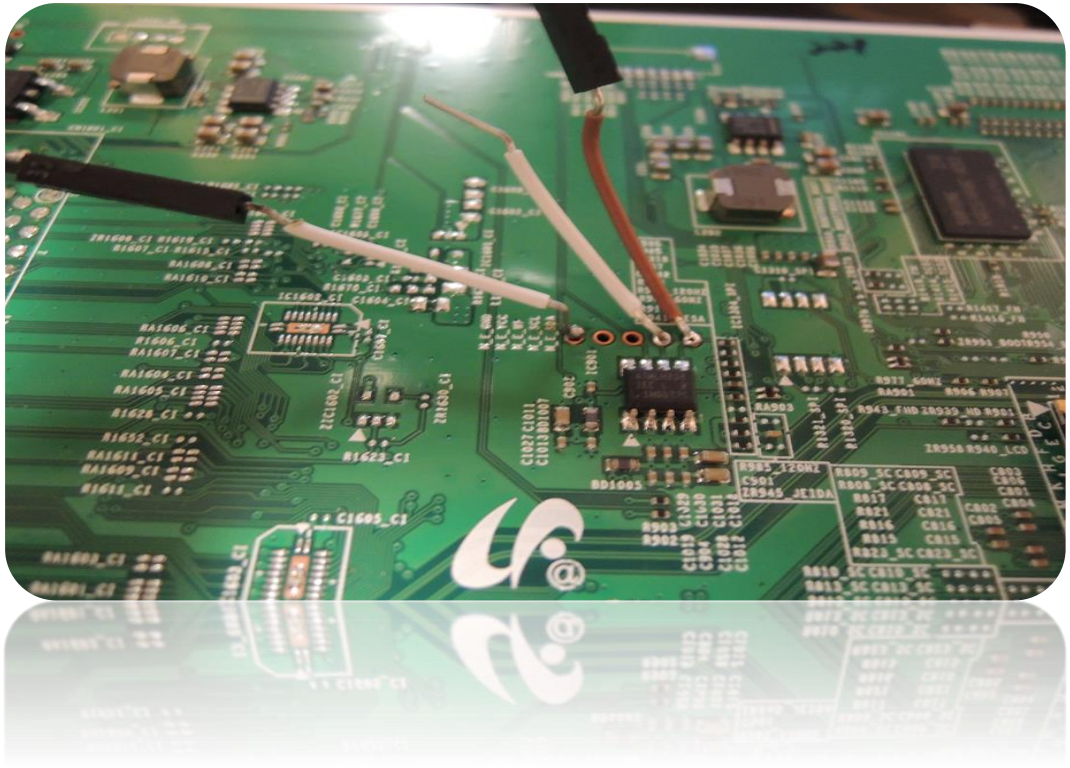

klmno789
나가기
2-1
프리미엄
TV 앱스
KBS
Coloring Book
Fruit Puzzle
Horoscope
Natural Objects
Natural Objects
MahJong
facebook
검색
TV 앱스
Invader
Horoscope
Coloring Book
Natural Objects
더 보기

TV 분해하기

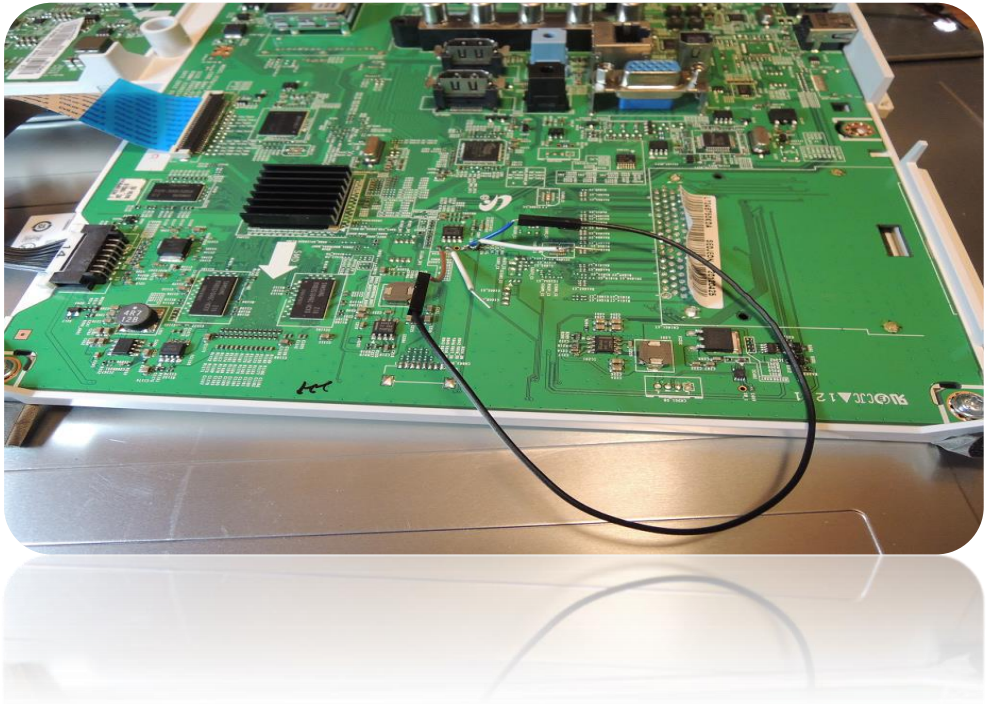
EEPROM 오작동 유발



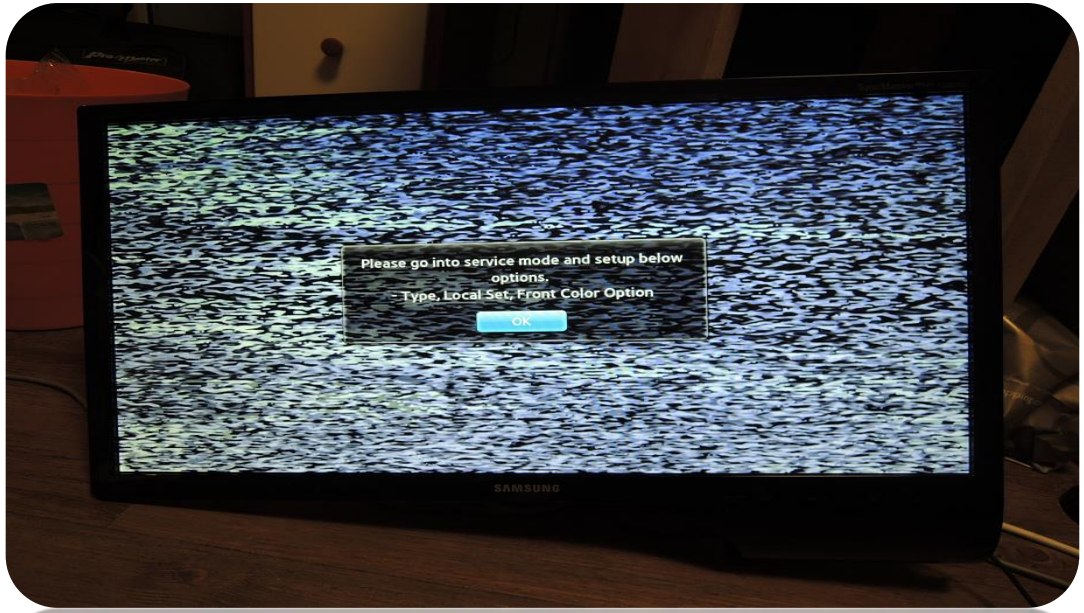
EEPROM 오작동 유발



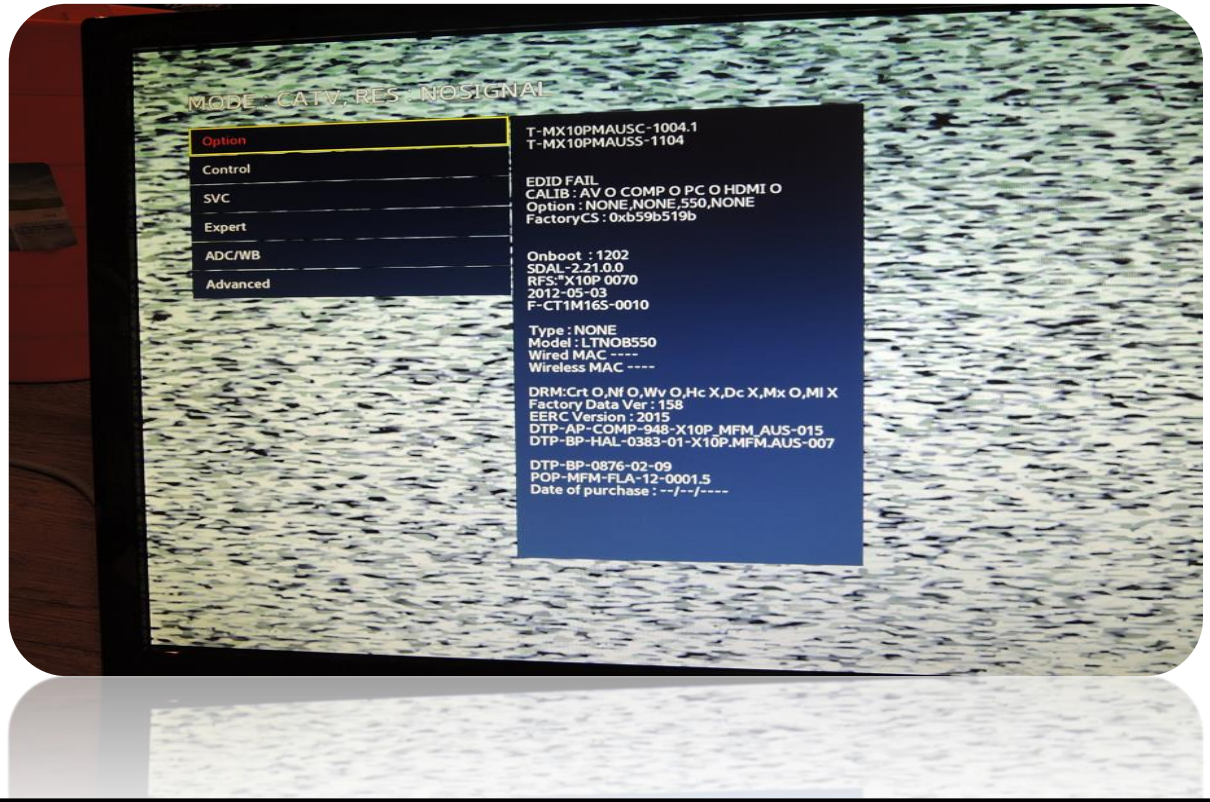
EEPROM 오작동 유발



오잉.. @.@


Please go into service mode and setup below options.
- Type, Local Set, Front Color Option
OK
SAMSUNG

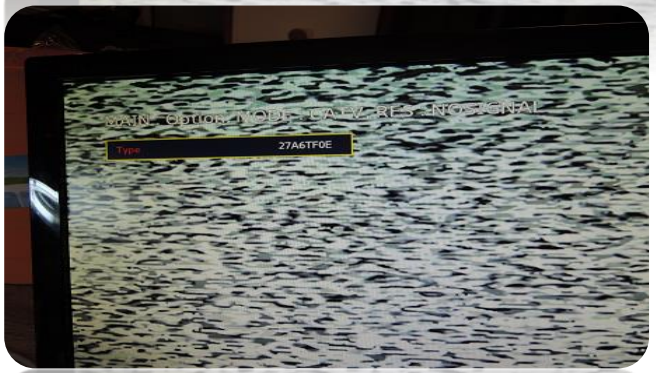
서비스 모드!!

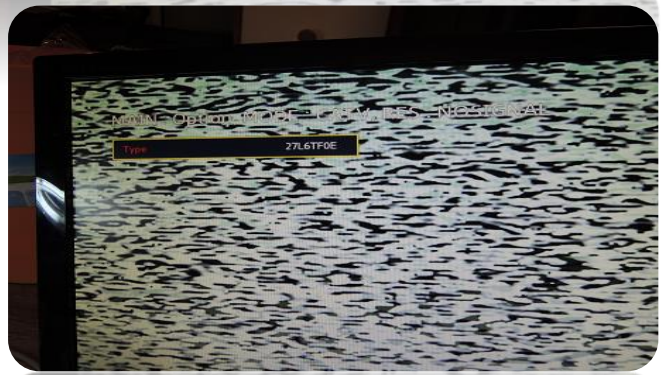

MODE : CATV, RES : NO SIGNAL
Option
Control
SVC
Expert
ADC/WB
Advanced
T-MX10PMAUSC-1004.1
T-MX10PMAUSS-1104
EDID FAIL
CALIB : AV O COMP O PC O HDMI O
Option : NONE,NONE,550,NONE
FactoryCS : 0xb59b519b
Onboot : 1202
SDAL-221.0.0
RFS:*X10P 0070
2012-05-03
F-CT1M16S-0010
Type : NONE
Model : LTNOB550
Wired MAC ----
Wireless MAC ----
DRM:Crt O,Nf O,Wv O,Hc X,Dc X,Mx O,Ml X
Factory Data Ver : 158
EERC Version : 2015
DTP-AP-COMP-948-X10P_MFM_AUS-015
DTP-BP-HAL-0383-01-X10P.MFM.AUS-007
DTP-BP-0876-02-09
POP-MFM-FLA-12-0001.5
Date of purchase : --/--/----

서비스 모드!!


MAIN Option MODE CAM/BES NO SIGNAL
Type 23A6TF0E

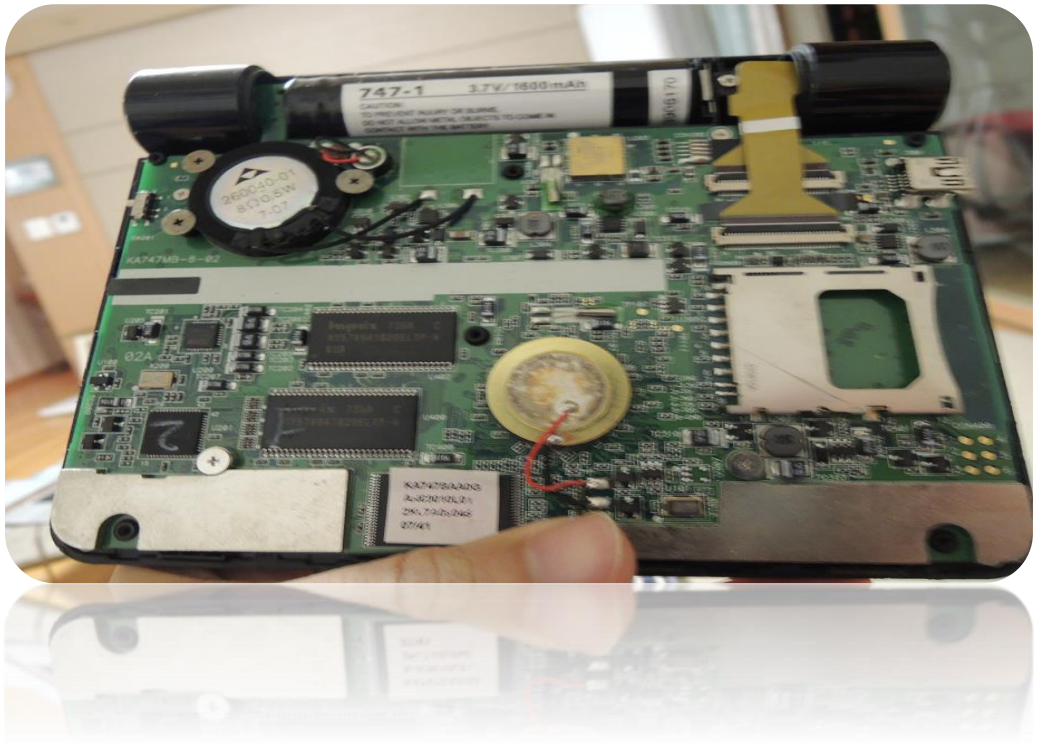

MAIN Option MODE CAM/BES NO SIGNAL
Type 24L6TF1E


MAIN Option MODE CAM/BES NO SIGNAL
Type 27A6TF0E

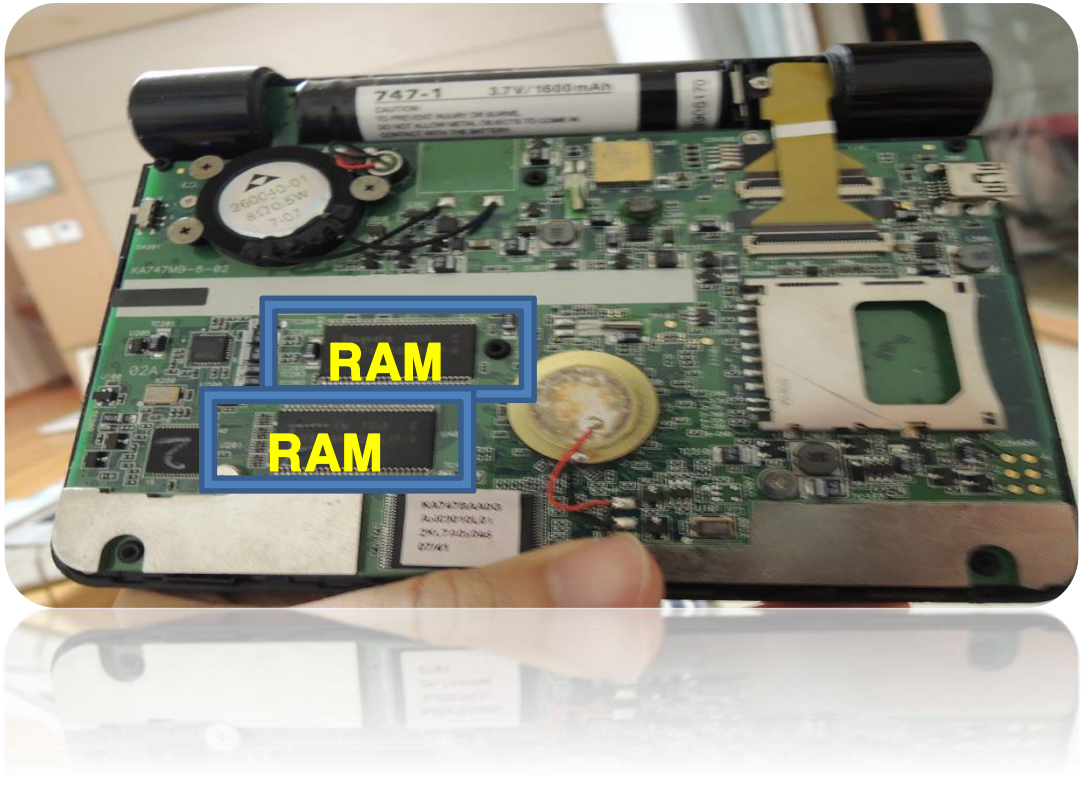

MAIN Option MODE CAM/BES NO SIGNAL
Type 27L6TF0E

전자사전 분해하기

전자사전 분해하기

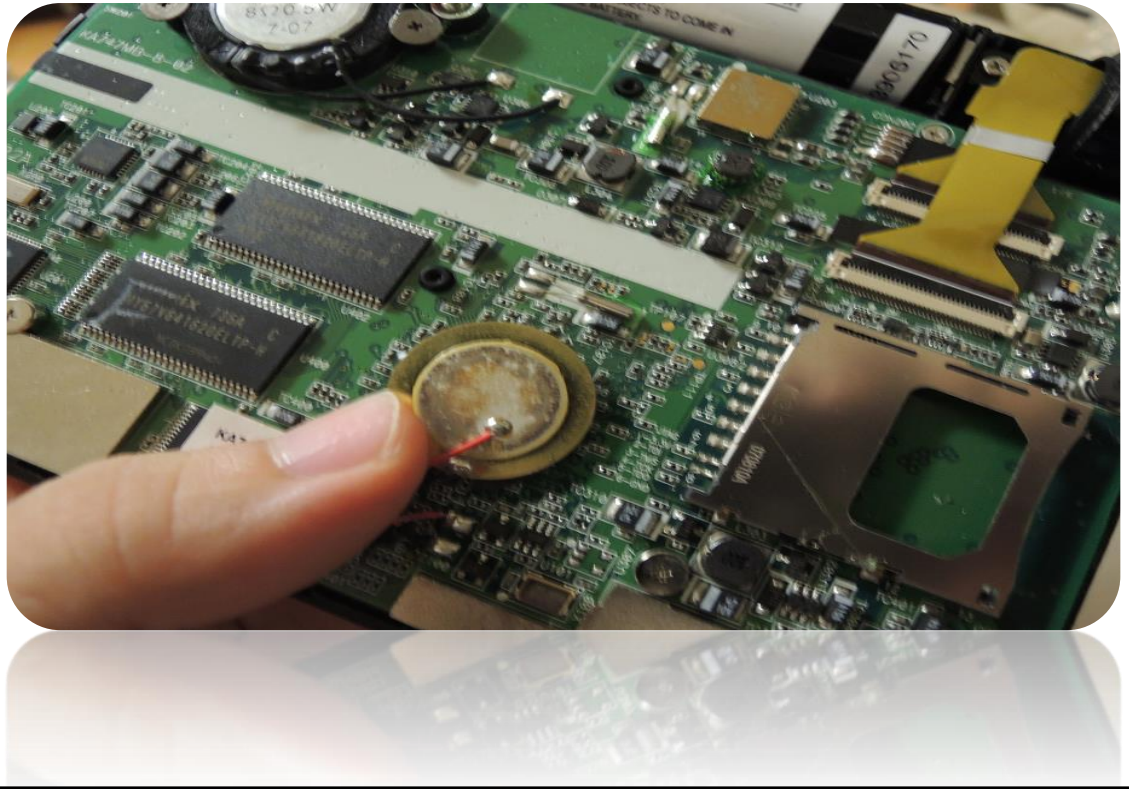


전자사전 분해하기

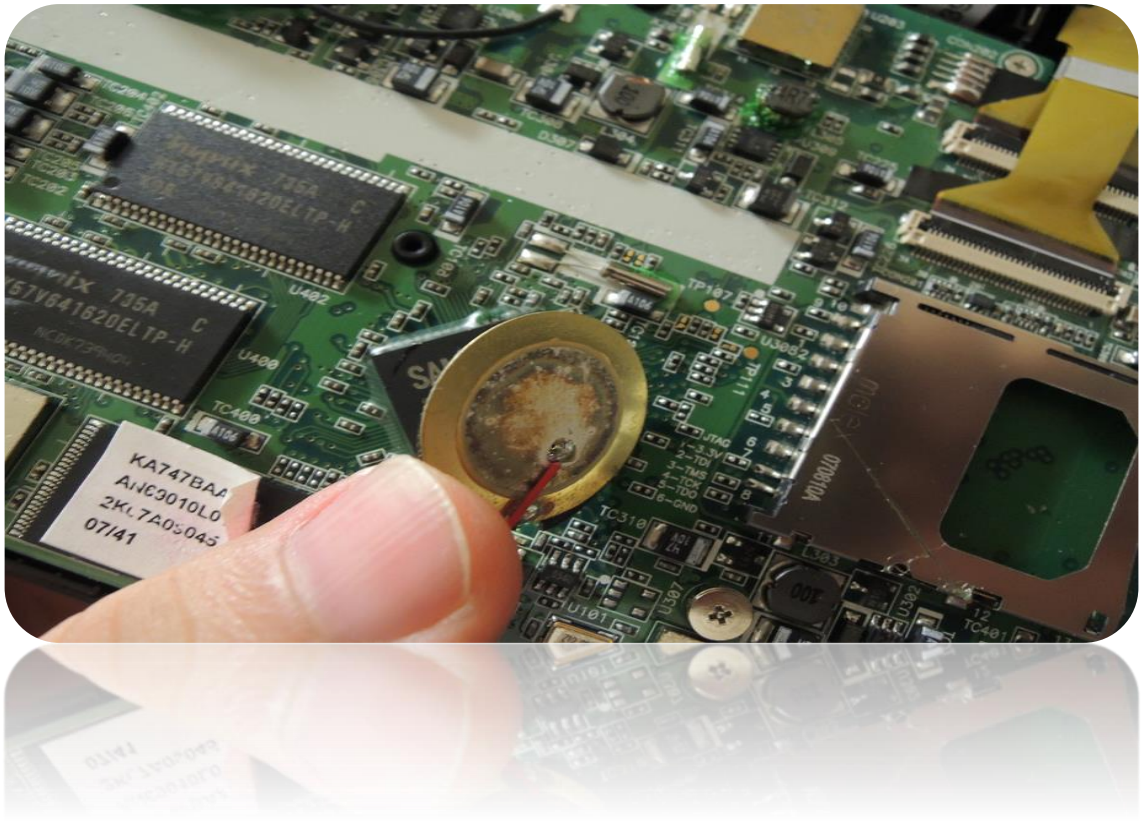


전자사전 분해하기

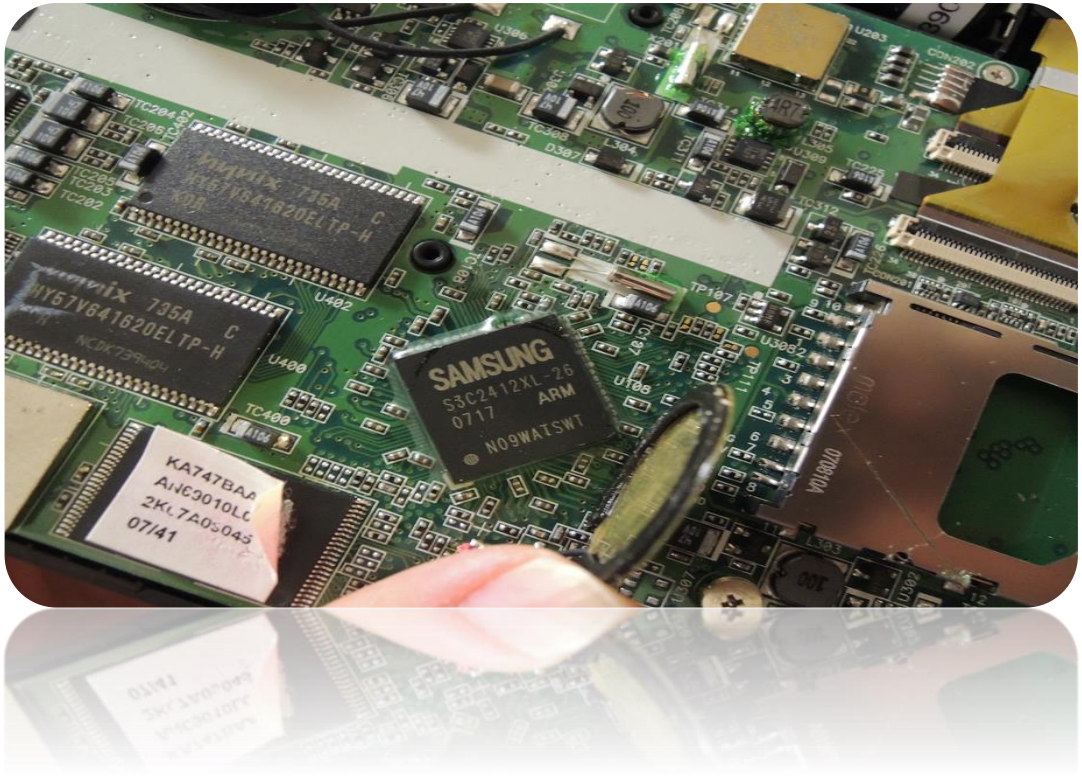
전자사전 분해하기



전자사전 분해하기


U402
U400
TC400
TP107
U3002
TC310
U101
U301
U302
TC401
JTAG
1—3.3V
2—TDI
3—TMS
4—TCK
5—TDO
6—GND

전자사전 분해하기



S3C2410AL26

S3C2410AL26-Y0R0

삼성 ARM920T, 소형 uBGA패키지,266MHz

큰이미지 보기

- 상품코드 5650
- 판매가격 19,000원 (부가세 미포함가)
- 제조사 SAMSUNG
- 적립금 190원
- 브랜드 SAMSUNG [브랜드몰바로가기]
- 수량 1
- 판매여부 품절입니다.

관심상품

Ubuntu on the 전자사전?

(현재 시도 중.. 이건 그냥 합성임 ㅎㅎ)

XBOX 360

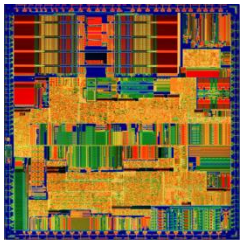
XBOX 360

- But.. 아직도 재조립을 못하고 있다능.. ㅠ.ㅠ

유용한 도구들

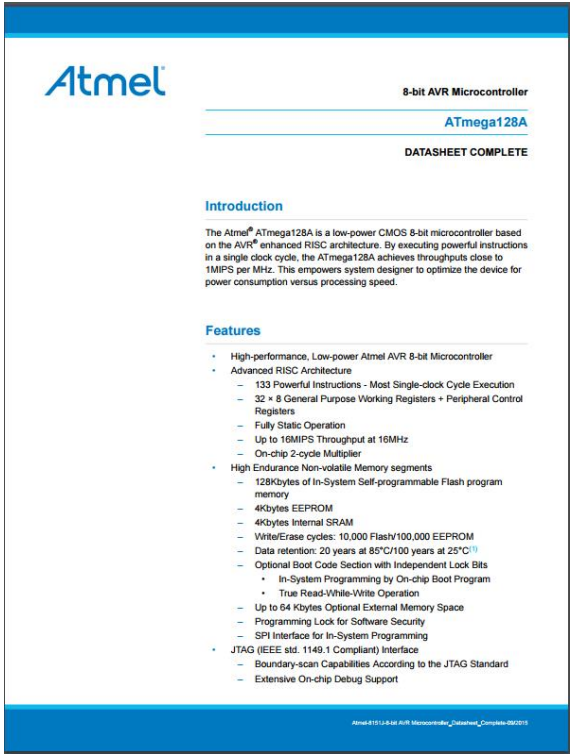
- 디지털 멀티 테스터
  - 전압, 전류, 저항 테스트
  - 통전 테스트

- USB 현미경
  - IC 칩, 소자 확대, 회로 패턴 분석
  - 500배율, 3만원대 제품 정도면 적합



LEVEL-2 : Datasheet 읽어 보기

- IC칩 모델명 검색 시 “datasheet” 단어를 추가하여 구글 검색
- CPU, Flash memory 위주로 datasheet 읽어 보기
- 처음엔 잘 모르겠어도 여러 번 반복해서 읽어 본다.
- 특히 Pin Map과 Memory Map 부분을 자세히 본다.



Atmel

8-bit AVR Microcontroller

ATmega128A

DATASHEET COMPLETE

Introduction

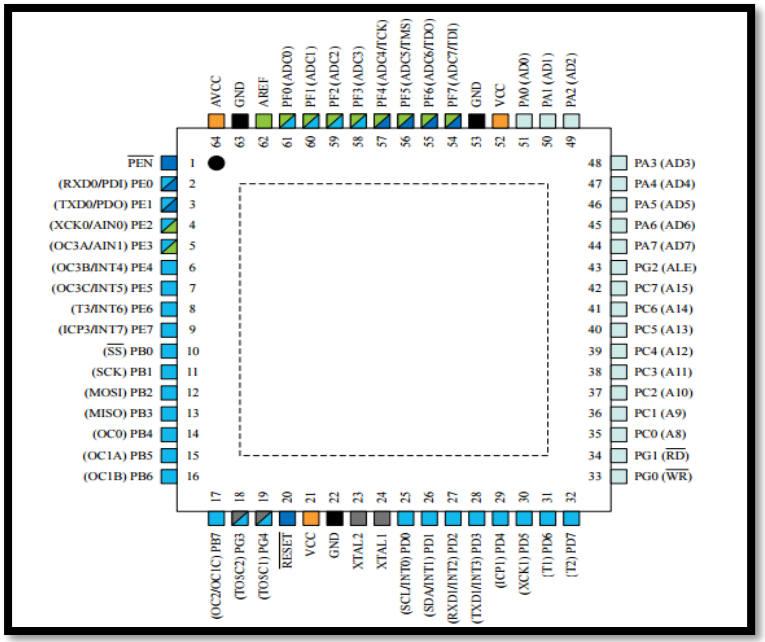
The Atmel® ATmega128A is a low-power CMOS 8-bit microcontroller based on the AVR® enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega128A achieves throughputs close to 1MIPS per MHz. This empowers system designer to optimize the device for power consumption versus processing speed.

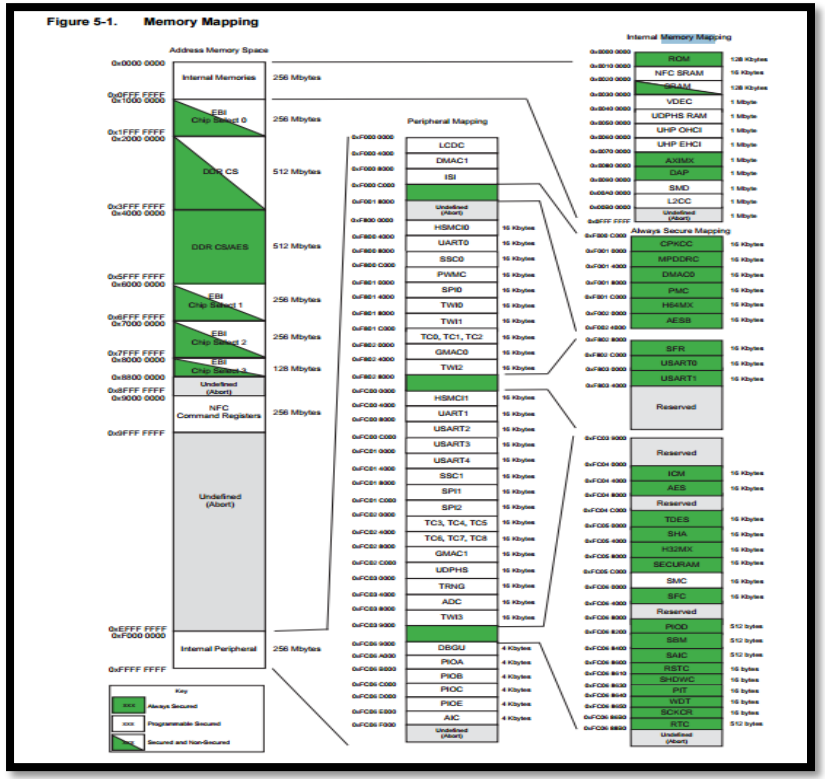
Features

- High-performance, Low-power Atmel AVR 8-bit Microcontroller
- Advanced RISC Architecture
  - 133 Powerful Instructions - Most Single-clock Cycle Execution
  - 32 × 8 General Purpose Working Registers + Peripheral Control Registers
  - Fully Static Operation
  - Up to 16MIPS Throughput at 16MHz
  - On-chip 2-cycle Multiplier
- High Endurance Non-volatile Memory segments
  - 128Kbytes of In-System Self-programmable Flash program memory
  - 4Kbytes EEPROM
  - 4Kbytes Internal SRAM
  - Write/Erase cycles: 10,000 Flash/100,000 EEPROM
  - Data retention: 20 years at 85°C/100 years at 25°C(1)
  - Optional Boot Code Section with Independent Lock Bits
    - In-System Programming by On-chip Boot Program
    - True Read-While-Write Operation
  - Up to 64 Kbytes Optional External Memory Space
  - Programming Lock for Software Security
  - SPI Interface for In-System Programming
- JTAG (IEEE std. 1149.1 Compliant) Interface
  - Boundary-scan Capabilities According to the JTAG Standard
  - Extensive On-chip Debug Support

Atmel-8151J-8-bit AVR Microcontroller_Datasheet_Complete-09/2015

Pin Map / Memory Map (CPU 예제)





Pin Map / Instruction Set (Flash Memory 예제)

3. PIN CONFIGURATION SOIC 150 / 208-MIL

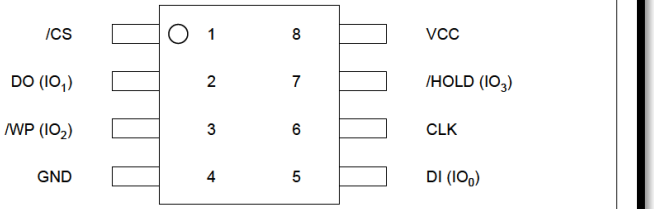


Figure 1a. W25Q16BV Pin Assignments, 8-pin SOIC 150 / 208-mil (Package Code SN & SS)

11.2.4 Instruction Set Table 3 (ID, Security Instructions)

INSTRUCTION NAME	BYTE 1 (CODE)	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6
Release Power down / Device ID	ABh	dummy	dummy	dummy	(ID7-ID0)(1)	
Manufacturer/ Device ID(2)	90h	dummy	dummy	00h	(MF7-MF0)	(ID7-ID0)
Manufacturer/Device ID by Dual I/O	92h	A23-A8	A7-A0, M[7:0]	(MF[7:0], ID[7:0])		
Manufacture/Device ID by Quad I/O	94h	A23-A0, M[7:0]	xxxx, (MF[7:0], ID[7:0])	(MF[7:0], ID[7:0], …)		
JEDEC ID	9Fh	(MF7-MF0) Manufacturer	(ID15-ID8) Memory Type	(ID7-ID0) Capacity		
Read Unique ID	4Bh	dummy	dummy	dummy	dummy	(ID63-ID0)

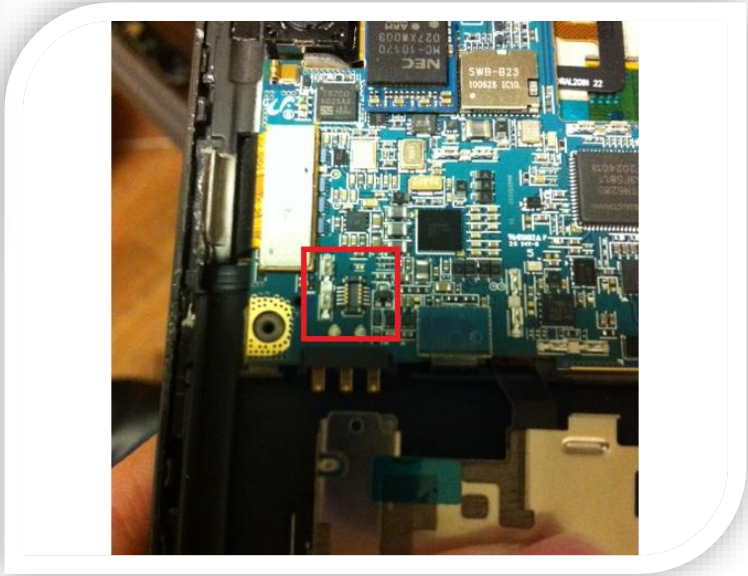
Level-3: Debug Port에 연결해 보기

- UART
  - Universal asynchronous receiver/transmitter
  - 하드웨어 통신 규약의 한 종류
  - 각종 디버그 메시지를 보거나, shell access 권한을 획득할 수 있다.
- JTAG
  - Joint Test Action Group
  - 하드웨어 디버깅의 국제 표준
  - 대상 장비를 실시간 디버깅하거나, 펌웨어를 획득할 수 있다.
- USB
  - adb shell, USB2TTL(UART), 저장장치
  - PC에 usb 케이블 연결 시 인식되는 장치를 확인한다.

다양한 연결 Port들을 찾아본다.

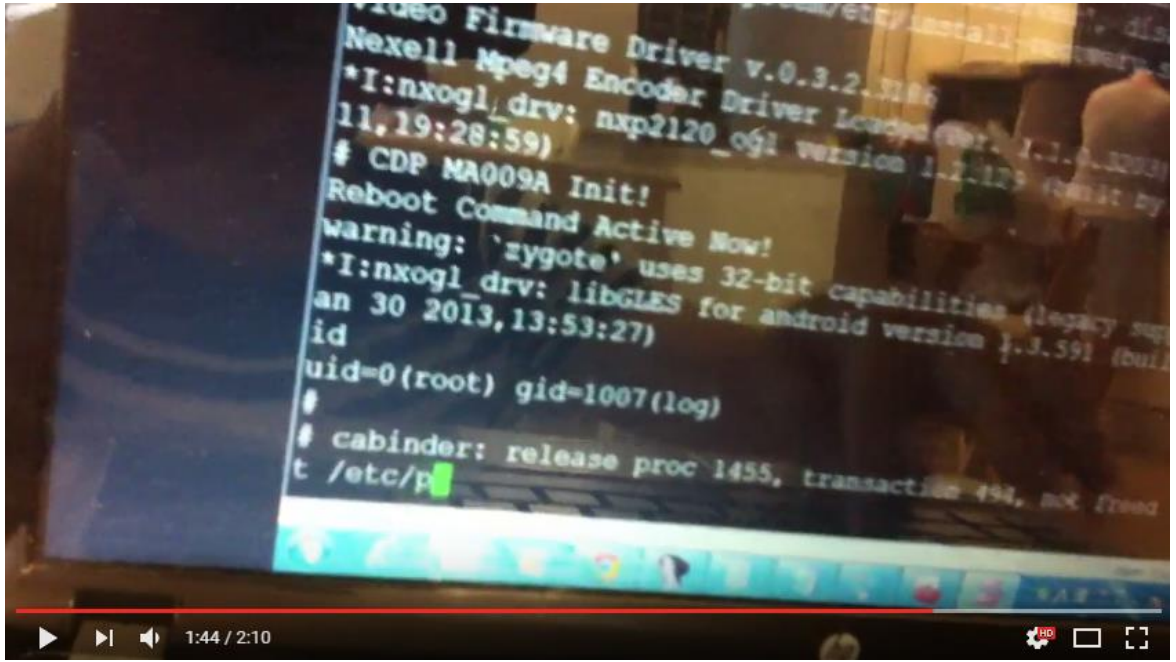
Wallpad UART

Smartphone JTAG



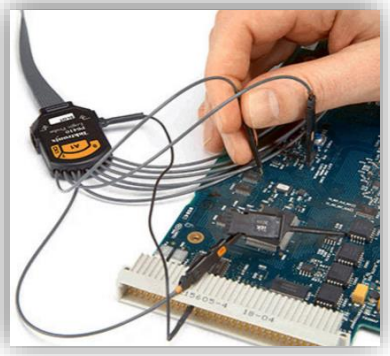
Wallpad UART 연결 예시

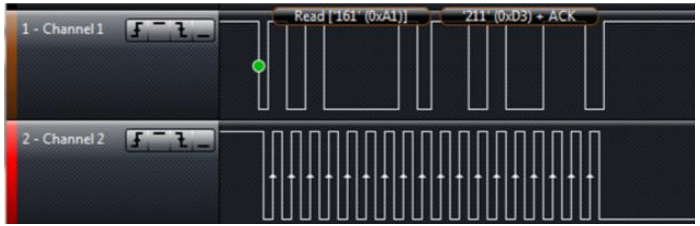
- https://www.youtube.com/watch?v=usyakFpspKs&t=71s



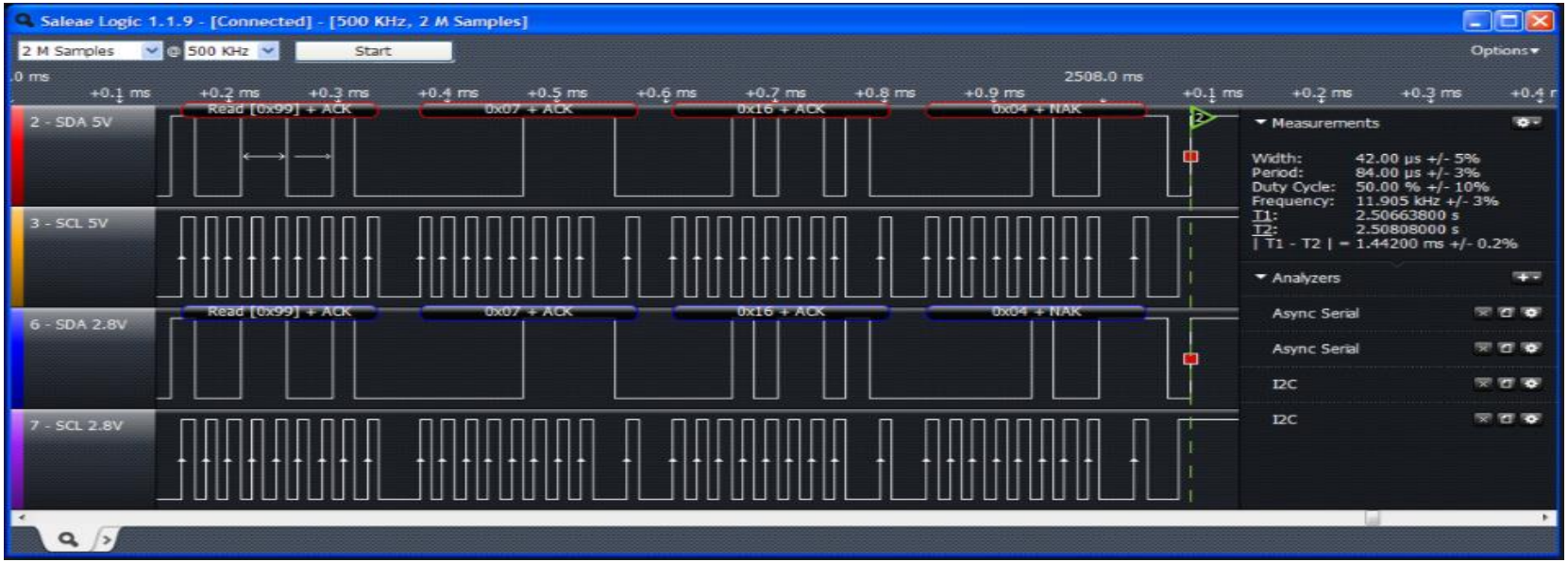
Level-4 : 전기 신호 분석해 보기

- 신호분석기(Logic Analyzer), 오실로스코프(oscilloscope) 이용
- 하드웨어 통신 신호 캡쳐/디버깅이 가능하다.
- 특정 핀의 용도 파악, 민감 데이터 유출 시 유용하다.
- 하드웨어의 세계에 대해 더욱 잘 이해할 수 있게 된다.
  - Clock 및 Rising/Falling edge에 대한 이해





무엇보다 이런 화면을 보고 있으면 친구들이 나를 진짜 하드웨어 해커라고 생각하게 됨

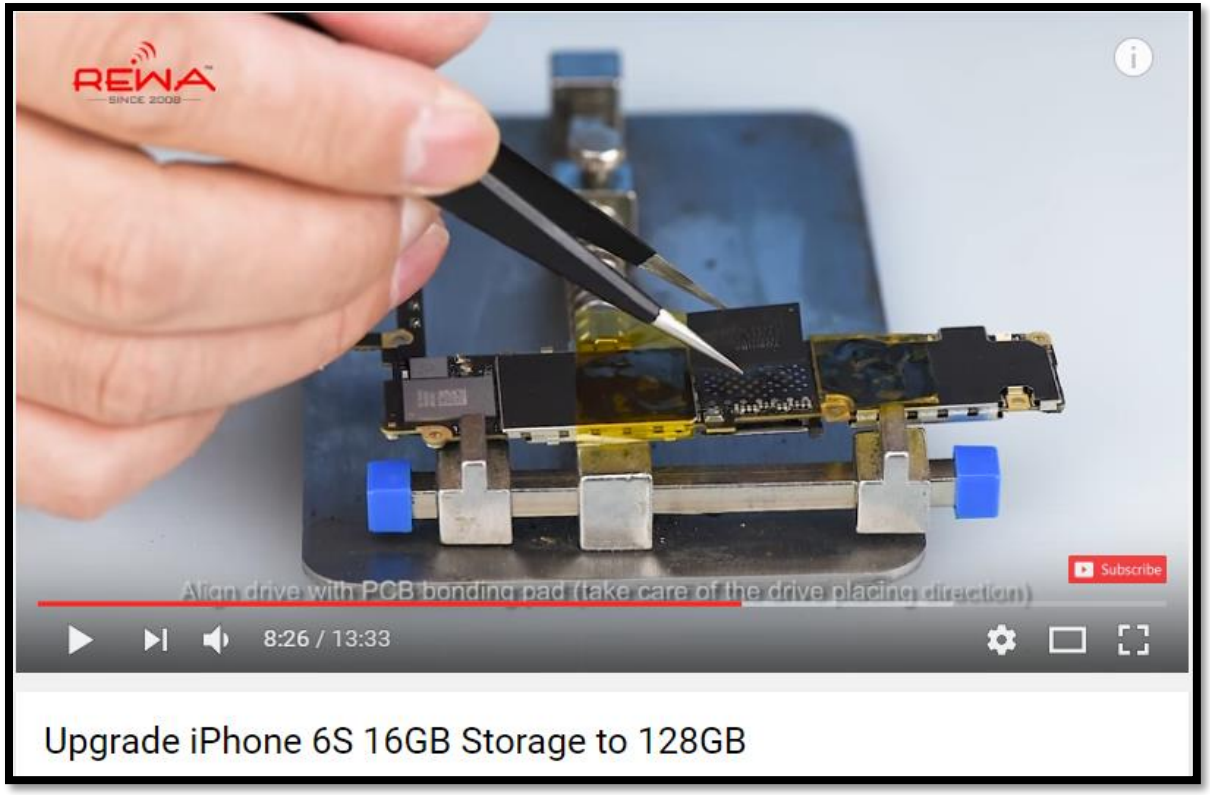


Level-5 : Desoldering

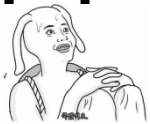
- IC 칩을 PCB에서 분리해 내는 작업을 의미
- IC 칩 교체 작업 시 필요함. (수리, Upgrade)

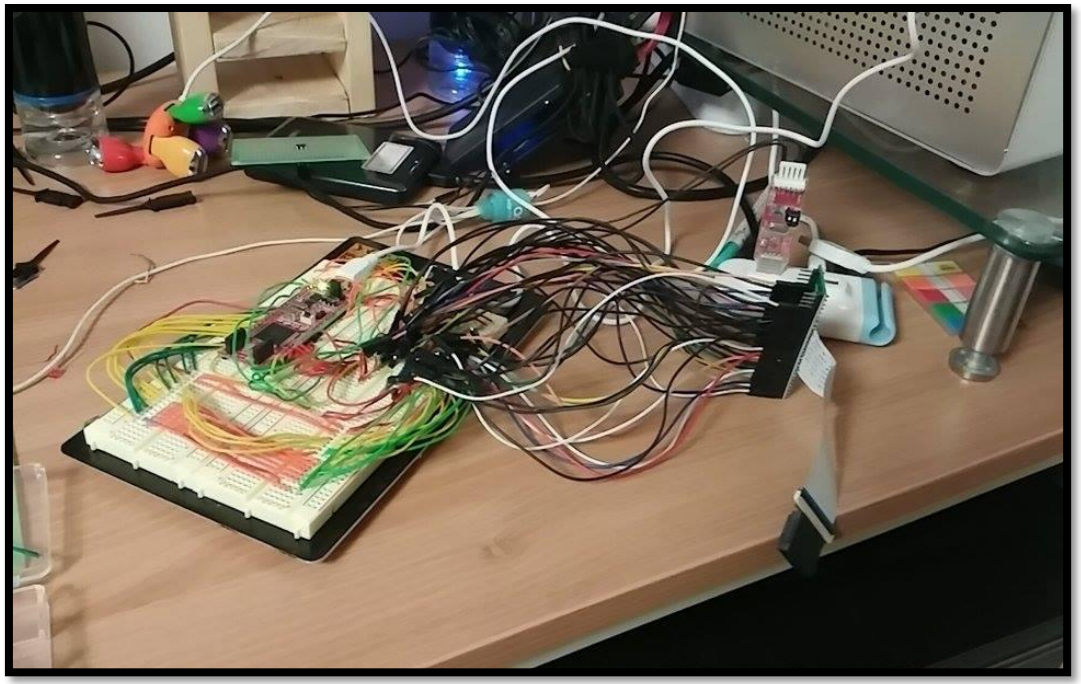
- Flash Memory dump 시 필요함.
  - 떼어 낸 Flash Memory 칩을 아두이노 등에 연결하여 READ Command 전송
- IC Pin Hijacking 시 필요함.
  - Ex> CPU와 Modem 사이에 통신하는 AT Command 신호 변조

iPhone Storage Upgrade



주의 : 만약 레고나 퍼즐 조립을 끝까지 못 한다면 성격 상 안 맞을 수도..





Level-6 : Side Channel Attack

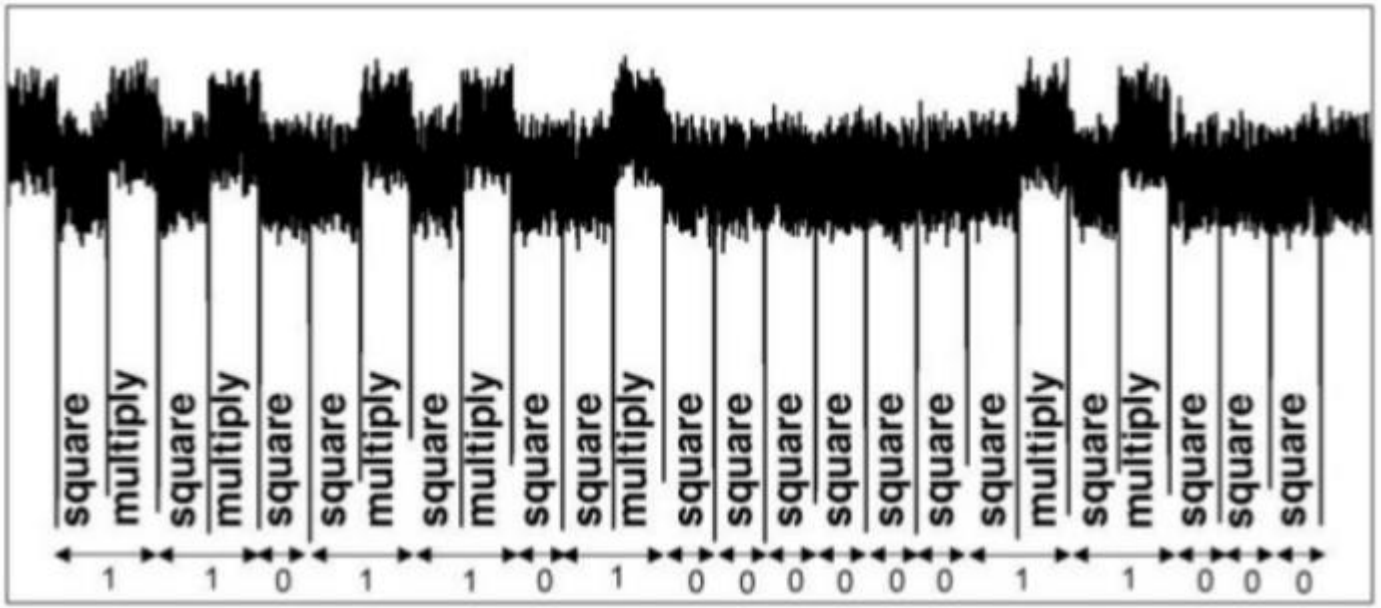
- 간접적인 정보들을 기반으로 중요한 데이터를 획득해 내는 기술
- 소비 전력(Power analysis) 분석, 소요 시간 분석(Timing Attack), 방출되는 전자기파/소리 분석 등의 방법들이 사용 됨
- 쉬운 것에서부터 매우 어려운 것까지 다양한 기술들이 존재함

전류 소모량은 작업량에 따라 다르다.

VS

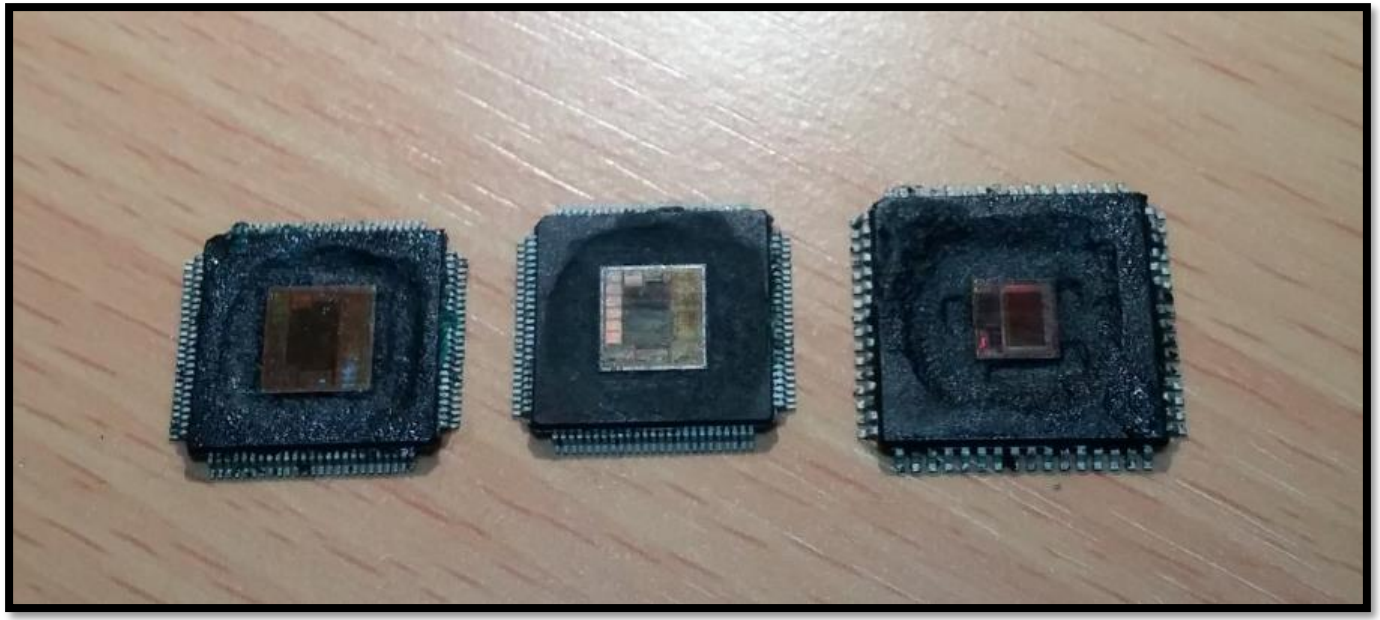
Instruction에 따른 전력 소모

- Secret Exponent value of RSA



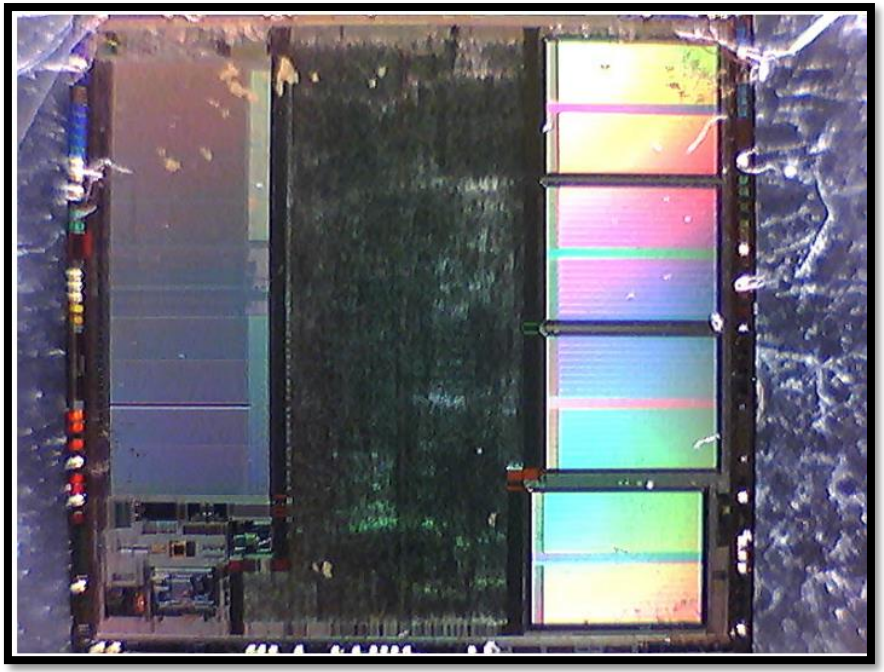
Level-7 : Decapping & Imaging

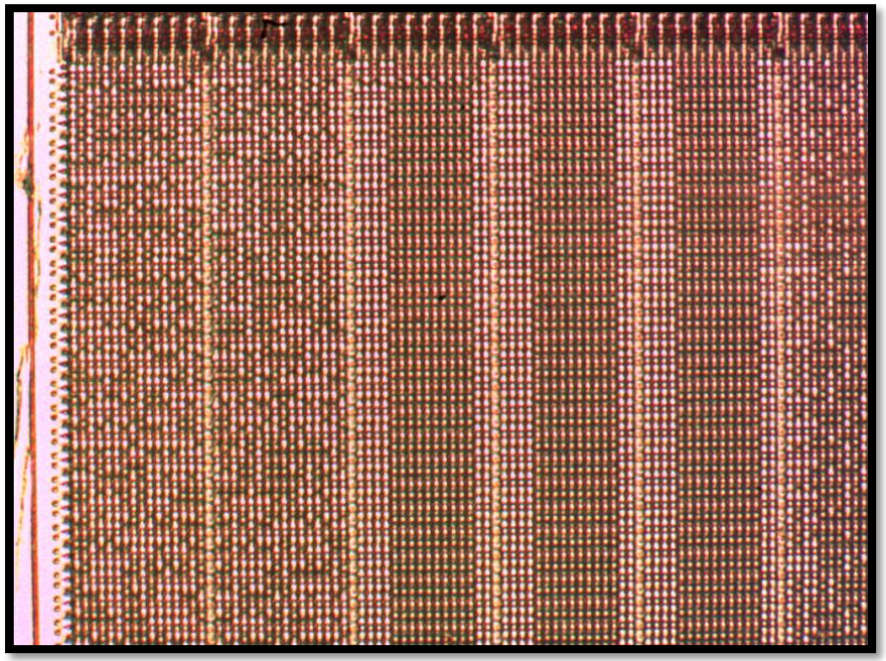
- 칩의 Package를 제거한 후, IC 회로를 분석하는 작업



Decapping 작업

Optical Imaging 작업

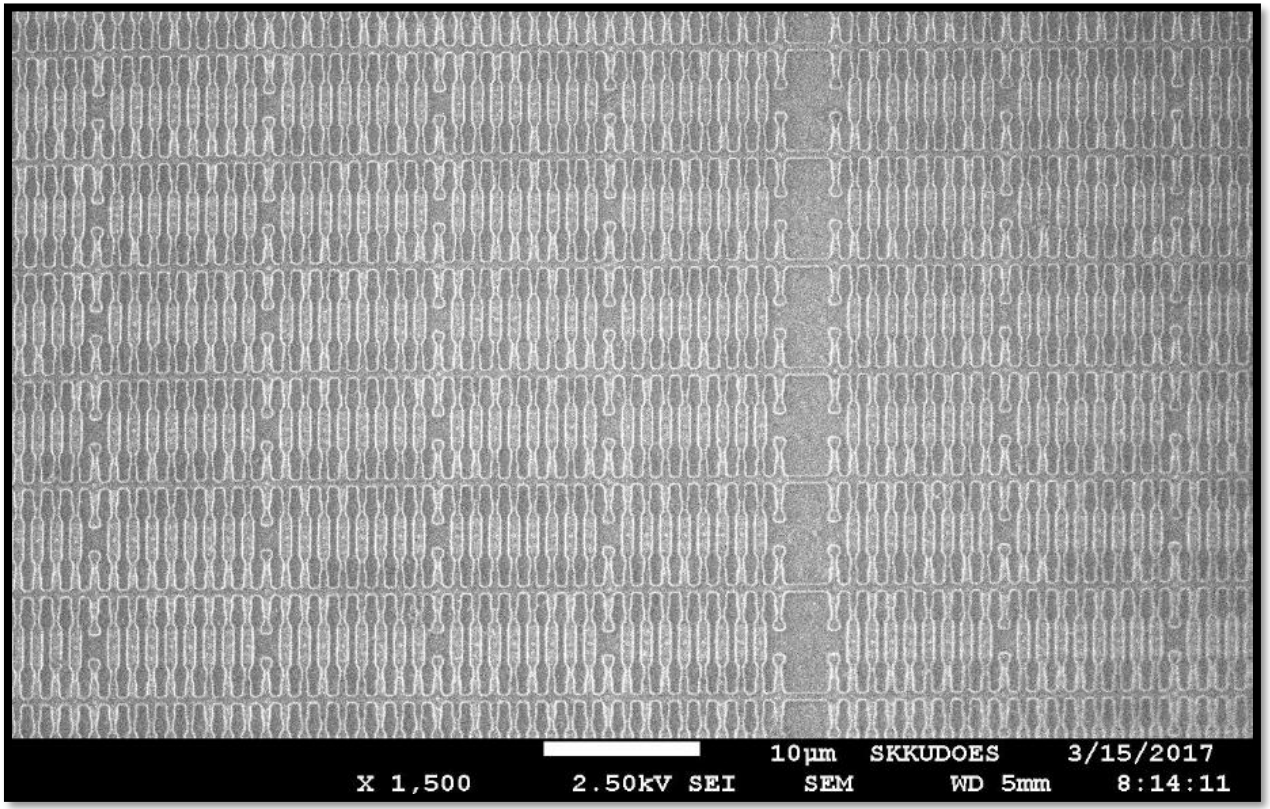




출처 : http://zacsblog.aperturelabs.com/

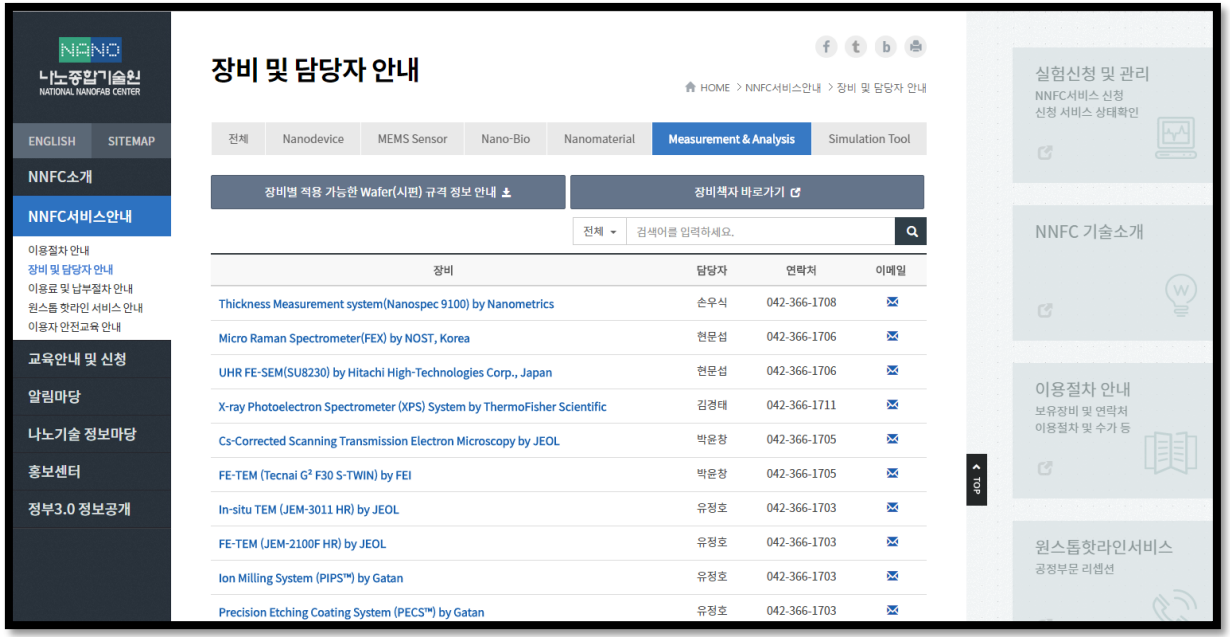
SEM Imaging 작업

SEM Imaging 결과



장비 사용 - 공용기기원

- 고려대 https://medicine.korea.ac.kr
- 경희대 https://crf.khu.ac.kr
- 나노종합기술원 https://www.nnfc.re.kr
- 동국대 https://equips.dongguk.edu
- 서울대 http://irf.snu.ac.kr
- 성균관대 http://ccrf.skku.edu
- 세종대 http://rfc.sejong.ac.kr
- 아주대 http://cmcm.ajou.ac.kr
- 인천대 http://www.uirf.or.kr
- 조선대학교 http://www.chosun.ac.kr
- 충남대 http://www.cnucrf.re.kr
- 한국산업기술대학교 http://cec.kpu.ac.kr



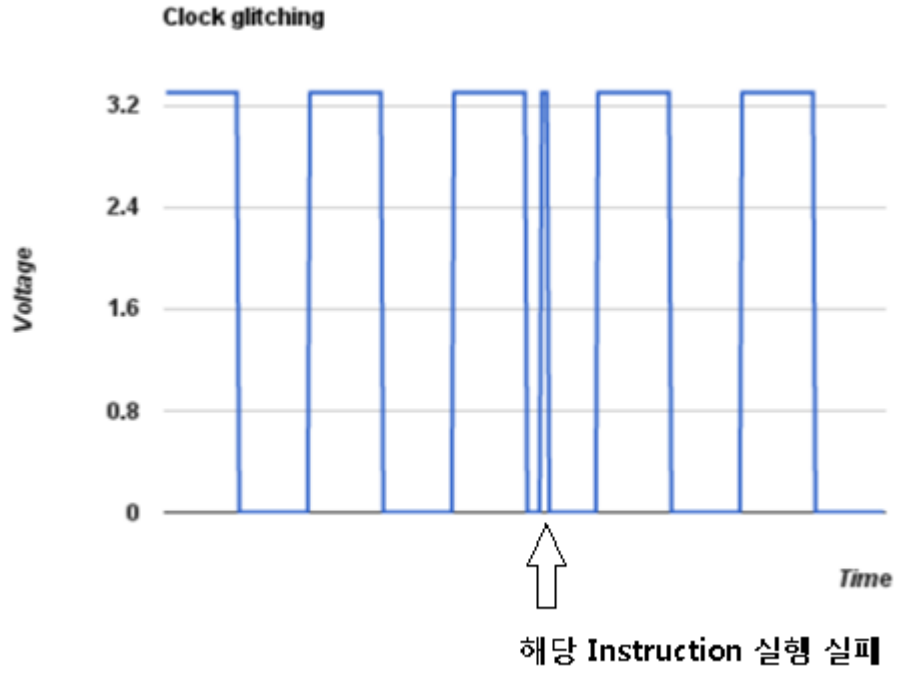
Level-8 : Glitching Attack

- IC 칩에 의도적인 오류를 발생시켜 오작동을 유발하는 기술
  - 이 오류가 때로는 좋은 "버그"가 되어 돌아온다.
  - Glitching의 뜻 : 프로그램 오류, bug, exploit, 어지러운

- 대표적인 Glitching attacks
  - Clock glitching : 비정상적인 clock을 인가하여 오작동 유발
  - Voltage glitching : 전압을 순간적으로 올리거나 내려서 오작동 유발
  - Thermal glitching : 정상 범위를 벗어나는 온도(hot or cold)로 오작동 유발

- 효과
  - Firmware dump, crypto break, bypass secure-boot or some checks

Clock Glitching Attack 예시



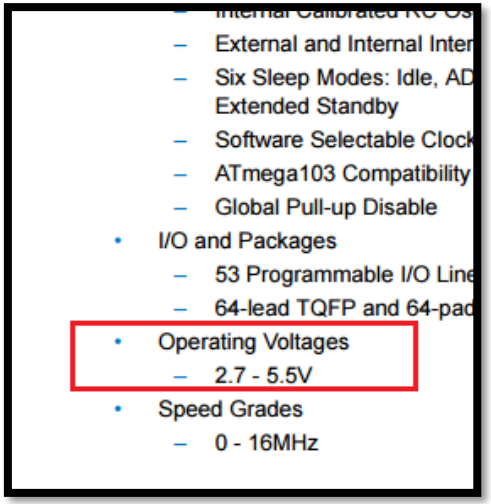
Clock Glitching Attack 예시 - Bypass secure booting

```
        LDA     #01h
        AND     $0100           ;the contents of the first byte of EEPROM is checked
loop:   BEQ     loop            ;endless loop if bit 0 is zero
        BRCLR 4, $0003, cont    ;test mode of operation
        JMP     $0000           ;direct jump to the preset address
cont:   LDA     #C0h
        STA     $000D           ;initialize the serial asynchronous port
        CLR     $000E
        BSET    2, $000F
        LDX     #50h
wait:   BRCLR 5, $0010, wait    ;upload user code
        LDA     $0011
        STA     , x
        INCX
        DEC     $0050
        BNE     wait
        JMP     $0051           ;jump to the user code
```

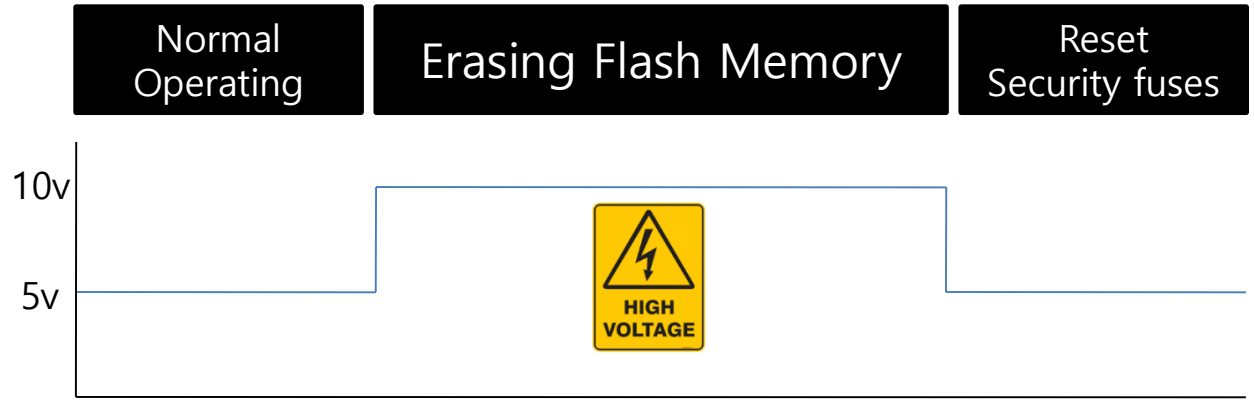
Figure 41. Example of the bootloader code responsible for security in MC68HC05B6 microcontroller

1. Secure Boot 관련 코드
2. User code loading 루틴
3. EEPROM에 저장된 security bit 체크
4. 만약 0이라면, 더 이상 진행하지 않음 (endless loop)
5. Clock Glitching을 통해 해당 Instruction이 Fail되게 만들면 Endless loop 탈출 가능

Voltage Glitching Attack 예시
- Bypass code protection



Datasheet

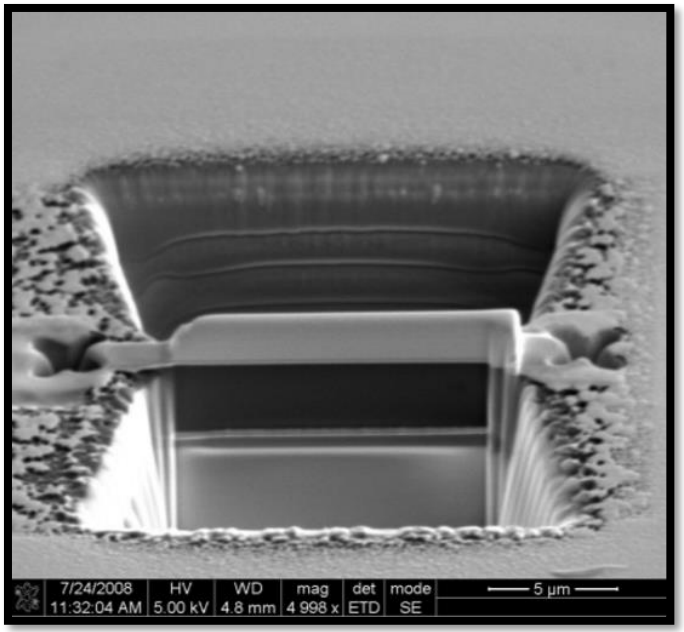


Level9 : FIB attack

- FIB = 집속이온빔시스템(Focused ion beam system)
- Ga이온 빔을 회로 내의 원하는 위치에 집속(Focus)시켜, 회로를 식각/증착 할 수 있는 장비
  - 식각 : 회로 패턴을 제거
  - 증착 : 회로 패턴을 추가 (기체 -> 고체)
- 회로에 수정을 가할 수 있음!
- Code Protection을 break할 수 있음
  - Security bit에 해당하는 메모리 소자의 출력을 GND나 VCC로 강제 연결시킴

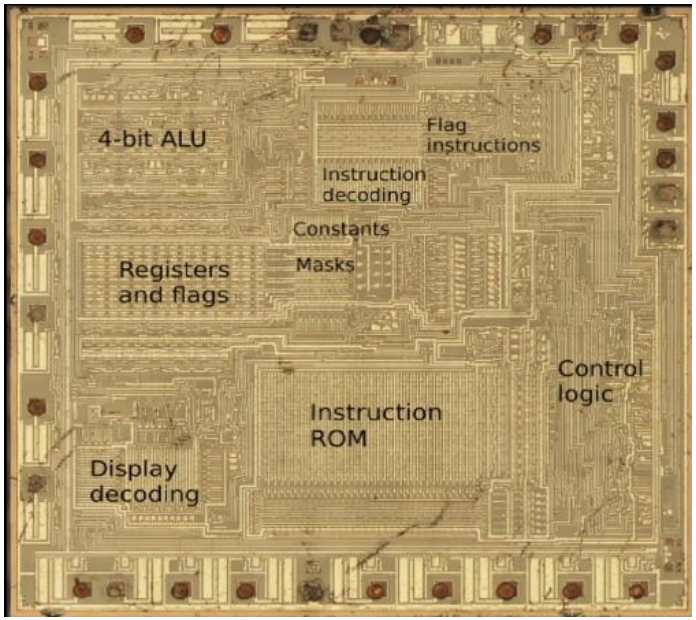
FIB 장비 예시

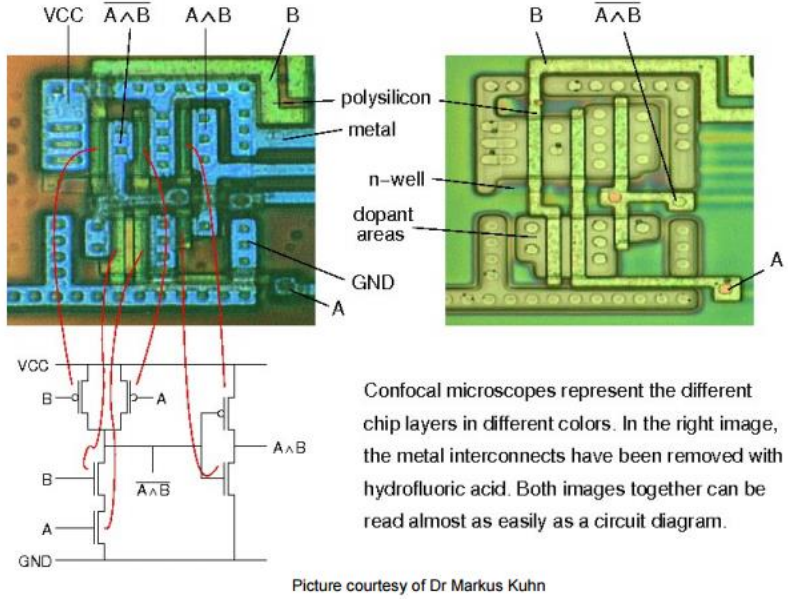

FB-2100
HITACHI


7/24/2008
11:32:04 AM
HV
5.00 kV
WD
4.8 mm
mag
4 998 x
det
ETD
mode
SE
5 µm

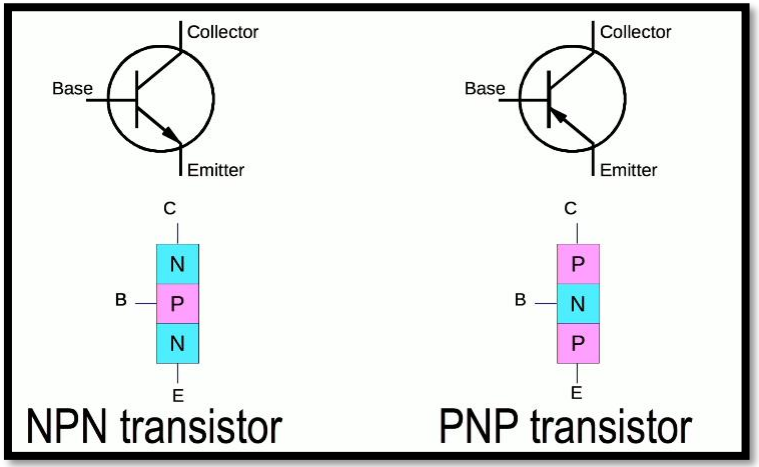
Level10 : IC Chip Reversing

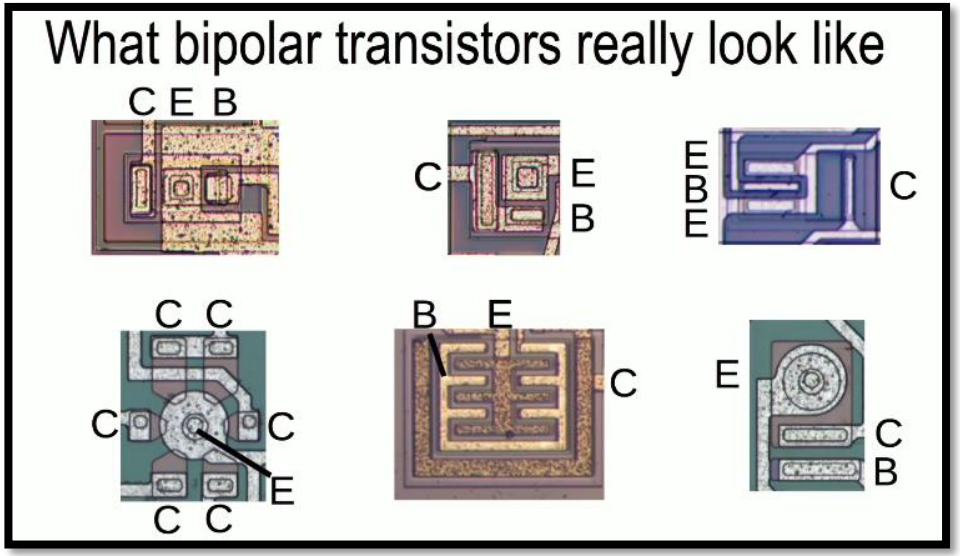
- IC Chip의 회로를 분석하여 용도를 attack point를 파악하는 작업
- 반도체공정 및 회로이론에 대한 지식이 뛰어나야 함





Book VS Real World

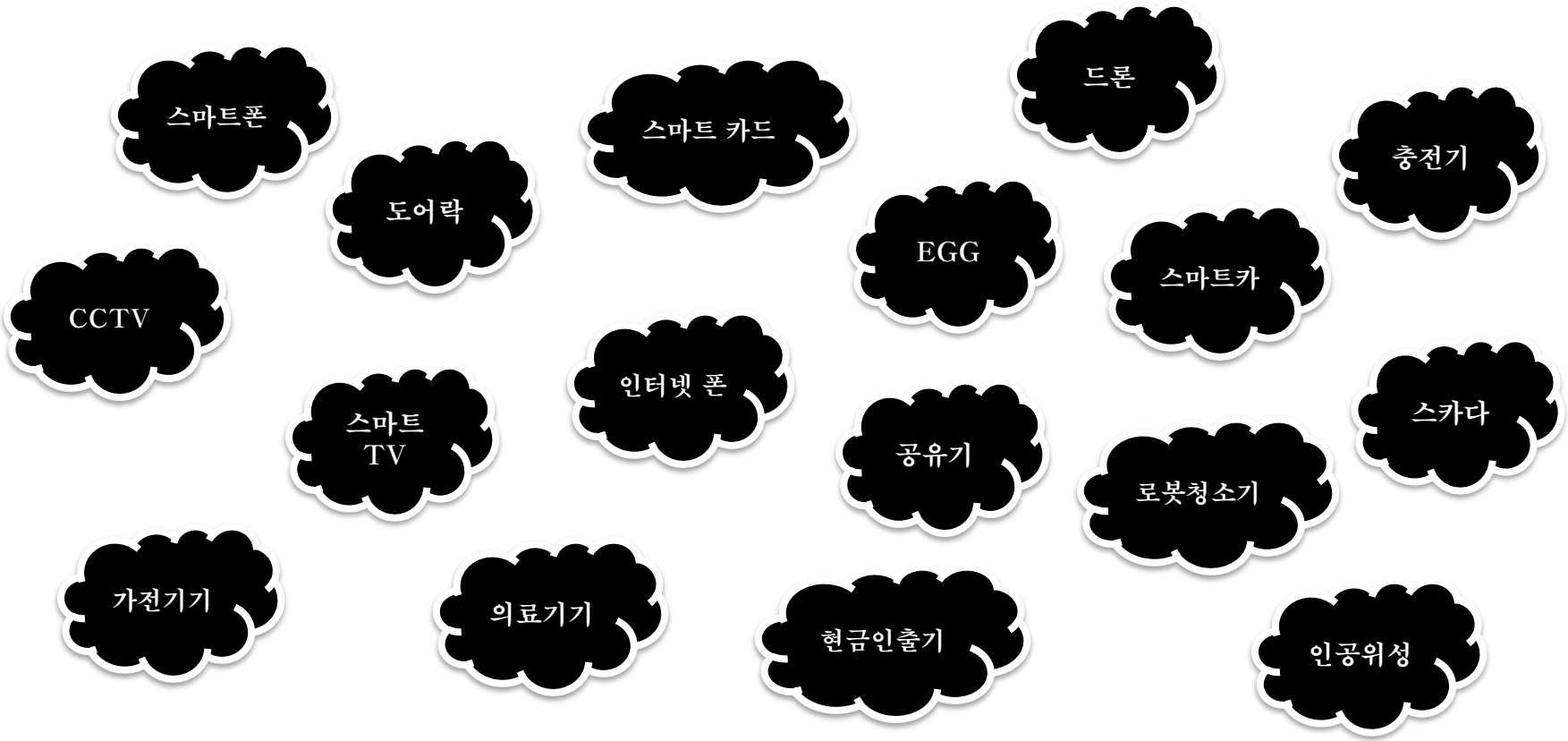




출처 : https://www.youtube.com/watch?v=aHx-XUA6f9g

하드웨어 해킹 사례들

하드웨어 해킹 사례들

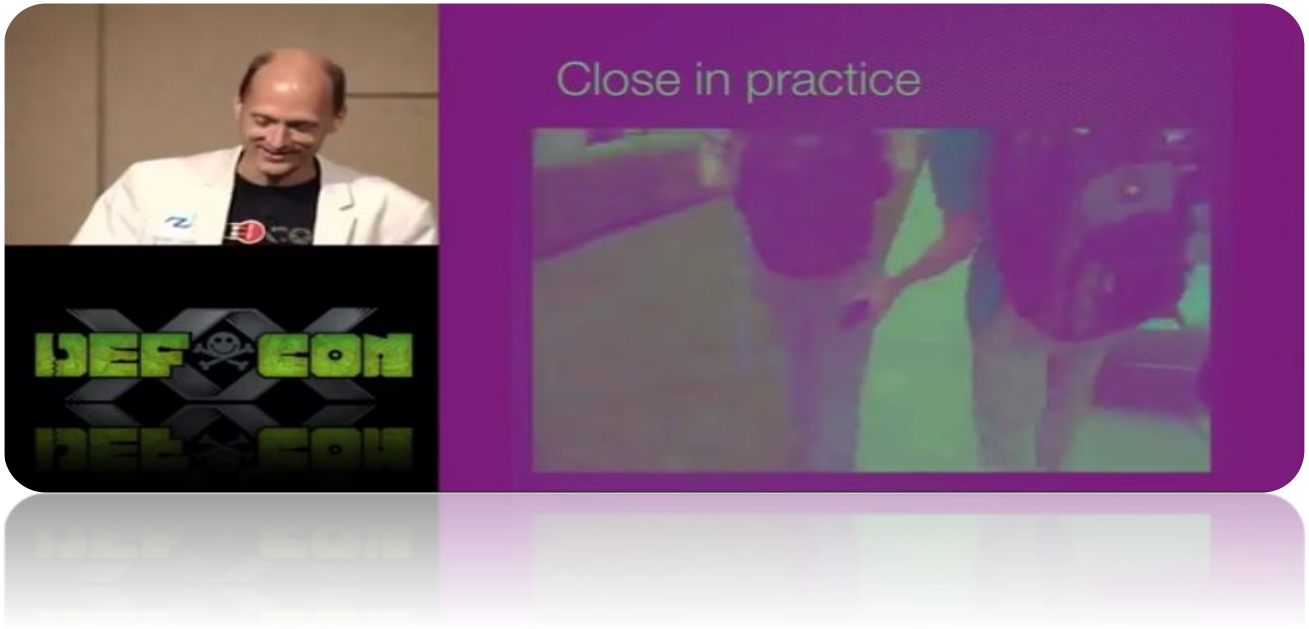

스마트폰
스마트 카드
드론
충전기
도어락
EGG
스마트카
CCTV
인터넷 폰
스마트 TV
공유기
스카다
로봇청소기
가전기기
의료기기
현금인출기
인공위성

스마트폰 NFC 해킹

- 개요
  - Near Field Communication
  - 2012~2014년도에 유행했던 스마트폰 해킹 방식
- 공격 방식
  - NFC 커널 레벨 프로토콜에서의 취약점 공격
  - 스마트폰 근처에 접근하는 것만으로 해킹 가능
- 공격의 피해
  - 스마트폰 장악

스마트폰 NFC 해킹

- 데모 영상
  - http://www.youtube.com/watch?v=eAe0-J2v7_I



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

- 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

- 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

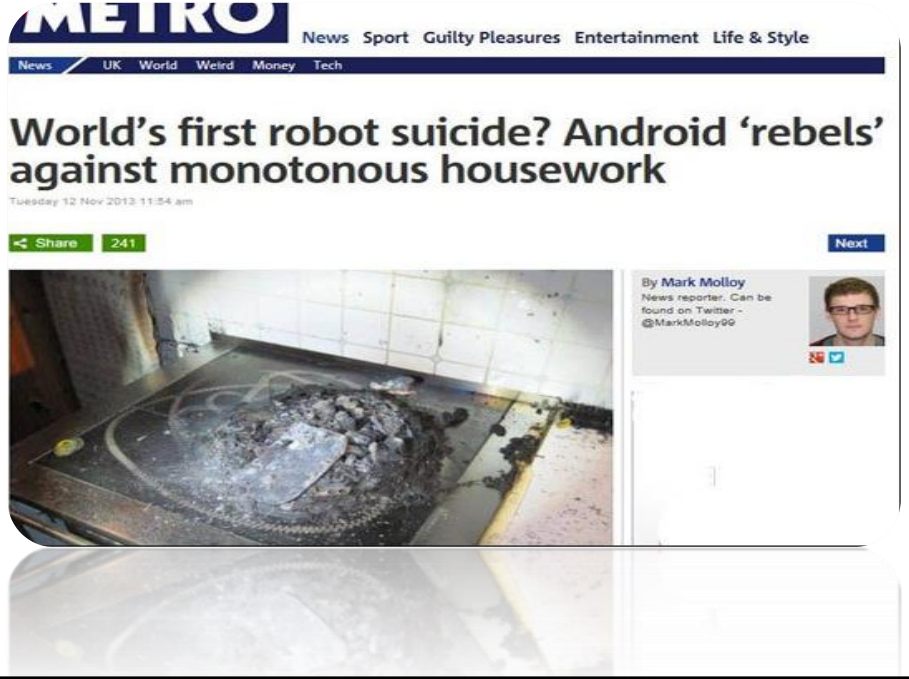
- 관련자료
  - http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1002077186
  - http://dailysecu.com/news_view.php?article_id=2014
  - http://www.boannews.com/media/view.asp?idx=31392

로봇 청소기 해킹

- 요약
  - 가정용 로봇 청소기를 원격 장악
- 공격 방식
  - 전용 프로그램 혹은 스마트폰이 로봇 청소기와 통신
  - 명령을 REPLAY하여 제어
  - 로봇청소기 내 원격 서비스에 대한 시스템 해킹
- 공격 피해
  - 도청 및 감시

로봇 청소기 해킹

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



가전기기 해킹

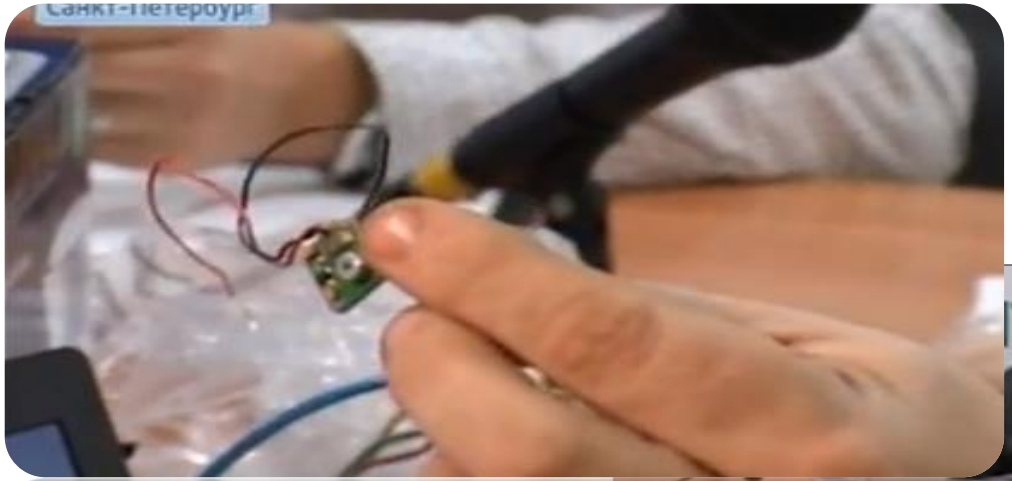
- 스마트 냉장고
- 스마트 오븐
- 스마트 세탁기
- 스마트 홈 네트워크
- …

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
- 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

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

해적 방송 출력

스마트 홈 네트워크 해킹

- 개요
  - 스마트 홈 네트워크의 심장부인 월패드를 해킹하여 전등/가스 제어, 현관 문 강제 오픈, 화상 카메라 해킹을 통한 사생활 감시 가능
- 공격 방식
  - 원격 서비스 공격
  - Telnet을 이용한 관리자 계정 접속
  - Packet replay attack
- 관련 자료
  - http://imnews.imbc.com/replay/2014/nw1800/article/3548499_13479.html

스마트 홈 네트워크 해킹


이브닝 이슈
'스마트홈' 보안에 취약
MBC
'스마트홈 해킹' 출입문까지 뚫는다?
사회
서울 혁신학교 내년 1백 개로··55개교 공모

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

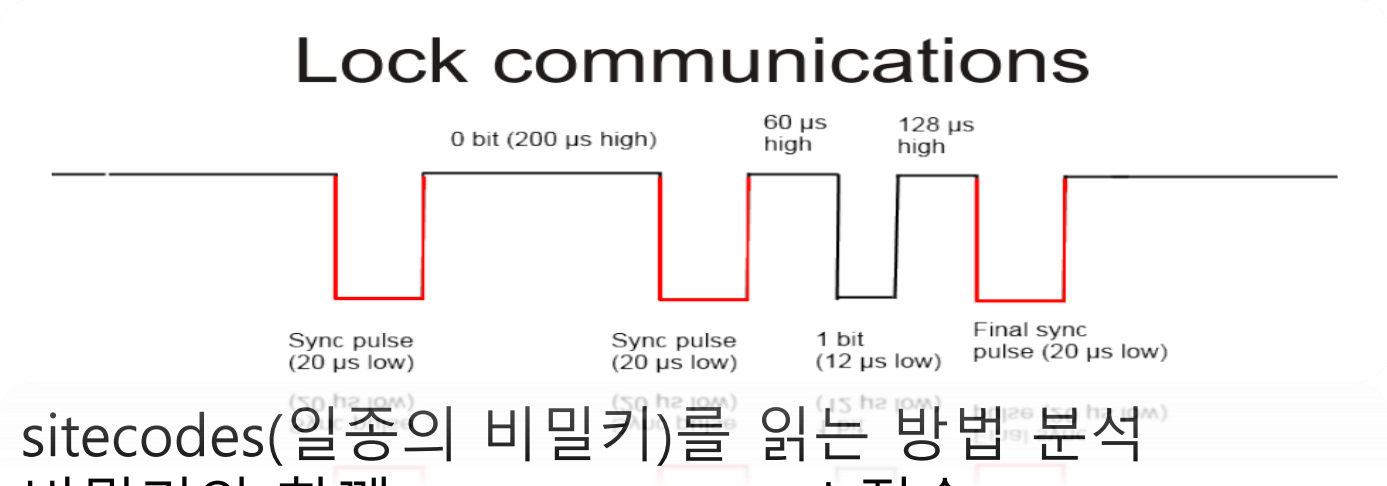
디지털 도어락

- 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

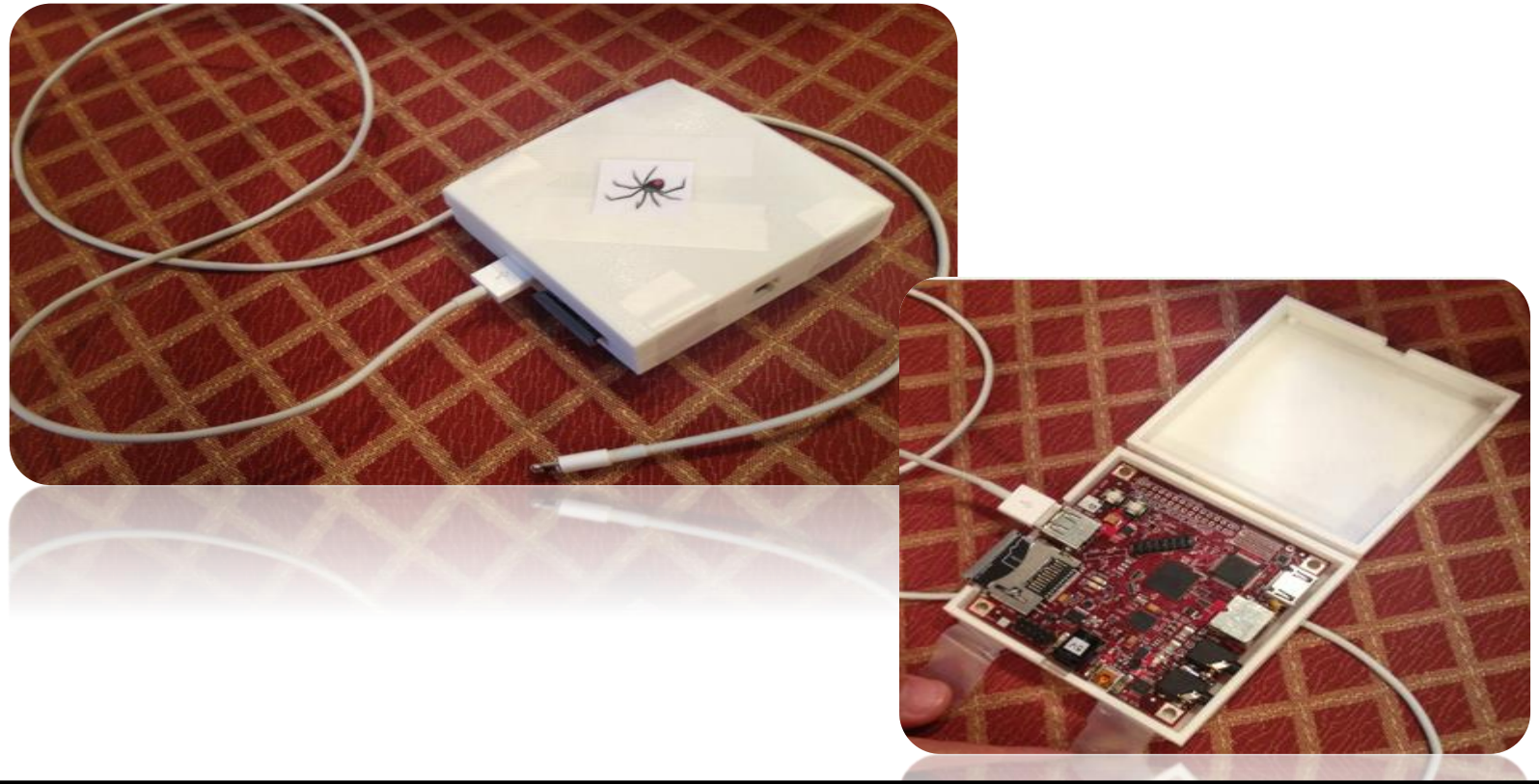
시연 영상

- 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

휴대전화 충전기 해킹



휴대전화 충전기 해킹

- 요약
  - 충전기로 위장된 해킹장치에 아이폰 연결 시 악성 앱 자동 설치 (2013-08)
- 공격 방식
  - iOS 개발자 모드 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

- 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

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

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

의료기기 해킹

- 심장박동기 해킹
  - 과전압 발생
- 인슐린 펌프 해킹
  - 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), Drone 해킹
- 스마트 카메라
- POS(판매시점관리)
- MP3 Player
- 디지털 프린터
- 가정용 게임기
- 배터리 해킹
- 항공기, 선박 해킹
- 스마트 카드 해킹

하드웨어 해킹 공부 방법 추천

- 추천 서적 for newbies
  - 뇌를 자극하는 하드웨어 입문
  - 만화로 쉽게 배우는 전기
  - 짜릿짜릿 전자회로 DIY
  - 당근이의 AVR 갖고 놀기
  - 일렉트릭 유니버스
  - 임베디드 레시피

- 추천 사이트
  - Youtube.com은 진리다!
  - 당근이의 AVR 갖고 놀기 커뮤니티
    - http://cafe.naver.com/carroty
  - HACKADAY
    - http://hackaday.com

임베디드 기기 취약점 분석 절차

- 장비 분해
- Debug 포트 연결 (UART, JTAG)
  - Shell 획득 혹은 Log message 확인
- 펌웨어 획득
  - 업데이트 파일, bootloader 이용, flash memory 추출, jtag 연결 등
- 바이너리 추출
  - filesystem mounting
- 기기 환경 분석
  - 취약점 공격 대상 선정 및 attack vector 구상
- 취약점 분석 및 Exploiting
  - gdb 디버깅, jtag 연결 등

하드웨어 해킹을 통해 얻을 수 있는 것들

- 임베디드 장비(공유기, CCTV 등) 0-day 취약점 헌팅
  - KISA 신규 취약점 신고포상제로 제보, 컨퍼런스 발표 등
- 컴퓨터 작동에 대한 더욱 깊은 이해
  - Clock, Transistor, Logic Gate, Interrupt,
- Fun! Fun!!
  - DIY : 하드웨어 지식이 쌓이면 원하는 장난감, 아이디어 제품을 직접 만들 수 있다.

마지막으로..

- 공부를 진짜 열심히 해야 한다!
  - 노력 없이 얻어지는 것은 없다.
- 즐겁게 공부하는 방법을 터득해야 한다.
  - 그룹 스터디, 컨퍼런스 발표, 업무로 경험할 수 있는 업체 취직 등
- 영어 공부는 필수다.
  - 100배 이상의 정보들을 흡수할 수 있다.

과 to the 제!

- 주변의 전자장비 한 개를 분해한 후,
  각종 IC칩들(CPU, RAM, FLASH)의 제조사,
  모델명 및 Spec에 대해여 분석한다.

- 과제 제출 기간 : 8월 31일 밤 12시
- 이메일 : cybermong@grayhash.com
- 제목 양식 : [BOB 6기 과제] 이름
- 문서 포맷 : PDF

QnA

감사합니다.