看雪 2018 安全开发者峰会

Kanxue 2018 Security Developer Summit

2000-2018

智能设备漏洞挖掘中的几个突破点

自我介绍

姓名：马良

- 绿盟科技　工业物联网安全实验室　工控安全研究员
- 专长：硬件和固件安全

- 2016 XPWN 西门子PLC工控蠕虫演示者；
- 硬件极客，技术宅

- 插播广告：对工业物联网有兴趣的朋友，欢迎联系我们

目录大纲

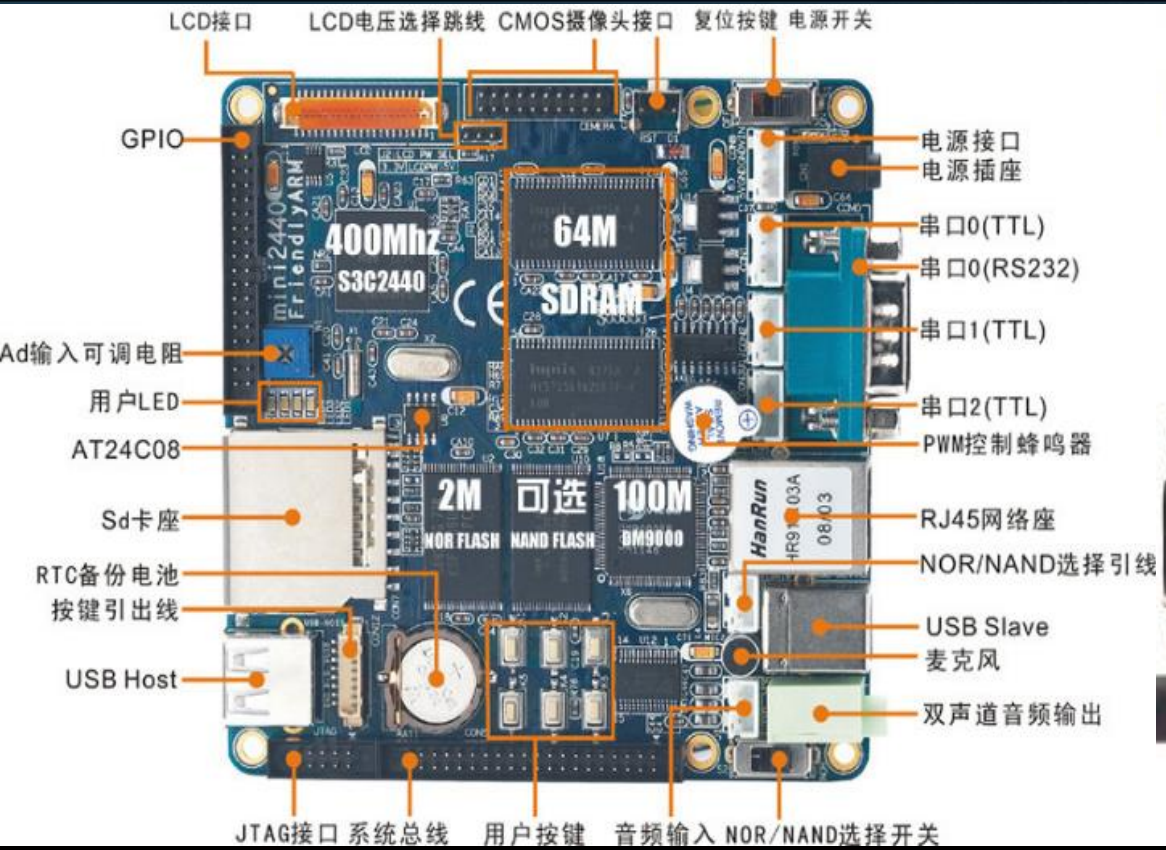
智能设备基础知识

提取固件的十种思路

从固件发掘漏洞的思路

智能设备的加固建议

智能设备的组成


LCD接口
LCD电压选择跳线
CMOS摄像头接口
复位按键
电源开关
GPIO
电源接口
电源插座
串口0(TTL)
串口0(RS232)
串口1(TTL)
Ad输入可调电阻
用户LED
串口2(TTL)
AT24C08
PWM控制蜂鸣器
Sd卡座
RJ45网络座
RTC备份电池
NOR/NAND选择引线
按键引出线
USB Slave
麦克风
USB Host
双声道音频输出
JTAG接口
系统总线
用户按键
音频输入
NOR/NAND选择开关
400Mhz
S3C2440
64M
SDRAM
2M
NOR FLASH
可选
NAND FLASH
100M
DM9000
HanRun

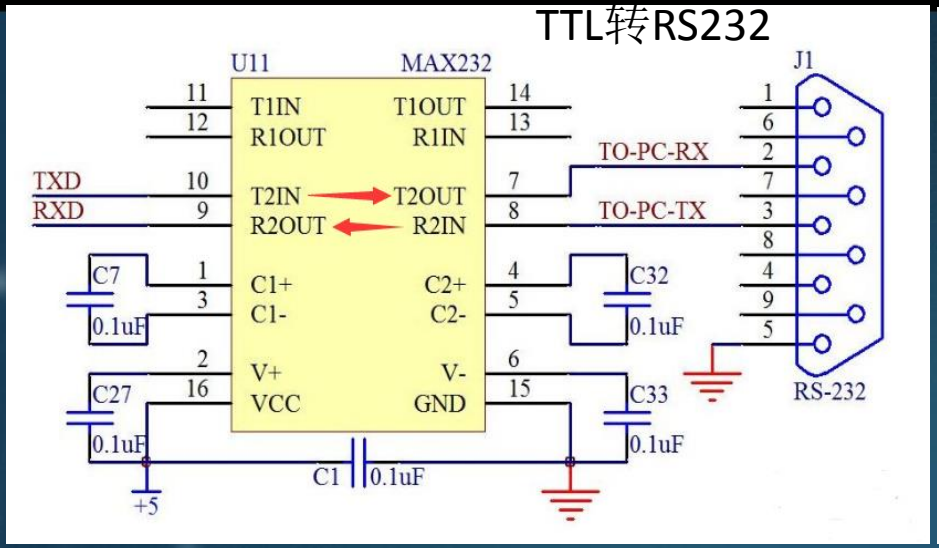

FriendlyARM
Loading...
FriendlyARM

智能设备的组成

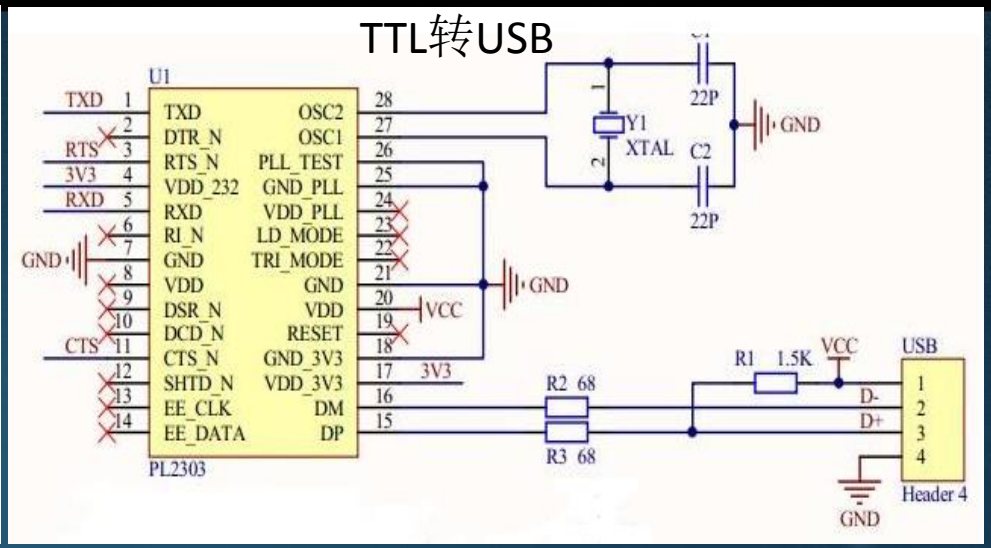
- CPU：X86/ARM/MIPS/PPC等
- 内存：SDRAM/RAM
- 存储：Flash/TF卡/SD卡/MMC卡/硬盘
- 串口：一般电路板会留，做调试用
- 网口：智能设备联网用
- USB口：接U盘做扩展存储用、也可接键盘和鼠标等
- 无线接口：Wifi/蓝牙/ZigeBee等
- bootLoader：Uboot等
- 操作系统：Linux/RT-Linux/VxWorks/uCOS-II等

智能设备的串口通信

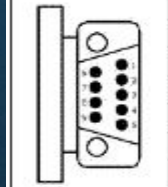
TTL转RS232



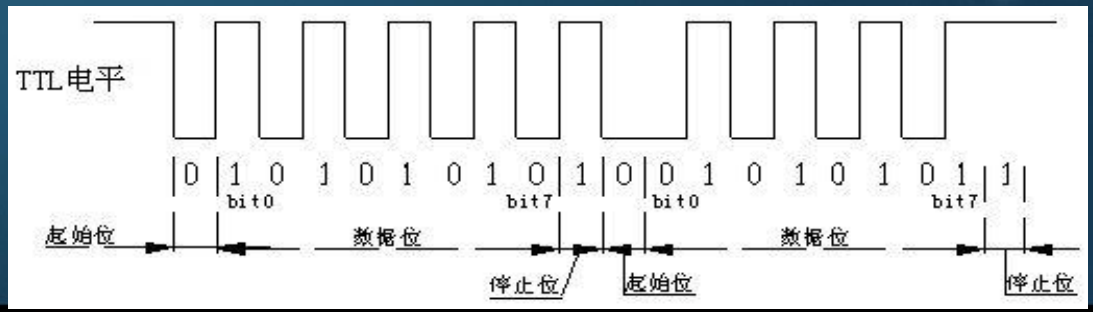
TTL转USB



串口DB9定义

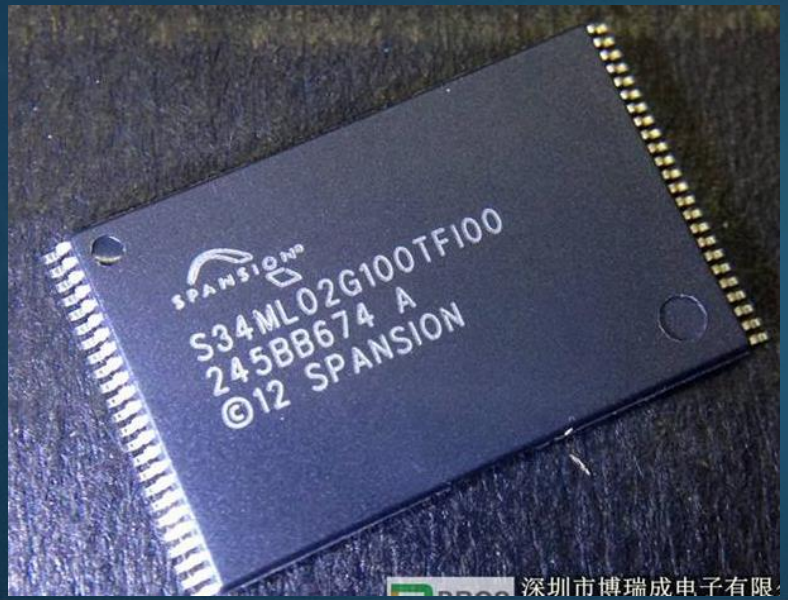


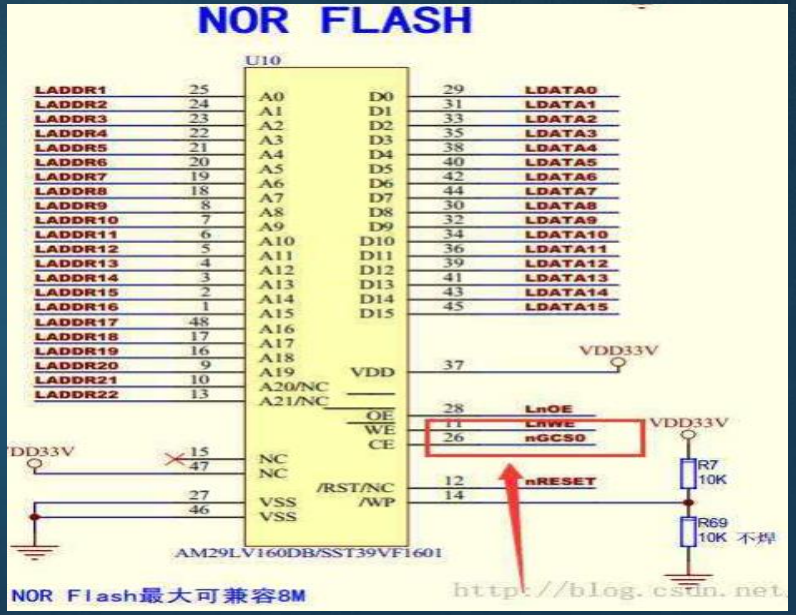
针脚	符号	输入/输出	说明
1	DCD	输入	数据载波检测
2	RXD	输入	接收数据
3	TXD	输出	发送数据
4	DTR	输出	数据终端准备好
5	GND	-	信号地
6	DSR	输入	数据装置准备好
7	RTS	输出	请求发送
8	CTS	输入	允许发送
9	RI	输入	振铃指示



智能设备的组成：Nor Flash

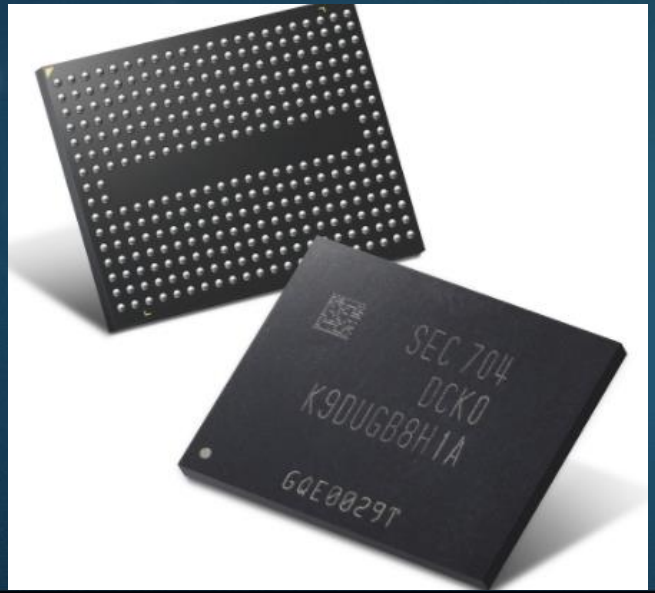
- 特点: 价格贵、容量小、地址线和数据线分开、CPU可直接寻址。
- 常用做代码存储

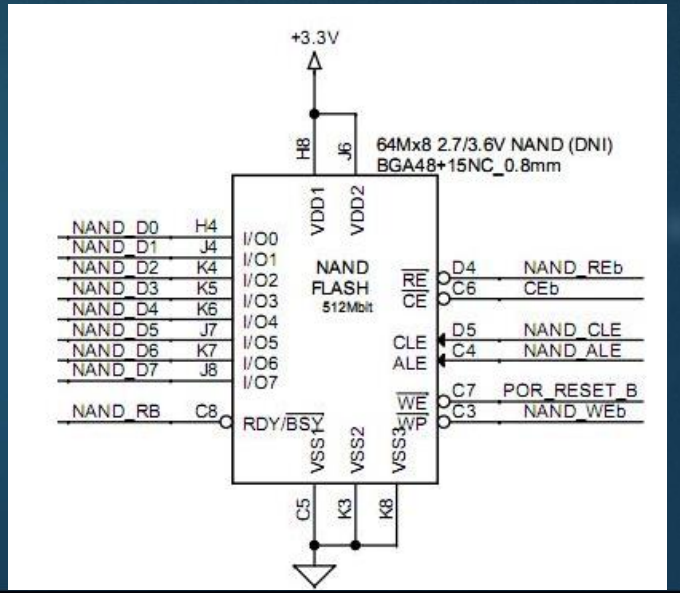




智能设备的组成：Nand Flash

- 特点: 便宜、容量大、共用地址和数据线、
- 大部分CPU的不可直接寻址, 需要驱动程序。常做数据存储用





Uboot和busybox

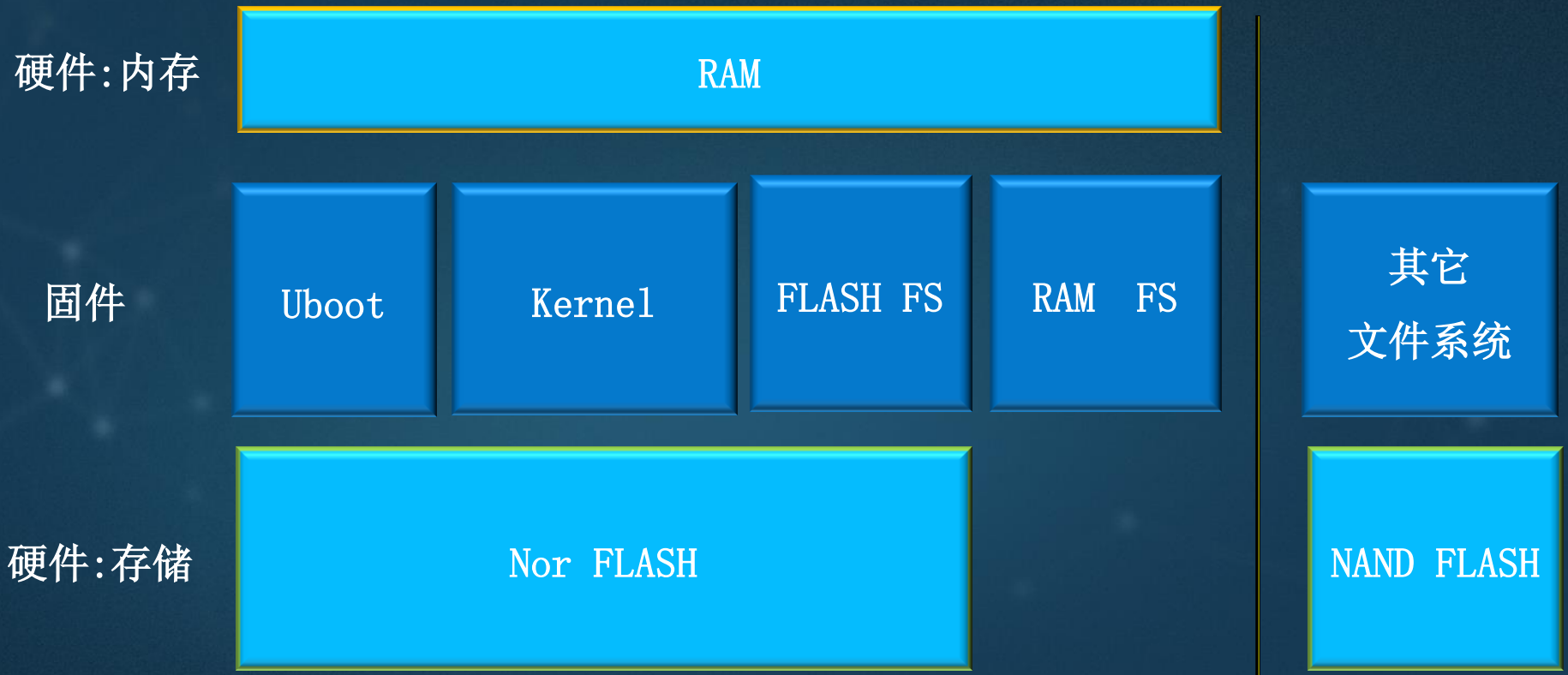
Uboot

- Uboot是用于嵌入式CPU(ARM、MIPS、PowerPC 、XScale等)的bootloader程序
- UBoot支持嵌入式Linux、VxWorks、QNX等多种嵌入式操作系统的启动引导
- Uboot支持：文件系统，简单的网络命令，TFTP， 串口等

BusyBox

- BusyBox 是一个集成了三百多个最常用Linux命令和工具的软件。
- BusyBox提供了一个比较完善的环境，适用于任何小的嵌入式系统。

简化的智能设备软硬件的协作关系(以Linux操作系统为例)



智能设备的维护接口

升级接口

- 下载固件接口(硬件接口:JTAG/SWD口;网络协议:TFTP/FTP; 自定协议)
- BootLoader升级接口
- SD/TF卡升级接口
- USB升级接口

调试接口

- 网络/USB日志接口
- 调试接口(一般为TTL串口;也有telnet/SSH网络协议等)

目录大纲

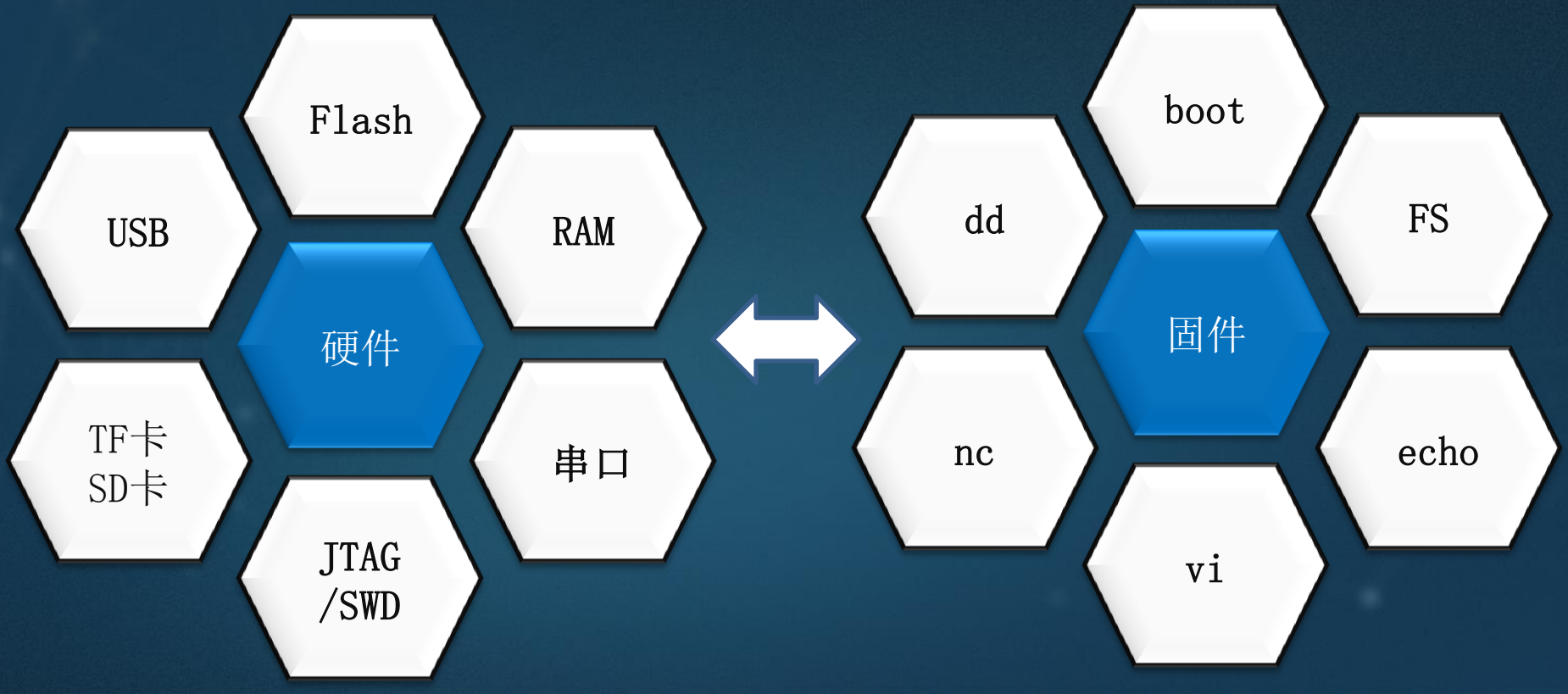
智能设备基础知识

提取固件的十种思路

从固件发掘漏洞的思路

智能设备的加固建议

固件提取思路



智能设备提取固件的十种思路

- 1、官网或联系售后索取升级包
- 2、在线升级，抓包获取下载地址
- 3、逆向升级软件,软件内置解包和通讯算法
- 4、从硬件调试接口:JTAG/SWD，利用调试工具的任意地址读取功能
- 5、拆Flash、Sd卡、TF卡、硬盘等,用编程器或对应设备读固件
- 6、用硬件电路的调试串口和固件的bootloader获取固件
- 7、通过利用网页和通讯漏洞获取固件敏感信息
- 8、用逻辑分析仪监听flash,ram获取信息
- 9、从硬件串口获取系统权限后,用tar、nc、dd、echo、vi等命令提取固件

一、官网或联系售后索取升级包

- 适用于官网提供下载智能设备固件的情况
- 有的厂家只能从代理和官方的售后提供固件

风险点：

- 官网可能 官网可能不提供固件;或不提供老固件
- 工控设备很少提供固件，或加密固件

二、在线升级方式提取固件

- 工具：HUB
- 软件：Wireshark
- 在线升级，抓包，分析固件地址，下载固件

- 新老固件通吃：
- 升级前记录下固件版本和名称，
- 升级后，根据命名规则拼接老固件地址

三、逆向升级软件,软件内置解包和通讯算法

- 厂家提供上位机升级软件，升级软件在升级前，先在上位机解密固件，

  再传输不加密的固件到设备升级的方式

- 解密升级固件部分；抓取数据包

四、从调试接口:JTAG/SWD等硬件接口获取固件

- 如果电路板上有现成的JTAG接口，用JTAG建立连接，读出烧录的固件。

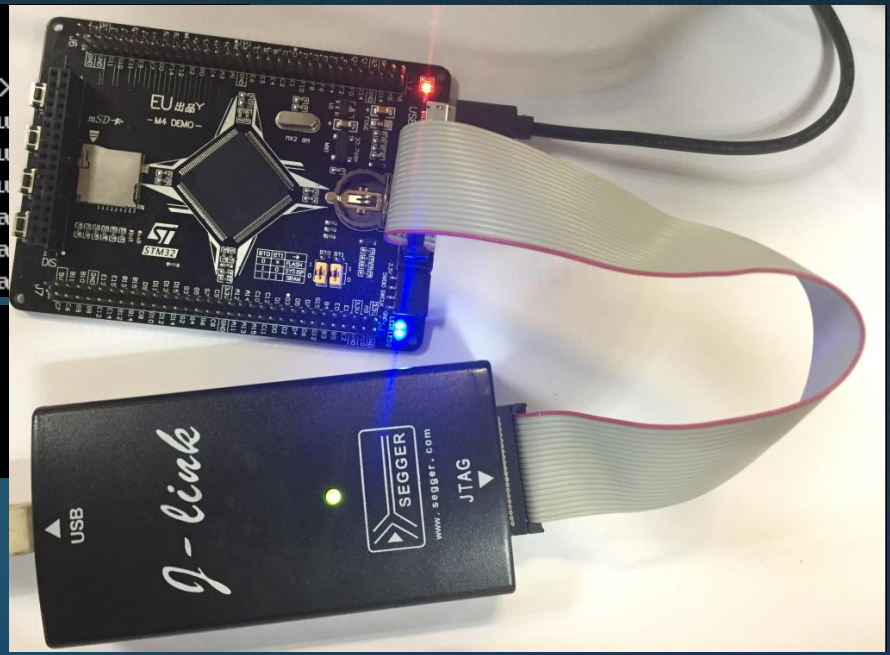
- 商业方案: Jlink, Xjtag
- 开源方案: GDBs, OpenOCD

- 前提:电路板上需要有JTAG接口，缺点：自带JTAG的电路板不多
- 例外: 固件保存在CPU内的FLASH, 并且没有启用加密

四、从调试接口:JTAG/SWD等硬件接口获取固件

```
st          Show hardware status
hwinfo      Show hardware info
mem         Read memory. Syntax: mem  <Addr>, <NumBytes>
mem8        Read  8-bit items. Syntax: mem8  <Addr>, <Nu
mem16       Read 16-bit items. Syntax: mem16 <Addr>, <Nu
mem32       Read 32-bit items. Syntax: mem32 <Addr>, <Nu
w1          Write  8-bit items. Syntax: w1 <Addr>, <Data
w2          Write 16-bit items. Syntax: w2 <Addr>, <Data
w4          Write 32-bit items. Syntax: w4 <Addr>, <Data
```

```
J-Link>st
VTarget=0.000V
TCK=0 TDI=0 TDO=0 TMS=0 TRES=0 TRST=0
Supported JTAG speeds:
 - 16 MHz/n, (n>=4). => 4000kHz, 3200kHz, 2666kHz, ...
```

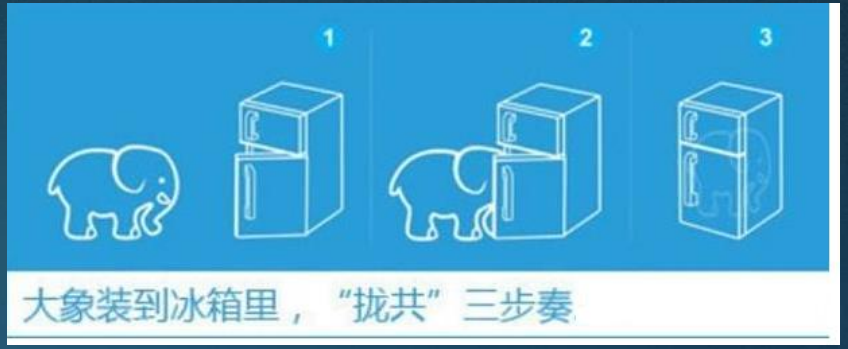


- 可以尝试读取要读取的地址，发现一些有用的信息
- 多尝试读取，少尝试写入。失败乃成功之母

五、拆Flash、SD/TF卡、硬盘等,用编程器获取固件

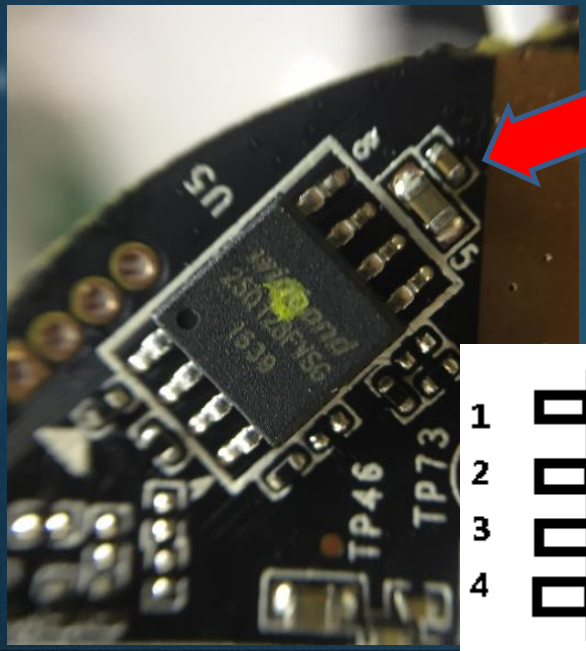
只需要三步:

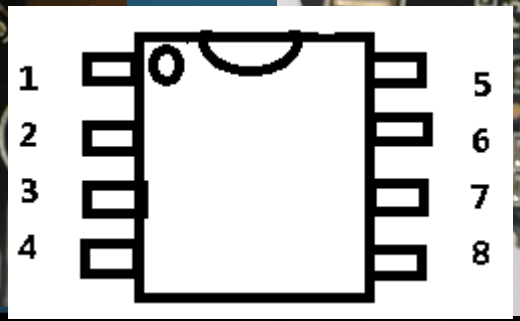
- 焊下flash芯片
- 用编程器提取固件内容
- 再把FLASH芯片焊回电路板

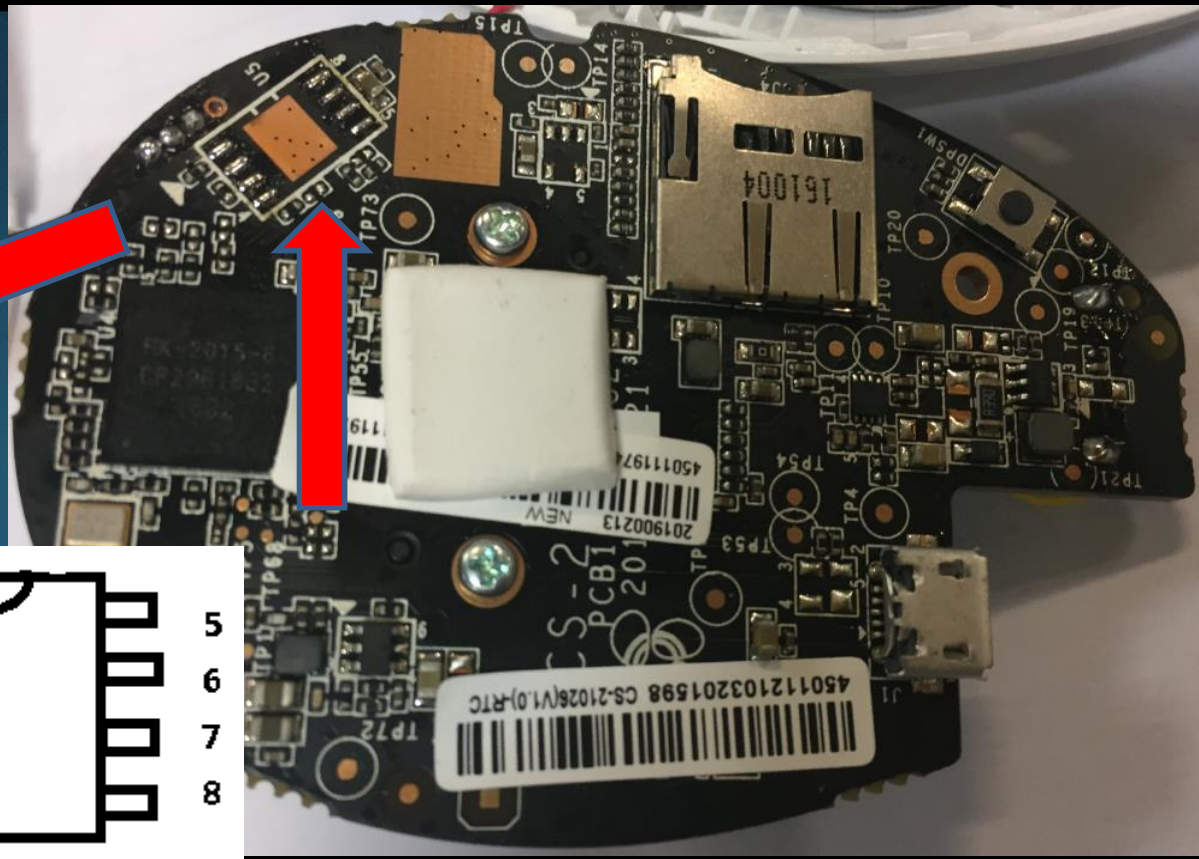


五、拆Flash, 用编程器获取固件

焊下flash芯片

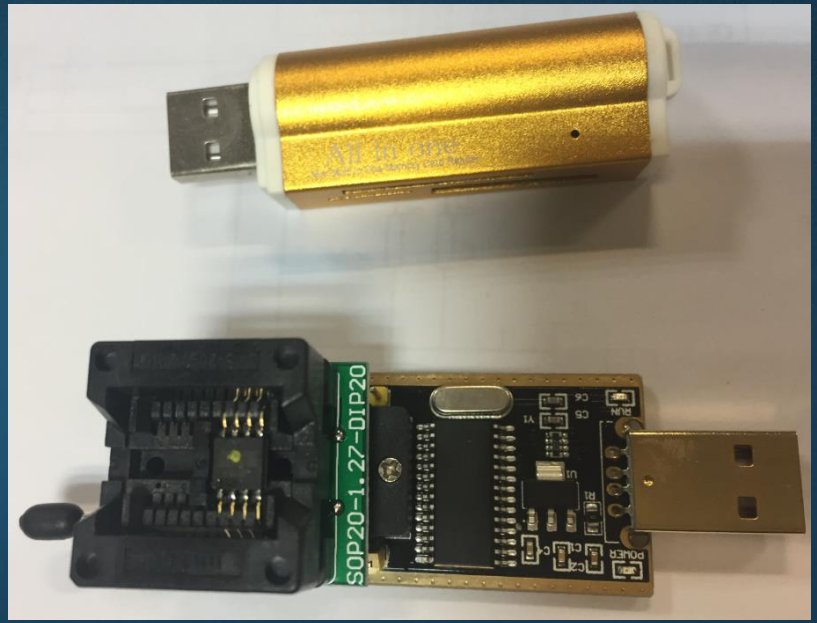






五、拆Flash、SD/TF卡、硬盘等,用编程器获取固件

用编程器读取固件内容,并保存为二进制文件



六、从串口(UART)调试口获取固件

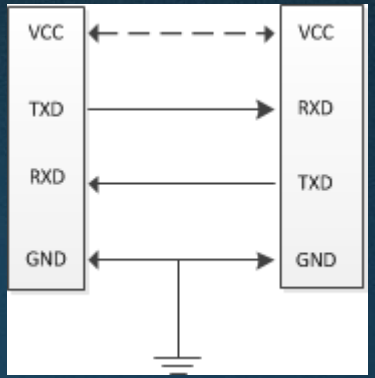
- 前提：开发板上有串口调试接，需要我们找出隐藏的串口。
- 串口按照电压有两种标准：RS232标准和TTL标准

  RS232标准：　　电压范围：-12V，+12V　（负逻辑）

  TTL标准：　　电压范围：0，5V

串口引脚识别方法：串口一般有4个引脚

- VCC：电源电压为3.3V　或 5V
- GND：电源电压地
- RXD：数据接收引脚，万用表测电压为低（硬件上拉也可能为高）
- TXD：数据发送引脚，万用表测电压一般为高



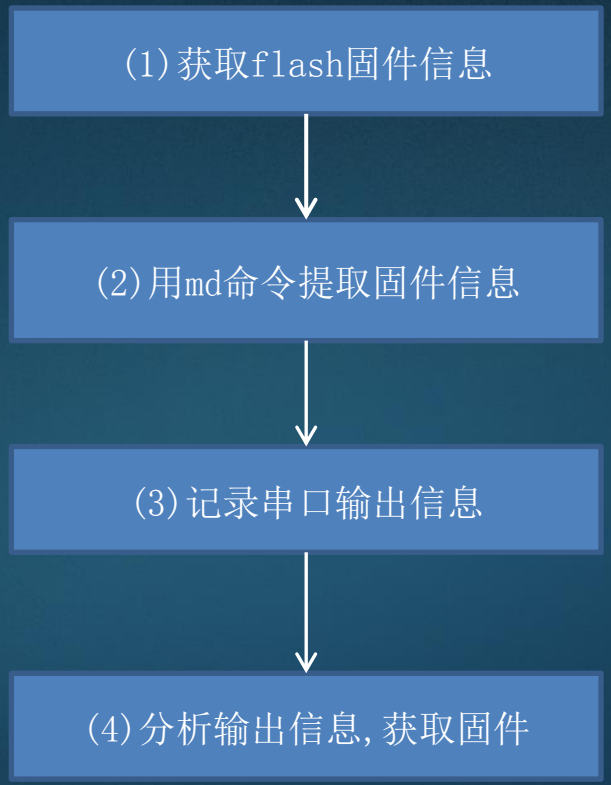
六、uboot提取固件: 认识uboot命令

```
=> help
bdinfo  - print Board Info structure
bootm   - boot application image from memory
bootp   - boot image via network using
BootP/TFTP protocol
cmp     - memory compare
cp      - memory copy
erase   - erase FLASH memory
flinfo  - print FLASH memory information
go      - start application at address 'addr'
loadb   - load binary file over serial line
md      - memory display
mm      - memory modify (auto-incrementing)
nfs     - boot image via network using NFS protocol
nm      - memory modify (constant address)
printenv- print environment variables
reset   - Perform RESET of the CPU
run     - run commands in an environment variable
saveenv - save environment variables to persistent
storage
setenv  - set environment variables
tftpboot- boot image via network using TFTP protocol
```

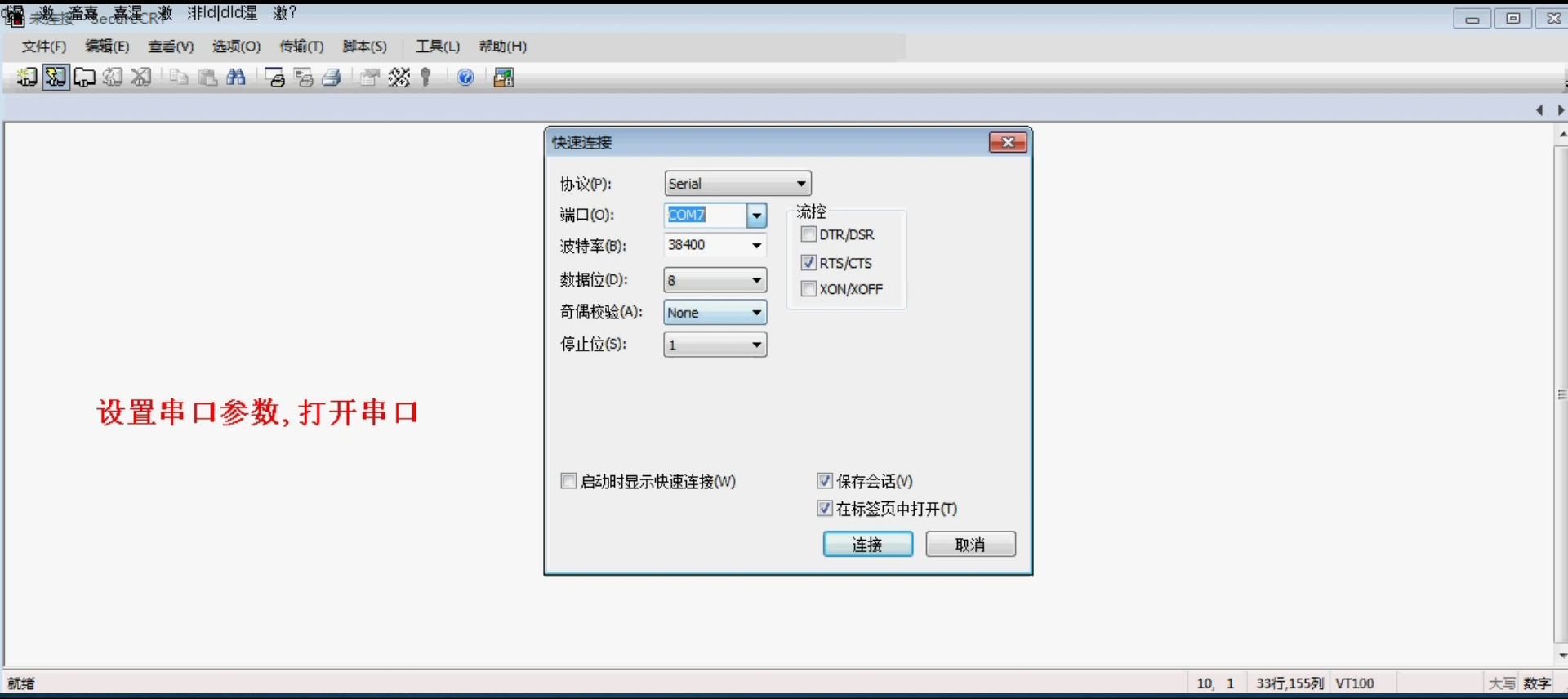
六、uboot提取固件: md命令

- md - memory display（显示内存内容）
- 用法： md 起始地址 长度 （地址和长度：一般为十六进制格式）
- 思考：md 命令是否能提取固件？ 怎么提取固件呢？

六、串口uboot提取固件流程

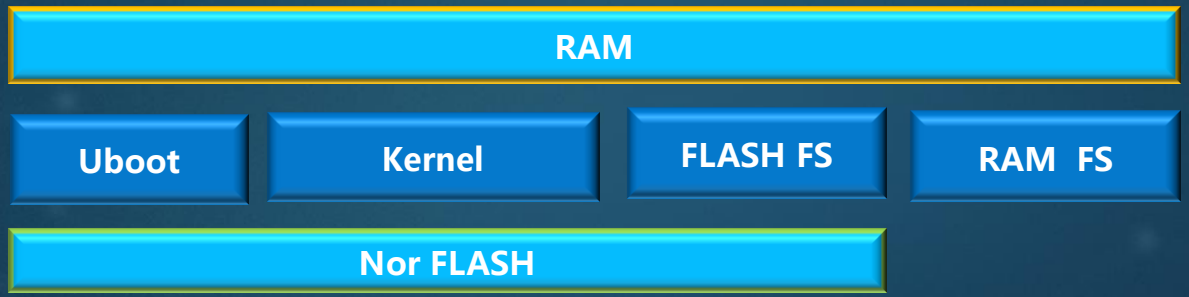


六、串口uboot提取固件(Demo)



六、uboot提取固件的难度: Level 1

用md命令直接读出固件
命令格式:md　起始地址　长度



六、uboot提取固件的难度: Level 2

先用特殊命令从Flash读固件到内存，再用md读取内存中的文件

命令格式:md　起始地址　长度

特殊命令指: mtdparts default、loada、loadk、cp、sf　read 、ext4load、fatload等

六、uboot提取固件漏洞总结

不是针对某一个厂商，几乎所有厂商都存uboot安全问题，很多包括知名大厂。

UBOOT的应用非常广泛。嵌入式LINUX的基本都用UBOOT引导。

Uboot是开源软件，但针对UBOOT做加固的厂商很少

本议题之后，希望相关厂商能加快修复此漏洞，尤其是工控方面的设备

有可能成为未来一段时间提取固件的流行方法

七、通过利用网页和通讯漏洞获取固件敏感信息

- 嵌入式系统的web界面权限配置不当
- 可以查看 /etc/passwd 和 /etc/shadow 内容

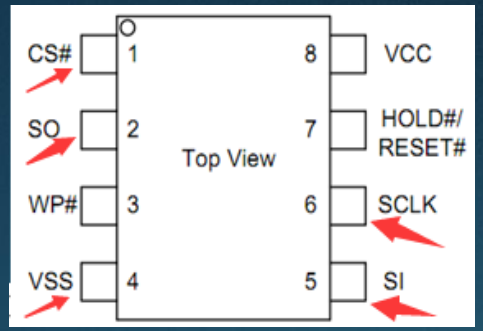
八、用逻辑分析仪监听flash,ram获取信息

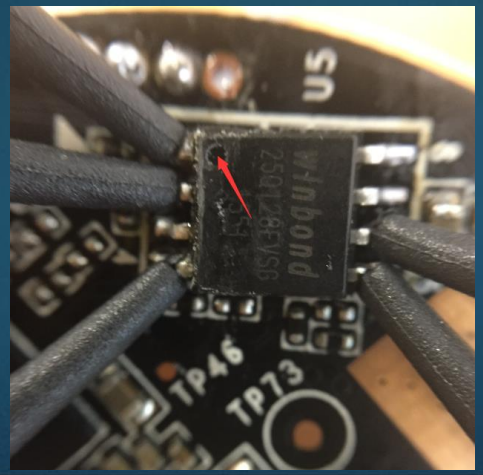
- 1.支持English/简体中文双语言 支持Windows XP/7/8/10系统
- 2.易用高效的用户界面设计 提供方便、直观、强大的分析功能
- 3.支持众多标准协议解析:UART/RS232/485,I2C,SPI,CAN,SDIO, DMX512,I2S/PCM,JTAG,LIN,Manchester,Modbus,1-Wire, SMbus,UNI/O,USB1.1,NEC红外,PS/2鼠标键盘,并口,等等...
- 4.10进制/16进制/2进制/ASCII码格式数据显示,方便观察分析
- 5.采样数据与解析数据均可导出,方便存档或其它分析软件使用

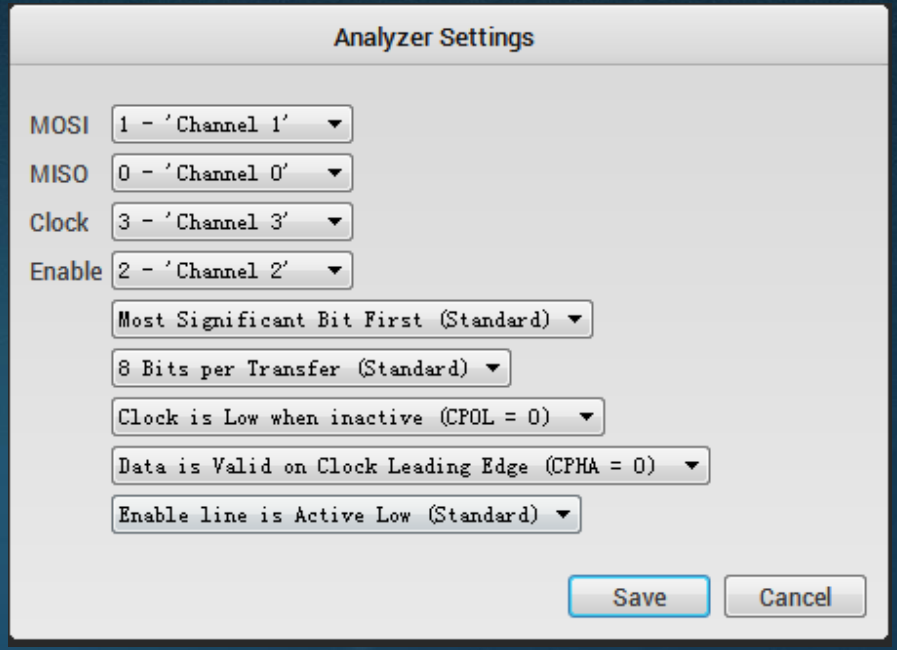
八、用逻辑分析仪监听flash信息

芯片引脚:
Saleae4 25Q128

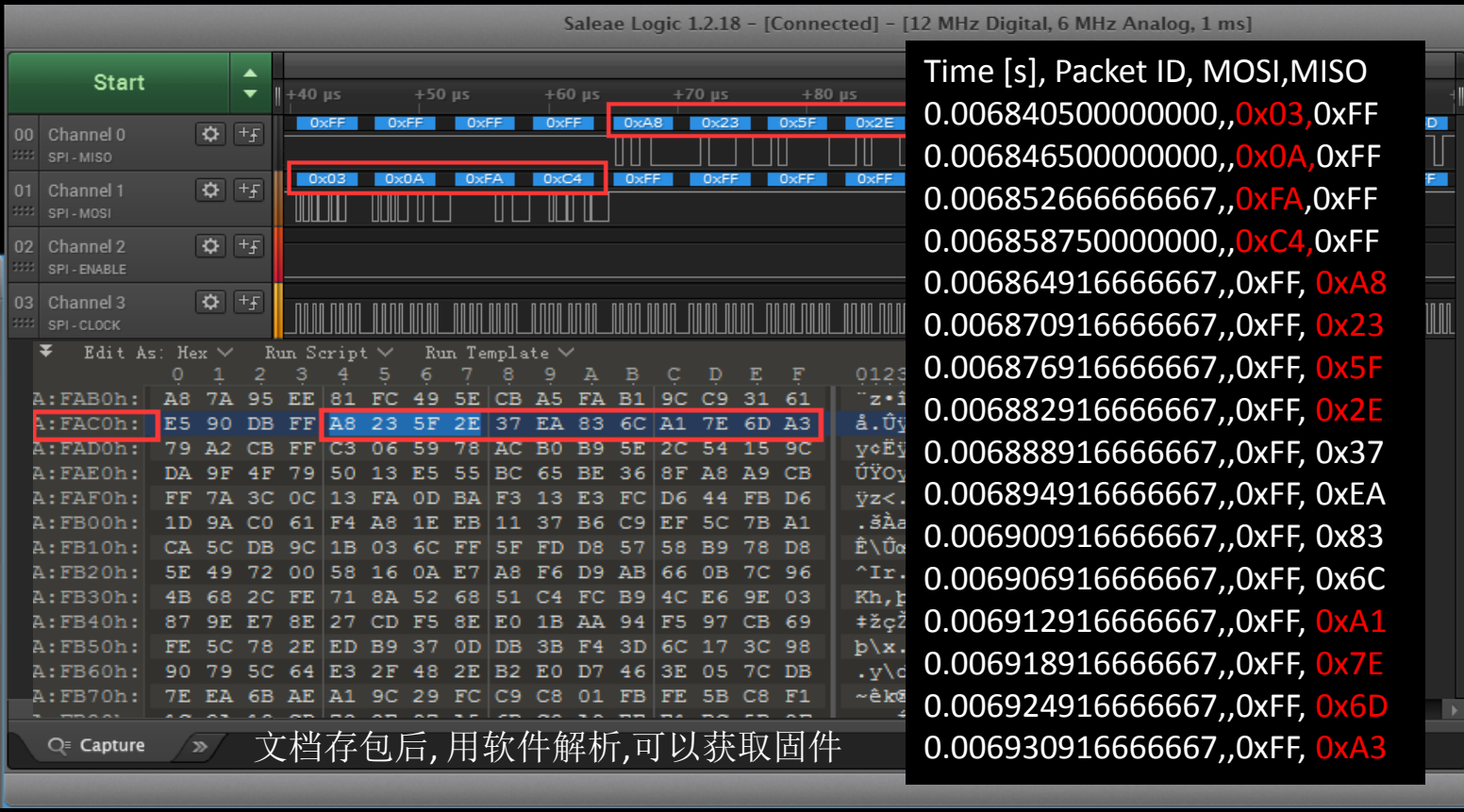
GND - VSS
0 - MISO
1 - MOSI
2 - CS
3 - SCLK







八、用逻辑分析仪监听SPI flash获取信息



Time [s], Packet ID, MOSI,MISO
0.006840500000000,,0x03,0xFF
0.006846500000000,,0x0A,0xFF
0.006852666666667,,0xFA,0xFF
0.006858750000000,,0xC4,0xFF
0.006864916666667,,0xFF, 0xA8
0.006870916666667,,0xFF, 0x23
0.006876916666667,,0xFF, 0x5F
0.006882916666667,,0xFF, 0x2E
0.006888916666667,,0xFF, 0x37
0.006894916666667,,0xFF, 0xEA
0.006900916666667,,0xFF, 0x83
0.006906916666667,,0xFF, 0x6C
0.006912916666667,,0xFF, 0xA1
0.006918916666667,,0xFF, 0x7E
0.006924916666667,,0xFF, 0x6D
0.006930916666667,,0xFF, 0xA3

文档存包后,用软件解析,可以获取固件

九、用tar/dd、nc 提取固件

- 1. 已获取系统shell权限(网络或串口)
- 2. 以下三条命令可用（或等价替代命令）
- ifconfig(获知或可配置IP)、nc、tar(zip/dd)

用法：

- 在串口命令模式下：
- 用tar打包固件，或用dd命令提取固件；
- 用ifconfig配置ip地址；用nc命令连接本地机器；
- 通过nc命令传送打包后的固件

十、综合应用

我想到了！
原来第十种固件提取方法是：前九种方法的融会贯通、综合运用！

十、综合应用

目前具体情况具体分析，方法非常多

案例:
串口或网口获取权限，先获取进入系统权限
拷贝固件的部分或打包文件到SD卡,U盘……

最后，还有一种用echo和vi命令获取固件的思路
理论实验:

```
[root@fel8xx:/home]# echo -e -n "\x31\x32\x33\x34" > ml_test
[root@fel8xx:/home]# echo -e -n "\x35\x36\x37\x0a" >> ml_test
[root@fel8xx:/home]# cat  ml_test
1234567
```

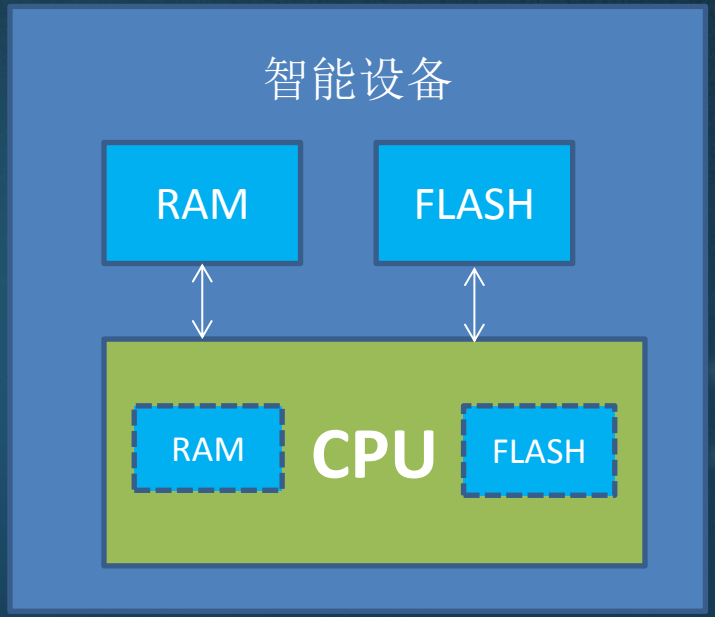
说明：可用输入命令的方式发送二进制文件。
发挥：可传送编译好的、盗取固件的”木马”

固件提取方法总结

- 智能设备普遍存在uboot提取固件的漏洞
- 智能设备的固件存储在flash里

  FLASH没有保护固件被非法读取的措施
- 硬件调试接口方便了开发人员，也方便了黑客
- 软件后门方便了维护工作，也方便了黑客入侵

- 结论:目前的智能设备架构存在一定的安全隐患



目录大纲

智能设备基础知识

提取固件的十种思路

从固件发掘漏洞的思路

智能设备的加固建议

智能设备安全测试流程概述

- 1、获取固件(本议题重点部分)
- 2、逆向固件
- 3、分析固件漏洞/调试固件/Fuzz漏洞
- 4、漏洞验证
- 5、完成测试文档(一般边测试,边记录)

智能设备固件拆解

- 查看固件有无加密：

  用文本编辑器打开固件，如果看到明文字符串，说明固件没有加密

- 用binwalk进行固件拆解：

  建议安装最新版本binwalk

  安装binwalk用到的各种依赖包　#./deps.sh

  binwalk -e 固件名　　//自动化（自动）提取

  binwalk –Me 固件名　//递归提取

智能设备固件密码破解

```
root@kali:/home# cd john-1.8.0/
root@kali:/home/john-1.8.0# ls
doc  pass  passwd  README  run  src
root@kali:/home/john-1.8.0# cd run
root@kali:/home/john-1.8.0/run# ls
10-million-combos.txt  digits.chr  john.conf  john.pot  lm_ascii.chr  makechr          password.lst      relbench  unique
ascii.chr              john        john.log   john.rec  mailer        password_big.lst  password_old.lst  unafs     unshadow
root@kali:/home/john-1.8.0/run# ./john ../passwd
Loaded 1 password hash (md5crypt [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:20:30 1% 2/3 0g/s 5780p/s 5780c/s 5780C/s marcsteiger
0g 0:00:20:38 1% 2/3 0g/s 5780p/s 5780c/s 5780C/s markovo4ka
rootit           (root)
1g 0:00:44:48 100% 2/3 0.000371g/s 5776p/s 5776c/s 5776C/s Fireitup
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/home/john-1.8.0/run#
```

从固件发掘漏洞的思路

- 从开发的维护用的调试后门入手
- 查找系统的敏感信息
- telnet/ftp/ssh有没有厂家留下的后门密码，尤其是明文密码
- 查看启用的网络端口，看网络应用有没有溢出点
- Web调用了哪些接口，对调用的接口和脚本用qemu调试，找攻击点
- 云端和app的调用流程和接口的安全问题

目录大纲

智能设备基础知识

提取固件的十种思路

从固件发掘漏洞的思路

智能设备的加固建议

信息隐藏

- 关键芯片打磨或腐蚀标识
- 用量大可以订制芯片封装
- PCB板标识不要暴露接口用途
- 进入uboot不要提示那么明显，进入方式只有开发人员才能知道
- 重要固件建议加密发布，不要在上位机解密固件，在下位机解密固件和刷入

调试接口

- 烧录固件后，出厂前损坏调试引脚。使其不能正常工作
- 进入uboot菜单需要非对称密钥验证
- uboot对固件要进行签名验证
- 暂时不需要的、不理解的uboot选项，建议去掉
- 系统权限尽量小，使其刚好满足运行条件
- busybox不用的功能裁剪掉（nc\dd\tar…）

其它加固建议

- 不要明文存储密码
- 密码尽量复杂，避免密码被猜出
- 关掉和应用无关的网络服务
- 程序的每一个分支的情况都有完整明确的处理逻辑
- 对用户的输入进行验证，对输出进行转义
- 对安全性要求高的产品，可以交由专业的团队进行安全测试

议题结束

谢 谢