安天硬件安全研究之路

微电子与嵌入式研发中心

桑胜田 （esoul@antiy.cn）

提纲

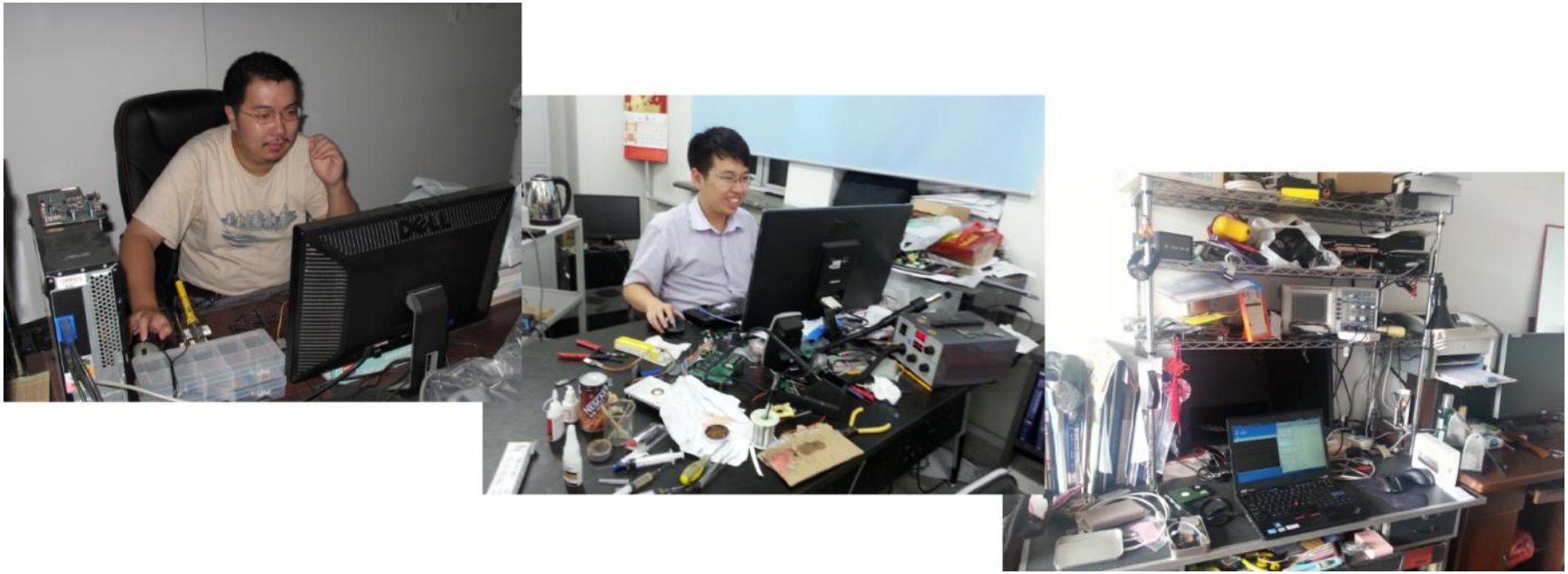
- 团队简介
- 工作及成果

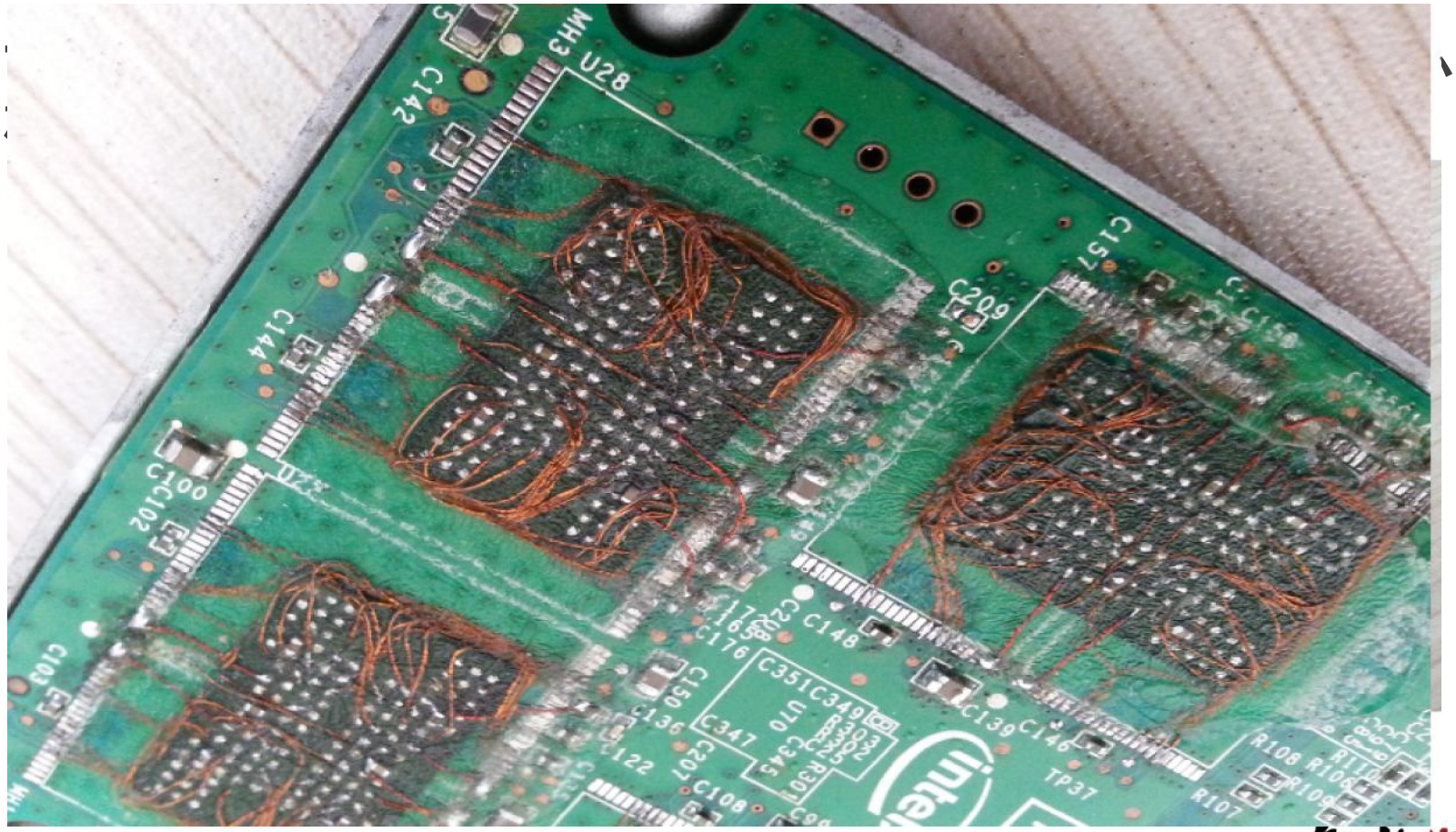
智者安天下

团队简介

微电子与嵌入式研发中心

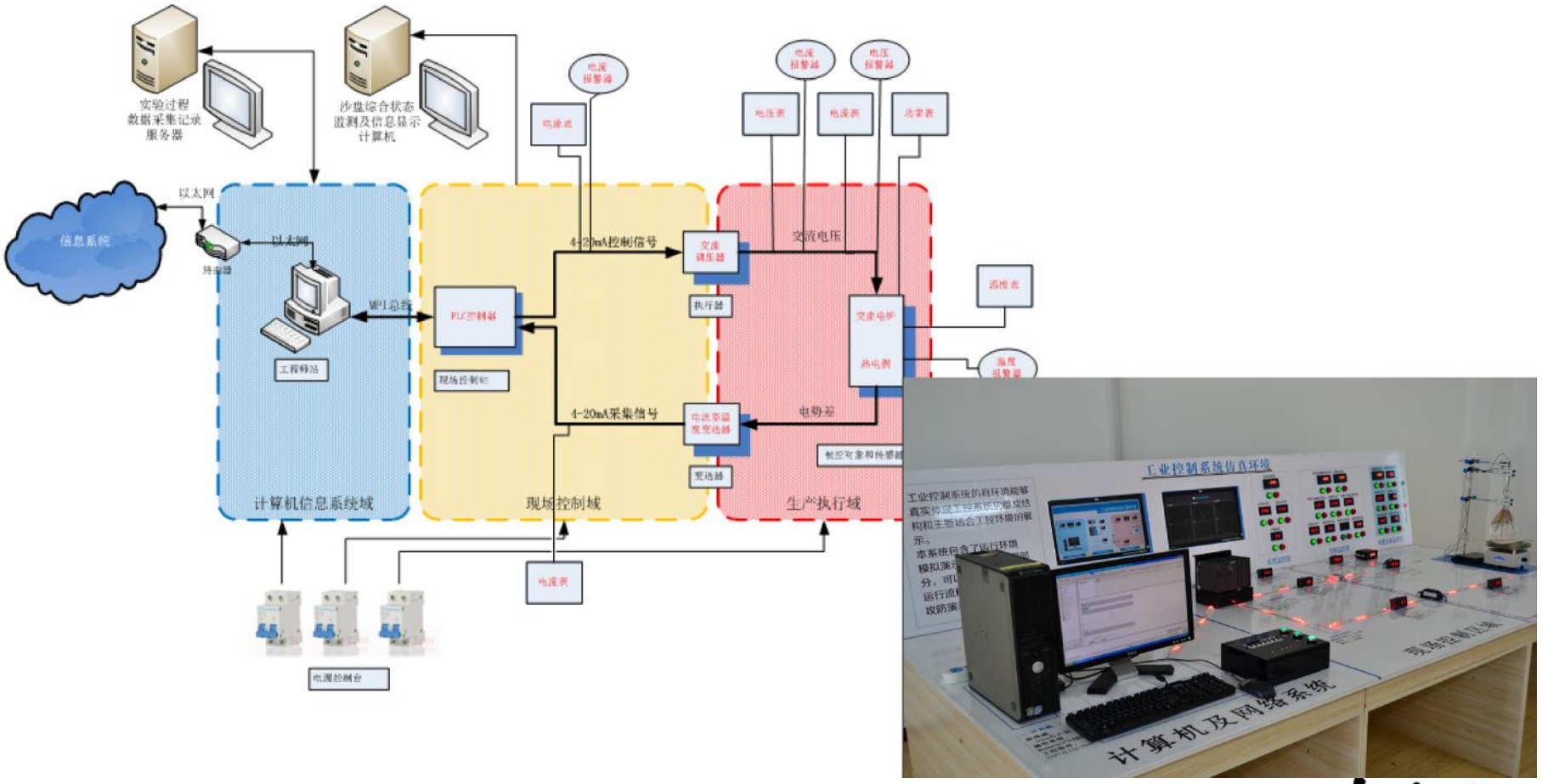
- 一群来自于计算机、自动化、微电子，甚至化工、机械专业的技术狂热分子。。。




U28
C142
C144
C157
C209
C100
C102
C148
C139
C146
TP37
R108
R107

工作及成果回顾

安天一直很重视硬件与设备的安全研究



工业过程控制系统仿真沙盘

早期（—2006）

- 硬件与电子产品的安全还没引起安全界和公众的注意。。。
- 研究成果很少公开发表
- 后续的部分展示：安全焦点峰会——XCon

还原冬天的神话（ XCon2008 ）

打印机“病毒芯片”事件之情景再现

事件背景和起因

某些媒体报道：海湾战争爆发前，美国情报部门获悉，伊拉克从法国购买了一种用于防空系统的新型电脑打印机。于是美国特工人员把一套带有病毒的同类芯片换装到这种电脑打印机里，从而通过打印机使病毒侵入到了伊拉克军事指挥中心的主机。当美国领导的多国部队发动“沙漠风暴”行动，空袭伊拉克时，美军用无线遥控装置激活了隐藏的病毒，致使伊拉克的防空系统陷入了瘫痪。

传言与源头的对比

国内报道

- 瘫痪伊拉克防空系统
- 瘫痪伊拉克情报系统
- 感染作战飞机

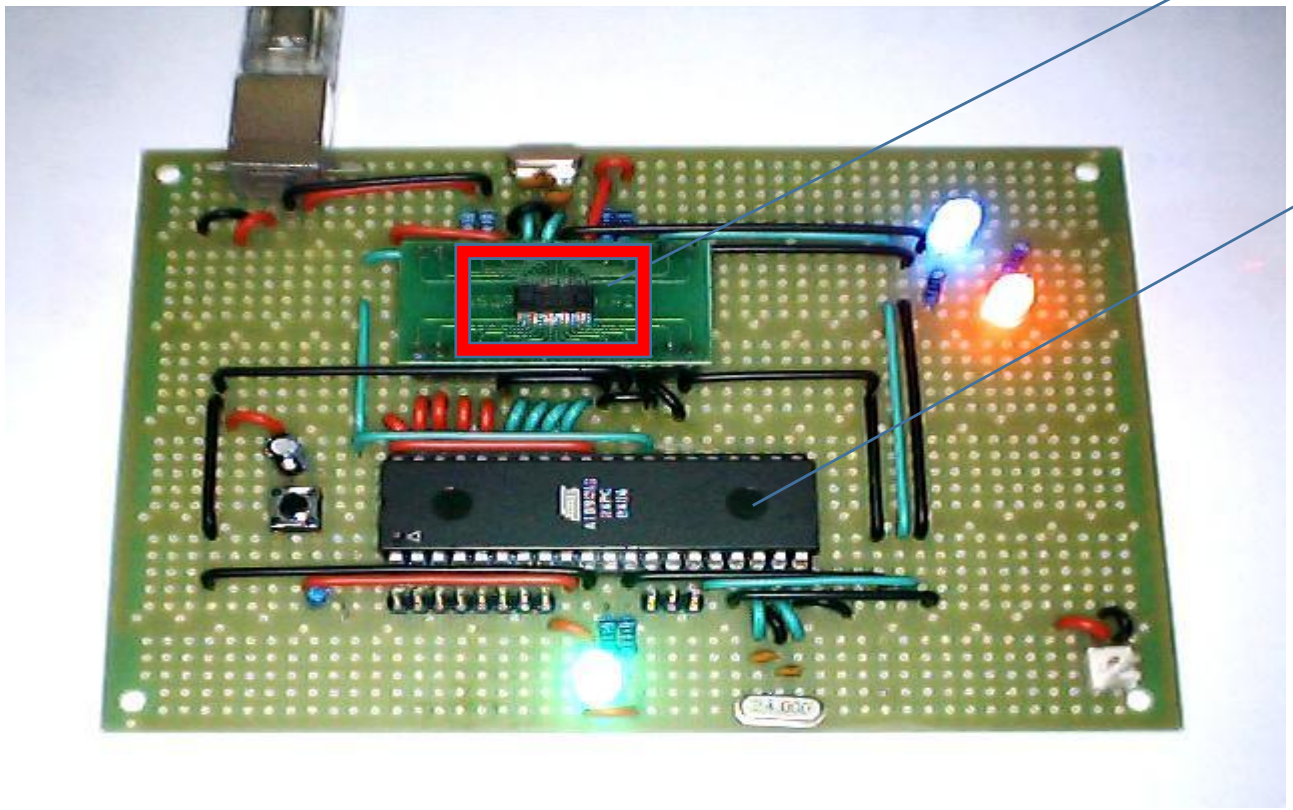
原始报道

- 以“disable”主机为目的
- 未评价实际效果，只说美方确信“worked as planed”

对此事件的基本结论

- 不修改配套软件，通过主机端有关上行信号处理漏洞难以构成溢出或者代码植入。
- 最大的可能性为美方在打印机中存放了触发器同时更换了驱动盘或者盘上的程序。
- 不必然是一个“病毒”程序，可能是引入一个错误的形式。
- 所谓的打印机“病毒芯片”不过而而。

自定义USB固件构造USB DoS攻击



PDIUSB12
USB设备控制器

AT89C52
单片机

演员介绍-Actors

Made In China

真正
遥控者

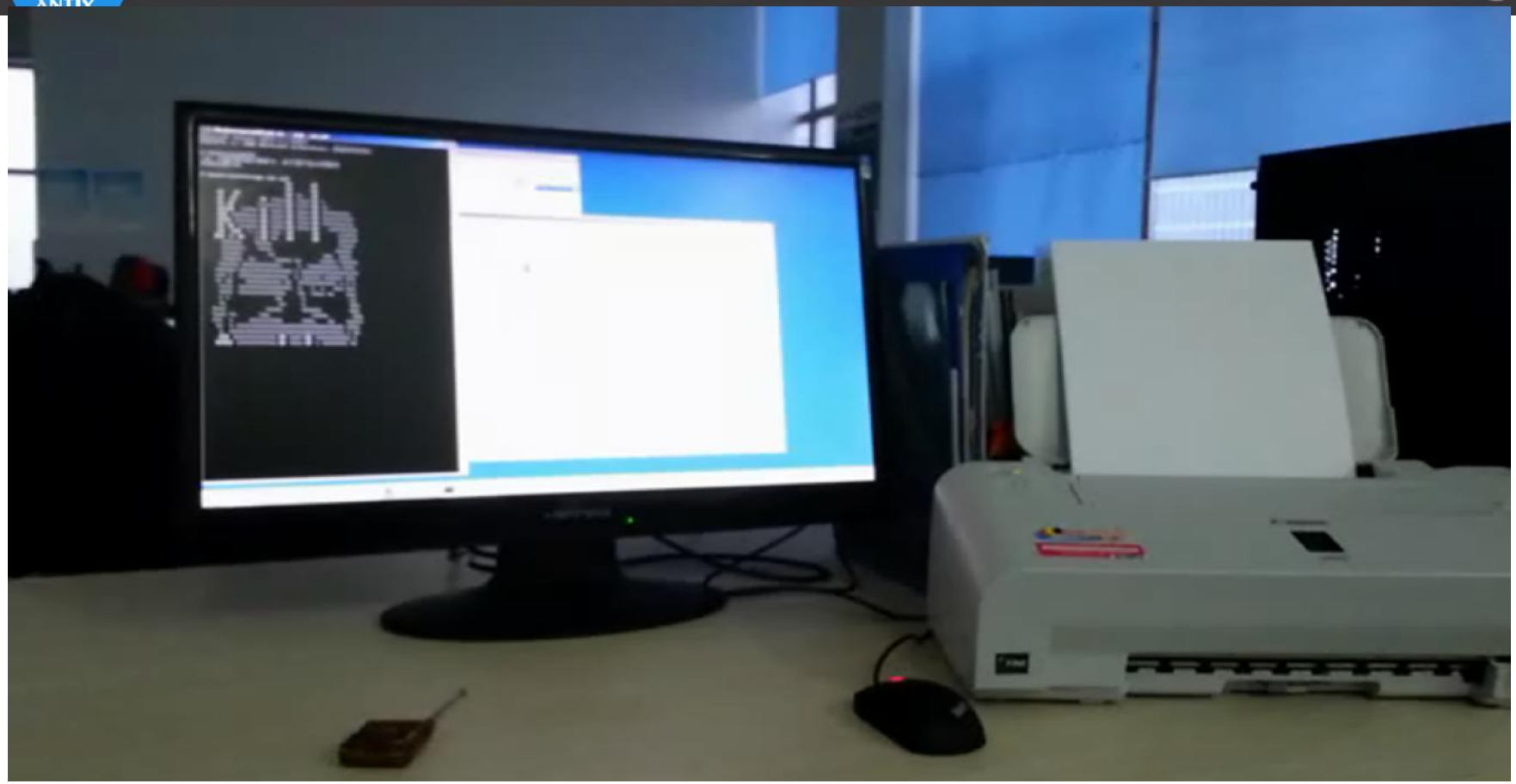
萨达姆

施瓦茨科普夫

美军军官

伊军雷达兵

美军电子战执行官



。。。时光穿梭到2014年

百度为您找到相关结果约366,000个

代号为 'BadUSB' 的 USB 漏洞具体是何情况,有多大危害? - 知乎

2014年8月6日 - BadUSB漏洞:该漏洞是利用将恶意代码存放在USB设备控制器的固件存储区,而不是存放在其它可以通过USB接口进行读取的存储区域,比如Flash等,这样,杀毒软件...

www.zhihu.com/question... 2014-08-08 - 百度快照 - 90%好评

黑帽大会2014:"BadUSB"首次亮相 - 51CTO.COM

2014年8月14日 - USB设备对你的企业安全构成严重威胁吗?在2014年黑帽大会上,专家展示了一种新的威胁,被称为"BadUSB",这种恶意软件可能通过常用USB设备渗透到你的...

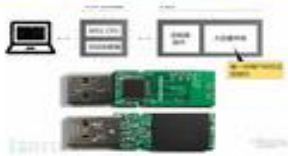
netsecurity.51cto.com/... 2014-08-14 - 百度快照

USB遭遇史上最大安全漏洞:全球数十亿设备受影响_TechWeb

2014年8月5日 - 位于德国柏林的SR安全研究实验室专家发现,该代号为"BadUSB"的重大USB安全漏洞,可以使USB接口控制器芯片固件被重新编程,用于恶意用途,而糟糕的是,这种...

www.techweb.com.cn/wor... 2014-08-05 - 百度快照

解密BadUSB:世界上最邪恶的USB外设_安全_比特网



2014年9月7日 - 在2014年美国黑帽大会上,柏林SRLabs的安全研究人员JakobLell和独立安全研究人员Karsten Nohl展示了他们称为"BadUSB"(按照BadBIOS命名)的攻击方法,这种...

sec.chinabyte.com/180/... 2014-09-07 - 百度快照

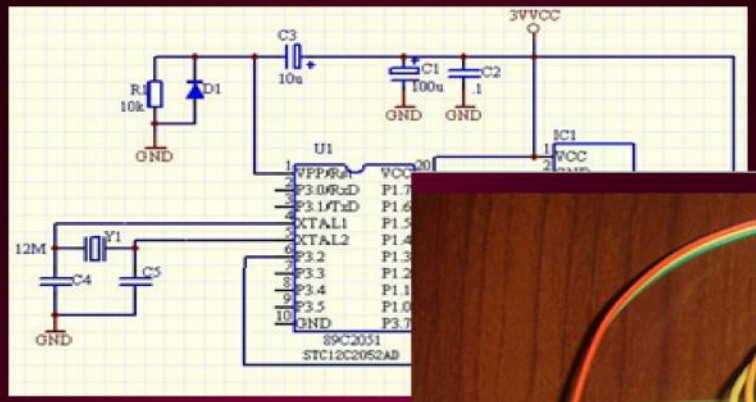
将USB 外设变成 BadUSB - 开源中国社区

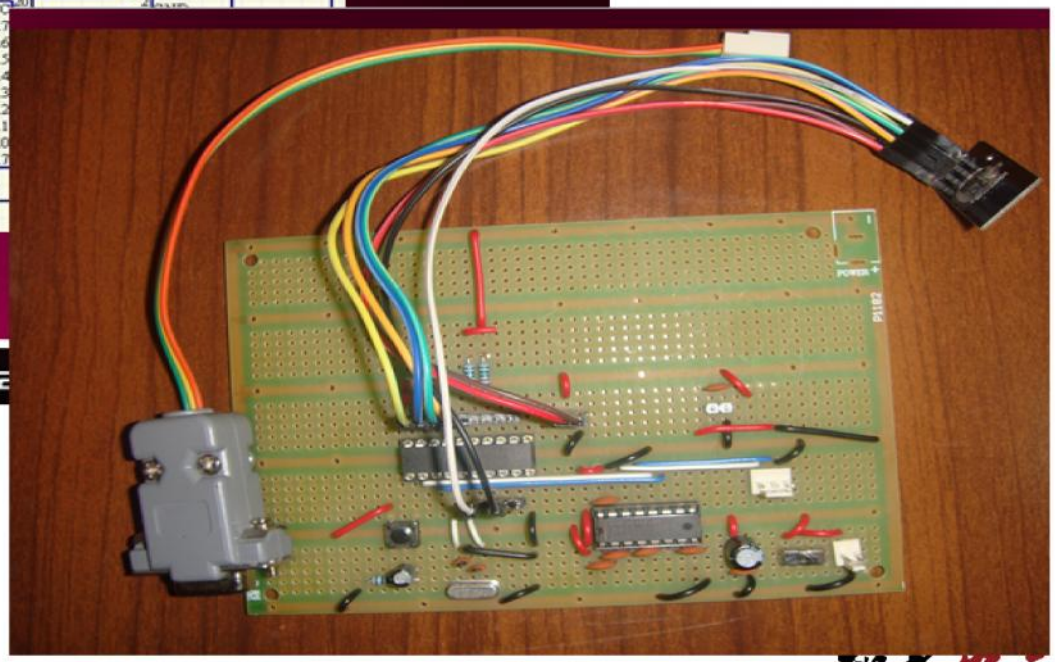
探索2.4GHz无线键盘的监听（ XCon2009）

2. 4GHz无线键盘工作原理

环境准备测试环境

电路图





选择测试对象

- 出品商：Delux
- 型号：*DL-K8000G*
- 价格：*398*元。
- SN：*K8000/0804003079*
- 系IT媒体评选的08年最令人期待的无线套装第三名

第二次监听

- 排出后，不击键有少量捕获（可能为干扰信号）。
- 多次点击A键
- 每次截获的不
- 不找到地址，

最终的结论

- 无跳频、无加密
- 地址

获取地址解决方案——穷举地址探测

可以支持的安全改进

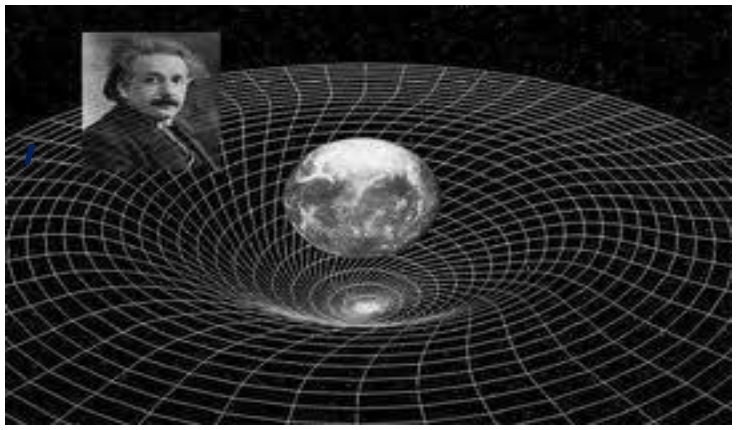
- 跳频技术
- 密钥交换握手协议和一次一密
- 个性化密钥的引入

攻击时间（ XCon2012 ）

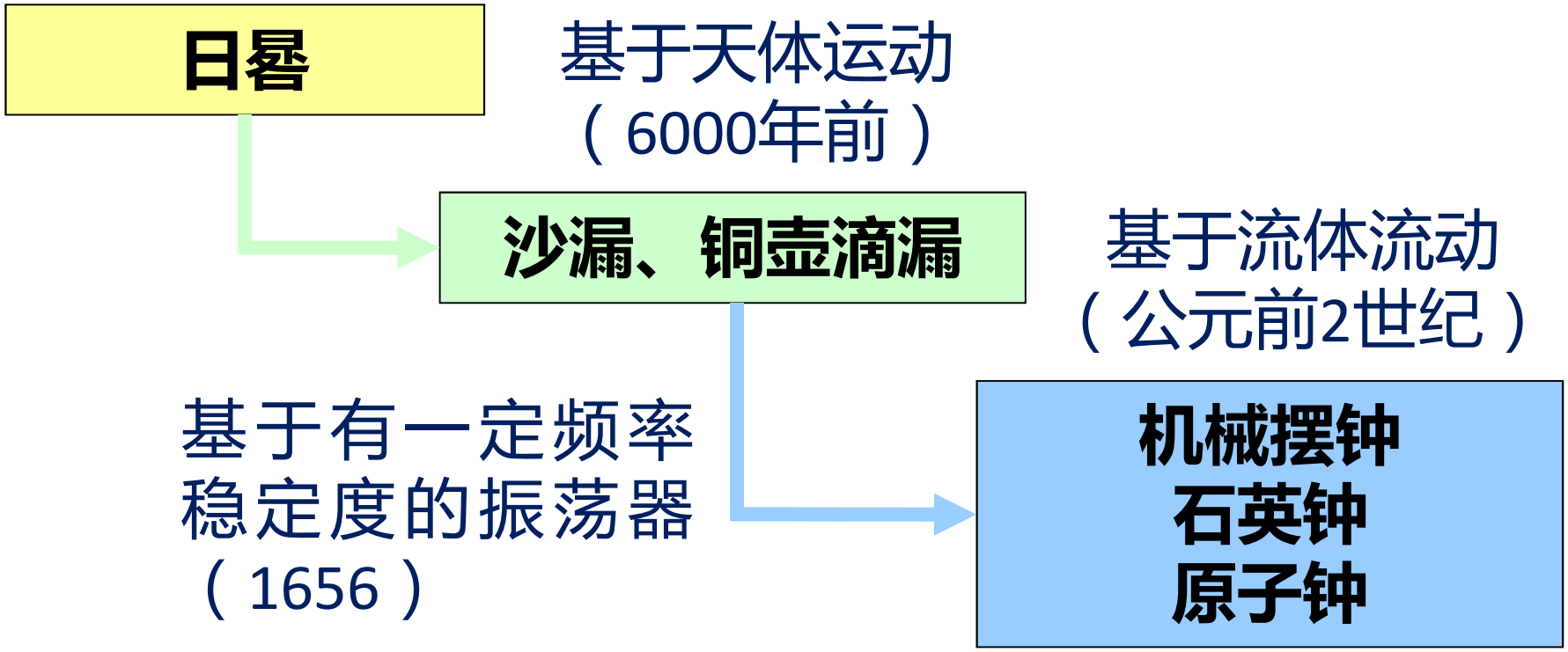
——传统计时器的安全风险

时间

- 日出而作，日落而息，人类社会从存在开始，就提出了计时需求。
- 相对论中，时间与空间一起组成四维时空，构成宇宙的基本结构。
- 在传统的犯罪学和计算机安全攻防领域，时间与空间相并列是最重要的关键要素之一。



计时器的发展


日晷
基于天体运动
（6000年前）
沙漏、铜壶滴漏
基于流体流动
（公元前2世纪）
基于有一定频率
稳定度的振荡器
（1656）
机械摆钟
石英钟
原子钟

现代计时器

- 现代社会严重依赖电子计时系统
  - 例如：著名的《萨班斯·奥克斯利法案》（Sarbanes-Oxley Act）、HIPAA（健康保险便利及责任法案）都要求准确的电子时间戳（Time Stamp）
- 现代工业和信息产业对时间准确性提出了很高的要求

工业应用中的计时与同步

- 大范围的工业应用（包括信息产业、金融业等应用）除了需要精确计时之外，还需要大范围内多个时钟都给出相同的时间，称为时间同步。
- 典型应用案例：
  - 铁路
  - 电网
  - 移动通信
  - 证券交易

计时与授时（Time Service）

- 实现时间同步的有效方式——授时。
  - 高精度计时工具发播标准时间信号
  - 接收标准时间信号校正走时或者进行时间同步
- “子母钟”即基于授时原理。
- 现代“授时”使用远程通信手段
  - 无线电波
  - 网络通信

可能的攻击时间基准方式

- 授时过程容易被攻击
  - 通过网络攻击NTP等授时协议
  - 干扰无线授时信号（长波、GPS等）

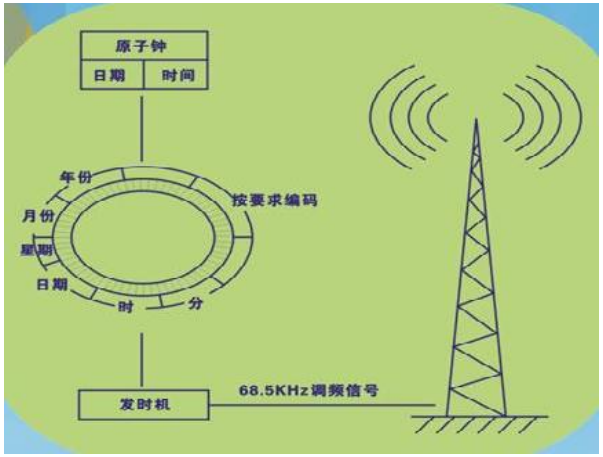
干扰无线授时信号

- 长波授时信号多属于明码信号
- 长波发射需要巨大的发射天线和强大的发射功率
  - BPC发射功率高达100kW
- 小型干扰设备能进行干扰吗？

干扰无线授时信号

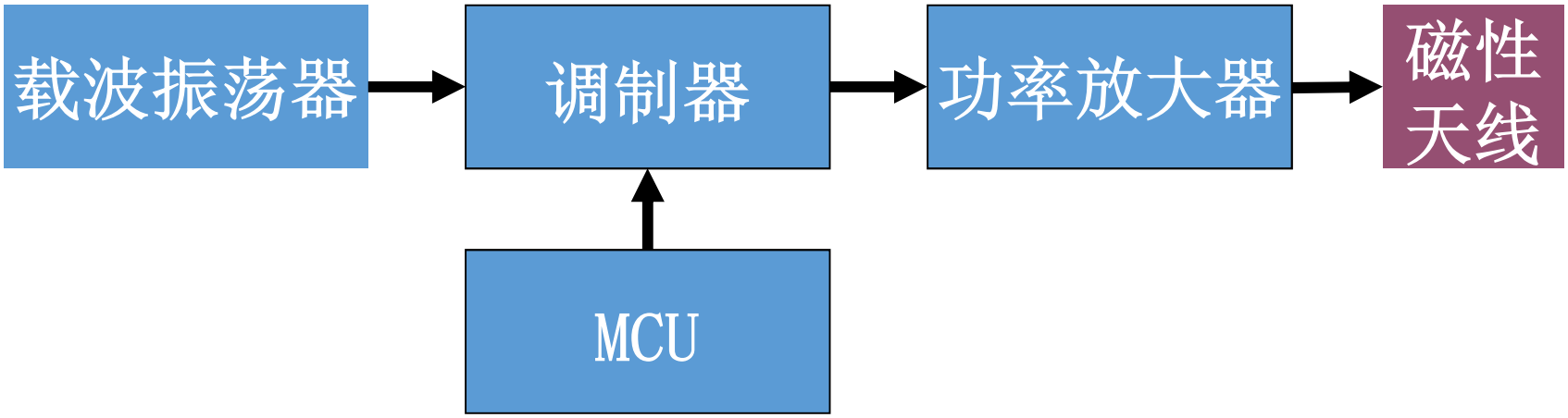
- 强弩之末
  - 到达接收端的电磁波很微弱
  - 一盏节能灯就可使信号的接收失效
- 短距离的长波发射可以用磁场能量发射的方法，使用磁性天线，不需要巨大天线

干扰无线授时信号



- BPC信号格式
  - 68.5kHz载波，幅移键控（ASK）调制，负极性调制。
  - 编码完全是明码，每20s发送一帧。

长波授时干扰信号发射器结构



自制BPC干扰信号发射器

演示：干扰无线授时信号

长波授时信号也被用于工控系统

- 西门子过程控制系统使用的长波授时信号
  - 德国77.5kHz DCF
- 西门子《SIMATIC PCS7功能手册（中文版 V7.1 2009.3）》

5.4.4 调试 DCF 77 接收机

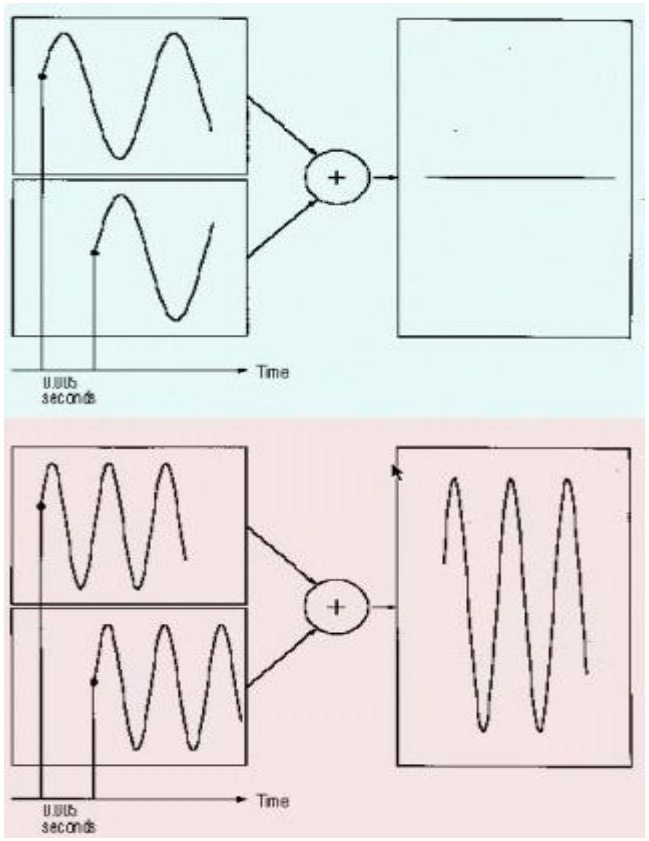
简介

在德国，DCF 77 是官方认可的标准时间。

DFC 77 无线信号的接收距离限制为离法兰克福/主区域 800 km 的范围内。 在接收不到 DCF 77 无线信号的地区，建议使用 GPS 接收机。 要将此无线信号用于 PCS 7 工厂的时间同步，需要使用 DCF 77 接收机。

电网同步问题

- 有F1和F2两台交流发电机给同一线路供电
- 如果二者发出的电相位正好相反，则发电互相抵消。
- 交流电网中各发电机必须同步运行（频率相位相同）

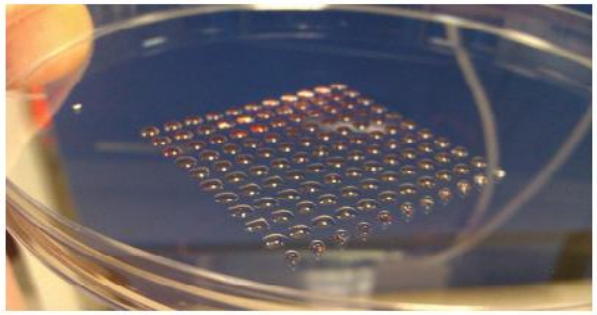


未来可能存在的攻击时间方式

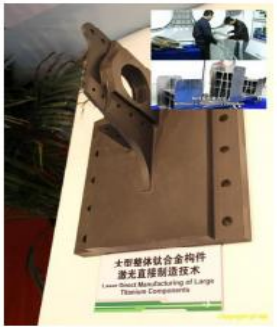
- 对石英晶体之外的高稳定性时间基准的稳定条件进行破坏（例如破坏恒温控制，校正条件等）：
  - 干扰、硬件木马、嵌入式软件木马等

对3D打印的安全攻击浅析(XCon 2013)

3D打印用于医疗定制



3D打印用于打飞机

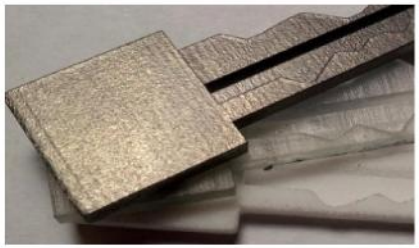


智者安天下

以前，我们关心
3D打印会对现实世界
带来什么新的安全威胁。

热点回顾：3D打印枪支

热点回顾：3D打印钥匙



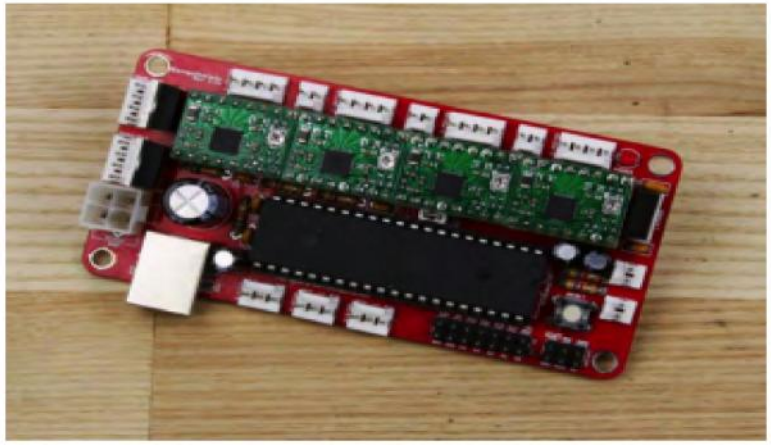
今天

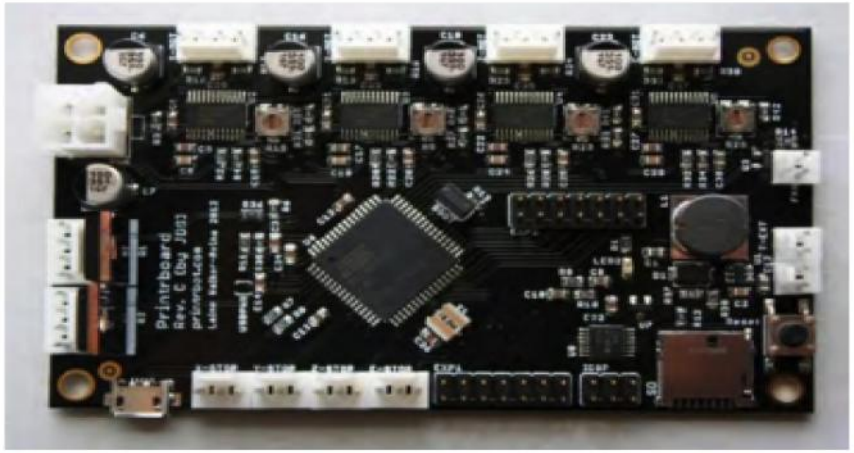
ANTIY 安天

- 换一个角度：对3D打印的安全攻击
  - 介绍3D打印技术和产业
  - 深入RepRap的工作流程和工具链
  - 简单务虚地讨论攻击的Who/Why/How/What/When
  - 分析可能的攻击目标和攻击方法
  - 三个PoC攻击演示和详细分析！

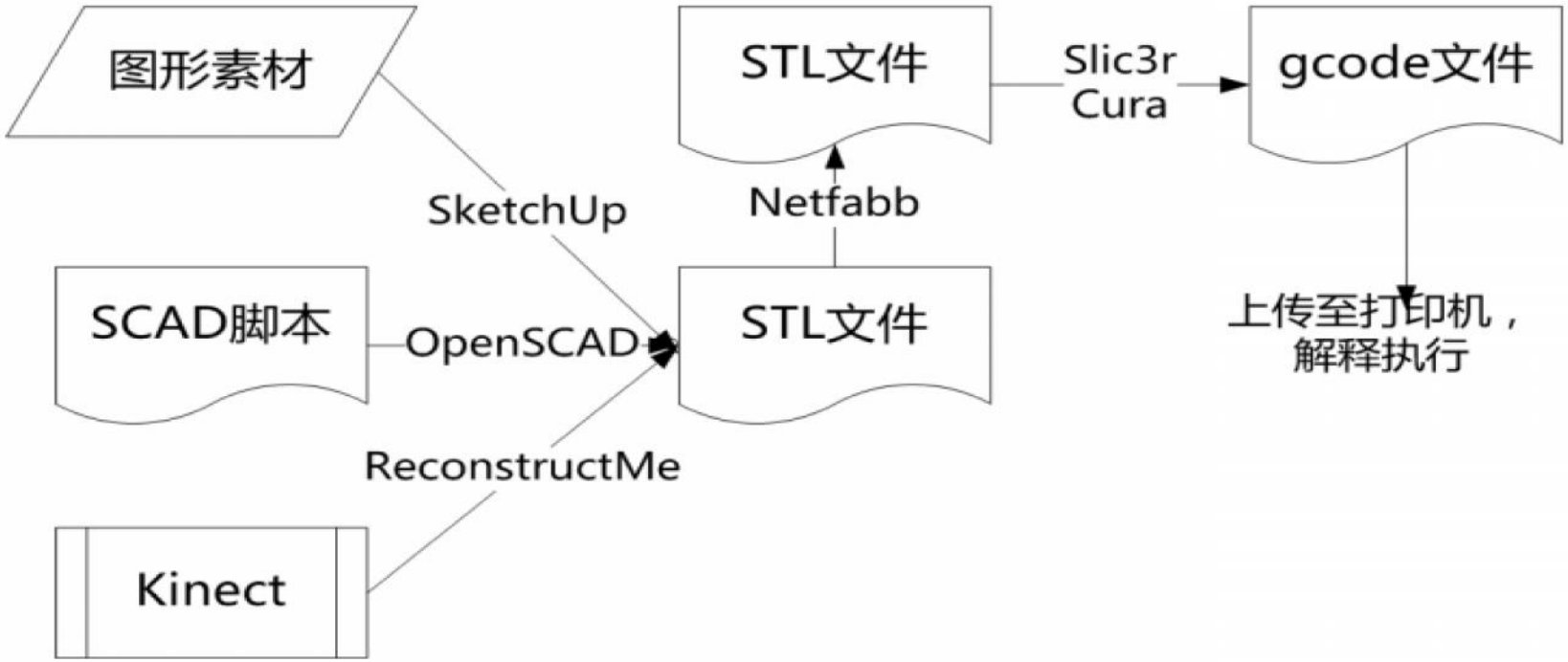
- 大思路：从桌面级开源3D打印机入手，为探索工业级3D打印系统的安全性做准备

RepRap：主控芯片和处理器





数据处理流程

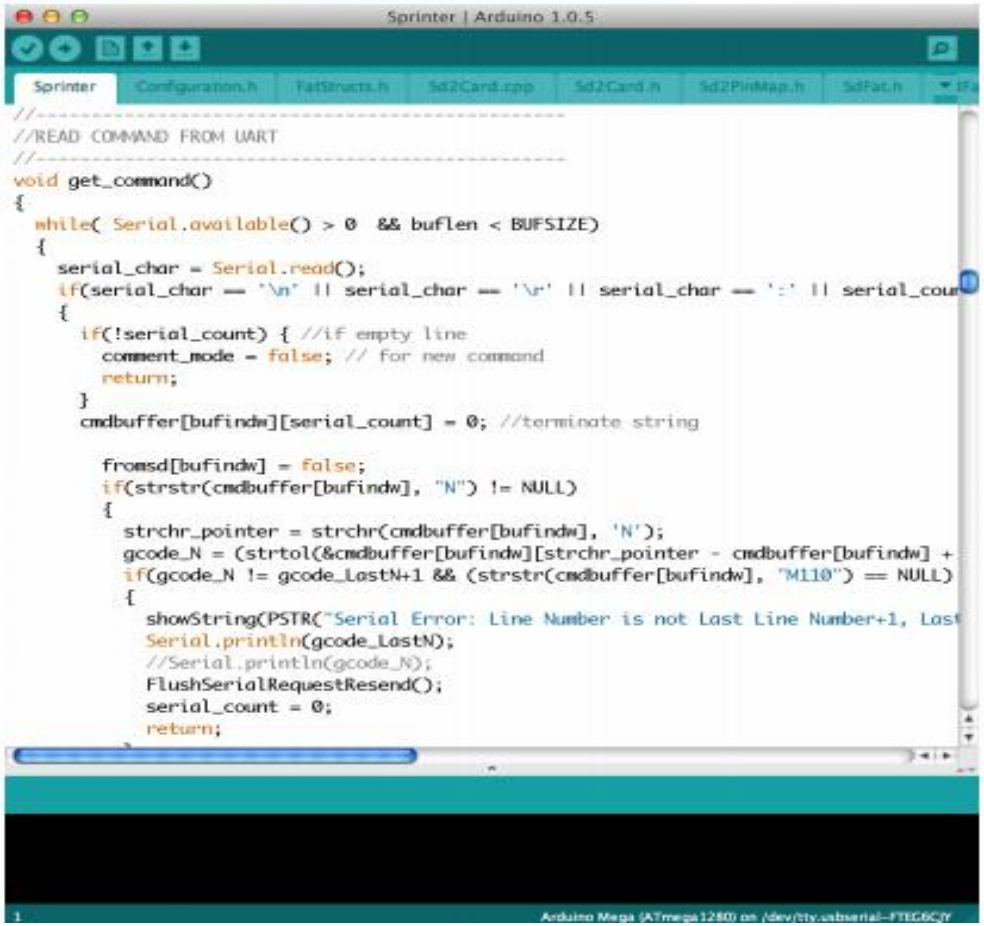

图形素材
SketchUp
SCAD脚本
OpenSCAD
Kinect
ReconstructMe
STL文件
Netfabb
STL文件
Slic3r
Cura
gcode文件
上传至打印机，
解释执行

Gcode文件

- 存储打印机的工作指令和参数
- 内容与机器相关
- 明文存储
- http://reprap.org/wiki/G-code

打印机固件

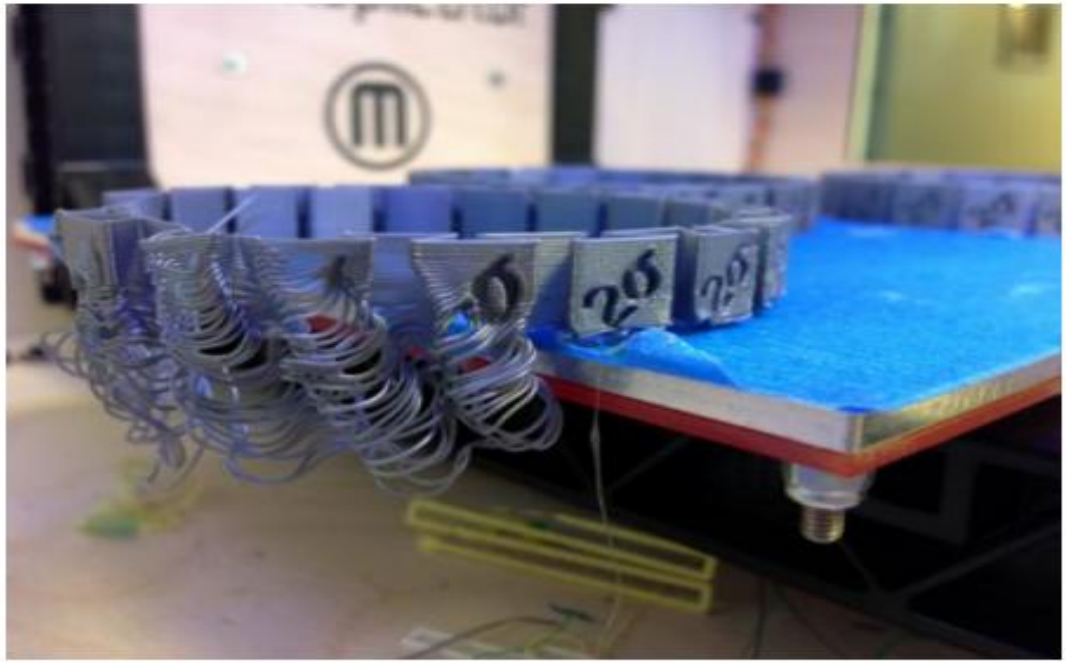
- 开源方案
  - Sprinter
  - Marlin
  - SJFW
- C/C++编写
- Arduino IDE或AVR交叉编译器编译
- avrdude烧录



智者安天下

务虚讨论

- What：攻击什么
  - 硬件设备
  - 数据和软件
  - 在线服务
  - 打印成品
- How：如何攻击
  - 篡改软件、配置
  - 篡改数据
  - 篡改固件



可能的攻击实现方法

PC软件

- 针对工具链的多种软件：
  - 建模软件
  - 切片软件
  - 控制软件
  - 编译软件

http://download.trimble.com/sketchup/sketchupmen.dmg
http://dl.slic3r.org/mac/slic3r-osx-uni-0-9-10b.dmg
http://software.ultimaker.com/current/Cura-13.06.5-MacOS.dm
http://koti.kapsi.fi/%7Ekliment/printrun/Printrun-Win-Slic3r-12J
http://arduino.googlecode.com/files/arduino-1.0.5-macosx.zip

- 攻击点：

打印机固件

- 篡改固件，修改内部逻辑
- 如何获得要篡改的固件?
  - 从源码编译：缺乏机器特定的配置数据
  - 从机器中下载并修改：如何自动修改

这就是我们马上要演示的

```
135 //===========================================================================
136 // Disables axis when it's not being used.
137 //===========================================================================
138 const bool DISABLE_X = false;
139 const bool DISABLE_Y = false;
140 const bool DISABLE_Z = true;
141 const bool DISABLE_E = false;
142
143 //===========================================================================
144 // Inverting axis direction
145 //===========================================================================
146 #ifdef I_AM_MENDEL
147 const bool INVERT_X_DIR = false;
148 const bool INVERT_Y_DIR = false;
149 const bool INVERT_Z_DIR = true;
150 const bool INVERT_E_DIR = false;
151 #endif
152 #ifdef I_AM_BUKO
153 const bool INVERT_X_DIR = false;
154 const bool INVERT_Y_DIR = true;
155 const bool INVERT_Z_DIR = false;
156 //const bool INVERT_E_DIR = false;
157 const bool INVERT_E_DIR = true;
158 #endif
159
160 //===========================================================================
161 //// ENDSTOP SETTINGS:
162 //===========================================================================
163 // Sets direction of endstops when homing; 1=MAX, -1=MIN
164 #ifdef I_AM_MENDEL
165   #define X_HOME_DIR -1
166 #endif
167 #ifdef I_AM_BUKO
168   #define X_HOME_DIR  1
169 #endif
170 #define Y_HOME_DIR -1
                                                    138,1         36%
```

- 让打印机的实际工作温度和观察温度不一致
  - 听起来很耳熟？ （Stuxnet）
  - 可能后果：
    - 温度达不到材料熔点
    - 挤出头损坏
    - 勉强工作，无法正常成型
- 通过修改固件实现
- 让整个过程完全自动化

几个新的方向

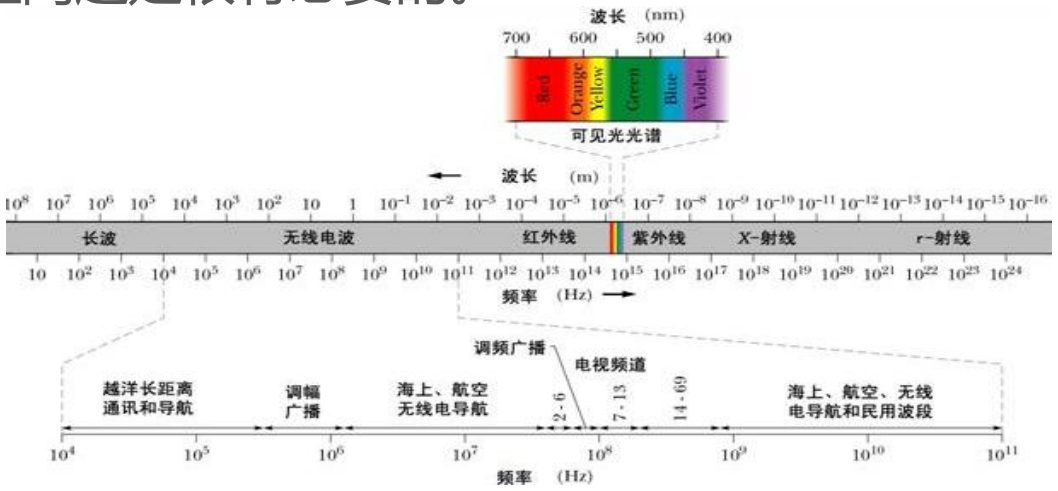
- 3D打印工具链和数据安全
- Arduino AVR固件安全
  - 可能影响更多其他的设备
- 工业级3D打印系统安全
  - 更像ICS的环境：封闭、“古老”、专用、重要
  - 不同的成型原理、软件工具链、硬件架构……
  - 更大的被攻击可能和后果影响

信号的可发现性(XCon 2014)

——Wi-Fi之外我们还能做什么？

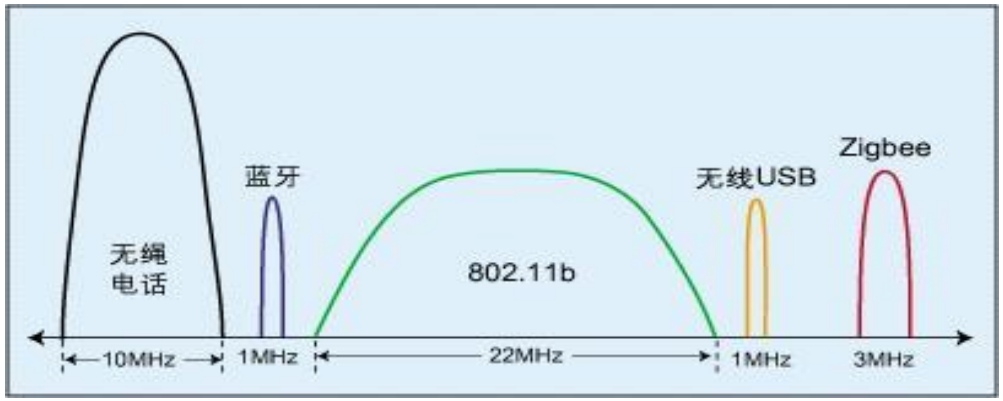
摘 要

- **安全性问题值得关注**
  - 以Wi-Fi、蓝牙等为代表的短程无线通信已经从方方面面渗透到我们生活中。
- **跳出传统视角**
  - 除了漏洞挖掘等传统视角，从更广阔的视野透视短程无线通信安全性问题是很有必要的。



ISM频段

- ITU-R (国际通信联盟无线电通信局)定义，免费使用的ISM频段(工业、科学和医用频段)。
  - *315MHz(非ITU-R ISM频段但我国允许使用，常用)*
  - 433MHz
  - 915MHz
  - 2.4GHz
  - 5.8GHz



常见短程无线通信

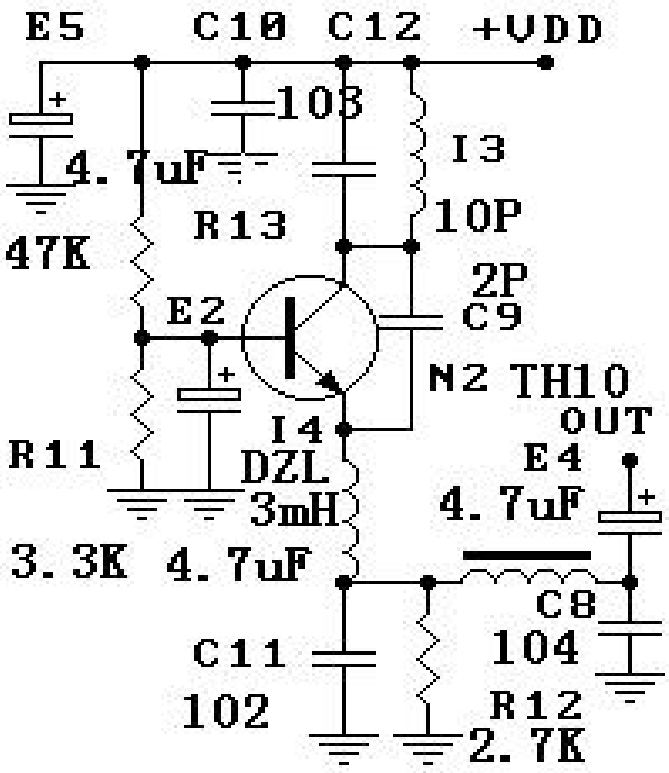
315MHz和433MHz

- 各类民用设备的无线遥控

2.4GHz

- Wi-Fi
- 蓝牙
- 自定义短程无线通信协议（例如2.4GHz无线键盘鼠标）

315MHz和433MHz频段的宽带接收

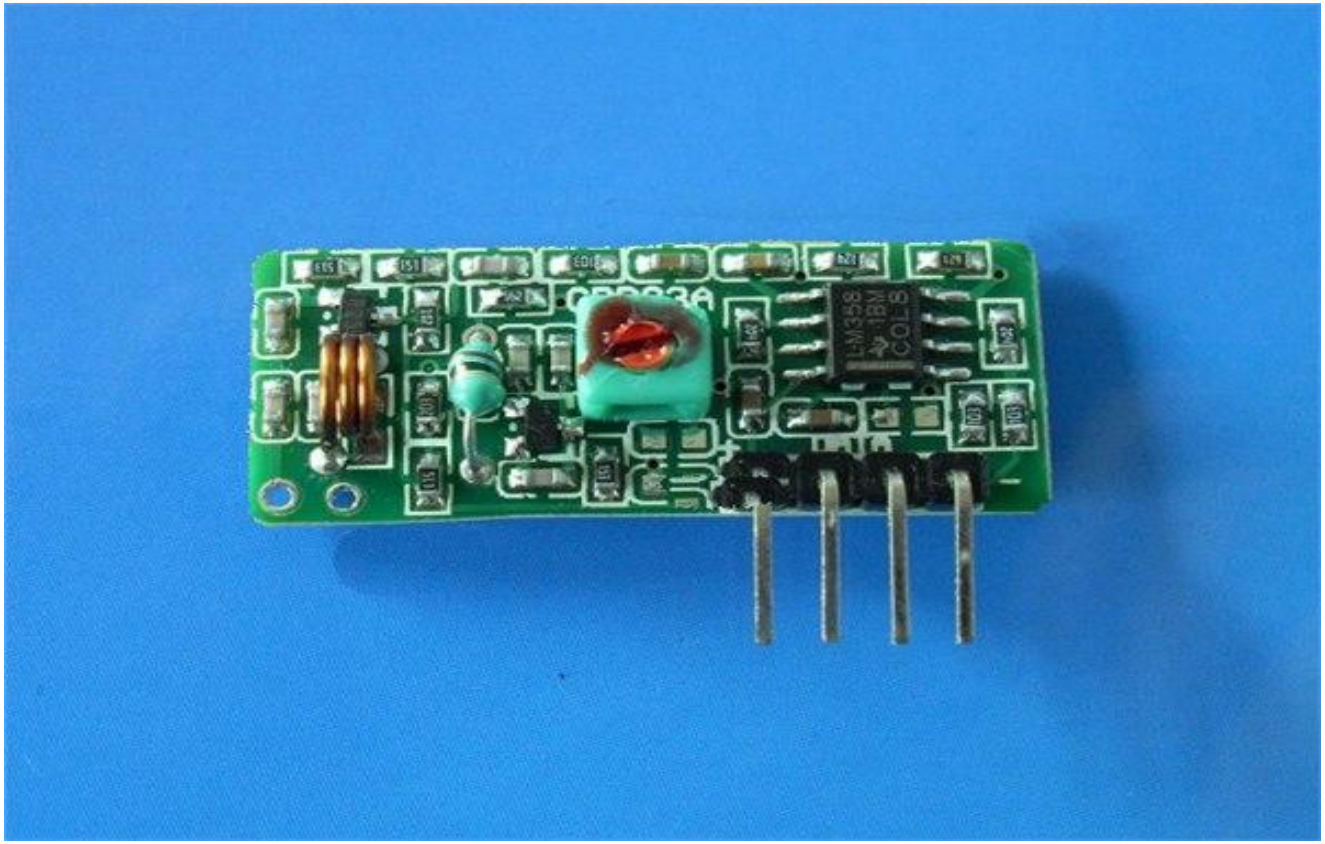


超再生接收电路

特点

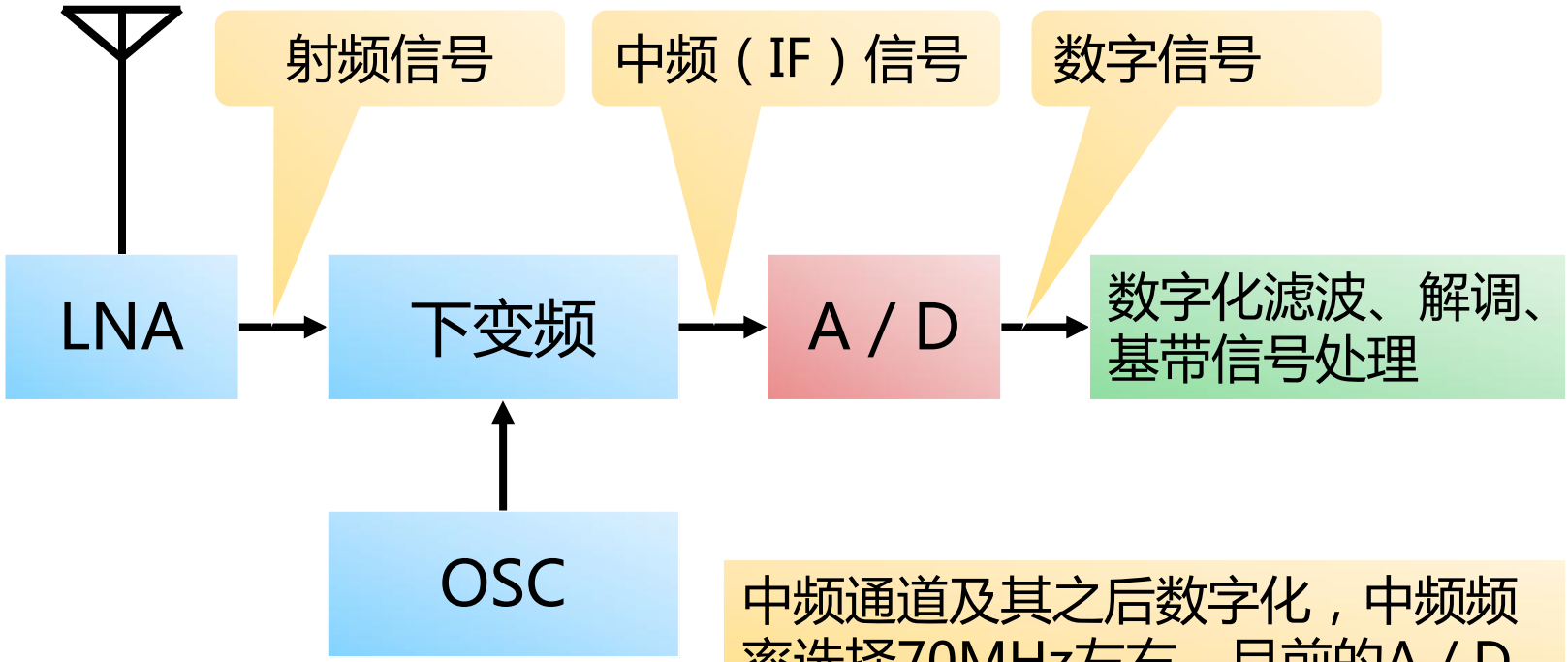
- 接收带宽较宽，一旦锁定接收频率，具有较好的接收性能。
- 适当改造电路，例如使用场效应晶体管（FET），可有效提升抗干扰能力。

演示1：宽带超再生接收315MHz信号

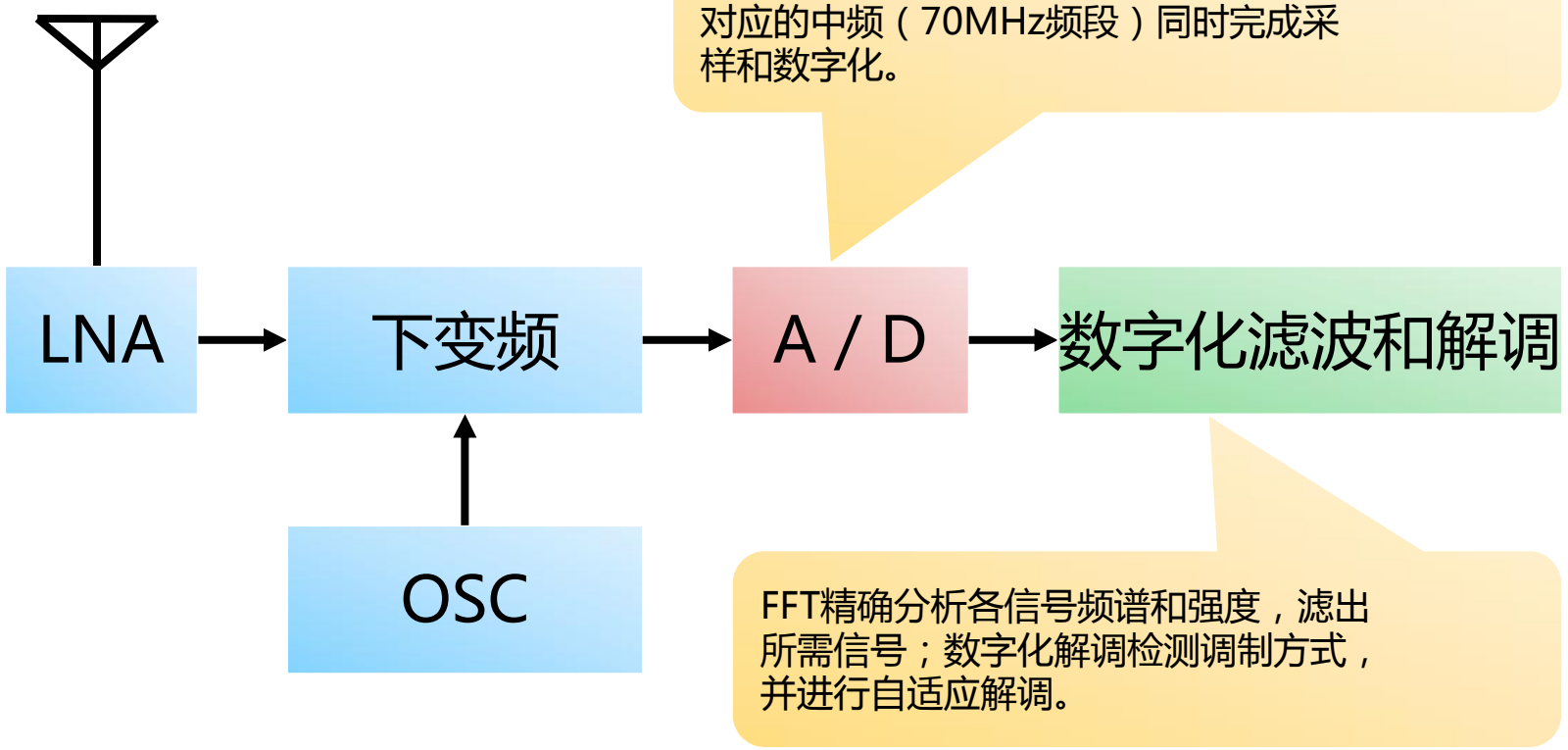


针对短程无线通信的攻击存在难点

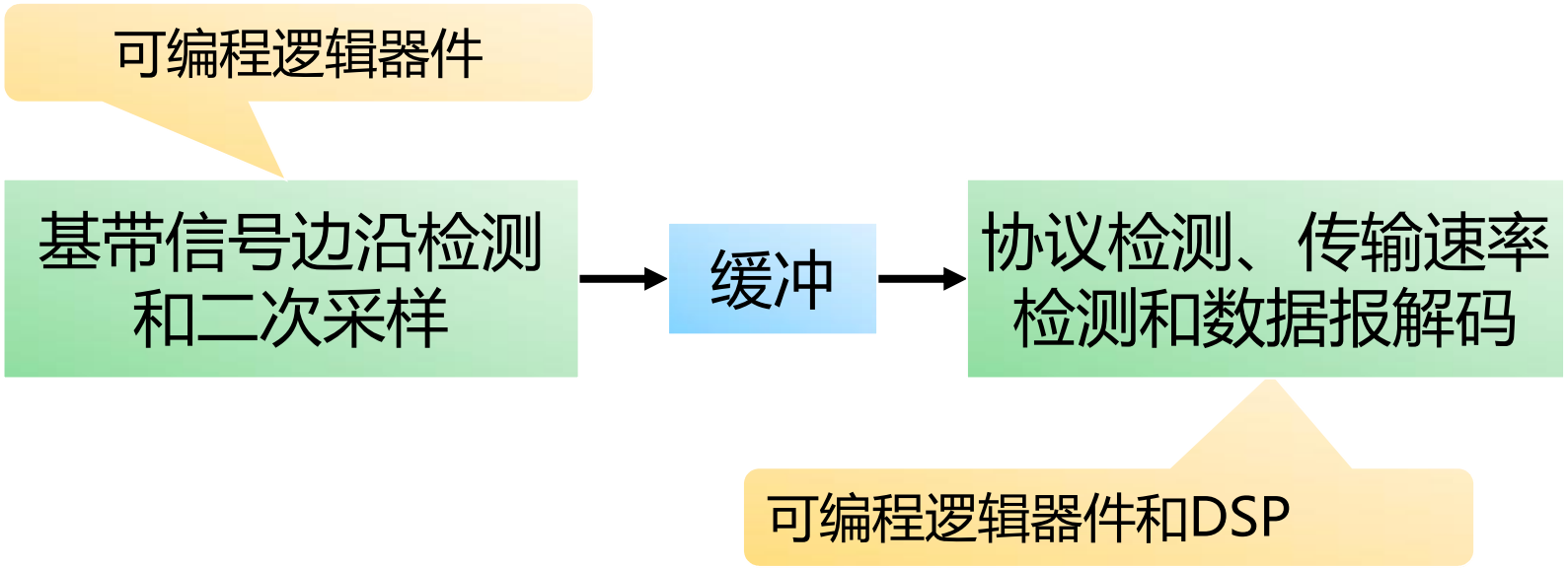
软件无线电（SDR）



使用软件无线电处理射频和中频



再配合数字化基带信号处理



实际SDR软硬件

- 软件
  - GNU Radio：http://gnuradio.org
- 硬件

USRP

bladeRF

HackRF One

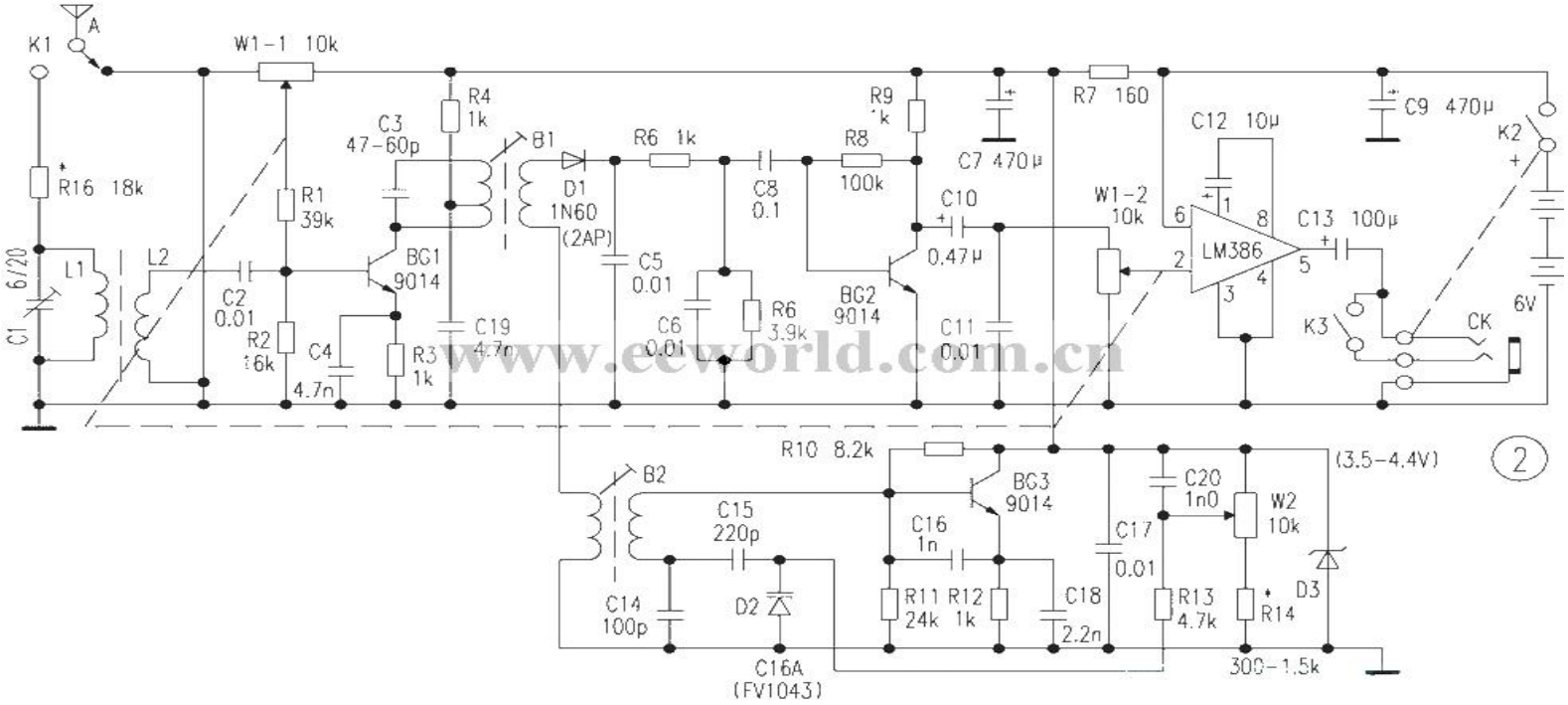
https://greatscottgadgets.com/hackrf/

- 无线电测向

测向机

定向天线

- PJ-80测向机电路图



短程无线通信的定位

- 定向天线（环形天线、八木天线、抛物面天线等）

八木（YAGI）天线

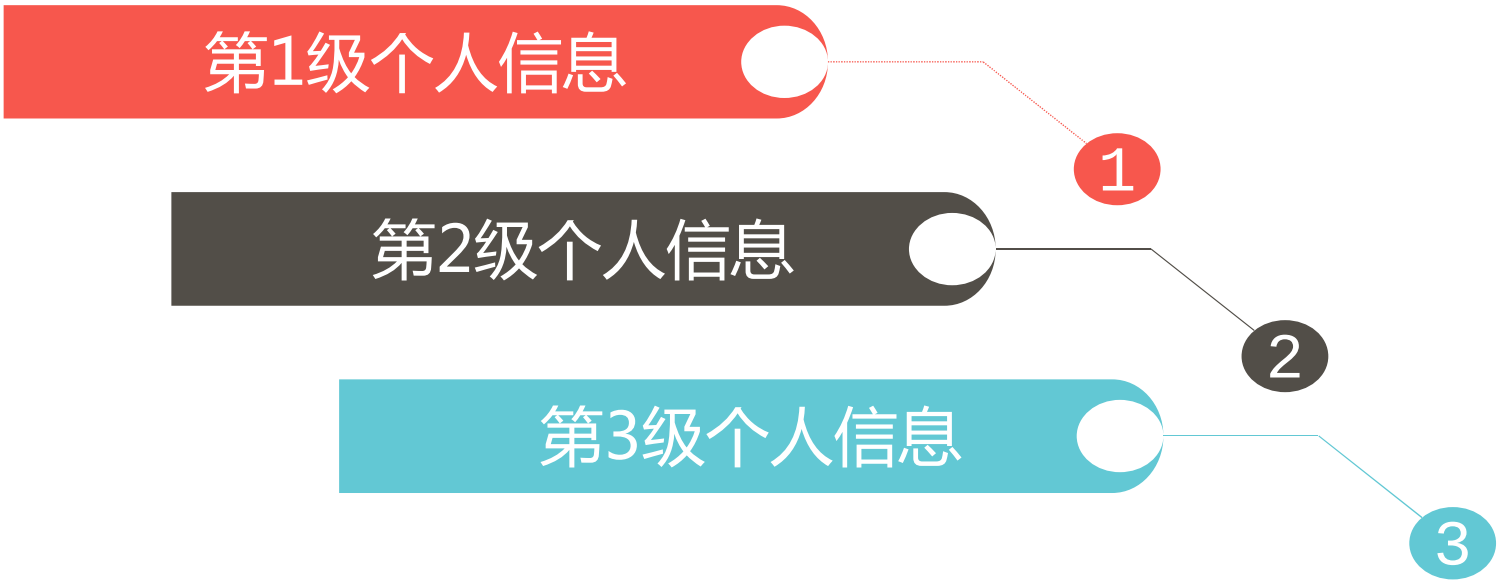
电视机室外天线即属于此类型

环形天线

抛物面天线

个人信息分级的依据

- 根据个人信息泄漏后可能导致的后果进行分级。



1级个人信息

- **定义**：泄漏后可能直接造成**<u>较大财产损失</u>**等严重后果的个人信息。

银行帐户用户名和密码

虚拟财产相关用户名和密码

保密性质的文档文件

程序

2级个人信息

- **定义**：泄漏后可能会对正常工作生活等造成**明显影响或者间接导致财产损失**等后果的个人信息。
  - 真实姓名、联系电话、家庭住址等详细信息
  - 即时通信工具用户名和密码
  - Wi-Fi密码

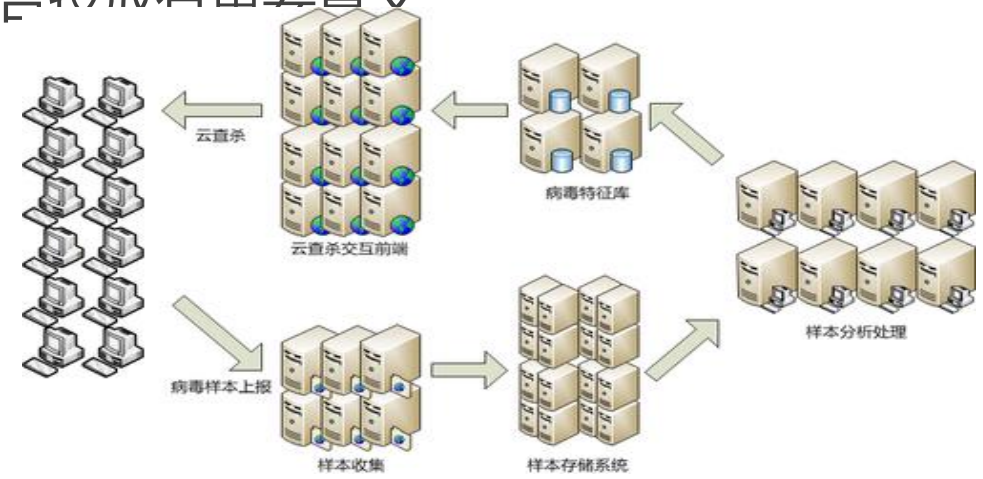
3级个人信息

- **定义：**以涉及个人工作生活领域、习惯、规律等为主的个人信息。

- *1级和2级个人信息一般可界定为个人隐私，但3级个人信息，特别是单个的3级个人信息不容易界定，收集3级个人信息属于“打擦边球”行为。*

3级个人信息收集的典型案例——云查杀

- 云查杀将可疑文件的文件名和散列值传输至云端，并不传输文件内容，因此一般不认为存在个人隐私泄漏。
- 特定IP终端用户的大量文件名信息被聚合到云服务器，大数据分析后对精准广告投放有重要意义



还原“虚拟人”——3级个人信息聚合结果

短程无线通信涉及到哪些3级个人信息？

1 315MHz & 433MHz

- 遥控窗帘——何时上班？何时回家？
- 遥控玩具——家里有小孩吗？
- 车钥匙——每天何时开车？

2 2.4GHz蓝牙

- 蓝牙耳机——有听音乐习惯？
- 蓝牙键盘鼠标——从事文字工作还是打游戏？

3 2.4GHz Wi-Fi

- 无线上网——每天何时上网？游戏or视频？

感谢大家的关注

esoul@antiy.cn