**撞锁：**标准的钥匙试讲锁销排成一条直线从而使得用户可以转动钥匙。通过适当的力量拍打撞匙（匙齿比一般的钥匙矮而尖），于是会有一个瞬间冲到合适的位置，而这个一个瞬间足够你把锁打开。一个熟手可能会比用真正的钥匙还要快。

**对抗撞匙：**增加一层侧销，他们也需要排列成直线才能打开锁。但是本质还是没有改变，只是麻烦了点。

**卡片**通常两种，磁条卡和RFID（Radio Frequency Identification）卡

    大多数**磁条卡**遵守ISO 7810、7811、7813标准，这些标准定义了磁条卡的尺寸以及卡片上被称为磁道1、2、3的数据词条。大多数磁条卡并没有相应的标准来保护数据，是明文存储，因此难以阻挡复制。攻击：<http://www.makinterface.de/>  和配套的Magetic-Strip Card Explorer进行卡片的读写。卡片中还可能存有地址、社会安保码、账户余额。防止修改就要使用校验和。我们通过对一张卡片使用前后的变化，以及和其他卡片的比较判断出各个部分的作用。

**RFID卡片**工作在135KHz或者13.56MHz。曾经有人研究过安全，但是被主要的厂商指控拦截了。工具：<https://www.openpcd.org/> -》proxmark3  内嵌了FPGA，可以对不同的RFID协议进行解码-》USRP 截获交流时候的无线电波。

    当卡片被读卡器（连接着系统）激活时，查询被发送给RFID卡，RFID卡对查询进行加密并使用卡内的私钥签名，一次作为应答返回给读卡器。读卡器在验证应答合法后，才会运行持卡人访问被保护的资源。

   常用门禁卡通常分为 IC 和 ID 卡，厚圆的是 ID 卡，薄的是 IC 卡。ID 卡常用的频率为 125KHz，IC 卡常用的频率为 13.56MHz，还有一种 915MHz 的超高频 IC 卡。手机自带的 NFC 频率为 13.56MHz ，所以手机只能模拟频率相同的未加密的 IC 卡，不能复制模拟 ID 卡。ID 卡：线圈是圆形的，并且线圈匝数比较多，集中在卡片中间，ID 卡不包含加密信息，ID 卡号读取无需任何权限，易于复制，安全性很低。一般情况下 ID 卡只做身份识别（门禁卡）用，ID 卡正在逐步淘汰。IC 卡：线圈是方形的，匝数比较少，分布在卡片四周。观察线圈的方式有一定的局限性，不排除有特殊定制的线圈形状。

通常**固件**镜像被直接加载在微控制器上，并像MS\_DOS下的COM文件一样总是从一个固定地址开始运行。使用strings，可以知道固件的文件系统类型，比如说cramfs-》mount -o lop -t cramfs /home/adam/0AA.EAAA /tmp/cram-》find /tmp/cram -name \*key、\*cert、\*pgp、\*gpg、\*der、\*pem寻找密钥

**蓝牙**的默认模式就是能被任何人搜索和连接。工具：Ubertooth，嗅探和重播2.4GHz的ISM波段范围内的80个蓝牙频道。嗅探会受到一定的wifi干扰。

**ATA** 在BIOS对硬盘读写之前输入口令。但是ATA驱动器个BIOS是通过硬件连接的，没有验证。用户向ATA驱动器发送指定口令就能够修改封锁口令，不过需要骗过BIOS。

    有的**U盘**有U3分区，一插上这个分区就会运行autorun.ini，一般制造商会在期中转入一个用来品牌宣传的ISO。U盘攻击常见的就是读口令或者按后门，至于美国的震网病毒是真的厉害，居然没有接触到真实系统就一次搞定伊朗了。传闻除了关闭自运行，还有在U盘插入前按住shift。

**ATM机子**在出厂的时候配置了相同的管理口令。每一个ATM都会记录交易日志，而且联网到银行。

**航空公司**在**飞机**上使用自己开发的系统，不超过windows xp水平。

**硬件操作：**

    通过硝酸去除环氧树脂涂层，注意后续安全处理。保形涂料可以使用MG化学品8319 来脱模，还可以还是用Dremel电磨进行细致处理。

    大一些的双列直插式芯片可以通过吸锡工艺拆除。表层贴的芯片使用chipquick工具或者高温气流去除。

    逻辑分析仪的逻辑探针连接到芯片的针脚上可以捕获信号的传输。适用于更小电路板的Thermo-BondCir。

    ROM编程器，如果有特殊的写保护，就需要FIB套件、微型定位器、通道