从红队角度看“锁”

360RedTeam-杨晓成

No.1 关于物理渗透

No.2 为什么要讲“锁”

No.3 边界突破

No.4 利用方式

No.5 实例&防护方式

关于物理渗透

前有古人

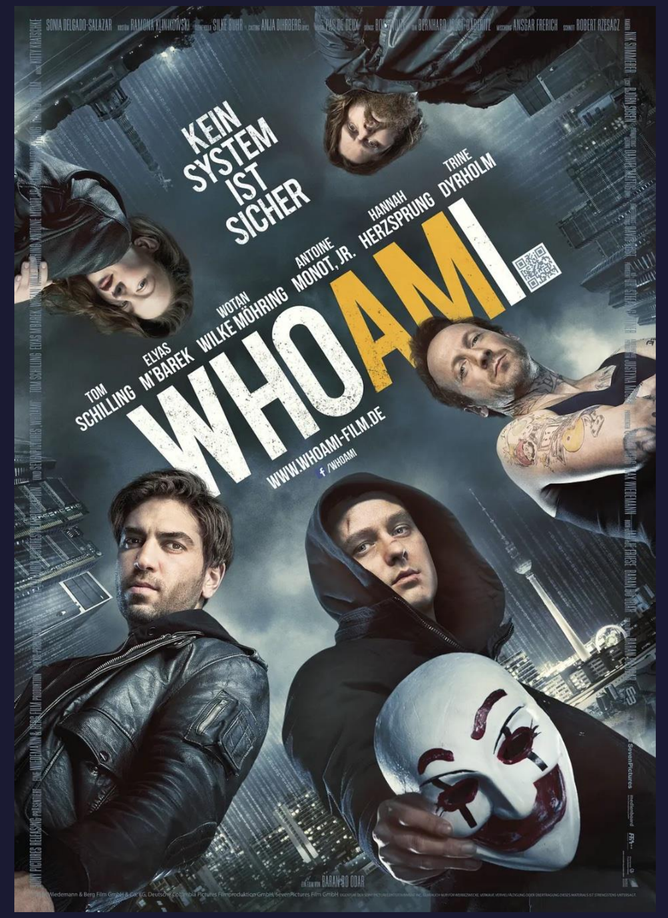
redteamsecurity

国外物理渗透&渗透测试安全团队，学习的榜样。

RedTeam
SECURITY CONSULTING

我是谁：没有绝对的安全

14年的电影，其中有一句台词
“人不能总藏在他的计算机后面，最大的安全漏洞并不是存在于程序或服务器内，人才是最大的安全漏洞”



后有来者

渗透从未变得如此轻松

攻击者角度

waf ?

Ids ?

物理隔离?

工控网络?

ALL BY PASS ！！

企业角度

识别环境中存在的物理安全控制缺陷

了解企业的实际风险水平

帮助解决和修复已发现的物理安全漏洞

Check！！

为什么要讲“锁”

从攻击者角度看渗透

边界突破

代码执行

任意文件上传

文件包含


找到约 2,630,000 条结果 （用时 0.55 秒）

歪酷cms任意代码执行漏洞- SecPulse.COM | 安全脉搏
https://www.secpulse.com/archives/22030.html
漏洞标题, 歪酷cms任意代码执行漏洞. 相关厂商, 歪酷cms. 漏洞作者, m1x7e1. 提交时间, 2014-01-12 12:17. 公开时间, 2014-04-12 12:17. 漏洞类型, 命令执行.

小众CMS vaeThink v1.0.1 代码执行漏洞挖掘分析– backup
https://4hou.win/wordpress/?p=32388
2019年5月25日 - 本文是对一个小众CMS（vaeThink v1.0.1）进行分析、代码执行漏洞挖掘和审计过程的记录，该CMS基于ThinkPHP5开发。作为一名代码审计的入门 ...

SecWiki/CMS-Hunter: CMS漏洞测试用例集合 - GitHub
https://github.com/SecWiki/CMS-Hunter
Contribute to SecWiki/CMS-Hunter development by creating an account on GitHub. ... Drupal/Drup
程代码执行漏洞(CVE-2017-6920) · Drupal远程代码执行 ...

某CMS最新版-远程代码执行- 先知社区
https://xz.aliyun.com/t/3855
2019年1月17日 - 初学审计的我很菜，跪求各位大牛指点； 认真分析这个漏洞，版本是HongCMS3.(
. 直接访问/index.php是不行的，还必须手动安装；

某CMS-5.0.190111后台代码执行（CVE-2019-7580） - 先知社区
https://xz.aliyun.com/t/3997
2019年2月4日 - 0x00 环境搭建. 首先去thinkcmf下载5.0的最新版 https://github.com/thinkcmf/thinkcmf/archive/5.0.190111.zip 切换到web根目录下，比如/var/www， ...


找到约 1,170,000 条结果 （用时 0.56 秒）

易酷CMS2.5本地文件包含漏洞- 谢公子的博客- CSDN博客
https://blog.csdn.net/qq_36119192/article/details/84590703
2018年11月28日 - 今天这篇文件主要记录凡诺CMS后台文件包含漏洞：0×01文件包含简介服务器执行PHP ... 文件包含分为两种，一种为本地文件包含，一种为远程.

凡诺CMS一处文件包含漏洞- Power_Liu - CSDN博客
https://blog.csdn.net/qq_36304918/article/details/85332687
2018年12月28日 - 今天这篇文件主要记录凡诺CMS后台文件包含漏洞：. 0×01 文件包含 ... phpmyadmin远程文件包含漏洞（CVE-2018-12613）. 12-13 阅读数 535.

【原创技术分享】Exponent-cms任意文件上传
https://www.anquanke.com/post/id/84514
2016年9月6日 - Exponent cms是一款国外的cms,功能比较强大。版本通杀的任意文件上传漏洞。攻击者可以通过该漏洞 ...

Drake CMS xhtml.php远程文件包含漏洞-漏洞公告- 彩70彩票平台 ...
www.ilexart.com/Article/html/2/5/2006/12772.htm
受影响系统： Drake Drake CMS 0.2.2.846 描述： Drake CMS是一款高效、可自定义的内容管理系统。Drake CMS在处理用户请求时存在输入验证漏洞，远程攻击者 ...

某CMS任意文件上传getshell（大量政府站） -
https://www.secpulse.com/archives/25114.html
漏洞标题, 某CMS任意文件上传getshell（大量政府站）. 相关厂
2014-06-09 13:46. 公开时间, 2014-09-07 13:48. 漏洞类型 ...

CVE-2008-2977 Ourvideo CMS 远程文件包含漏洞-漏洞情报、漏洞详情 ...
https://www.anquanke.com/vul/id/1115534
2008年6月23日 - Ourvideo CMS 远程文件包含漏洞OurvideoCMS是一款基于MySql和php的媒体内容管理系统。OurvideoCMS9.5中存在多个PHP远程文件包含漏洞 ...

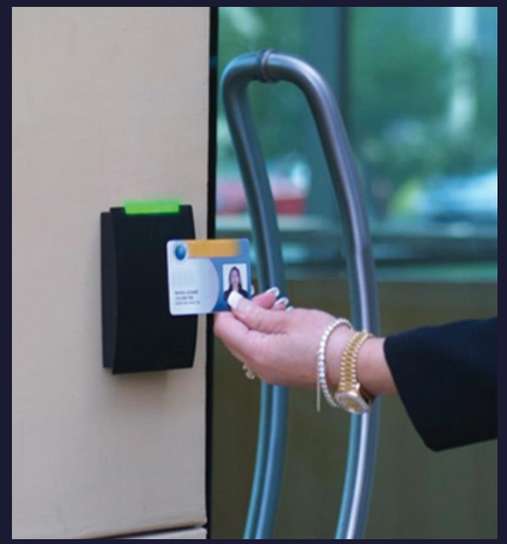
某大学CMS的任意文件上传漏洞- SecPulse.COM | 安全脉搏
https://www.secpulse.com/archives/21082.html
2014年2月18日 - 漏洞标题, 某大学CMS的任意文件上传漏洞. 相关厂商, 北京清元优软科技有限公司. 漏洞作者, happylyang. 提交时间, 2013-11-20 11:32. 公开时间 ...

某通用型政府cms任意文件上传漏洞/文件包含/未授权访问| 乌云漏洞库 ...
https://shuimugan.com/bug/view?bug_no=54821
某通用型政府cms任意文件上传漏洞/文件包含/未授权访问| 乌云漏洞库,乌云镜像站, WooYun 漏洞库, WooYun 镜像站.

CVE-2018-19562：PHPok 4.9.015存在任意文件上传漏洞- CVE中文 ...
www.iwantacve.cn/index.php/archives/87/
2018年11月25日 - 一、漏洞摘要漏洞名称: PHPok 4.9.015存在任意文件上传漏洞上报日期: 2018-11-25漏洞发现者: F0rmat产品首页: https://www.phpok.com/软件 ...

机械锁

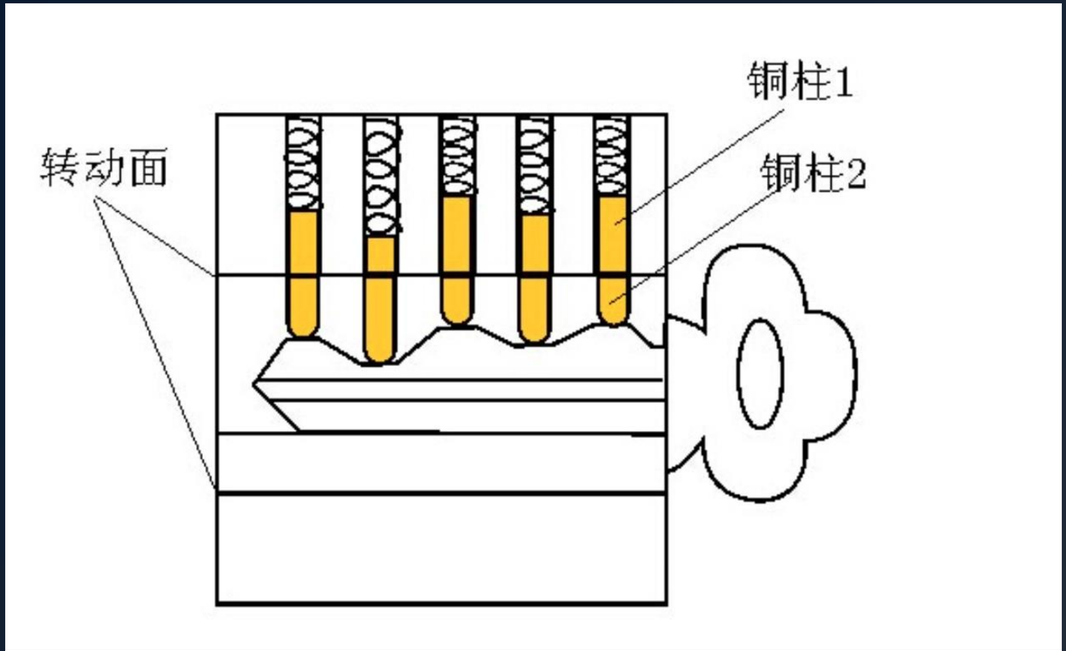
电子锁（智能门锁）



门禁&安保

利用方式

机械锁原理



铜芯

铜制的圆柱形锁芯，转动时可锁上或打开，锁芯分内锁芯和外锁芯。

弹子

铜弹子分内弹子和外弹子，圆柱形，长短不一，装在内外锁芯的圆孔中。

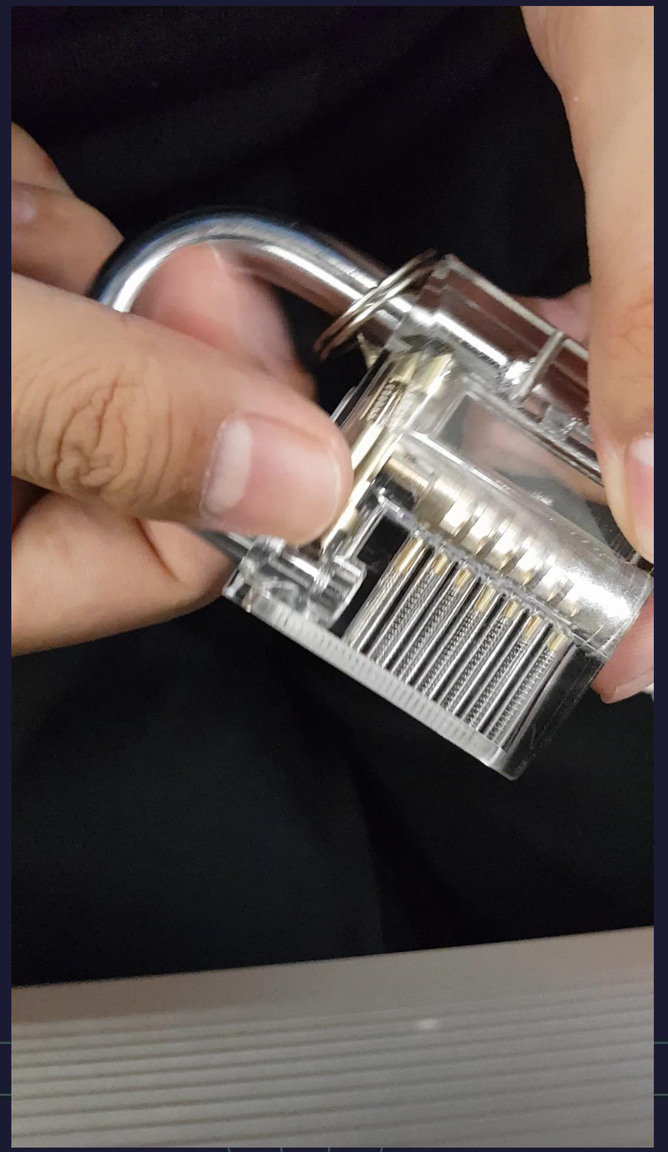
弹簧

装在外锁芯的圆孔中。顶住弹子。

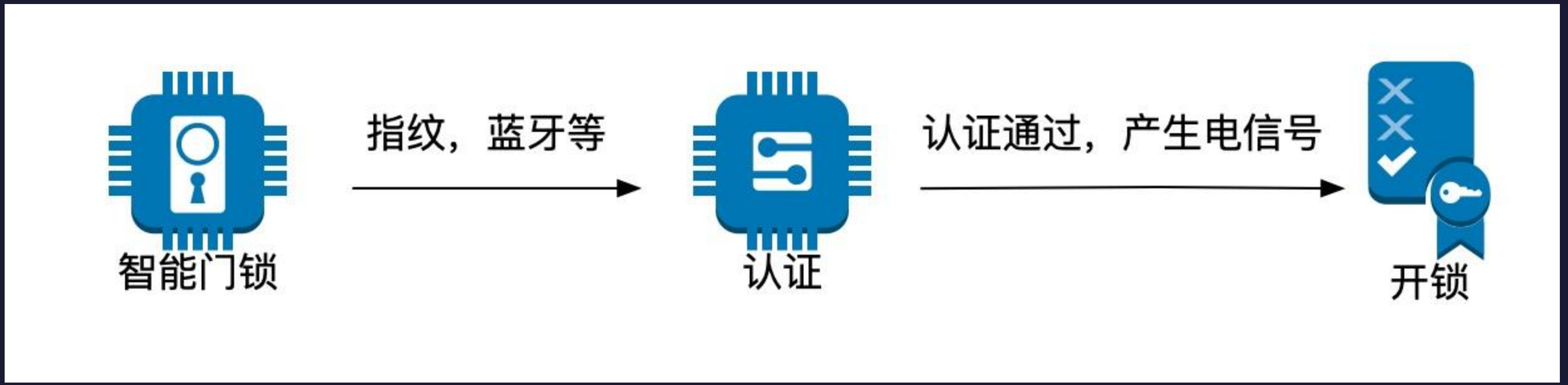
锁舌

开锁时伸缩的部分。圆柱形内锁芯转动时带动锁舌。

开锁视频



智能门锁



工作流程

如何利用通用方式开启门锁

重启

有些门锁设计为当系统重启会自动打开门锁

产生感应电流

产生感应电流，可能会使电机工作或者认为是正确的校验从而开门

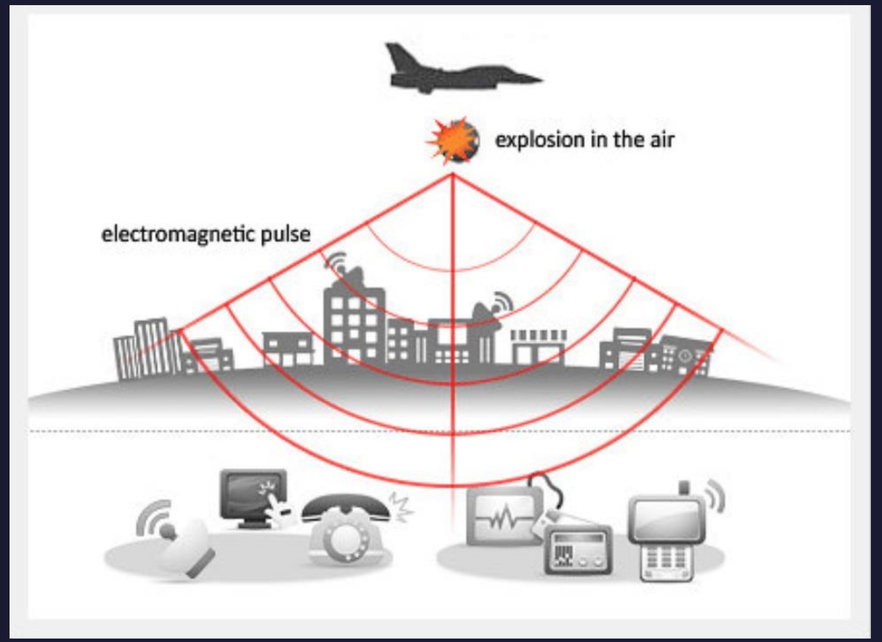
破坏

当内部电路元器件被破坏后，会打开门锁

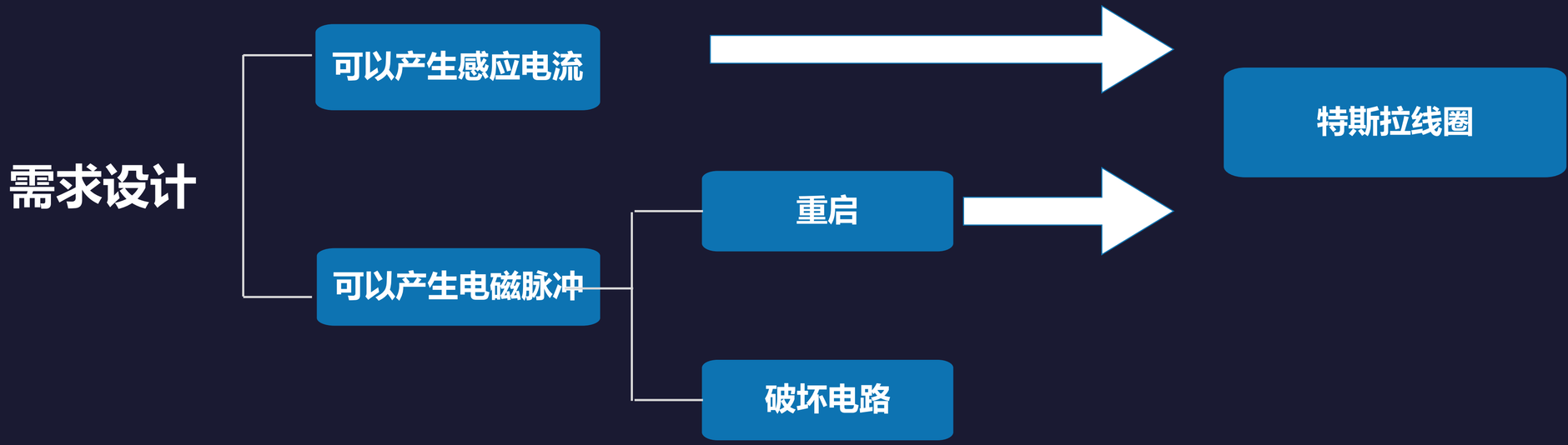
EMP（电磁脉冲）

电磁脉冲

电磁脉冲的最长时间通常只会持续一秒钟。任何没有受到保护的电器和任何连接到电线的东西，如电力系统、电子设备、微芯片等都将会受到电磁脉冲的影响而导致无法修复的损坏



工具设计



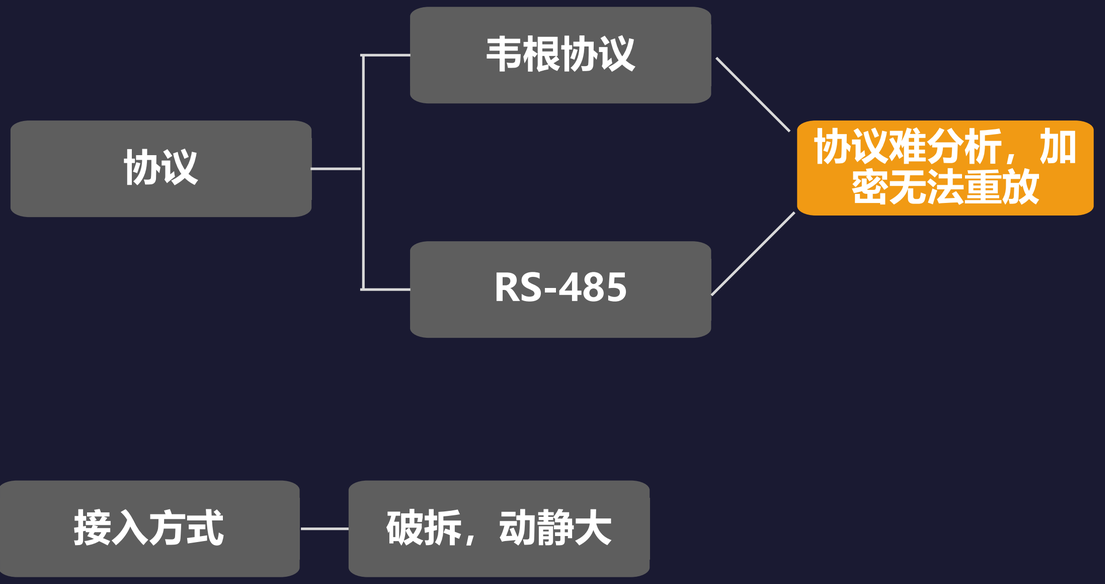
自制EMP

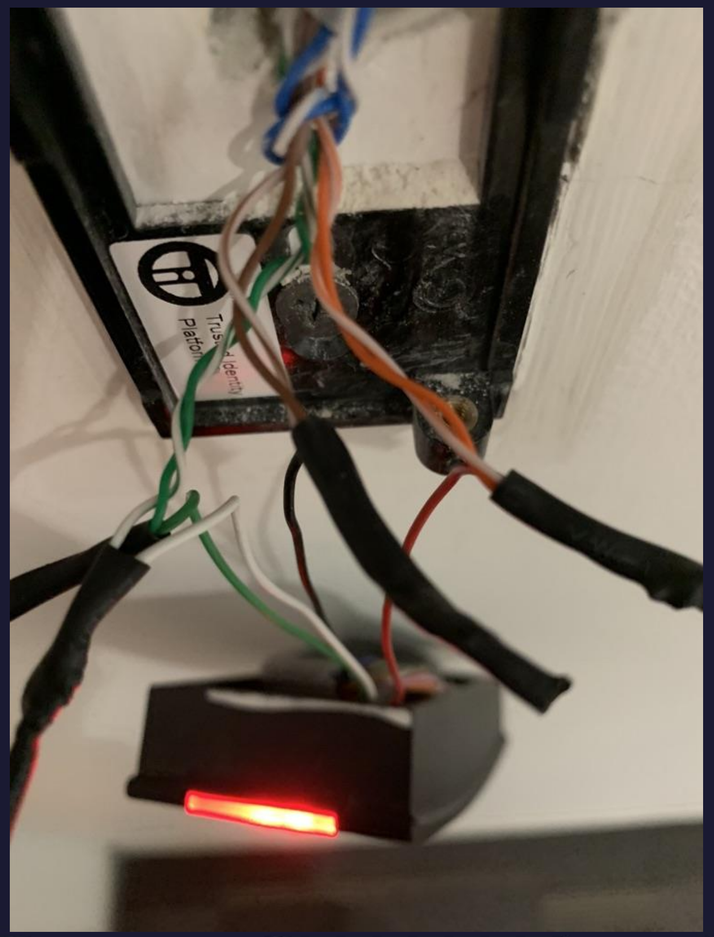
门禁

门禁的重要性

在一些大公司，依靠于门禁设置权限，
比如重要的机房，档案室，办公室等。

门禁

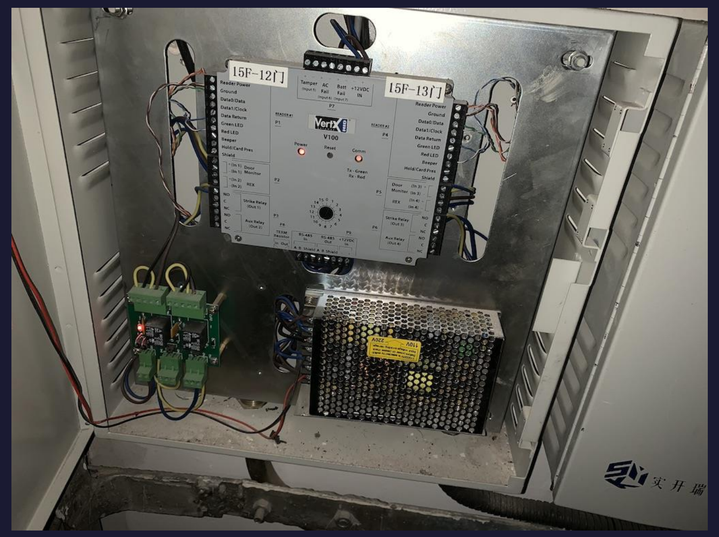


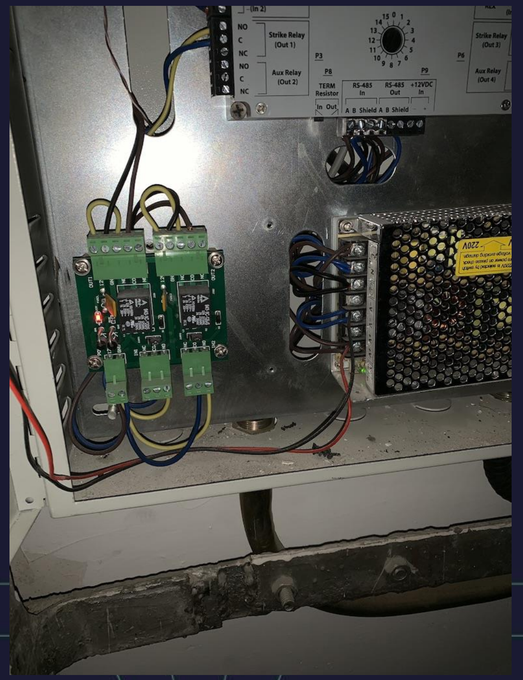


取巧

取巧来开门

门禁一般设计为一断电保持常开，那么只需要把该门禁断电即可打开相关门禁（消防）。
控制电路一般都在大楼的弱电井中，进入弱电井（机械锁）就可以成功的对其进行断电。





防护方式

机械锁

选择

企业选择超b类锁，不建议使用A级锁，目前几乎所有的企业内部都使用的A类锁

防护

重要设施（弱电井等），摄像头，活体检测等设备多重防护

管理

制度上的管理，离职人员钥匙回收，钥匙不能带出一定范围等

智能门锁/门禁&安保

选择

选择带EMP防护的门禁/智能门锁。
门禁卡选择cup卡，无法被复制。

管理

制度上的管理，门禁卡丢失要及时告知管理部门，禁止代打卡等。
门禁权限相关问题。
进入园区大楼等要设置门禁设备，安保要严格，访客一定要有对应人迎接。
围栏等破损修补。

谢谢 & 问答