

## 二

# 27 你可以得到我的心，却得不到我的人 - 物理安全设备

从这一章开始，我们要开始讲解和介绍网络安全。我们先来看一下物理安全设备，可能这个是最被大家所忽视的一部分。因为基本不会有哪一门课会讲解这个。让我们一起来开始吧。

### 视频监控

提到视频监控，我相信大家都不会陌生，当然有好的有坏的，比如某些你上的网站（你懂得），我就不说了，还有我们马路上的监控，商场里的监控等等。如今，摄像头已经变得非常便宜。其实我们大多数人都会随身携带一个摄像头（你的手机），这在15或20年前是完全闻所未闻的。另外，你也在网上可以购买连接网络或者无线网络的摄像头，而这在过去10到20年中是没有的。当然这也促进了很多产业的发展。这意味着企业可以更有效地监控企业发生的事情（保护安全，以及预防危险等等）。另外，现在也已经建有非常健壮和有效的数据网络，需要大量的存储空间，这使我们可以保存很多视频。

此外，我们也完全可以以相对较低的价格购买适合自己房屋的摄像头（价钱还是会决定一切）。比如在我的车道上有一个摄像头，用来监视会不会有人来试图打开我的车门，将零钱或者其他物品从车上拿走，所以我在那儿装了一个小摄像头，以便发生意外的时候，知道是谁以及什么时候发生的。当然这些都是小事情，你也很可能会在公司的极为敏感的领域IT部门使用摄像头，例如在数据中心等地方，以便知道谁在数据中心的以及他们正在使用什么设备。使公司可以确定在其中从事工作的人是合法的管理员，还是什么可疑的人在用设备做些对公司不利的事情（不知道你听没听过，数据是未来的核心竞争力，当然我们这里不是讨论数据）。你还可以使用视频记录来查看谁在何时进行了操作。对于数据中心来说，这是一个性价比非常合适的选择。你当然还可以安装运动检测器，并且运动检测器可以帮助处理各种其他的事情。比如，如果有人在数据中心的某个区域，或者他们可能在某个机柜中打开，它可以发出警报。我们可以将这些运动探测器放置在我们想知道某个人何时在某个区域活动的区域。比如我前面说的车道上的相机也可以是由动作启动的，也就是说监控并非一直在记录。如果没有任何动作发生，它只会闲置在那里。一旦有人经过摄像头或在摄像头附近行走，那便是摄像头开始记录的时间，这也使得我们可以节省一些空间（虽然硬盘已经很便宜了），并使监视和回放这些视频文件更容易一些。

### 资产追踪

在大多数企业中，你会发现资产跟踪可能会从会计部门开始。你可以使用某种类型的资产跟踪标签，通常就是一个非常简单的标签。上面要贴上你公司的名称，比如CSDN。它经常有条形码和与之相关的数字，公司会将这些标签贴在公司的资产上比如笔记本电脑。在美国还有税务的问题，这里就不讲了。比如刚才讲的标签贴在笔记本上，公司能够扫描该标签（比如什么时候设备寄给你，什么时候你还回去）。一般会将标签贴到有价值的东西上，比如笔记本电脑，PC，平板电脑或其他具有实际实际价值的设备上。你不会找到附在钢笔和铅笔上的资产标签，因为它们的价值非常有限，不值得追踪这些东西。但是任何具有实际价值的设备都将获得这样的标签。此外，当我们尝试对设备进行故障排除时，你也可以使用这些资产跟踪标签来帮助跟踪设备的位置。比如现在你在家工作，如果电脑出现任何问题，你可以使用标签致电公司的support部门。也许该标签还与公司的特定地理区域相关联。最后，当我们谈论公司资产时，公司不希望用户在不需要设备的情况下对其进行篡改。因此，有时在出厂时，你会看到一小段胶带被安装在设备上以进行篡改检测。比如电脑上会说：“如果这个胶带被打开了，保修将失效”。或者，有时也可以在设备上加锁。比如你家里的煤气表或电表上会看到小锁，它只是一个篡改证据锁，通常嵌入某种塑料的金属丝，很难拆开再放回去。这样它就可以用来检测系统是否遭到篡改。这种篡改检测是技术人员确定是否有人已经在尝试破坏设备的方法。

## 设施使用

接下来，让我们讨论一下设施访问和使用，我们来讨论一下如何授予需要访问某些房间的个人访问权限，这些房间中通常会装有许多昂贵和重要的设备，例如我们的数据中心。因此，我们要做的是将某种锁放在该门上，然后分发与之相对应的锁。（不知道你公司有没有呀，就是有一个电子锁，然后给你一张卡，你可以扫那个卡去开门）。其实将物理钥匙分发可能会出现一些问题。有的公司会使用同一把钥匙或者门卡，这个卡可以打开公司的任何一扇门。你能想象一下，如果这个卡或者钥匙丢了，公司是不是要去换了所有的锁（门卡的话，现在通过程序可以解除其权限）。因此，现在取而代之的是，通过设施访问，我们经常会使用某种类型的智能卡，也许是你的ID徽章，其中内置了一些电子设备，可让您通过某种类型的垫板对其进行扫描，如果你的门板打开了，徽章被确认可以进入该设施，所以我们有这些卡可以给我们访问。这也带来了一些安全问题，因为它上面可能贴有你帅气照片和名字，其实这个还是会有安全隐患，比如说你卡丢了，你一般不会第一时间发现，等你发现了在通知IT部门，在去换卡，这期间会有很多的可能性，比如有人可以捡到或者偷了你的卡，然后冒充你来进入（玩过HITMAN的人基本都知道吧）。随着科技的进步，我们也在渐渐的解决这个问题，这就是为什么我们可能要引入某种类型的生物特征识别扫描的方法，例如指纹读取器和眼睛扫描，面部扫描或手掌扫描，诸如此类的东西将有助于增强对安全设施的访问权限。但是，如果你和我一样是标准的电影脑残粉，则可以通过生物识别技术做一些令人作呕的事情，以解决这一问题。例如用某人的手指以用作指纹验证或以某种方式获得某人的眼球以用于视网膜扫描。有许多公司将提供技术来帮助抵御这些无用的生物识别技术的破解（我确实很喜欢阿里巴巴，技术确实领先，还记得脱口秀大会上，颜怡颜悦说她们双胞胎只解开过一次人脸识别）。当然，现在的技术发展的真是日新月异，比如我现在的车，有一个电子小钥匙。我只需将钥匙放在口袋里，然后走上车就可以启动汽车，而不必像以前那样将钥匙真正

的插入点火装置中。

总结一下，我们研究和探讨了一些具有IT物理安全性的东西。我们谈了一些有关视频监控的内容。我们讨论了资产跟踪以及如何使用一些标签来帮助我们创建组织中所有资产的清单。最后，我们讨论了设施访问以及如何使用徽章，生物特征识别，智能卡等等，或者只是普通的老式物理锁来保护我们的设施免遭未经授权的访问。

[上一页](#)

[下一页](#)