责任编辑:李欣 美编:孙月 组版:杜敏

安全专家称,借助安全漏洞和技术设备

你的手机能杀人

电脑和网络虽然给人们的生活带来极大便利,但同时也埋下了安全漏洞的隐患。利用这些安全漏洞,掌握了相关技术的不法之徒只需一部智能手机,就能控制人体内的植入式医疗设备,从而杀人于无形之中。这并非科幻小说的场景,美国安全专家认为,在不久的将来,智能手机的确可能成为“杀人武器”。

在不久的将来,不法分子可以利用智能手机控制人体内的植入式医疗设备,神不知鬼不觉地夺人性命

A 手机程序 “出卖”病人的身体

2011年10月,几十名科技爱好者聚集在澳大利亚墨尔本的洲际大酒店,观摩总部设在美国西雅图的IOActive电脑安全公司的最新研究成果。来自该公司的研究人员巴纳比·杰克展示了一种巧妙的谋杀他人的新方法,由于担心被别有用心的人利用,杰克特地在讲解时掩盖了很多细节。此外,杰克还要求人们在观看展示时不要拍摄任何照片。

杰克的研究跟心脏起搏器和植入式心脏复律除颤器有关,超过300万名美国心脏病患者植入了这些小型电脑设备,它们能监控患者的心跳,在需要时发出电流来稳定患者的心跳。为了检查和调试这些设备,很多医生使用无线设备来遥控,这是一种看似安全的方式。

但是现在,杰克展示了如何用一种定制的发射器来遥控这些心脏植入设备,这种发射器可以在10米以内的地方发出遥控信号,这些信号跟心脏植入设备的生产商配备的遥控器的信号没什么差别。接到假冒信号的指示后,心脏植入设备可以突然发出830伏特电流,让心脏病患者立即死亡,而且人们很难发现他是被谋杀的,可能以为是一起设备出错引发的悲剧。

这并不是巴纳比·杰克第一次研究新颖的谋杀方式,2010年他曾向人们展示如何通过无线设备遥控植入式胰岛素泵提供致命剂量的胰岛素,从而杀死植入者。此外,2009年他曾入侵一台银行自动取款机的系统,让它自动吐出大量钞票。杰克看起来像是个喜欢制造麻烦的人,但却是IOActive电脑安全公司花钱雇他这么做的。在研究过程中,杰克对智能手机日益强大的威力产生了特殊的敬畏。恐怖分子已经使用手机在伊拉克和阿富汗引爆炸弹了,但杰克认为随着科技的进步,在不久的将来智能手机很可能成为一种新的谋杀工具。

杰克表示,现在他需要用特制的工具来操纵植入人体的医疗设备,但在不久的将来智能手机就能做到这一点。事实上,花个几分钟在网上搜索一下,你就能发现有几十家企业在研发医疗设备的智能手机应用程序,比如心脏起搏器、心脏复律除颤器、电子耳蜗、胰岛素泵等等。

对工程师们来说,医疗设备的智能手机应用程序有明显的优点:智能手机可以持续将病人的数据传给医院电脑;医生可以通过远程遥控改变治疗方案,无需再让病人专程来一趟医院;如果医疗设备哪里出了问题,医疗专家们可以通过远程遥控立即得知并对设备进行调试。

但不幸的是,对杰克这样的人来说,医疗设备的智能手机应用程序的缺点同样明显,比如医生不是唯一可以掌控应用程序的人。智能手机将病人的身体跟医生的电脑“连接”起来,但同时它也是跟互联网相连的,这就意味着其他智能手机也能共享这个“连接”。智能手机应用程序可谓将一个人的身体器官交到了地球上的每个黑客、网络骗子和数字暴徒的手上。

新科技的普及也意味着它们会被图谋不轨的人掌握,迄今为止,大部分网络犯罪跟金融和人的名誉有关,网络骗子偷取金钱、挖掘隐私,但很少牵涉到人身伤害。不过越来越多的植入式设备必将拉近网络犯罪跟每个平凡人之间的距离。

B 电脑网络 给坏人以可乘之机

大型电力和电话网络长期以来一直被电脑网络控制,但现在类似的电脑网络也日益应用于电表、闹钟、电冰箱等日常用品,因此它们很快也能被远程控制。目前市场上的每辆汽车都有内置电脑设备,很多这样的设备都能从外部被接入。

从2007年起,美国的每辆新车都要配备轮胎压力监测系统,电子传感器会将轮胎的问题传达给车载电脑,车载电脑就会令仪表盘上的警告图标开始闪烁。这一系统固然提高了汽车的安全性,但同时也为坏人提供了可乘之机。除此之外,如今每辆汽车上都有电子控制系统,指挥和监控汽车的方方面面,而这些系统使用的软件在编码上有惊人相似,因此很多软件都能轻而易举地从外部被控制。汽车的电脑系统变得越来越复杂,InterTrust 科技公司的一个安全研究小组表示,现在的汽车每时每刻都暴露在网络环境之下,跟电脑、平板电脑、智能手机没什么差别。

轮胎压力监测系统就是一个例子,它通常由4个传感器组成,每个传感器跟一个轮胎气门阀相连接。当车轮开始转动时,传感器被启动,通常它们每分钟都会将轮胎的运行状况报告给监测系统。每个传感器在报告时都会使用其特有的识别号码,每个轮胎都有特定的识别号码。2010年,美国南卡罗来纳大学的研究者们发现了能在约40米远的地方解密轮胎识别号码的方法,这就意味着,如果有人拿着可以解读轮胎号码的设备,就可以在40米以内的范围内跟踪任意一辆车,每个轮胎都会变成自动追踪装置。

世界上最大的轮胎压力监测系统生产商施拉德电子曾公开嘲笑南卡罗来纳大学的这项研究,该公司称通过轮胎来追踪汽车“不仅不实际,而且几乎不可能”,并强调轮胎压力监测系统是安全可靠的。这无疑激起了安全专家们的斗志,一年之后,华盛顿大学和加州圣地亚哥大学的研究者们就成功入侵了轮胎压力监测系统。他们在实验中追踪汽车,录下车中人的谈话,启动上了锁的汽车,这所有的一切都是通过入侵了汽车网络的智能手机发出的指示完成的。

反病毒公司麦卡菲的首席技术官斯图亚特·麦克卢尔表示,这种安全漏洞是无法阻止的,美国政府不管这个,安全全部依赖于生产商,大约90%的生产商对安全漏洞问题并不重视,就跟电脑软件公司一样,直到大量信用卡信息被盗用,才引起软件公司的注意。“我们生活在一个反应社会里,”麦克卢尔说道,“坏事发生后人们才会认真对待它。或许只有当植入式电脑被当作杀人工具并夺走数条人命之后,才会引发足够的重视。”

C 科技潮流 提供便利,也带来威胁

奥巴马的经济刺激方案提供45亿美元实施“智能网络”项目,其中就包括给数以百万计的家庭装上智能电表,而欧盟则启动了到2022年全面使用智能电表的计划。智能电表可以让电力公司实时监控每个家庭的用电量,它会随时将数据上传至网络,不过与此同时,它也提供了巨大的安全漏洞。由于智能电表记录了家庭用电量的实时变化,也就意味着,它监控了家里发生的一切。通过研究一个家庭的智能电表记录,美国马萨诸塞大学研究者们就能推断出这一家有多少人口,他们什么时候使用电脑、咖啡机、烤面包机。

跟个人电脑一样,智能电表电脑也容易受到病毒等威胁。早在2009年,IOActive安全公司的迈克·戴维斯就能通过类似病毒的编码来感染智能电表。受到感染的电表还能将病毒传染给附近的电表。从理论上来说,智能电表病毒能让整个社区的电表都陷入瘫痪,也能感染智能电表公司的中央控制系统。而普通人通常不会察觉自己家的智能电表能带来什么威胁,同样地,也不会觉得新的通过智能手机或平板电脑就能控制的温度、安全和照明系统有什么威胁。然而事实上,有网络系统的地方,有就漏洞。

如今,将电脑技术应用到任何事物上已成为不可阻挡的潮流,但生产商和消费者都没有考虑到这样做的潜在威胁。当然,现在这些威胁距离人们的生活还有一定距离,现在只有高级专家才具有利用这些安全漏洞的技术。但使用简单化和普及化是电脑软件的本质,在20世纪80年代,优秀的计算机科学专业学生罗伯特·T·莫里斯制造第一代网络蠕虫病毒花了几个月时间,而现在,制造病毒所需的技术和时间越来越少,网络安全威胁则随之增长。

巴纳比·杰克已经研制了Electric Feel软件,它能在人群中扫描到植入式医疗设备的存在。尽管杰克声称,创建该软件只是为了研究目的,但如果落入不法之徒的手中,它将造成严重后果。在美国,目前约有2000万人体内植入了某种医疗设备,随着人口老龄化,这个数字只会继续增加,而能被智能手机接入的这些医疗设备的数量也会增加。智能住宅、智能汽车离人们的生活越来越近,而它们所带来的威胁亦是如此。这些由电脑系统控制的设备,黑客往往能轻易利用它们的安全漏洞,通过智能手机就能远程操控。

一名安全专家表示:“10年之后,电脑将无处不在,并且它们将无线连接。你将能通过某个人的汽车来危害他植入体内的胰岛素泵吗?你将能通过破坏某个人家里的照明系统来诱发他急病发作吗?你将能使用智能手机来运行这些漏洞吗?也许在不久的将来,没有什么是不可能的。”

现代快报记者 李欣 编译