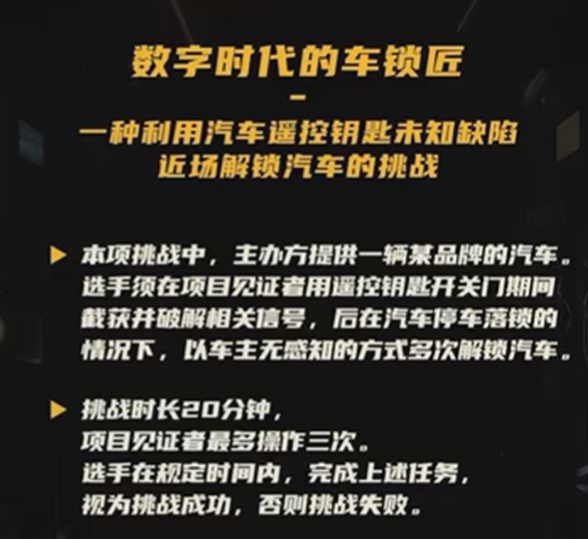
**GeekPwn**

**——202赵一谦**

**近日，GeekPwn 2022国际极客破解大赛在上海落下帷幕。GeekPwn与Pwn2Own、Defcon并称世界三大黑客赛事，是全球最大关注智能生活的安全极客大赛，每年吸引着众多极客团队参与，聚焦前沿AI安全、机器人安全、智能生活安全与产业安全等领域，揭示了诸多未知漏洞，为行业安全防护提供了有效支撑。截止2021年，GeekPwn已负责任地披露了近千个高危漏洞。**

**而作为区块链金融社区的一员，我们当然需要时时刻刻关注这些安全问题，所以我就去了解了一下。往年GeekPwn比赛有很多让我印象深刻的选手和项目。如14年破解特斯拉，可以远程控制汽车移动。15年破解pos机，无限刷卡。17年传奇女黑客tyy破解四款共享单车。**

**其中，我最感兴趣的一个项目就是数字时代的车锁匠，规则简单来说就是主办方提供两辆不同品牌的汽车。选手需要在车主，遥控钥匙开关门的期间，截获并且破解车钥匙的信号。在汽车上锁之后，用车主无法察觉的方式多次解锁汽车。**



**看完之后，我总结了一下破解思路。现在的汽车都是通过远程按开关解锁车辆，这是远程无钥匙进入系统，也叫RKE。当我们按一下钥匙之后，它就可以发出开关车门的信号了，十分方便。但是方便也会带来隐患。低端的RKE系统发送器每次发送的时候，都会发送一个固定的识别码，这些识别码往往就是一些比较小的简单的一些数字。只需要在你旁边捕获这个信号,然后重新把这信号回放一下，就可以把车开走了。而且它基本都是一些较小的数字，就算我们用暴力破解，不断去试，也可以破解出你的识别码，然后也可以把你的车开走。**



**后来汽车厂商进行了升级，发明了一种叫滚动码的东西。滚动码的工作原理就是车钥匙里面存了当前的滚动码，当用户按下钥匙的瞬间滚动码会附加上一个功能码（就是你开门还是关门）一起发给汽车。汽车里面也有一个滚动码，滚动码匹配上了，就会执行功能码，如果不匹配他就不执行任何的动作。车钥匙和汽车里面的滚动码始终是保持一个同步。假如我的车钥匙被误触了几次，那车钥匙里面的滚动码就会向前推进好几步。这个时候就跟车里的滚动码不同步，这种情况下汽车其实是允许接收后面指定数量的滚动码，只要你在这个发送的窗口之内，他认为都是有效的。成功接收之后汽车会把滚动码重新同步一遍。在2015年的Defcom上，有个黑客就分享了一个简易的攻击系统叫ROW键。当车主首次按下钥匙的时候，ROW键就会利用无线电设备发送噪声干扰，而且会拦截你的第一次解锁的信号，同时他还会把你的第一次解锁信号给保存下来。车主就就没有办法解锁车辆，于是车主会在按一次解锁键在第二次的时候 ROW键会再拦截这个信号然后把第一个的信号给车发过去这时车会解锁。但车主不知道这个过程，车主的第二次信号已经被那个简易的系统给保存下来。ROW键是永远的把你上一个信号，给你的车先拦截掉，然后给你的车发过去，然后再保存你的下一个信号，因为下一个信号是没有被使用的，所以可以随时利用这个信号去解锁车辆。**

**2021年的RollBack也提供了一种破解思路：** **当受害者首次按下钥匙按钮时，RollBack设备发送噪声拦截信号Unlock1，与此同时截获该信号。当首个信号遭到拦截未能解锁车门时，受害者极大概率会再次尝试。在第二次按下钥匙按钮时，RollBack不会拦截信号Unlock2，只会捕获它，因为车辆顺利接收到了Unlock2，车门被解锁了。接下来，车主如往常一样使用车钥匙开锁、关锁，可能会重复 n 次。接下来攻击者控制 RollBack设备重放之前捕获的两个连续“解锁”信号 Unlock1和 Unlock2，当重放Unlock1时，车门还是处于锁定状态，但是重放Unlock2 之后，车门被打开了。可以发现在攻击者重放了连续的两个滚动码之后，车辆中的滚动码计数器重新同步到了之前的滚动码n，因此会响应 n+1 次发送的命令。RollBack 成功利用一次后，它还可以根据需要再重新利用多次，而无需从头开始重做任何事情。简而言之，一次捕获两个信号，就可以无限期地访问该车辆。**