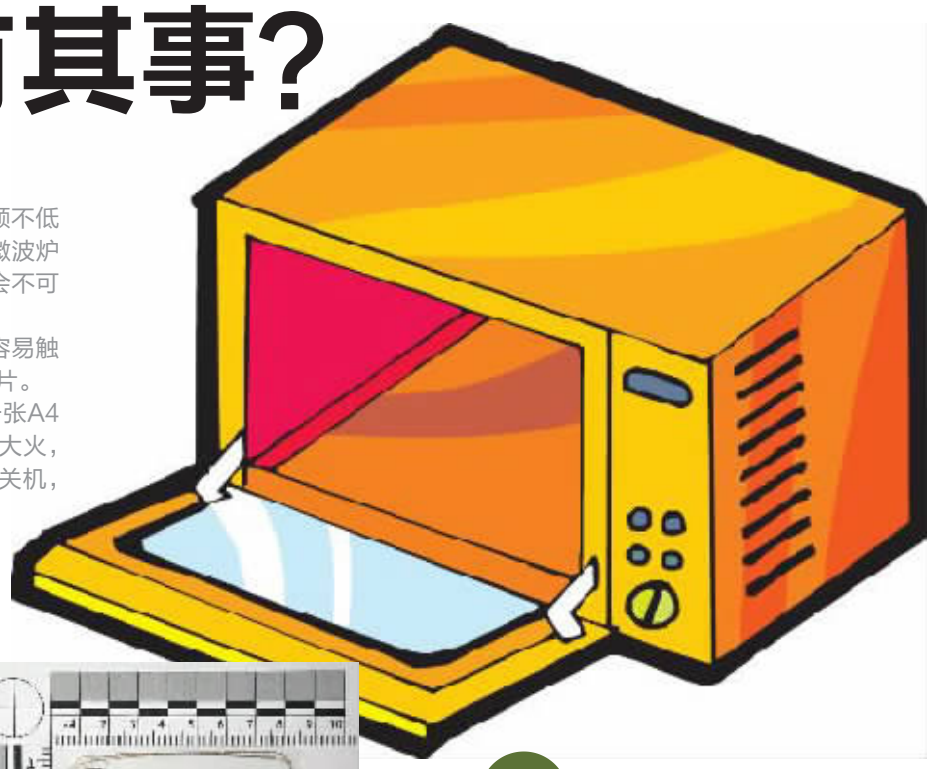
微波炉“叮”5秒，公交卡余额变百万 是传说还是确有其事？



最近小编在网上发现一个应该是来自香港的帖子，其宣称将一张余额不低于300元的八达通（香港公交卡）放入微波炉中用最大火力“叮”大约5秒，微波炉所产生的电磁波就能影响八达通内的数据芯片，造成数据溢位，最终余额会不可想象地增加，成千上万都没有什么困难。

保证卡中余额300元以上的目的是为了占用芯片中更多的内存，更容易触发数据溢位。帖子还附上了一张余额高达380万的八达通闸机提示信息照片。

无独有偶，内地论坛也流传着类似的说法，不过略有不同。首先，拿一张A4纸或者报纸，将公交卡包裹起来，要确保两边都是3层，放入微波炉，档位：大火，定时25秒。然后开机，发射电磁波，电荷累积，金额增加，时间到了请立即关机，到此，充值成功。

是个彻头彻尾的恶作剧

对于这些说法，有必要切实求证一下。两种说法中都有提到一个很关键的词语“电磁波”。实际上，公交卡是属于非接触式IC卡（即集成电路卡）。

而手机上用的SIM卡、早期的公共电话卡和新一代的银行卡这种有裸露触点的，则属于接触式IC卡。公交卡这类非接触式IC也的确是通过电磁波进行无线通讯的。

这么看来，微波炉从最基础的原理上来说的确是可以影响到公交卡的，难道这个说法不是谣言？

但又有人指出了，公交卡是属于RFID卡，通常的工作频率在13.56MHz，而微波炉所产生的微波频率高达2450MHz，根本就是跟荷兰人讲河南话的状态。

RFID卡又是什么？不是说公交卡是非接触式IC卡吗？到底IC卡和RFID卡是什么关系？

RFID全称radio frequency identification，中文学名射频识别，可以说大部分RFID卡基本上也都是非接触式IC卡，二者并不冲突。

RFID技术应用范围很广泛，除了可以作为消费卡之外，也常常作为物品的电子标签，在相当大的电磁场范围内都能有效地被识别。

著名的运动用品超市迪卡侬就采用了RFID技术，将RFID线圈芯片封装在衣物的内衬标签里，收银结账时将商品放置在特定的区域内就能准确地识别出商品的信息，不需要激光扫描条形码这样繁琐的步骤。

其实，微波炉充公交卡的都市传说是个彻头彻尾的恶作剧。把公交卡放进微波炉，微波作用于卡内的芯片，瞬间起火，管你什么牛鬼蛇神，卡内余额多少，通通轰杀。

退一万步说，就算用的是专业的RFID读写设备，也并不能随意读取修改公交卡。

公交卡所用的Mifare系统十分有保障

公交卡一般采用飞利浦电子公司（现已更名为恩智浦半导体公司）的Mifare解决方案，通信频率为13.56MHz，用户所用的卡片内包含天线和芯片。

使用最广泛的是Mifare Classic 1K卡，Mifare系列卡片拥有一定的储存空间，用于储存余额信息和最近的通讯记录。公交卡不记名、不挂失、不补办，充值需要通过设备写入信息，基本上都是将余额信息储存在芯片中，而扣费所用的读卡机只记录资费的变化值，上传服务系统。

相比之下，银行卡内的芯片则不记录余额信息，只存有账户身份验证信息，账户余额信息都存储在银行系统网络中，修改这些余额信息难度不亚于攻破NASA。

如果单纯从通信原理上来看，公交卡又的确是能被非法充值的，可是为什么我们几乎很少听到有类似的犯罪案件发生呢？

实际上公交卡所用的Mifare系统安全性还是十分有保障的。读写机在读取卡片时，先会向卡片发送一段请求信息，卡片中的天线收到信息向读写机发送随机数，二者通过特定的密钥运算，比对结果最终验证其合法性后，才能读取和修改卡内信息。

所以，并不是什么机器都能够读取和修改公交卡的，只有知道对应的密钥与算法才能够操作。

所以说，Mifare公交卡不仅不可能被什么微波炉、电磁炉、电吹风这些东西轻易改写，而且安全性还相当高，是一种十分可靠的解决方案。

链接

曾有高中生破解Mifare饭卡，修改余额

2008年，一位德国的研究员和美国弗吉尼亚大学计算机的博士合作用电脑成功破解了Mifare经典芯片，也是十几年来全球应用范围最广的IC卡芯片，顿时引起了各国的恐慌。

甚至有高中生用简单的设备就能破解学校的Mifare饭卡，修改余额至上万，成为“饭堂王思聪”。

实验工具有：电脑一台、ACR122U-A9 Mifare读写器一台、带NFC功能的手机一台，Mifare Classic Tool（简称MCT）软件、饭卡一张。

首先在手机上安装有MTC软件，开启手机NFC，尝试用软件自带的默认密钥访问饭卡。

NFC功能实际上是RFID的衍生产品，除了可以模拟成被动的RFID标签外，还可以读取RFID标签、甚至是点对点传输。

此处用手机NFC简单尝试可判断饭卡的加密情况。

小哥发现他学校的饭卡并不是完全加密的，有部分扇区（逻辑储存分区）仍然采用默认的密钥，可以采用验证漏洞进行破解。

简单来说，就是访问未加密的扇区，通过与卡之间数据交换的加密算法反推出其他扇区的密钥。破解出所有扇区的密钥后就如同将饭卡扒光了一样，可以顺利进行下一步工作。

接下来就是对卡中的十六进制数据进行解析，确定每组数据的功能。比较繁琐的是需要在修改数据后再到饭堂的刷卡机验证数据的功能，需要多次尝试才能将所有数据的作用弄明白。

最终成功破解学校饭卡，不仅拥有上万的余额，还能拥有各种拉风的名字。

虽说成功修改了饭卡中的数据，但这并不意味着万事大吉，因为计费系统中的数据异常必然会泄露出非法的行径，甚至可以通过卡中的身份信息追查到始作俑者。

■据SME