当心密码出卖了你

◎“对称密钥”如何成为二战日军的催命符
◎密码专家为什么热衷破解同行弄出来的密钥
◎预防黑客,我们能做些什么

不知你是否看过一部名为《窃听风云》的电影?它似乎预言了个人通信安全危机的悄悄降临。

2009年底,德国计算机专家诺尔博士正式宣布破解了GSM制式手机的通信密码a5/1,并公开了破解方式。如今,你甚至不需要任何一件电影中那般专业的器材,而只需要下载一个软件,再购买一台滤波器,就可以轻易窃听到身边GSM制式手机的通话。

这样“耸人听闻”的开场白一定让你感到不安,不过可能更让你感到无奈的是:GSM在通信中使用的密钥其实早已经被解开了,对于业界来说,这早已不是一个新闻。可能你的通话在你不经意间早就被人窃听。而且,受到波及的不只是手机通话,你平时浏览的网站、写的电邮,甚至网上购买的商品的信息,都会以明文的方式在他人眼皮底下流过。在不安全的信息传输过程中,你的个人信息会被人窥视得一清二楚……

密码本是保护我们个人信息不致泄露的一种手段,但现实有时正好相反 资料图片

什么是“对称密钥”和“不对称密钥”

说到密码破解技术,我们首先要明白密码的含义。在当代社会,数字通信技术被广泛应用,而有数字通信的地方,就有密码技术。个人隐私、商业机密和国家安全,都建立在高度发达的密码技术之上。简单地说,密码技术是将可理解的信息变换为一般人不可识别的信息,同时又可复原原信息的技术。

一个没有学过莫尔斯电码的人听到“滴答”声只会觉得是噪音,而懂得电码的人则能从滴答声中获得信息量巨大的情报。电影《风声》中所描述的,就是利用莫尔斯电码来传播暗杀命令的场景。而孩童时期的我们为了迷惑父母和老师,常将出去踢球说成“去补课”的行为,也同样可以被认为是一种密码设定,事实上,这就是最简单的加密。

明文信息变换为加密信息的过程,称为“编码”或“加密”;复原密文的过程,称为“译码”或“解密”。而编码和译码的关键就在于加密的方式,如同开锁的钥匙,称为“密钥”。

密码的初衷是为了保护我们的隐私,但随着破解手段的成熟,它倒可能反过来成为出卖你的罪魁祸首。二战时,美军正是因为破译了日军的电码密钥,才能在太平洋战场上屡屡占得先机。虽然其最主要的原因是美军打捞到了日军的密码本,进而通过密码本破解了电码;但更深层的原因是日军加密与解密使用的是同样的密钥——这种收发密文双方使用同样密钥的模式,称为“对称密钥”。其缺点很明显:一旦任意一方泄露了密钥,加密信息就形同虚设。

“对称密钥”还有一点不安全,在于通信双方无法鉴别对方身份。比如美军在破解日军密码后,便可以伪装成日军部队与本部及其他部队通信而无法被发现。为了克服这一缺陷,专家们提出了“不对称密钥”。与对称加密技术不同,不对称加密技术在加密解密中使用两种密钥,一个称为“公钥”,另一个称为“私钥”。两把密钥互为补充,一个负责加密,另一个就负责解密。用公钥加密的信息,只有用私钥才能解密,反之亦然。而由于“私钥”与“公钥”具有方向性,所以可以很容易就确认通信双方的身份。

“万能钥匙”与破解方法

由于技术限制,在GSM制式最初的研发中并没有采用不对称密钥,而是使用了对称密钥进行鉴权(确认身份)与通信。鉴权的加密方式由于SIM卡克隆技术与“黑手机”技术的出现已经形同虚设,其本身并不需要破解密钥,只需要复制信息即可;只不过,盗用身份的技术其实并不用于窃听,而主要用于盗窃话费。另外,技术专家也有相应的防范措施。

而对通信的加密建立在两个前提之上:首先,通信的加密方式是建立在鉴权基础之上的;其次,通信与鉴权的加密方式是不同的。每次发起通话时,GSM网络都会根据手机密钥生成一个临时的通信密钥,而诺尔博士破解了这个生成临时通信密钥的变换程序,换句话说,从此,任何人都可以手拿“万能钥匙”打开GSM通信的大门。

为了防止这种手拿“万能钥匙”到处闯空门的做法,密码专家在不对称密钥的基础上提出了“数字签名”,加入了数据验证环节。数字签名技术除了使得保密性更高、身份验证更完备以外,用户数据的完整性也得到了保障。这就杜绝了黑客在数据传输过程中虽无法破解加密,但能够恶意篡改密文而导致译码失败的情况。因此,数据签名获得了在法律上与签字画押同样的效应。而你在生活中可能早就接触过这个名词:在网上购物,或是在手机上安装软件时,都会跳出“数字签名”的窗口要求你确认。

窃取信息、破译密码技术的日益更新,让人们防不胜防 资料图片

跟你聊天的好朋友可能你并不认识

但数字签名也不完全是安全的。数字签名检验信息完整性最常用的算法是MD5函数,这是上世纪90年代麻省理工学院开发出的一套校验算法。无论数据的大小如何,MD5函数都能将其变换为一个唯一的固定长度的数值,如同一个人的指纹,具有独特性。经常下载软件的人大概都知道,为了鉴别软件是否曾被第三方更改,发布方都会提供一个MD5的校验码,哪怕对软件进行一个字节的改动,都会导致MD5校验码改变。

但在2005年的国际密码年会上,来自中国山东大学的王小云教授提出了MD5算法的漏洞,并对其进行了破译。这一漏洞最直接的后果就是,两份不同的文件可以得出同一个MD5校验码,而这时,数字签名就失去了作用。在信息已经被修改的情况下,身份是否能被确认已经不重要了——即便进入了房间也毫无意义,因为你连房间都进错了。

更糟糕的是,由于MD5算法的广泛使用,结合普通密钥,它可以直接被用来作为“鉴权”的方式,而不必再用复杂的“数字签名”中的特殊算法。当你登录邮箱输入密码时,系统后台会使用MD5算法来校验你输入的密码信息,但这并不是明文表示的;而当你忘记密码时,管理员会发给你一个随机密码,不过管理员自己却看不到这个密码,因为他只能看到MD5计算后的校验值。GSM制式被破解的部分是密钥,而王小云教授的算法不能看到信息的明文,但却能伪造身份。设想一下,当你认为你在与最好的朋友聊天的时候,对方实际上却是你不认识的人,这有多可怕。

“绝对安全”并不存在

但并非所有黑客都能像王教授这样,在算法的基础层面上将整个密码系统彻底动摇。更多的时候,他们的做法并不触及密钥,而是采用更经济,技术手段更低的方式来危害用户安全,这才是绝大多数信息犯罪惯用的方式。这些黑客大多利用系统漏洞,采用字典破解法与穷举破解法来获得用户的密码,进而获得操作权限与有价值的信息来进行犯罪。要预防这样的手段,除了使用正版系统并第一时间升级外,还要注意自身的密码保护。

归根结底,由人所设计的密码必然会被人所破解。在密码学中,完全的安全称为“无条件安全”,是指密文透露的明文信息不够多,而导致无法从密文确定到唯一的明文。这就像是破译古代文字,若是没有一定的确定解读方式,那么便可以有无数种解读方法,只不过,这些解读结果几乎没有意义。而密码学家比较关心的是第二种安全——“计算安全”,这是指在一定的计算条件下,密码在一定长的时间内不能被破解。但随着电脑技术的发展,计算速度已经完全超出了人类的想象,a5/1密码在问世之初,曾被证明使用一台电脑得花上10万年才能计算出密钥,然而诺尔博士只用了80台电脑在3个月内就将其破译了。

或许你会对诺尔博士或王小云教授这样的密码专家提出异议:为什么要去破解密钥或算法?实际上,以GSM制式通信加密技术被破解为例,早在上个世纪就有人破解了当时GSM通信中较弱的a5/2算法,从而迫使各移动通信运营商使用了更强的a5/1算法;在这之后又有组织提出了未公开的破解方式,不过,这种新式的不公开破解方式让GSMA(制定GSM标准的国际组织)及运营商无从下手,而正是诺尔博士的公开破解让我们有了补救机会。王小云教授等专家提醒了我们:密码使用中总有被忽视的环节,正如同没有绝对的盾一般,绝对的安全也是不存在的。

李世一/文 摘自《环球》杂志

»链接

破译美国政府密码的中国高手

在2008年12月举行的“中国青年女科学家奖”颁奖典礼上,由18位来自中科院和中国工程院的院士组成的评审委员会,将奖项授予清华大学和山东大学的双聘教授王小云,以表彰她在密码分析领域作出的杰出贡献。

王小云是一位解码高手,十年内破译五部顶级密码。

2005年,在美国加州圣芭芭拉召开的国际密码年会上,王小云宣布她的研究小组已经成功破解了MD5、HAVAL-128、MD4和RIPEMD四大国际著名密码算法,掌声经久不息。几个月后,她又破译了更难破译的SHA-1。

MD5由国际著名密码学家、美国麻省理工学院的R. Rivest教授于1991年设计。MD5密码算法的运算量达到2的80次方,即使采用现在最快的巨型计算机,也要运算100万年以上才能破解。但王小云和研究小组用个人电脑,几分钟内就可以找到有效结果。

SHA-1密码算法由美国专门制定密码算法的标准机构美国国家标准与技术研究院与美国国家安全局设计,早在1994年就被推荐给美国政府和金融系统采用,是美国政府应用最广泛的密码算法。《崩溃!密码学的危机》,美国《新科学家》杂志用这样的标题概括王小云里程碑式的成就。因为王小云的出现,美国国家标准与技术研究院宣布,美国政府5年内将不再使用SHA-1,取而代之的是更为先进的新算法,微软等知名公司也纷纷发表各自的应对之策。

设计一种新密码大约需要8年,破解需要10年左右,密码学就是在这种不断的创立和破解中发展的。世界密码学界早已开始新密码的设计工作,预计到2012年新一代安全密码将产生。

虽然现在是信息时代,密码分析离不开电脑,但对王小云来说,电脑只是破解密码的辅助手段。更多的时候,她是用手算,手工设计破解途径。