如何让我们的密码更安全?

个人信息安全 之 揭秘

“请输入账号密码……”这个我们在众多网站司空见惯的模式,一不小心,就成为出卖我们信息最大的凶手。伴随着互联网诞生第一天就出现的个人密码,在今天依然是普通用户、网站管理员和黑客之间斗争的永恒对象。如何保证密码不被黑客盗取?没有最安全的密码,但我们至少可以让自己的密码变得更安全。

泄密探因
密码要经过一段旅途

为什么会发生如此大规模的密码泄露事件?中国软件评测中心高级工程师朱璇表示,问题出在两个方面,使用者的密码设置过于简单,网站管理出了问题。

当我们登录一个普通网站时,密码要经过这样的一段旅途:我们先在键盘上输入密码,网站将其上传到服务器,然后在服务器中保存,当我们丢失密码时,需要通过某种验证才能重新获得密码。

这每一个环节,都可能被黑客攻击,获得密码。

在输入密码阶段,黑客只需攻击个人计算机终端,当计算机中了木马病毒时,键盘里敲击的密码就可能被黑客截获,病毒也可能搜索计算机文件,获得里面和密码相关的信息。

在密码上传阶段,朱璇表示,密码信息上传到服务器,这段旅途虽短,但很多网站,包括一些论坛,都没有把密码明文加密的习惯,成为黑客攻击的薄弱环节。

如果上传的密码过于简单,也很容易被黑客用“暴力攻击”的形式获得,最常用的是“词典式攻击”。黑客手中会有一个海量密码的词典,如果用户使用简单的信息,如姓名、生日、电话等,黑客可以设计一个小程序,计算出来。因此,很多网站在登录密码页面会使用验证码,防止电脑的词典式攻击。

服务器保存
明文保存密码相当危险

密码到达终点,即网站服务器,它的保存方式也被黑客盯上。此次密码泄露,就是因为很多网站以明文形式保存用户的密码,而没有任何加密,当黑客攻击进入服务器后,就可以直接看到裸露的密码原文。

果壳网“死理性派”主编吴苏介绍,明文保存密码相当危险,黑客只要获得了密码数据库,再复杂的密码,都可以看到。

他介绍,现在网站服务器已经有了很普遍的加密方法,叫做哈希函数。比如,英文里“狐狸在冰上跑”和“狐狸在冰上走”两句话,通过哈希函数一转化,很快变成了完全让人摸不着头脑的组合“52ED879E”和“46042841”。

但即使用了哈希函数加密,也不代表无懈可击。

密码分析学家阮风光说,如果一串被哈希过的密码被盗,只要密码过于简单,黑客同样可以获得。

通常,黑客手中,都有一份很长的列表,称为“碰撞库”,里面储存的是很多常用密码对应的哈希值。朱璇介绍,现在网上有专门的网站对哈希值进行破解,根据密码难度进行收费。“比如要破解admin123,属于最常用的前1万个密码,你只要花1毛钱,如果密码是123456,就可以给你免费破。”“万恶之源是密码过于简单。”朱璇说。

密码矛盾
安全和便利不可兼得

“互联网安全问题分成管理层面和技术层面,密码安全横跨两个层面。”朱璇说。

对于网站而言需要考虑的安全因素太多了。比如,开发代码中是否存在漏洞,服务器所处的地理位置是否足够安全,服务器是否有密码,操作系统是否打了补丁,等等,任何一个环节出了漏洞,其他环节再安全,也可能被黑客攻进。

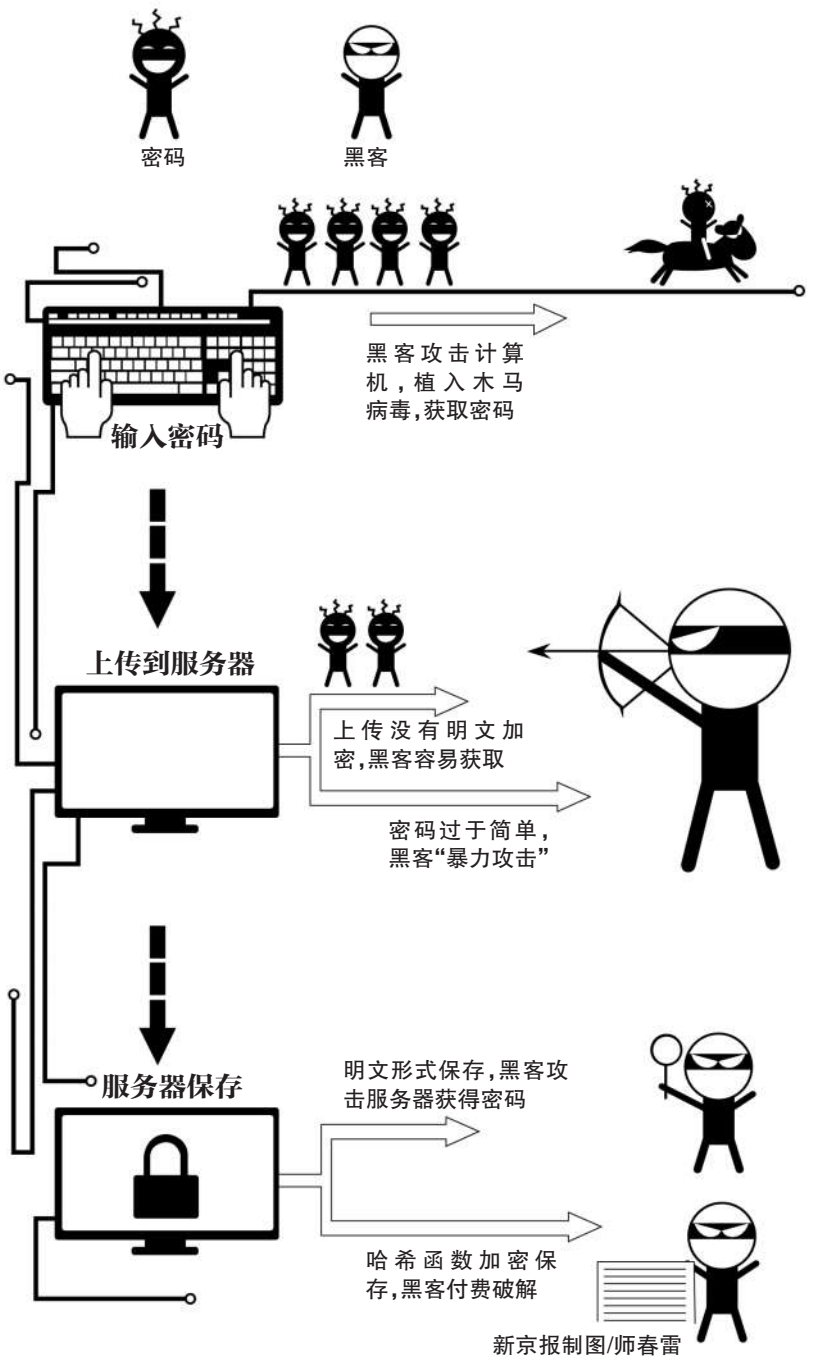
“一切都是需要花钱的,”阮风光说,“比如你要在服务器中对密码进行加密,就可能需要雇用有安全背景的人来写软件。”

目前,科学家和工程师们也在尽量让身份识别变得更为容易,如生物指纹、或视网膜鉴别等等方式,但即使这些额外的保护措施,同样需要花钱。“人们得意识到,更高的安全度,就意味着更多的钱。”阮风光说。

他表示,计算机科学技术发展到今天,人们也一直没解决密码安全性和便利性的矛盾,始终没有完美的解决方式。原则上,密码越长,越安全,可是也越难记住,哪怕记在电脑或者纸上也是不安全的。此外,用户如果在不同网站使用不同的密码,也更安全,但是却很不方便,很难记住这么多的密码。“要安全,就得舍弃方便,要舍弃麻烦而图便利,就可能不安全。”

本报记者 金煜

密码之旅:每个环节都可能被攻击



新京报制图/师春雷

■ 密码防盗指南

1	有足够的安全意识,避免在社会层面受到密码诈骗。
2	不同安全等级的网站设不同强度的密码。对于网银等和个人利益直接相关的网站,一定要设置超强的密码。
3	测试网站的密码安全性,在注册一个网站时,如果你输入密码“123456”也能通过,这个网站肯定不安全。同样,对密码长度没有要求,不能使用特殊字符,或者无法区分大小写的网站的安全性能也不高。
4	减少使用常用的个人信息,尽量不用自己的生日作为密码。尽量使用和自己个人信息不相关,或者距离远的信息。
5	利用经典密码学,设置自己的加密“函数”或规律。比如,你可以选取“不管三七二十一”,抽出其中的数字“3721”,对个别数字进行替换或移位,把“7”变成英文字母中的“L”,把“1”变成英文字母“i”,变成“3L2i”,这样,密码就稍微复杂一点。
6	多组合密码。搭配各类数字、字母、大小写、特殊符号的组合,比如一个10位长的随机密码,由于常用键一共有95个,因此一共会有(95的10次方)种组合,较难在短时间内被“暴力”破解。你可以把“3L2i”加上符号变成“3#L*2 i#”。
7	在你的密码“3#L*2 i#”和另一个人的密码“123456”之间,黑客肯定首先盗取后者的密码,一旦一个网站的密码发生泄露,你可以比有着简单密码的后者拥有更多的时间进行密码修改。
8	最后,隔一段时间,换一下自己的密码,总是能让密码更安全的。

■ 历史

互联网开创密码伴生

“互联网开创第一天,就有了密码。”清华大学高等研究院访问学者,密码分析学家阮风光说。上世纪60年代,互联网雏形初现,当时的计算机体形庞大,一台就占据整个机房。

由于每台巨型计算机被很多人共享,为了辨别不同用户身份,需要设置密码,这也决定了此后互联网设置密码的目的:辨别使用者。

事实上,密码学要比计算机的历史古老得多。从古罗马时期开始,各国打仗时就常常使用密文形式来传输信息,二战时密码技术更是突飞猛进。今天,在小说如《达芬奇密码》中,我们也时常能读到让人心驰神往的密码破译故事。

中国软件评测中心高级工程师朱璇介绍,古典密码学主要有两个基本原理,即“移位”和“替换”,比如,将数字往后移一位,3变成4, 7变成8,或者将字母A换成D,都可以起到加密作用。

现代密码学建立在传统密码学基础上,但增加了大量数学、物理学、计算机科学的内容,其对当前互联网技术发展、军事及国家安全、以及商贸、金融等行业的发展起到了至关重要的作用。

■ 密码泄露案例

国外发生过多起严重的密码泄露案件。

1998年,互联网安全网站CERT发现黑客袭击了18.6万多个加密密码,其中,47642个密码被盗。

2009年,社交网站Rockyou.com发生严重密码泄露,3200万个密码被盗,其密码以明文形式在服务器上存储。

2011年,索尼公司连续遭受四轮黑客袭击,致使过亿用户信息泄露,这些个人信息中包括用户账号密码、电子邮箱、家庭住址、生日等信息。索尼公司公开致歉,美国联邦调查局介入。此事成为近年来最大的网络安全事件。

2011年,第一个推行网络实名制的国家韩国发生个人信息泄露事件。韩国青瓦台、外交通商部、国家情报院等国家机构等共40个网站遭到攻击,造成大量用户信息外泄。去年年底,韩国广播通讯委员会提交报告,将逐步取消网络实名制。

责编 颜颖颛 美编 李铁雄 责校 李立军