# 口令破解与防范技术研究

尚旭哲，王润田，孙颖，付瑜菲
（中国人民公安大学，北京 100038）

**摘 要：**随着计算机网络的不断发展和网络功能的日益完善，信息资源共享也愈发普遍，直接导致了信息安全保密问题突出、公民隐私权受侵害的风险大幅提升等一系列问题。因此，及时发现和应用信息安全维护措施尤为重要，口令安全作为信息系统安全的重要环节之一，是保护信息不受泄露的首道屏障。基于此，文章以当前口令保护研究现状为背景，通过对口令破解、口令加密以及口令安全的研究，总结归纳出行之有效的信息安全保护技术，力图为筑牢网络安全“防护网”建言献策。

**关键词：**口令；口令破解；口令加密；口令安全
**中图分类号：** TP393.08 **文献标识码：** A

# The research on password cracking and prevention technology

Shang Xuzhe, Wang Runtian, Sun Ying, Fu Yufei
(*People's Public Security University of China, Beijing 100038*)

**Abstract:** With the continuous development of computer network and the improvement of network function, the sharing of information resources is becoming more and more common, which directly leads to a series of problems, such as problems of information security and confidentiality, and the risk of infringement of citizens' privacy rights. Therefore, timely detection and application of information security measures are particularly important. Password security, as a part of information system security, is the first barrier to protect information from leakage. Based on this, based on the current research status of password protection, this paper summarizes the effective technology through the research of password cracking, password encryption and password security, and tries to make suggestions for building a network security "protective net ".

**Key words:** password; password cracking; password encryption; password security

## 1 引言

伴随着互联网时代的到来，计算机网络在即时通信、商业沟通等领域得以广泛应用，信息安全保密问题日益突出，公民在获得极大便利的同时面临着个人信息泄露的风险。如今的操作系统和常用软件都不同程度地采用了加密技术，密码的出现在一定程度上解决了信息的安全性问题，但是由于CPU运算速度与网络传输速率的不断加快，对于密码强度和加密方法的要求也逐渐提高。有矛就有盾，有人破解，就会有人防范。对于用户而言，最为有效的防范措施就是提高口令强度，即通过增加口令长度、采用非常规字符等方式实现口令的相对安全；对于系统而言，保证安全性就要安装和管理补丁，正确配置系统参数，及时升级更新系统，防止因系统漏洞造成的口令泄露、删除或修改。

在对口令安全进行分析论述之前，本文研究

人员认为有必要对口令的内涵进行了解。口令是由数字、字母、特殊符号组成的仅为被授权人所知的字符串。值得区分的是密码和口令两组概念，二者之间区别相对模糊，相较于密码而言，口令的长度较短、强度较低、更容易受到攻击与破坏。其实在一般情况下，可以忽略口令和密码的细微区别，视为同一概念处理。

## 2 口令破解方式探析

### 2.1 直接获取

直接获取即通过监听、木马等方法直接获取用户相关信息。有时获取的密码是经过哈希加密后的密文，这一部分将在本文的暴力破解中进一步阐释。

（1）木马入侵

特洛伊木马程序一般可以主动修改系统中的Telnet和login程序，以便将用户的账号和口令记录到一个文件中，然后将这个文件发送给黑客。由于木马在注入远程客户机时成为了计算机内部的合法程序，往往不易被管理者发觉。

（2）窥探监听

黑客利用与被攻击系统接近的机会，安装嗅探器或者对这些信息进行监听和窃取，从而获取账户和口令。黑客所使用的嗅探器通常只收取而不发送数据包，所以在检测过程中不易被管理员发现，对信息安全具有一定的威胁性。

（3）后门潜入

后门是计算机系统设计者预先设计的一种可以绕过系统已有安全设置获取访问权限的系统登录方法，以方便设计者在开发期间对应用程序和操作系统的调试和修改。通常在程序设计开发完成后，大部分后门会被删除，不过仍然存在少数后门遗留情况。这些后门具有很好的隐蔽性，为熟悉系统的人员提供了越过对方安全设置潜入系统进行信息窃取和破坏的方法。

（4）社会工程学

社会工程学在信息安全领域被誉为“一种让他人遵从自己意愿的科学或艺术”。当黑客将社会工程学应用于信息获取时，无须入侵目标系统即可实现。例如，某网站因系统漏洞，泄露了大量用户信息，黑客便可以通过这些信息得出用户在其他网站上的账号及密码，从而获取种种权限。

再如近些年兴起的电信诈骗案件，嫌疑人通过拨打诈骗电话、发送诈骗短信、构造钓鱼网站等一系列手段，充分利用被害人贪婪、恐惧等心理因素，套取其银行账户密码或胁迫其转账，这也是一种典型的社会工程学攻击。

### 2.2 暴力破解

（1）字典穷举法

当直接获取口令难以奏效时，黑客往往会利用字典穷举法实现系统入侵。即首先采用“Finger远端主机名”找出主机上的用户账号，然后根据用户的姓名、生日等信息生成一个字典，并从字典中选取一串字符作为口令输入远端主机，申请登陆系统。若口令正确，则进入系统；反之，程序将按照字典顺序进行尝试，直至发现正确的口令或者字典中所有字符串被尝试完毕。随着计算机CPU处理能力的增强，字典攻击成为最“简单便捷”的口令破解方法。如表1所示，针对不同组合数字符集，不同系统完成“攻击”所需时间不同且差异较大。

（2）哈希碰撞

由于哈希计算无法像函数那样实现输入与输出的一一对应，这就可能导致原信息经过哈希计算后得到同一个“代号”，这种情况被称为哈希碰撞。以MD5为例，一个MD5值由32个16进制数组成，也就是说所有的MD5值最多可以不重复地表示1632段不同的信息。假设现在有1632+1段互不相同的信息，根据鸽巢原理，这些信息中至少有一对信息的MD5值相同，即出现了MD5值的碰撞。

哈希碰撞在口令破解领域具有重要意义。如果黑客掌握了用户口令的哈希值，那么只需找到与其对应的哈希等价明文即可当作口令使用。并且如果服务端程序出现重大漏洞，还可能会出现哈希伪碰撞的情况。例如，在使用Php脚本的Apache服务器中，如果哈希值的比对采用的是双等号比较而非三等号比较，且比对的两边都是以“0e”开头的不同哈希值时，这两个哈希值会被

表1 各系统破解不同组合数字符集所需时间

| 时间 / 字符集 | 每秒攻击站点 10000 次的 Web 程序完成字典攻击所需时间 | 脱机使用高效率服务器或台式机完成字典攻击所需时间 | 大规模并行处理器集群完成字典攻击所需时间 |
|---|---|---|---|
| 6 个字符（无特殊组合），共 22.5 亿个组合 | 3.7 周 | 0.0224 秒 | 0.0000224 秒 |
| 6 个字符（有特殊组合），共 7.6 万亿个组合 | 2.4 世纪 | 1.26 分钟 | 0.0756 秒 |
| 10 个字符（无特殊组合），共 3.76 千万亿个组合 | 1194 个世纪 | 10.45 小时 | 37.61 秒 |

当做数字0的若干次方来处理,最终的结果是二者都为0，比对结果相同。任取一段信息，它的哈希值以“0e”开头的概率高达1/256，在这种情况下，口令破解的效率被提高了1630倍。

（3）彩虹表破解

现阶段应用体系中，口令的鉴别通常是通过在服务端将用户发送的口令进行哈希加密后与数据库中的哈希值比对来进行的。因为哈希函数是单向函数，即便黑客获取了服务器数据库中的数据，也无法根据哈希值反推得到口令明文。破解哈希值的一种常用手段就是彩虹表破解。如图1所示，彩虹表破解是一种典型的以空间换时间的破解方法，它将众多哈希值及其明文提前计算并进行存储，需要时根据哈希值查找明文即可实现破解。

虽然彩虹表有着惊人的破解效率，但是安全人员仍然有办法防御彩虹表。最有效的方法就是“加盐”，即在密码的特定位置插入特定的字符串，这个特定字符串就是“盐”。“加盐”后的密码经过哈希加密得到的哈希串与“加盐”前的哈希串完全不同，例如：“加盐”前Hash（“hello”）=5D41402ABC4B2A76B9719D911017C592，“加盐”后Hash（“hello”+“QxLUF1bgIAdeQX”）=61819A2E9B721831243EBA1AEABA8486。黑客利用彩虹表得到的密码也并非真正的密码。即使黑客知道了“盐”的内容、“加盐”位置，还需要对散列链进行修改，彩虹表也需要重新生成。因此，“加盐”能大大增加利用彩虹表进行口令破解的难度。

（4）分布式破解

无论是在登录界面多次尝试进行暴力破解，或是对哈希值进行碰撞，都需要进行大量的计算与操作，此时就可以利用僵尸网络进行分布式破解来提高效率。僵尸网络是指采用一种或多种传播手段，将大量主机感染僵尸程序，从而使攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指

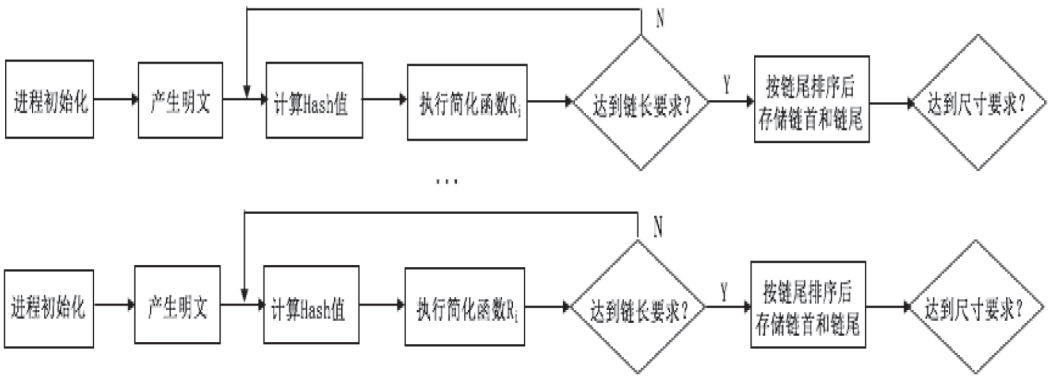


图1 彩虹表构造框图

令，组成一个僵尸网络。利用僵尸网络进行分布式破解，就是增加用于破解的设备数量，给每个设备分配适当的破解范围，从而提高破解效率。同时由于被感染主机的网络地址各不相同，在进行在线破解时，数据量巨大且无序，防御方难以对攻击流量进行有效的监控和阻挡。

## 3 口令安全问题研究

### 3.1 口令加密技术研究

（1）口令鉴别机制

鉴别是任何加密方案的第一步，可以用来分辨用户的真实身份，防止攻击者假冒合法用户获取访问权限。用户鉴别的方法有很多，一般分为标准的身份验证协议和可扩展的身份认证协议。其中，最传统的就是通过用户名和口令进行鉴别。

最简单的口令鉴别机制即明文口令鉴别。由于口令在存储和传输过程中保持明文形式，一旦用户数据库被非法入侵或者用户与服务器之间的通信链路被监控，用户信息便会被窃取。为解决这一问题，实际应用中口令鉴别机制在鉴别用户时，是在用户计算机上通过某种算法对输入的口令进行加密，得到口令的推导形式。计算机将这个口令推导形式发送到服务器中，在用户数据库中进行验证比较。口令推导形式与消息摘要非常相似，所以也可以使用口令的消息摘要技术。

值得思考的是，这种方法并不能避免攻击者获得登录权限。因为攻击者只要在用户名及口令的消息摘要传送过程中进行截获，隔段时间再向服务器发出，即可通过身份鉴别，成功登录账号，这就是所谓的重放攻击。为有效防范此类重放攻击，系统可采用一次口令技术，即通过非常规字符串口令以及时间戳验证机制实现口令鉴别机制的相对安全。如图2所示，基于RSA公钥密码体制的一次一密口令验证模型是一种典型的一次口令技术。

（2）口令加密传输

用户计算机具有加密功能，可以有效解决明文口令的传输问题。事实上，这种功能还可以应用于对用户口令的消息摘要加密随机数。这对于客户/服务器程序是可以完成的，但是对于Internet应用程序，客户机是没有任何加密功能的Web浏览器，因此这种加密功能受到限制。

鉴于此，用户需要在客户机和服务器之间利用安全套接层协议（SSL）之类的技术进行连接，客户机需要验证服务器的数字证书以鉴别服务器，然后利用SSL加密客户机与服务器之间的所有通信。这时口令不需要任何应用层的保护机制，有效避免了加密功能受限的影响。其工作过程为：（1）用户计算机用SSL对口令进行加密，并将加密后的口令同用户名一同发送给服务器，请求登陆；（2）服务器的用户鉴别程序对用户名和已经加密的口令进行鉴别；（3）服务器将鉴别结果反馈给用户计算机。

### 3.2 加强口令管理，防止口令猜测

口令是信息系统鉴别用户身份合法性的重要凭证，而且口令的安全级别可以间接地决定系统的安全级别。因此，口令管理尤为重要。口令管

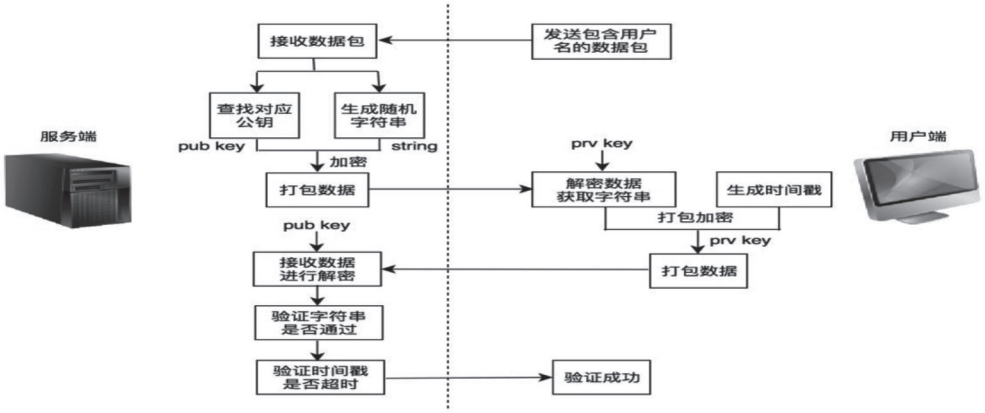


图2 基于RSA公钥密码体制的一次一密口令验证模型工作流程图

理的内容主要包括口令的选取、保存、保密、定期检查和更改周期等方面。具体的口令管理策略为：（1）设定最小口令长度；（2）设置口令最长使用期限，一般不得超过42天；（3）限制用户登陆失败次数（建议为3~5次）。如果超过次数，系统将自动锁定账号并禁止在一定期限内登陆，或者需要管理员的认证才可以再次登陆账号；（4）目标主机的管理员可以设置一些账号诱骗黑客攻击，以发现并查明黑客身份。

除加强口令管理外，使用强口令防止口令猜测也可以有效避免攻击。强口令具有五个特点：（1）从大写字母、小写字母、数字、符号四类字符中任意选取三种以上组合形成口令，且避免连续；（2）至少包含8个字符；（3）定期修改；（4）明显区别于以往密码且避免使用字典单词；（5）使用KeePass等软件帮助管理。

### 3.3 口令安全研究进展

（1）口令破解技术发展趋势

口令只是防范攻击者入侵的第一道防线，防止入侵者获取口令，可以有效减少其攻击系统的可能性。但是，获取口令并不一定需要登录系统，在不登陆系统的情况下，攻击者仍然可以破解口令，进行系统攻击。

目前，口令安全所面临的威胁大致可以分为暴力破解、漏洞攻击和社会工程学攻击三个方向。随着网络安全技术的规范化和体系化发展，用户口令的强度与漏洞攻击的成本越来越高，实现也越来越困难。于是，诸如电信诈骗、钓鱼攻击以及诱饵计划等社会工程学攻击手段逐渐成为口令破解的主流。由于社会工程学攻击往往利用的是人类思维或性格上的短板，因而无法像程序逻辑漏洞那样进行修补。此外，攻击者不需要掌握太多的技术基础。低成本、多手段、高收益的特性使得社会工程学攻击成为未来很长一段时间内口令安全所面临的主要风险。

（2）口令安全防御演变进程

传统理论认为，所有的口令都是可以破解的。根据破解的难易程度，可以划分密码算法的安全等级。就现阶段的研究而言，两种情况的用户口令相对安全，即被加密数据价值小于破译算法的代价或者破译密码所需时间大于加密数据的有效期。

根据口令的不同特征，可将其分为用户所知道的、用户所持有的以及用户所特有的三种。用户所知道的口令是指字符串口令；用户所持有的口令是指类似于U盾等实物令牌；而用户所特有的是指指纹、虹膜等生物口令。由于方便快捷这一特性，字符串口令为绝大多数信息系统所普遍使用。同时针对该种口令的攻击方式发展较为完备。目前，只能通过加强口令管理、提升口令强度的方式实现相对安全，但无法从根本上解决问题。于是，在未来一段时间内，越来越多的高安全要求信息系统会采用数字证书、硬件令牌以及生物特征等口令形式。但是仅仅依赖于单一因子，系统无法彻底抵御社会工程学攻击，将会再次面临字符串口令所经历的类似问题。

因此，在对口令形式不断创新的基础上，系统需要尝试使用（双）多因素身份验证，使得攻击者仅仅通过口令猜测或口令破解无法获取相关权限。作为（双）多因子的一部分，诸如心跳、步态、脑电波等高级身份验证方法也将成为口令安全防御的发展方向。此外，人机检测、新型云WAF以及分布式集群防御等技术也需要进一步研究进而实现更深层次、更加智能的安全防护。

## 4 结束语

本文从口令破解、口令加密以及口令安全三个方面介绍了当下口令保护研究现状。从论证中不难看出，伴随着网络技术的不断进步，加密系统的性能以及口令破解技术都有了充分的发展。口令安全是保护信息系统安全的第一道屏障，做好口令的保护措施也是信息安全维护的关键所在。无论是口令加密还是口令管理，其发展都将迈入一个新的台阶。正如前文所说，没有任何口令是绝对安全的，也没有任何系统是无懈可击的，网络攻击者和防御者之间的博弈是信息安全领域的永恒话题。这不仅需要立法者从规范层面予以设定，亦需要全民信息安全意识的提升，从而实现网络空间的相对安全和公民个人隐私权的有效保障。

## 参考文献

[1] 胡志远.口令破解与机密技术研究[M].北京：机械工业出版社，2003.07（黑客防线）.

[2] William，Stallings.密码编码学与网络安全——原理与实践(第三版)[M]. 刘玉珍译. 北京:电子工业出版社，2004.

[3] 魏为民,袁仲雄.网络攻击与防御技术的研究与实践[J].信息网络安全,2012(12):53-56.

[4] 高危险僵尸网络攻击模式全解析[J].计算机与网络,2010,36(19):42.

[5] 王伟兵,文伯聪.基于彩虹表技术的分布式密码破解研究[J].中国人民公安大学学报(自然科学版),2017,23(01):79-84.

[6] 何文海,信佳佳.网络信息安全中存在的问题及数据加密技术研究[J].网络空间安全,2019,10(01):24-26.

## 作者简介：

尚旭哲（1999-），男，汉族，山东济宁人，中国人民公安大学，本科；主要研究方向和关注领域：公安学、信息安全。

王润田（1999-），男，汉族，山东烟台人，中国人民公安大学，本科；主要研究方向和关注领域：公安技术、网络安全。

孙颖（1999-），女，汉族，江苏苏州人，中国人民公安大学，本科；主要研究方向和关注领域：公安学。

付瑜菲（1999-），女，汉族，北京人，中国人民公安大学，本科；主要研究方向和关注领域：公安学、密码学。

（本文为“2020年429首都网络安全日”活动征文）

（上接第97页）

## 作者简介：

吴宏锋（1976-），男，汉族，北京人，博士，北方工业大学，副教授；主要研究方向和关注领域：数论、密码学。

胡振华（1995-），女，汉族，山西吕梁人，北方工业大学，硕士；主要研究方向和关注领域：密码学。

（本文为“2020年429首都网络安全日”活动征文）