密码创建方案①

梁世庆[1]　孙波成[2]

（1.襄樊学院 湖北 襄樊 441053；2.西南交通大学 峨眉校区 四川 峨眉 614202）

摘　要： 密码是计算机安全的重要组成部分，是保护用户各类账号的前线。本方案的目的在于建立一个创建强密码，保护这些密码以及更换频率的标准。内容有密码的安全性，密码保护标准，密码构造指导方针等。研究了用于个人、基于家用的机器、与工作相关的网络系统的密码方案。

关键词： 密码；密码方案；网络系统

Password Design Method

LIANG Shi-Qing[1], SUN Bo-Cheng[2]　(1. Xiangfan University, Xiangfan 441023, China; 2. Emei College, Southwest Jiaotong University, Emei 614202, China)

Abstract: Password is the main protection of computer safety, and the safeguard for different accounts. This paper sets up a standard to create strong password, protect these passwords and change time. It discusses password safety, protection criterion and conformation method. It studies password strategies for personal computer, work correlative system and network.

Keyword: password; password method; network system

1　前言

密码是您的系统和个人信息的第一道防线。这个系统的规模可以是任何大小，从一台计算机到一个住宅报警系统到由数百或数千台计算机组成的企业网络；信息可以是任意类型的，从社会保险号码到私人信件到机密文档。通过与用户名的结合，密码向您提供了一套访问这些系统的凭证。用户名通常是某种形式的“账户”，创建它是为了让您将它和密码一起使用[1]。

密码有着广泛的应用，本文只涉及基于计算机的系统。以下是用密码进行保护的系统示例。

- 工作站
- 应用程序：电子邮件、Word、Excel 等。
- 服务器登录
- 路由器(其它设备)登录
- 网站
- 网站
- 电子商务站点
- PDA(个人数字助理)

2　密码保护标准

不要将密码文件保存在您的本地机器或共享的网络上。这里仅是通过文件级别访问来进行保护的，而且机器本身可能被泄漏。如果有人对某个文件夹重新设置许可权，并且错误地设置了许可权，那么，该文件夹内的子文件夹的许可权也被重新设置，这会引起泄漏该网络上的所有密码。

在创建密码保护时还要避免其它几个问题：

①绝不要将个人信息用作密码的基础。举例来说，如果您是一个 Star Trek 迷，则不要将您所有的密码设置成“Spock”、“Vulcan”甚或“Spock1”。任何

① 基金项目:西南交通大学峨眉校区基金(10401x10096004)
收稿时间:2009-11-26;收到修改稿时间:2010-03-30

了解您的人都可以轻易猜出这些密码。

②不要通过电话向任何人透漏密码。

③不要在电子邮件中透漏密码。

④不要和家庭成员共享密码。

⑤不要在调查问卷和安全表格是透漏自己的密码。

⑥保存密码的唯一安全的地方是您的脑袋或上锁的保险箱，只有您知道这个保险箱的开箱密码组合。

⑦有效密码必需相当长，但又不能长到您无法记住它们的程度。三个字符的密码太短了。

不要使用基于您放在办公桌上的物品的密码。如果在一位客户的办公桌上看到他孩子的照片，随后有可能通过使用他孩子的名字闯入了他的服务器。

不要使用应用程序的“记住密码”功能，不要将密码写下来放在办公室的任何地方，不要不加密就在文件或者任何计算机系统中存储密码。

至少每隔 6 个月就更换密码，除了系统密码，它必须每季度更换，建议更换时间 4 个月[2]。

3 常规密码构造指导方针

因为密码是系统安全的一个至关重要的组成部分,而且他们又相对容易地被破解。密码的破解就是为了未经授权登陆一个系统或账号去计算出或解除密码的过程。这比大多数的使用者想象的更加容易。破解和入侵的不同是代码是被破解，机器是被入侵。密码可以以多种不同的方式来破解。最简单的就是利用词表或字典程序来暴力破解密码。这些程序利用词表或字母组合来跟密码对比，直到找到与之相匹配的。破解代码就象科幻小说似的，可以在 Packetstorm 或 Passwordportal.net 上去搜寻"密码破解机"。也有为数众多的密码破解工具可利用，这些工具平常的人都会使用。

入侵者的另外一个容易捕捉密码的方法就是通过社会工程学：从某人的键盘操作上物理的捕捉密码或者通过利用电话模仿 IT 工程师来询问。只要稍微研究一下这个密码正在被搜寻的用户的一些信息，许多用户创建的密码可以被猜测出来。研究密码的另外一个技术途径就是通过嗅探器，它监视在网络上传输的原数据并且破译它的内容。"一个嗅探器能够读取从你的机器送出的每次按键,包括密码"。可能现在有某个人至少已经拥有了你的某个密码。

密码用于不同的目的，一些较为常见的用法包括用户级账户、Web 账号、电子邮件账号、屏幕保护程序、语音邮件密码以及本地路由器登陆。因为很少有系统支持一次性令牌(只使用一次的动态密码),因此应该清楚如何选择强密码。

拙劣的、弱的密码有以下特点：

①密码少于 8 个字符。\

②密码是语言字典是可以查到的词。

③密码是常用词，如：

④家庭成员、宠物、朋友、同事、偶像明星等等的名字和生日。

⑤计算机术语和名称、命令、站点、公司、硬件和软件。

⑥地址和电话号码之类的其他个人信息。

⑦像 aaabbb、zyxwvuts 和 123321 这样的词或者数字。

⑧上述任何拼写的逆转。

强密码有以下特点：

大写字母：如果您有“区分大小写”的功能，则将大写字母和小写字母结合起来使用可以提供一些保护。这样,您可以使用密码“HeyYou”,它与“heyyou”不同。加入大写字母就添加了一层复杂性，使密码更难破解。

特殊字符：使用象“#”或“%”这样的特殊字符也会添加复杂性。采用“money”一词，在它后面添加 #（money#），这样您就拥有了一个相当有效的密码。

数字：使用数字也会增加这个混合体的复杂性。如果您的社会保险号码是 123-45-6789，可以将最后四位数字和一个容易记忆的单词(譬如“money”)一起使用，产生出您的密码“money6789”。

助记符短语：如果您是电影或歌曲的短语收集者，您可以采用一条精彩的短语并将它制作成密码。假定您是 Star War 迷。您可以采用短语：“May the Force Be With You”，然后使用每个字的第一个字符来创建密码“MTFBWY”。

替换：您可以用数字或符号替换字。如果您知道“$”符号相当于“money”一词，那么，您可以将它结合进密码方案中，如“Ilove$”。这是一个容易记忆而又难以破解的密码。 设法创建容易记住的密码。这么做的一个方法是根据歌名、断言或者其它短语创

建密码。比如，短语可能是“This May Be One Way To Remember”，密码可以为”TmBlw2R!”或者TmBl>r~ 或者其它变化。

4 有效密码方案

下面，我们研究用于个人、基于家用的机器、与工作相关的系统和网络的密码方案，以及专门用于不使用基于 CiscoSecure 的 Tacacs+ 的 Cisco 路由器和交换机的密码方案。CiscoSecure 是一种产品，它不使用典型的保存在设备本身的登录密码，而是使用 Tacacs+ 协议允许象 UNIX 服务器这样的外部来源执行路由器和交换机的登录验证。

4.1 基于家用的个人 PC

基于家用的个人 PC 上的有效密码方案是使用了上述理论的组合。您会希望密码十分容易记忆，因为一旦忘记它，您没有破解密码的技能，进入自己的机器就成了问题。您还需要考虑以下方面：

①如果您正在运行 Windows 9X 平台，您不必担心密码，因为密码对于本地机器安全性毫无意义。您的密码是基于概要文件的，如果您按下 Cancel，就可以绕过机器的登录。此外，可以通过重新引导机器来绕过密码保护的屏幕保护程序。

②如果您正在运行 Windows NT、2000 或 XP 平台，则需要确保不要忘记您的密码。您需要确保用良好的密码锁定 Administrator 帐户，并确保将密码隐藏好以免您的机器被入侵。但是，如果您忘记了密码，则希望有办法找回它。可通过创建一个保护该密码的新帐户和密码来完成这一点，这样您就有了一扇“后门”。

基于家用的安全性和企业安全性有很大差异，因此其原则是基于个人级别的舒适和偏好。这里有一个易于记忆的家用密码方案：混合使用昵称、大小写字母以及您的社会保障号码的最后四位数字和一个特殊字符。您创建的密码可能类似于：Butch#8976

本例也可以用于网站、银行帐户和其它个人使用的系统。实际上，此类密码是不可能破解的，并且易于牢记。

4.2 网络管理员系统

如果处在任务繁重的网络管理员位置上，将要负责许多系统的密码。

密码保护遵循与先前相同的规则，只是范围更广了些。您很可能有许多系统需要用密码保护，更有甚者，您甚至根据希望授予用户的访问类型划分密码 级别。换言之，可以将 Cisco 路由器的登录访问分成多种级别，每种级别授予比前一级别更多的特权。

可以使用本文第一节中所列举的同样的理论(大写、特殊字符等)，但需要作一些新的更改。您需要提出一个主题，而不是采用一个易于牢记的好名称或单字。用于网络服务器的密码方案中,以下是它可能的几种情况：

表 1　网络服务器密码方案

服务器名	服务器类型	密码
MNN-DC-1	域控制器	Pink$DC1
MNN-DC-2	域控制器	White$DC2
MNN-DNS-1	DNS 服务器	Black$DNS1
MNN-DNS-2	DNS 服务器	Red$DNS2
MNN-DHCP-1	DHCP 服务器	Green$DHCP1
MNN-WINS-1	WINS 服务器	Orange$WINS1
MNN-FS-1	文件服务器	Yellow$FS1

请注意每台服务器的密码都包括颜色和一个特殊字符(所有密码都使用了同一特殊字符)以及服务器名的一部分。此外，注意大小写字母的使用。这些密码被破解的可能性极小。这是一种可靠密码方案的示例；它是有效的，并且您不费太多力气就可以记住它。此外，可以(并且应该)根据自己的需求进行定制。

4.3 Cisco 管理员密码方案

下表显示了 Cisco 路由器的有效密码方案。Cisco 路由器需要两种密码级别：初始密码和启用保密密码(enable secret password)。

表 2　Cisco 路由器的有效密码方案

初始密码	启用保密
DoNot$	$HackMe
DoNot$	$PingMe
DoNot$	$CrackMe
DoNot$	$SpoofMe

因为 Cisco 路由器接受区分大小写的密码，所以

此处您拥有很好的大小写模式、特殊字符和易于牢记的短语。

对于 Cisco，需要用来登录到路由器的初始密码和用于更安全的访问的二级密码，可以将二级密码配置为启用保密。这个图表提供了如何配置这个选项的思想。通过将密码方案与喜欢的东西(如影片)相关联，就更有可能记住它(并不是所有与安全性相关的工作都必需成为苦差事！)；但更重要的是 一 确保它是安全的。

5 结语

密码是必需的，尽管有些不便，但已成为我们生活的一部分。所有系统都需要密码，以拥有易于实现的第一级别的访问安全性。各级 IT 专业人员和用户所面临的问题是，我们如何使用它们以及如何才能不遗忘它们？在本文中，我们研究了如何有效地创建单独的密码和密码方案。密码和密码方案必需难以破解而易于牢记。因为密码难以记忆和理解，人们往往只花很少的精力创建它们，因此会危及自己和他人的安全性。但是，记住这一点很重要：无论密码或密码方案多么有效，总是存在着与密码相关联的一定程度的风险。

参考文献

1 Rob Shimonski.Create effective passwords. http://www.ibm.com/.

2 Scean Convery 著,王迎春,谢琳等译.网络安全体系结构.北京 [illegible]