安全密码管理

安全密码管理

在使用电脑的过程中，我们无时无刻不在与密码打交道。如果自己设置的密码被别人猜到或破译，那么则会重要资料、个人隐私被泄露。因此安全密码的管理是与每个人都相关的一件大事。本专题中将用实例介绍如何安全密码的创建、管理和破解。

密码的相关定义

密码是一些无间隔的字符，用于决定请求访问电脑系统的用户确实是特定的用户。密码短语是比通常的密码（典型的是 4 到 16 位字符）要长的字符串，用于创建数字签名（编码的签名可以证明真的是发送信息的人）或者在信息的加密或解密中。

- ❖ 什么是密码和密码短语

安全密码的创建

本部分中以实例讲解了如何创建安全的密码系统，实例问题如下：我是高级信息安全主管。我的公司想要使用一位员工的社会安全号码的最后四位数，妈妈的小名和出生的城市作为一个程序的密码认证系统。我应该干预那些安全问题呢？如果有，什么时候使用这些信息（特别是社会安全号码的后四位）呢？

- ❖ 如何创建安全的密码系统

密码的管理

强大密码的创建后，出于安全的需要，仍然要定期更改管理员密码，还有管理员离开的时候也要更改密码，不只要更改主要系统，备份的密码也要改。此外密码的维护和更新也需要定期进行。在本部分钟还介绍了密码维护和管理的一些案例，供大家参考。

- 如何安全地向用户发布密码？
- 用户和管理员密码的升级、选择和记录
- 密码要定期更改吗？
- 域中本地管理员密码的安全变更
- 如何更改域内 300 台计算机的本地管理员密码？

密码的破解

密码破解器是用户验证电脑或者网络资源的不知道的或者被遗忘的密码的应用程序。它也可以帮助人类破解者获得对资源的非授权访问。密码破解也是黑客获得电脑或者网络访问的最简单、最常用的方法。另外本部分还将介绍一款快速的密码破解器 Ophcrack，它使用一个叫做彩虹表（Rainbow tables）的特别运算法则。

- 什么是密码破解器？
- 密码和密码破解
- Ophcrack：密码破解更轻松

什么是密码和密码短语

密码

密码是一些无间隔的字符，用于决定请求访问电脑系统的用户确实是特定的用户。多用户或者受安全保护的单用户系统要求单一的名称（通常称为用户 ID），而且是大家都知道的。为了验证输入用户 ID 的，需要用户输入第二个证明，密码，而这个系统的密码只有这个人知道。典型的密码是在 4 位和 16 位之间，取决于电脑系统的设置方式。当输入密码后，电脑系统就会谨慎的把这些字符不再显示器上显示，以防别人可以看到。

在选择密码或者设置密码的优秀的标准包括：

- 不要选择了解你的人可以轻易菜刀的密码（例如，不是信用卡号码、生日或者小名）
- 不要选择在字典中可以找到的单词（因为有些程序可以快速的试验字典中的每一个单词！）
- 不要选择正在流行的单词
- 不要选择和前一个密码相似的单词
- 选择字母和至少一个数字的混合密码
- 选择容易记住的单词

很多网络都要求定期更改密码。

密码语句

密码短语是比通常的密码（典型的是 4 到 16 位字符）要长的字符串，用于创建数字签名（编码的签名可以证明真的是发送信息的人）或者在信息的加密或解密中。例如，

Phil Zimmermann 流行的加密程序，Pretty Good Privacy 当签名或者破解信息的时候需要密码短语。密码短语的长度通常达到 100 个字符。

(作者：SearchSecurity.com Staff 译者：Tina Guo 来源：TechTarget 中国)

如何创建安全的密码系统

问：我是高级信息安全主管。我的公司想要使用一位员工的社会安全号码的最后四位数，妈妈的小名和出生的城市作为一个程序的密码认证系统。我应该干预那些安全问题呢？如果有，什么时候使用这些信息（特别是社会安全号码的后四位）呢？

答：在你描述的系统中存在巨大的安全风险。最小的风险是使用社会安全号码的一部分。

提议的认证系统应该取决于企业的大小和位置，认证系统可能存在可以被黑客利用的副本。可能有两个或者更多的人的姓例如“Smith”一样，而且作为了妈妈的小名，而且出生在同一座城市。如果你的企业位于一个大型城市，这些副本的结合可能比预期的更加常见。

编写脚本重复试验常见的姓何城市名称来破解密码系统对于黑客来说可能太复杂。社会安全号码的最后四位数不可能出现重复，但是仍然存在问题，隐私问题。在 0000 到 9999 之间共有 10000 个，而脚本可以在一秒的若干分之一的时间内运行完毕。所以，社会安全号码对于顽固的入侵者构不成障碍。

如果入侵者是聪明的社会工程攻击者，而且做足了工作，就可以获得员工的名字，甚至在编写脚本前，这都是致命的问题。攻击者然后可能使用这些用户名编写细致的脚本，继续搜索密码，并获得对系统的无障碍的访问。

这种使用脚本重复普通单词和名字的攻击叫做字典攻击，因为这些信息可以从字典上获得。

我推荐使用不常见和更隐秘的字符来认证密码系统的用户。使用内部员工不在外面使用的数字结合其他不常见的出名字（妈妈的小名或者其他）之外的标识符和城市。还有，

当然，确保你所使用的超过八个字符，而且是字母和数字的混合体，而且不是可以轻易被识别的单词或者常见名称。

并不存在可以提供使用员工标识符的安全密码系统的公式。尽管如此，提议的系统很脆弱。

(作者：Joel Dubin　译者：Tina Guo　来源：TechTarget 中国)

如何安全地向用户发布密码？

问：给新用户发送密码的最好方式是什么？我发现服务台或者系统管理员发布原始密码的方法不安全，用户甚至都可以得到权限的提升，在第一次登录后就可以改变密码。

答：一方面，你所描述的就是给新用户发布密码或者给以存在的用户重设丢失的密码的适当做法。发布临时密码，然后再在第一次登录时更改就是最好的方法。另一方面，为了原始密码发布密码并不是那么好的注意。

这样的情形很容易受到社会工程共济的利用。如果一个恶意用户，不论是在公司内部或外部，了解这一点，他们就可以简单地打个电话，申请重设密码，并模拟合法用户。那么你可以怎么做来避免呢？

首先，所有发布的的原始密码都应该是每个用户都不相同。不应该给服务台的员工相同的密码，或者规则很容易猜到的密码，例如用户 ID 的变更。

大部分的认证系统，包括 Active Directory，都有一种可以设置到用户帐户中的功能，该功能要求用户在第一次登录后更改他们的密码。另外，例如 Windows Sever 2003 的 Group Policy Objects（GPO）都可以配置所需要的密码长度和复杂度，这样就可以使用户的密码不容易被猜到或者破解。

即使如此，发布原始密码的安全性还可以进步。这里是一些附加的建议和最佳实践可以帮助你的服务台和系统管理员：

1. 总是给新用户或者要求密码重设的用户唯一的密码。避免容易猜到的规则。
2. 对新的临时密码设置时间限制。临时密码应该只能用一次，并且必须在，例如 24 小时内激活。否则，它就失效，而且用户必须再打一次电话来更新密码。不要让临时密码永久化或者永远可用。

3. 保留新密码或者重设密码的所有请求的纪录。在旧帐户的周期检查中使用纪录。检查密码样式。来自同一个人或者部门的周期性密码重设要求可能表示他有问题。

虽然如此，一般来说，在下一次登录时更改发布的临时密码是保护用户信任状的最好做法。

(作者：Joel Dubin 译者：Tina Guo 来源：TechTarget 中国)

用户和管理员密码的升级、选择和记录

什么

定期的审计可以使密码符合安全策略。

何时

每个季度或者半年一次，取决于你的 CIA2 等级。

为什么

为什么推荐八个字符的密码？使用快速的电脑，六位或者更少的密码可以在一两天内破解。七个字符的密码可以在四个月内破解。在八位的密码被破解前，就应该已经把密码改为新的八位字符串了。这样就可以保护帐户。

战略工具

更改用户密码可以使用操作系统的结构通知倒计时时间表来通知用户他们的密码将在 XX 天 内失效。强制使用混合文字和数字的密码。提供战略建议，例如使用罕见短语和数字—字母置换的创造性使用，这样他们就不会写下来了。

定期更改管理员密码，还有管理员离开的时候也要更改密码，不只要更改主要系统，备份的密码也要改。不要忘了热/温/冷网站备份。在一个安全的位置记录密码。使用下面的密码工作表，帮助说明管理员密码

Possible passwords (some default), per server:	Do you know all of the passwords to your system?	How often should they change?
1. Boot		
2. Eeprom		
3. Database Administrator		
4. Server root		
5. Browser		
6. Clients		
7. UPS monitoring software		
8. Router administration		
9. Firewall administration		
10. Any other applications/systems that mount to yours		
11. Any/all applications on the server		
12. Systems you ftp/telnet to		

更改设备密码是另一个问题。如果在结构中拥有 500 个路由器怎么办呢？应该用户管理员工具推动配置和密码。因为不用手动操作节省的时间和精力更值得损失。一个较小的暴露痕迹就意味着要在减少系统流量使更改而引起的问题减少的时候考虑每年一次更改这些密码。

在任何情况下都要确认所有的帐户都用户强大的密码——不计入空的、默认的或者 guest 帐户——而且密码检查机制都已经被保护着。

最后是系统密码处理。密码会以各种形式穿过系统——明文文本、自动更新、硬编码或者加密/隐藏在计算机代码中。你需要知道系统上每个组件的作用，并做出相应的保护。系统上有默认的密码吗？也要更改以下。

（作者：Shelley Bard 译者：Tina Guo 来源：TechTarget 中国）

密码要定期更改吗？

问：在最近的公司安全会议上，有个话题是密码和密码更新。风险管理组提出一种观点是不要让终端用户定期更改密码。他们说系统帐户和系统管理员层应该继续这么作，但是一般用户不能。我觉得他们的观点有些奇怪，因为共享密码的用户总是问题。还有，随着我们采用单点登录，我认为这是在目前的安全意识环境中的不寻常的进步。风险管理的争议是如果一个密码足够强大，就没有定期更改的理由。

答：我也看到了这种趋势，以及对密码思考的“新”方式。我们都被带入了这样一个怪圈“密码最少要八个字符，必须每 30 天更改一次”。根据我作为一个顾问的经验，如果用户经过了六到十二个月的培训（这很重要），安全依然很强大。我们都知道编写（并对其好处进行否定）没有任何个人意义的复杂密码是人类的天性，特别是当他们必须要经常更改的时候。我崇尚对安全和便利的权衡，因为如果不这样，只有黑客可以胜利。记住这是理想的情况。如果你怀疑因为有人共享密码、通过明文文本邮件传送，并在没有保护的硬盘上存储而导致密码很容易受到攻击，那么这些密码就需要经常更改。

（作者：Kevin Beaver 译者：Tina Guo 来源：TechTarget 中国）

域中本地管理员密码的安全变更

问：在域中的 300 台电脑上，保护本地管理员密码的变更的最安全的方法是什么？

答：变更本地管理员密码是防御入侵这进入工作站和造成大破坏的很好的安全方法。

但是，如果你仍然想要控制域层面的电脑或者通过 Active Directory 控制电脑就记住这一点。一定要在对工作站进行变更前把域管理员组增加到本地管理员组。另外，也不能通过域远程管理电脑。

在域中的多个电脑上变更本地管理员帐户和密码有两种自动的方法。一种是编写一批脚本，另一种是使用微软的工具，如果电脑上运行的是 Windows。

首选的方法是使用微软工具 cusrmgr.exe。它是 Windows 2000 的 Resource Kit 中的工具，但是也可以在其它 Windows 版本上使用。它是通过使用 cusrmgr.exe 在域中的工作站循环运行一批脚本起作用的。

为了简要地强调脚本的方式防止可能出现的情况，可以在 Active Directory 域中的工作站上的 Web 上获取 VBScript 和 Windows Script 脚本的搜索和更新。通常 25 行的脚本就可以起作用了。

（作者：Joel Dubin 译者：Tina Guo 来源：TechTarget 中国）

如何更改域内 300 台计算机的本地管理员密码？

问：对域内 300 台计算机的本地管理员密码进行更改，什么是最安全的方式？

答：更改本地管理员密码，是一种很好的安全措施，可以防止工作站被入侵和恶意破坏。

但是，如果你仍想通过域或是活动目录（AD）对计算机进行控制，一定要注意下面这一点。在对工作站进行更改前，首先一定要将域管理员组加到本地管理员组。否则，你无法通过域对计算机进行远程管理。

对域内多个计算机进行本地管理员帐号和密码的更改有两种自动途径。一种是写脚本，另一种是如果机器运行 Windows 就使用微软工具。

使用微软工具 cusrmgr.exe 是较好的办法。该工具是 Windows 2000 Resource Kit 的一部分，不过也可以用于其他 Windo ws 版本。通过使用 cusmgr.exe 在域内对工作站循环运行脚本，从而实现更改密码。

为了简要突出脚本方法并提出可行的意见，网上的 VBScript 和 Windows Script Host 中提供了一些脚本，可以用来搜寻和升级活动目录域内的工作站。通常来说，一个长度为 25 行的脚本就可以完成。

（作者：Joel Dubin 译者：Eric 来源：TechTarget 中国）

什么是密码破解器？

密码破解器是用户验证电脑或者网络资源的不知道的或者被遗忘的密码的应用程序。它也可以帮助人类破解者获得对资源的非授权访问。

密码破解器使用两种主要的方法验证正确的密码：强力或者字典搜索。当密码破解器使用强力的时候，它会运行预先确定的长度内的字符组合，直到发现被计算机系统接受的组合。当进行字典搜索的时候，密码破解器搜索字典中的每一个单词，找到正确的密码。密码字典的存在是因为很多不同的话题和综合话题，包括政治、电影和音乐等。

有些密码破解程序搜索字典的单词和数字的混合体。例如，密码破解器可能搜索 ants01；ants02；ants03 等等。当用户被建议在密码中增加数字的时候就变得有意义了。

密码破解程序可能还可以验证加密的密码。在从电脑的内存中找回密码后，程序也许可以破解它。或者，通过使用和系统程序相同的运算法则，密码破解程序就可以创建和原始密码匹配的密码加密版本。

(作者：SearchSecurity.com Staff 译者：Tina Guo 来源：TechTarget 中国)

密码和密码破解

密码破解是黑客获得电脑或者网络访问的最简单、最常用的方法。虽然不容易破解的强大密码的创建和维护都很简单，但是用户通常会忽略这一点。因此密码是信息安全链条中最弱的一环。在密码受到攻击后，它原是的所有者就不能唯一能使用这个密码访问系统的人了。这时候，坏事儿就开始了。

黑客有很多获取密码的方法。他们可以简单地通过询问或者在用户键入密码的时候偷窥来获得密码。黑客还可以在本地电脑上通过使用密码破解软件获取密码。为了跨网络获得密码，黑客可以使用远程破解功能或者网络分析器。

本文中将演示黑客从网络上获取密码多么简单。我列出了电脑网络上的一般的密码漏洞，并描述了帮助系统上的这些漏洞被利用的对策。

如果你进行了测试，并且实施了本文中列出的对策，就可以很好的保护系统的密码。

密码漏洞

当你平衡安全成本和保护信息的价值的时候，用户 ID 和密码的综合通常都很合适。尽管如此，密码给安全造成了错误认识。恶意认识了解这一点，并且把破解密码作为攻入电脑系统的一步。

信息安全中如果仅仅依靠密码的一个重大问题时不止一个人知道密码。有时，这是故意的，通常情况下不是。你不知道除了主人还有谁知道密码。

知道密码并不会让这个人成为授权用户。

有两类的密码漏洞的一半分类：

- 企业的或者终端用户的漏洞：包括终端用户缺乏密码意识，企业没有执行密码策略。
- 技术漏洞：包括若密码和密码在电脑系统上的不安全的存储。

在电脑网络和互联网出现前，用户的物理环境是对密码安全的附加保护层。目前电脑已经有了网络连接，这层保护就没有了。

(作者：Kevin Beaver 译者：Tina Guo 来源：TechTarget 中国)

Ophcrack：密码破解更轻松

信息安全的基本原则之一是确保系统使用强大的密码：即有一定长度，混合字母、数字和其它特殊字符的密码。确定你的密码是否强大的一个方法是，把你的密码输入密码检验器里，例如微软的密码检验器。微软的工具可以检查足够的长度和复杂度。

这些更为复杂的密码，被认为是“强大”，因为他们比简短、更容易猜的密码要花费更长的时间来破解。但是，即使强大的密码，使用一个叫做 Ophcrack 的开放源代码的工具，也能够在数秒内破解。

Ophcrack 是一个非常快速的密码破解器，因为它使用一个叫做彩虹表（Rainbow tables）的特别运算法则。强力破解工具通常每秒尝试破解成千上万种字母、数字和特别字符的组合。但是，通过尝试每个可能的组合来破解一个密码，需要花费几个小时或者几天。彩虹表预先计算密码使用的哈希表，通过比较已有的哈希表，允许快速密码查找，而不是从头开始计算它们。

从另一种方法考虑它，有人已经使用与 Windows XP 和 Vista 一样的运算法则，将数百万计的潜在密码生成密码哈希表。Ophcrack 简单地加载已有哈希表的兆字节，并且把 Windows 中的密码哈希表和其巨大的数据库进行比较。当匹配时，Ophcrack 以纯文本格式显示密码。

Ophcrack 在局域网管理器（LM）和 NT 局域网管理器（NTLM）哈希表中工作，并且有可以破解 Windows XP 和 Windows Vista 密码的彩虹表。它带有一个光滑的 GUI，可以在 Windows、Linux/Unix 和 Mac OS X 上运行，或者来自可启动的 LiveCD。Ophcrack 有能力

从安全帐户管理器（SAM，Security Accounts Manager）里获取密码哈希表。SAM 是 Windows 用于存储那些受保护的用户密码的注册表数据库。

Ophcrack 不是恶意软件，有其合法用途。例如，大多数 Windows 密码恢复工具会用一个新密码代替一个旧密码，但是在打开鉴定调查中发现其他档案时，知道真实的密码可能是有用的。此外，用 Ophcrack 测试一个已知的密码，使彩虹表达到最佳，能帮助验证密码是否非常强大。

不过，Ophcrack 使用的访问 SAM 的工具之一是 pwdump。在安装过程中，许多病毒扫描程序会把它作为恶意软件，进行标记并隔离，因为它能创建用于盗窃数据的秘密远程连接。Ophcrack 需要 pwdump，以在 SAM 中转储哈希表，因此它与 pwdump 的结合，也许会为一些道德黑客提供一个不安的风险水平。

（作者：Scott Sidel　译者：李娜娜 来源：TechTarget 中国）