为计算机用户提供的安全意识培训电子月刊

OUCH!

文章内容涉及以下几个方面

- 问题
- 解决方案
- 案例

双因素身份认证

客座编辑

Fred Kerby 是本期的客座编辑，曾在美国海军水面作战中心达尔格伦分部任信息安全保障经理，SANS 的高级讲师和信息安全课程负责人（SEC301）。Fred 也是信息安全导引课程（MGT512）和安全基础课程的讲师（SEC401）。

中文译者

诸葛建伟(Jianwei Zhuge)博士，中国清华大学网络工程研究中心副研究员，中国教育和科研网 CERNET 安全应急响应组 CCERT 成员，The Honeynet Project 正式成员和中国分支团队负责人。新浪微博：@清华诸葛建伟，博客：(netsec.ccert.edu.cn/zhugejw).

黎荣熙，清华大学本科生。

问题

为了使用像电子邮件，在线银行或者在线购物这样许许多多的网络服务，你必须首先证明自己的身份。这个证明自己身份的过程被称为身份认证，身份认证通过 一些你知道的信息（密码），你拥有的物品（智能手机）或者你的一些特征（视网膜或指纹扫描）来达到验证你身份真实性的目的。传统上最常用的身份认证方法是利用用户名和相应密码，而使用这种方式的问题是显而易见的：攻击者想要获得你在线账户的权限和信息唯一需要做的事情就是去获取你的密码，更可 怕是，如果你在多个地方使用相同的用户名和密码，你的损失可能会更大。为了 更好的保证你账户的安全，网站正倾向于使用超过一个身份判据的认证方法。下 面我们就来解释它是什么，以及你为什么需要使用它。

解决方案

更安全的认证方式使用不止一个证据，你不仅仅需要知道像密码这样的信息，也还需要持有你的智能手机或者提供你的指纹。双因素认证就如同它听起来的那样，你需要两

双因素身份认证

个以上的步骤去证明你的身份，一个通常意义上的例子就是你的银行卡。 你必须持有你的银行卡并提供你的密码。如果一个攻击者窃取了你的银行卡，除非他知道你的密码，否则这张卡对他毫无用处。这个例子说明，双因素认证更加保证了你的安全。在线双因素认证的工作方式类似于你的银行卡和密码。当想登录你的在线账户时，你需要首先使用你的用户名和密码，但是当你正确输入密码之后，你并不能直接登录你的账户，而是会让你提供另一个证明你自己身份的证据，比如刚刚发送到你手机的验证码或者你的指纹，如果你不能提供这第二个证据，你就不能正常登录这个账户。双因素认证就这样保护了你的安全。即使一个攻击者获得了你的密码，你和你的账户仍然是安全的，因为他无法通过双因素认证。

案例

让我们一起来看一个双因素认证发挥作用的例子。Gmail 是最广为使用的在线服务之一。许多人只使用用户名和密码登录他们的 Google 帐号。Google 现在正在提供安全级别更高的双因素认证。Google 的双因素认证需要你的密码和智能手机来完成认证。为了证明你持有你的手机，Google 会向你的手机发送一条包含一次性验证码的短信（关于信息费用的问题，请查看运营商的服务计划）。然后你输入这个验证码。当然，如果你希望的话，你可以在手机上安装一个生成一次性验证码的应用，来避免受到 Google 短信的困扰，也不必和电信运营商纠缠不清。使用更加安全的身份认证的价值是，即使攻击者获得了你的用户名和密码，他们也不能获得你的帐号的控制权，除非他们还能获得你的手机。你和你的信息从而获

采取一些简单的措施，你就能够在丢失手机的时候保护你的信息了。

双因素身份认证

得了保护。

需要了解的是，发送到你手机上的验证码是一次性的。每次你需要验证的时候它们都是不同的。这样，你每次登录你的 Google 帐号时，都需要经过这样一个双因素认证的过程。另外，这个功能默认是没有被开启的。如果想要开启这个功能的话，请登录你的 Google 帐号，进入帐号设置，选择安全选项卡并按照双因素认证的说明操作即可。

其他一些网站也提供双因素认证，像 Dropbox，Paypal 甚至也许是你的银行网站。这些服务也许支持你的手机，或者其他的像 Paypal 使用一个特殊的为你生成的验证码。其他的网站也许会使用特殊的 USB 设备（例如 Yubikey）来达到这样的效果。如果你正在使用的任何一个服务支持双因素认证，我们强烈建议你开启这个功能。

网络资源

为了方便阅读，一些链接使用了短链接的形式。为了减少安全问题，OUCH!的短 链接总是为你展示最终的地址并在试图访问时请求你的权限。

Google 双因素认证:

http://support.google.com/accounts/bin/answer.py?hl=en&answer=180744

Paypal（Ebay）的安全密钥:

https://www.paypal.com/us/cgi-bin?cmd=xpt/Marketing_CommandDriven/securitycenter/PayPalSecurityKey-outside&bn_r=o

常见的安全条款:

http://preview.tinyurl.com/6wkpae5

SANS 今日安全小贴士:

http://preview.tinyurl.com/6s2wrkp

了解更多

请订阅每月一期的 OUCH 安全意识培训电子期刊，或访问 OUCH 电子期刊汇集，您也可以通过访问 http://www.securingthehuman.org ，来了解更多的 SANS 安全意识培训计划。

中文版

CCERT 是中国大陆最早成立的网络应急响应组，是蓬勃与和平发展的中国在互联网安全领域上的一支领先和负责任的安全团队。请访问 www.ccert.edu.cn 来了解我们 。

期刊编委会: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner; 中文翻译组织：诸葛建伟（Jianwei Zhuge）