针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 什么是加密?
- 静态数据加密
- 传输数据加密

加密

什么是加密?

你可能听过人们使用“加密”这一术语以及如何使用它来保护你自己以及你的信息，然而，加密这一概念可能比较模糊。而且，加密并不能让你高枕无忧，它也有其局限性。本期，我们将以浅显易懂的语言解释什么是加密，为什么你应该使用加密以及如何才能适当地使用它。

客座编辑

Christopher Crowley（@CCrowMontance; +ChrisCrowley）是在华盛顿特区工作的一名顾问，同时是SANS Institute“移动设备安全和道德黑客”（SEC575）课程的首席讲师以及“事件响应团队管理”（MGT535）的作者。

你的设备上存储了大量诸如财务文档、图片、邮件、医疗记录等敏感信息，一旦你的某个设备丢失或者被窃，得到你设备的人就有可能访问其上所有敏感信息。除此之外，你可能还会在线进行敏感交易，比如访问网上银行或者进行网购。如果一个网络攻击者监听你的线上活动，他们就能窃取你的所以信息，诸如你的财务账号或者信用卡卡号。加密通过确保未经授权的人无法访问或修改你的信息而让你免受这些情况的侵扰。

未经加密的信息叫做明文，任何人都能轻易地读取、访问它。加密则是利用复杂的数学运算和一个独一无二的密钥，将这种信息转化为一种不可读的形式，我们称之为密文。密钥如同一把开门和锁门的钥匙，可以用来给信息上锁和解锁。密钥的一个常见形式就是密码，只有拥有密码的人才能解密和访问信息。要保护加密信息就要保护密钥。总体上讲，加密有两种形式——一种是加密静态数据（如存储在笔记本上的数据），另一种是加密动态数据（如线上传输的信息）。

加密静态信息

加密静态数据主要是为了防范计算机或者移动设备遗失或被窃的情况发生。十五年前，这个问题并不存在，因为大多数计算机大而笨重，你根本难以挪动。今天，许多笔记本仅有几磅重，移动设

加密

备甚至仅有几盘司。这些设备神通广大，能存储大量信息，但同时很容易遗失。除此之外，其它移动媒介同样能存储敏感信息，USB闪存驱动器或CD就都是这样的媒介。一个常见的加密这些媒介的技术叫做全盘加密（Full Disk Encryption，FDE），这意味着系统上的任何东西都会被自动加密，你不需要决定什么该加密和什么不该被加密。现在大多数操作系统都自带全盘加密功能，你只需要开启这个功能。举个例子， Mac OS X自带FileVault，而一些版本的Windows自带Bitlocker。如果你的计算机支持全盘加密，我们强烈建议你开启这一功能。另外，大多数手机也支持针对内部存储的全盘加密功能。例如，只要你设置了一个密码，iPhone和iPad搭载的iOS就自动应用全盘加密功能。要判断你公司的计算机或移动设备是否支持全盘加密，资讯一下前台或上司；如果是个人电脑，就联系你的电脑制造商或者浏览在线说明文档。

加密是保护信息的有效方式，但是其有效程度取决于密钥强度。

传输数据加密

传输过程中的信息同样容易遭受攻击。如果数据未被加密，它就能被监听并且捕捉。这也就是为什么你要加密诸如访问网上银行、发送电子邮件或访问社交媒体网站等敏感的网络传输过程。HTTPS是最常见的线上加密方式，它意味着浏览器和网站之间的流量是被加密的。找找URL里面的https://、浏览器上的锁形标志或者地址栏的绿条，这些都是通信加密的标志。你可能会同时注意到这三个迹象，这取决于你的浏览器。除此之外，无论你哪次连接到一个公共WiFi网络，能使用加密就一定要使用加密。最后，发送、接收邮件时也要保证你的邮件客户端通过加密信道传输数据。大多数邮件客户端都提供加密功能，你的互联网服务提供商（ISP）也可能能帮助你开启你邮件客户端的这一项功能。

加密

以适当的方式实现加密

无论你使用哪种类型的加密以及你如何使用它，它们几乎都拥有一些共同的步骤，通过遵循这些步骤你才能合理地使用加密。

- 加密强度取决于密钥强度。如果某人猜到或者破解了你的密钥，他们就能访问你的数据。你需要保护你的密钥。
- 如果你将一个密码作为你的密钥，它一定要够长够安全，而且你千万别丢失或者忘记了它。如果你把它给忘了，你的数据就解密不了访问不了了。
- 加密强度还取决于计算机的安全程度。如果你的计算机被入侵或者受到感染，网络攻击这就能绕过你的加密机制。因此，一定要保证你的计算机和移动设备也处于安全之中。
- 如果有多重加密方式可选，总是选择强度最高的。

了解更多

订阅OUCH！安全意识月刊，访问OUCH！过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：http://www.securingthehuman.org

相关资源

Mac OS X Filevault: http://support.apple.com/kb/ht4790

iOS加密: http://support.apple.com/kb/ht4175

Android加密: http://www.androidauthority.com/how-to-encrypt-android-device-326700/

Windows加密: http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

保护你的电脑: http://www.securingthehuman.org/ouch/2012#december2012

密码管理器: http://www.securingthehuman.org/ouch/2013#october2013

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：成自豪

