电脑用户安全意识月刊

OUCH!

本期摘要

- 什么是数据加密?
- 什么数据能够被加密?
- 如何正确加密

数据加密

什么是数据加密?

你可能听很多人提到过“数据加密”这个概念，以及应该如何使用数据加密来保护你自己和你的个人信息。然而，数据加密有时又非常令人困惑，并且你需要了解它本身的局限性。本期简报将深入浅出地讲解什么是数据加密，数据加密将如何保护你的信息和如何正确的加密数据。

客座主编
Francesca Bosco (@francibosco) 是联合国区域间犯罪和司法研究所研究人员及项目官员，负责管理网络犯罪、网络安全以及科技滥用等相关领域的项目，同时也是the Tech and Law Center的联合创始人。

你的个人设备上通常存储了大量的敏感信息，比如私人文件，照片以及邮件等等。如果你的某个设备遗失，那么存储在上面的所有敏感信息都有可能被持有该设备的人所获取。另外，当你在网络上进行诸如网上银行或网上购物等敏感交易的操作时，如果有人监控你的在线活动，他们很有可能会盗取你的银行账号或者信用卡号等个人信息。而此时数据加密能够通过防止未经授权者获取或更改你的个人信息的方法，来保障你的利益不受到侵害。

数据加密的历史可以追溯到几千年前。虽然现在的数据加密比以前要复杂得多，但其最终目的是一样的，即将秘密信息从一个地方传送到另一个地方，并确保在此过程中只能由授权者读取其内容。当信息没有被加密时，被称之为明文，这种信息可以轻易地被任何人获取或者阅读。而数据加密则可以将明文转换成一种不可读的形式，即密文。当今的数据加密通过复杂的数学运算以及独特的秘钥设计将你的信息转换成密文。秘钥，顾名思义就像一把钥匙，用来给你的信息上锁或者解锁。大多数情况下，你的秘钥就是一个密码。

什么数据能够被加密?

通常来说需要对两种数据进行加密：一是闲置的数据，比如已经存储在你的移动设备上的数据；二是传递中的数据，例如正在接收的电子邮件或者正在发送给朋友的短信。

数据加密

加密闲置的数据对于保护遗失的电脑或者移动设备上的个人信息非常重要。现如今的电子设备非常强大并且能够存储大量的信息，但同时也非常容易丢失。与此类似的还有其他类型的移动媒介，比如U盘或者移动硬盘，也能够用来存储敏感信息。全盘加密是最为广泛使用的数据加密技术，主要通过对整个磁盘进行加密从而进行防护。采用这种技术意味着系统上的所有内容都将被自动加密，而不需要你决定哪些数据需要被加密。现在的大多数电脑都自带全盘加密功能，不过有时你可能需要手动开启该功能。在Mac电脑上，该功能被称为FireVault，而Windows电脑则可以根据不同的系统版本使用Bitlocker或者Device Encryption。大多数移动设备也支持全盘加密。iPhone和iPad上搭载的iOS系统会在你设置密码后自动开启全盘加密。谷歌公司要求从安卓 6.0 棉花糖系统开始，当设备硬件达到一定标准后将默认开启全盘加密功能。

数据加密是保护个人信息的强有力的方法，但其安全程度取决于你的秘钥强度。

传输过程中的信息也同样容易受到攻击。如果数据没有被加密，它有可能会在网络上被监控，修改以及获取。这就是为什么你需要确保所有敏感的网上交易和谈话数据都要被加密。最常用的网络数据加密是超文本传输安全协议（HTTPS），将你的浏览器和网站之间的数据交换全部加密。你可以通过确认地址栏链接中是否包含https://，浏览器是否显示锁型图标，或者地址栏是否变成绿色来进行辨别。另一个例子是收发电子邮件。大多数电子邮件客户端支持用户自行开启的加密功能。第三个例子是在线聊天，比如使用iMessage，Wickr，Signal，WhatsApp或者Telegram等。这一类的应用软件使用端对端的加密方式来防止第三方获取传输过程中的数据，从而保证只有你以及你正在交谈的对象能够获取聊天内容。

如何正确加密

通过数据机密保护个人信息的关键在于正确地进行加密。

- 数据加密的安全性取决于你的秘钥强度。如果有人能够猜到或者得到你的秘钥，那么他就能够

数据加密

获取你的数据，所以一定要保护好你的秘钥。如果使用密码来作为你的秘钥，那么请确保该密码是特殊的强密码。密码越长，越难被攻击者猜中或者暴力破解。不要忘记你的密码，因为没有秘钥，即便是你本人也无法获取被加密的数据。如果你不能够记住所有的密码，那么我们推荐你使用密码管理器。

- 数据加密的安全性取决于设备的安全程度。如果你的电子设备存在系统漏洞或者被植入了恶意软件，网络攻击者有可能绕过你的加密从而盗取你的数据。这也是为什么必须采取一些措施来保护你的设备安全，例如使用杀毒软件、强密码以及使用最新版本的软件。
- 很多移动设备的应用软件和电脑程序提供强数据加密来保护你的数据安全。如果你正在使用的应用或程序没有加密功能，请考虑使用其他具有加密功能的程序。

了解更多

订阅OUCH! 安全意识月刊，查看OUCH!往期内容，以及了解有关SANS安全意识方案的其他内容，尽在 securingthehuman.sans.org/ouch/archives.

Dyn is a cloud-based Internet Performance company. Dyn helps companies monitor, control, and optimize online infrastructure for an exceptional end-user experience. Through a world-class network and unrivaled, objective intelligence into Internet conditions, Dyn ensures traffic gets delivered faster, safer, and more reliably than ever.

相关资源

Encryption Explained:
http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

密文: https://securingthehuman.sans.org/ouch/2015#april2015
密码管理器: https://securingthehuman.sans.org/ouch/2015#october2015
恶意软件: https://securingthehuman.sans.org/ouch/2016#march2016
平板电脑安全使用手则: https://securingthehuman.sans.org/ouch/2016#january2016

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
翻译：陈柳希

