電腦用戶安全意識月刊

OUCH!

本期話題

- 什麼是加密？
- 信息靜止加密
- 信息傳遞加密
- 正確實施加密

加密

什麼是加密?

編輯嘉賓

Christopher Crowley（**@CCrowMontance**; **+ChrisCrowley**）是在華盛頓特區的顧問。他是SANS課程「移動設備安全和道德黑客（SEC575）」主任講師，以及「應急響應團隊管理（MGT535）」課程的作者。

你可能會聽到人們用“加密”這個詞，以及和你應該如何使用它來保護自己和你的信息。然而，加密的概念顯得比較撲朔迷離。而且，加密不能保護你的一切，它也有其局限性。在本月刊中，我們會簡單的來解釋什麼是加密，為什麼你應該使用它，以及如何正確地使用它。

你有巨大數量的敏感信息在你的設備裡，如財務文件，圖片，電子郵件或醫療記錄。如果你有一個這樣的設備丟失或被盜，設備上所有一切非常敏感的信息都可以通過這個設備取得。此外，你可能會進行敏感的網上交易，如網上銀行或在線購物。如果網絡攻擊者監控你的上活動，他們可以竊取你的所有信息，如你的金融賬戶或信用卡號碼。在這種情況下，加密可以保護你確保未經授權的人無法存取或修改你的信息。

沒有被加密的信息，被稱為純文本。這意味著任何人都可以輕鬆地讀取或訪問它。加密將此信息轉換成一種非可讀格式,稱為密文。加密的工作原理是利用複雜的數學運算和一個獨特的鑰匙來把你的信息轉換成密文。鑰匙是用來鎖定或解鎖你的信息，就像一個鑰匙可以鎖門和開門。一個常見的鑰匙例子是一個密碼，只有擁有該密碼的人可以解密和訪問你的信息。為了保護你的加密信息，你需要保護你的密碼。一般來說加密有兩種方式，你可以在信息靜止的時候加密數據（如存儲在你的筆記本電腦中的數據）和信息傳遞中加密數據（如網上傳遞信息）。

加密

信息靜止加密

加密是一個有力的方式來保護你的信息，但它只是強如你的鑰匙密碼。

在信息靜止時加密的主要目的是為了保護在你電腦或移動設備丟失或被盜的情況下的信息。十五年前，這不是一個問題，因為大多數電腦都很大，笨重的台式機的設備都很難移動。今天，許多筆記本電腦的重量只有幾磅，而移動設備只有幾盎司。這些設備非常強大而且持有大量信息，但也很容易丟失。此外，其他移動媒體也可以容納敏感信息，如USB盤或CD-ROM。一種常用的加密這些信息的方法被稱為全磁盤加密（FDE）。這意味著，系統中的一切都被自動加密，你不用決定什麼加密或什麼不加密。大多數操作系統現在配備了內置的全磁盤加密，你只需要啟用它。例如，Mac OS X包含的FileVault，和某些版本的Windows包含的Bitlocker。如果你的電腦支持全盤加密，我們強烈建議你啟用它。此外，大多數手機都支持全盤加密內部存儲設備。例如iOS上，iPhone和iPad的操作系統，一但密碼已設置，自動應用會全磁盤加密。想要了解在工作中你的電腦或移動設備是否支持全盤加密，請詢問你的幫助台或主管。如果是你的個人電腦，請聯繫你的電腦製造商或查看網上文檔。

信息傳遞加密

信息在傳遞中也是脆弱的。如果數據是不加密的，它可以在網上被監視和捕獲。這就是為什麼你需要確保任何敏感的在線交流，如網上銀行，發送電子郵件或訪問社交媒體網站都是加密的。在線加密的最常見的類型是HTTPS。這意味著你的瀏覽器和網站之間的所有通信都有進行加密。查找有https://開頭的網址，出現在瀏覽器上的鎖，或者你的地址欄變成綠色。這些都是跡象表明，通信是加密的。根據你的瀏覽器與網站，你可能會在同一時間看到所有這三個。此外，每當你連接到公共Wi-Fi網絡時，一定要盡可能同時使用加密。最後，發送或接收電子郵件時，請確保你的電子郵件客戶端設置是通過加密通道來發送電子郵件。大多數電子郵件客戶端提供加密的，另外，你的ISP（網絡供應商）也許能夠幫助你在你的電子郵件客戶端上啟用加密。

加密

正確實施加密

無論你正在使用哪種類型的加密或如何使用它, 幾乎所有形式的加密都有一些共同的步驟來正確使用它:

- 你的加密的強度和你的鑰匙密碼強度一樣。如果有人猜測或損害你的鑰匙密碼, 他們將有機會獲得你的數據。所以你需要保護你的鑰匙密碼。
- 如果你使用的是密碼, 確保它是一個長度高的, 安全的密碼, 不要丟失或忘記它。如果忘記密碼, 你自己的數據將會被鎖定。
- 你的加密只是強如你的電腦的安全性。如果你的電腦已經被入侵或感染, 網絡攻擊者可以繞過加密。因此, 一定要保持你的電腦或移動設備的安全。
- 如果你有不同的加密選擇, 一定要選擇最強的方法。

進一步了解

歡迎訂閱OUCH!電腦用戶安全意識月刊, 以及瀏覽前期OUCH!檔案。想要進一步了解SANS安全意識的方案, 請瀏覽我們的網站http://www.securingthehuman.org.

參考資料

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
保護你的電腦: http://www.securingthehuman.org/ouch/2012#december2012
密碼管理: http://www.securingthehuman.org/ouch/2013#october2013

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻譯：巴珊珊

