Cryptography Engineering Critique2 310555004 呂佳柔

Paper: Whitten, Alma, and J. Doug Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” USENIX Security Symposium. Vol. 348. 1999.

Summary:

這篇論文作者對名為 PGP 5.0 的 security program 進行了研究，為了驗證他們的假設: 有效的安全性需要不同的可用性標準，並且不用通過適用於其他類型的用戶界面設計技術來實現。

首先給出作者的結論，儘管 PGP 5.0 具有吸引人的圖形使用者界面，但它的使用者界面無法實現有效的安全性，因為它的界面設計標準模型對於未熟悉該領域的人去使用是不安全的，所以使用者會意外暴露了他們在這個過程中要保護的訊息，不只這點，作者還有其他更詳盡的分析。最後作者提出了一些策略以提高可用的安全性，研究如何將安全功能壓縮為真正需要且適合特定人群需求的實用方法，同時又不會犧牲提供給使用者的安全完整性。

Strengths:

作者團隊選擇使用兩種方法去評估 PGP 的可用性，兩種方法在不同的層面上都各有優缺點，而作者將這兩種方法視為互補的評估策略，我認為相當的不錯，而且會比在實驗室測試直接驗證認知演練(cognitive walkthrough)提出的觀點更為現實及有效率。

Weaknesses:

雖然說作者提到測試參與者普遍接受過電子郵件的教育和經驗，但事實上甚麼樣的程度是接受過電子郵件的教育和經驗，作者沒有詳細寫出，在我的理解意思是受測者只要會發送信件跟辨識釣魚信件就可以了，那這樣的人選是不是也會影響到認知演練的結果呢?

在最後的部分，雖然作者的案例研究中詳細提出了幾種設計策略，但是對於一些使用者來說，需要教學才有辦法進行操作，以了解如何學習及管理相關的安全性使用操作。但一般使用者可能不會將大量的教程閱讀完，所以可能需要有警告消息、指引等等，以便提供使用者正確的指導教學。

Reflections:

作者團隊提出之測試場景的想法內容，是讓參與者通過電子郵件將活動計劃更新發送給活動團隊的其他成員，使用 PGP 進行隱私和身份驗證，我覺得這樣的測試內容相當有意思。我也是從論文中第一次了解到認知演練(cognitive walkthrough)，這是一種可用性/易用性評估技術，研究者透過觀察使用者行為的樣子，來描繪出對使用者行為的文字紀錄。而平常有時候會接觸到的使用者

調查，又是不一樣的東西，兩者不能替代，雖然同樣都是搜集使用者行為的方式，但是認知演練跟使用者調查最大的不同在於，認知演練的觀察對象通常是團隊內部的人員，甚至會是研究員自己觀察自己的使用行為，並記錄下來。

如果我是撰寫這篇論文的作者之一，我可能會在挑選參與者的階段時，選入一些有基本密碼學知識的人選，因為作者提到此篇論文的使用者測試是由 12 名不同的參與者進行，在測試之前，沒有人能夠描述公鑰和私鑰密碼之間的區別，所以我在想如果有基本密碼學知識的人是否會對 PGP 介面操作又有不一樣的想法出現。