Critique 6: b07902127 資工二 羅義鈞

The Tangled Web of Password Reuse

Summary:

這篇 paper 在講網路上的文字形式密碼重複使用的情形。本文指出當使用者於某一個網站的密碼被破解時，直接使用該密碼去登入其他網站成功的比率不低。以作者的 database 統計結果來看，其高達 43%。除此之外，多數使用者使用其中一個密碼的 substring 作為其他密碼的比率為 19%，這表示多數使用者資訊安全的層級大幅降低至最低層級的保護。作者透過資料的分析與匿名使用者的問卷調查，去推測面對需要密碼限制與組合的網站時，使用者頃向什麼樣的 transformation pattern，以及修改密碼、重組的習慣。最後再透過設計的演算法，去分析得到的數據結果以評估可行性，亦能讓使用者測試密碼替換的好壞。

Strengths:

1. 作者設計的演算法既簡單，針對 substring 又有成效，可以讓普遍的使用者作為測試工具檢驗自己於不同網站的不同密碼是否為有效果的替換。而這個演算法是 feasible 的，嘗試次數不會過多，於現實中是可用的。
2. 作者資料的分析整理以及問卷調查大幅提升了對於使用者密碼設定的理解與行為模式，這有助於設計出更有效率的演算法，也讓更多人知道該如何去實行密碼安全性的驗證。

Weaknesses:

1. 作者得到的 database 裡，絕大多數的使用者僅使用兩組不同的密碼，這對於作者的研究結果會有偏差，因為目標應該是多個不同網站使用者會如何替換密碼，然而樣本中大多使用者僅有一組不同的密碼。
2. 在歸類之中，做的的演算法對於 others 的破解僅佔了 4%，成效並不好。然而，許多 others 中的密碼是非常相似的。這也是演算法簡單反面的缺點。

Reflection:

1. 密碼的歸類上只有分類為相同、子字串、others，如果可以對 other 再多做一些分析，或許可以得到更多關於密碼的資訊，而不會讓目標被侷限住。
2. 在密碼的使用上如果密碼數量以及相異性太大，我們會因為不容易記憶和嫌麻煩而不這麼做。因此如果能找出有效替換密碼並且方便使用者去使用和記憶的方式，會大幅讓資訊安全提升，且使用者也會更願意去實踐，而不是只有單純去宣傳教育而已。

Reference: http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf