Critique 9: b07902127 資工二 羅義鈞

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

**Summary:**

Diffie-Hellman 演算法被廣泛使用於 Internet Protocol 的 key exchange，然而實際上有安全上的疑慮。由於 Diffie-Hellman 的假設是數學上計算困難導致無法以 real time 完成運算，因此並沒有對來源進行身份檢驗。這導致中間人攻擊的可行性：透過"The number field sieve algorithm for discrete log"做預處理運算，針對常用的 512bits group 就能達成 real time 效果。再配合 downgrade attack，使得 TLS Diffie-Hellman 有一定的比率會被破解。這個 attack 被作者定義為 Logjam attack。作者同時也對 768, 1024 bits group 做了 computation 的分析，認為國家級的運算資源是有辦法去破解的，也針對 1024 bits group 一旦被破解會造成的影響去做分析。最後，作者對於 Diffie-Hellman 的安全性提出了一些建議：他認為使用 ECDH 會是最有效率與最根本的解決方法，這會讓 precomputation 失去效果。而其他方式如禁止使用 DHE_EXPORT，以避免 downgrade attack 等。

**Strengths:**

1. 對於 Logjam attack 進行方式，有清楚的數學模型，且如何作為中間人的攻擊互動過程寫得十分清楚，便於理解。
2. 對於 computation time 的分析有數據做為佐證，統整成表格讓理解更加容易。

**Weaknesses:**

1. 沒有說明 ECDH 是如何做到讓 discrete log problem 變得更加困難，只有說這方法可行。
2. 作者說 768 bits group 是可以破解的，但是對其沒有佐以任何數據分析。除此之外，1024 bits group 也只是數學的估計，沒辦法實際去執行。

**Reflection:**

這篇 paper 讓我對於 Diffie-Hellman 有更進一步的了解。我認為 Diffie-Hellman 仍舊是可行的 Key-exchange 演算法，只是 group 需要取至少 1024 bits 的，或是如作者所說，改使用 ECDH(Elliptic Curve Diffie-Hellman)的方式。而這篇 paper 也讓我瞭解到即便 protocols 有進行了更新，如果對於舊的不安全版本依舊支援的話，就會讓攻擊者有機可趁。Diffie-Hellman 是十分廣泛使用的演算法，因此如果作者提出的漏洞沒有做適當的處理與修補，對資訊安全所造成的影響是非常大的。作者如果能對他提出的建議做更進一步的說明，相信對於研究者會有更多的幫助。

Reference: https://weakdh.org/imperfect-forward-secrecy.pdf