撰寫：陳約廷
日期：2018.05.15
標題：Reading critique - ForceHTTPS: Protecting High-Security Web Sites from Network Attacks

---

Summary

這篇論文推出了一個新的機制－－ ForceHTTPS ，試圖解決網路上不安全連線所帶來的資訊安全危險。首先在 Proposal 中提出 ForcesHTTPS 的方法，就是對 HTTPS error 做更嚴格的限制。

- 非 HTTPS 的連線(HTTP)會被強制轉成 HTTPS 連線
- TLS error 會直接中斷當前 session
- 網頁內容中非 HTTPS 的要求會被直接視為連接錯誤

再來是 Threat Model。 ForceHTTPS 假設攻擊者可以攔截封包或者是假裝伺服器或者連接者，或是單純網站設計不當的網頁開發者。也列出 ForceHTTPS 無法保護的攻擊方法－－釣魚網站或者惡意程式或是瀏覽器的設計不良。

接下來 Related Work 中把現有的保護機制分為兩大類：

1. 使用者控制類

- 使用者即便強制 HTTPS 連結，但是如果 cookie 是以 HTTP 傳輸的話，仍然會外漏出資訊與可以被竄改，進而綁架這個連結 session
- 現有對憑證錯誤的警告就是一個簡單的對話筐，而這個也導致使用者習慣於馬上通過對話筐而忽略背後的危險
- 對 HTTPS 連結加 HTTP 內容也是簡單的警告視窗，並無真正攔阻警告的效果

2. 網站控制類

- 即使 cookie 是透過 HTPS 傳輸，如果使用者誤入攻擊者架設的惡意網站， cookie 仍然會在偽造的憑證下被竊取

ForceHTTPS 可以讓所有連線一直維持在 HTTPS 的保護之下，也對不安全的憑證做更嚴格的 error handling ，但是如果網站不提供安全連線， ForceHTTPS 是無法保護使用者的。如果網站設計者在網頁中有 XSS, CSRF 或者在 URL 中安插 script 這種不良設計，仍然可以被攻擊者拿來當作漏洞攻擊。但是大致來講 ForceHTTPS 在網站健全的情況下，可以有效的預防竊聽者竊聽傳輸內容。

Strength(s)

- 有效解決網路連線中可能被竊聽的問題
- 解決方法容易且無大量成本

Weakness(es)

- Introduction 中的 Unknown intent 應該是冗贅可以被刪去的
- Related work 中與 ForceHTTPS 的比較沒有很清楚，僅寫出 ForceHTTPS 怎麼做，沒有說解決與沒有解決什麼
- 對釣魚網站沒有用，這個明顯的問題應該被提出在討論裡

Reflection(s)

這篇論文清楚的寫出了提出的機制 ForceHTTPS，如果我是作者應該會把 Related work 與 Discussion 的位置互換，並增加 Related work 中與 ForceHTTPS 的比較。未來也可以 survey 提出的機制是否正確的解決了可能被 eavesdrop 這個問題。