Critique 4:

Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web

Summary:

這篇介紹 Let's Encrypt：一個公開免費且自動化的 CA，得以讓網路加密更加普及化。文中提及 HTTPS 的架設過程十分麻煩又容易出錯，加上要花費不少錢去獲得 CA，造成網頁的設計者不願意去使用較安全的 HTTPS。除此之外，若無法在憑證過期前更換，網頁會在使用者使用時顯示不安全，造成該網頁使用者的下滑。也因此本文推廣了 Let's Encrypt 的優點，最主要就是自動化的好處，同時介紹了其創立歷史、發展與優勢和實際系統、結構的說明。最後再提出至今仍未解決的安全問題，希望更多人能投入研究，讓網路加密更加普及化，安全層級得以更加提升。

Strengths:

1. 自動化：Let's Encrypt 提供自動化的 CA，大量減少人力與時間去完成憑證，同時避免了人為操作時的失誤。除此之外，以 90 天作為週期去更新憑證，時間比一般的憑證需經過數月至一年的時間才更換要來得短不少，既增加了安全性，又不會說短到做一些做一些手動的更新會來不及。
2. 免費且公開的資源，且 security 的效果也還可以，甚至能幫忙避免掉一些設定上的失誤和疏失，這讓 HTTPS 的普及率很有效的提升。雖然說 security 層面仍不是最直接的提升，但是相對簡單容易的操作已經讓誤用情形減少許多，使用者的安全能得到一定程度的保障。

Weaknesses:

1. 自動化只是改善了憑證問題，但是沒有將其解決。最根本上的問題是 domain validation 自身並沒有加密保護，因為他是由那些網站加入 PKI 的 bootstrapping 機制。最糟糕的情形是攻擊者暫時掌握一個 domain，然後把 key 改成他們控制的 key。
2. Let's Encrypt 反過來被網路釣魚給大量使用。由於沒有辦法去偵測網站內容的安全性，CA 被濫用的問題仍無法解決。

Reflection:

HTTPS 的使用對於網站的安全性有顯著的提升，Let's Encrypt 確實對於其推廣有很大的助益。然而延伸出來的相關問題也十分麻煩。我認為作者對於 Let's Encrypt 的歷史與非營利的運作方式介紹篇幅有些過多，若是能多講一下實際面的操作方式和運作模式，會能更幫助理解。整體來說，這仍是非常棒的 CA，相信對於網路資訊安全有相當的幫助。