Capsicum: Practical Capabilities for Unix

一、成員

1. 洪盛益(40947047s), sheng-yihong@acm.org,
2. 黃冠棠(40947025s), i0905108390@gmail.com,
3. 黃定凡(41047032s), din2009siuc@gmail.com

二、動機

在我們寫程式的時候，難免會寫出一些安全性上的漏洞，修補漏洞的過程困難且繁雜，而且並不能一勞永逸，畢竟程式碼越寫越大，漏洞會越來用多，那我們便需要一種更上層的方法來控管，Capability 便是這種概念下的產物，capability 考慮的點不再是寫出安全的程式，而是對程式的權限做限制，讓程式符合最小權限原則，就算底下的程式寫出漏洞，也會因為 Capability 的原因沒有權限執行。

三、介紹

那我們提案的內容就是基於 FreeBSD 的一個 Capability 實作 - Capsicum

Capsicum 是一個輕量的capability和沙盒框架，他可以限制程式的權限，讓他無法使用不需要的功能，如果我不需要 wirte 權限，我可以把他關起來，以提升系統的安全性。
他提供和 capabilities 兩個 kernel primitives，以下分別介紹。
capability mode :他會限制程式讀取global的OS namespaces，只有授權過的功能才能使用，一旦設置，他的 children processes 也會繼承同樣的設定。
capabilities :限制 file descriptors 能進行的操作，例如由 open 回傳的 file descriptors 能進行 read 和 write，但不能進行 fchmod。

四、期末報告流程

1. 介紹主題
2. 介紹 Capsicum 的 source code
3. 介紹 Userland program 的 Patch
4. 漏洞展示

五、漏洞展示
Demo 一個 reverse shell,（受害主機）在未使用 Capsicum 的情況下，攻擊者會成功拿到被害主機的 shell 。使用了 Capsicum 之後由於攻擊程式的權限被最小化，因此該程式沒有受害主機中其他檔案的讀 or 寫權限。

Reference:
我們只需要一個 Reference，裡面有當年的投稿論文跟演講，還有後面的一些其他 BSDCAN 的介紹，甚至還有哪些程式被 Patch
https://wiki.freebsd.org/Capsicum