UNIX環境下CGI安全問題之研究

蓋國建

國立清華大學 計算機中心

新竹市光復路二段101號

E-MAIL：kckai@cc.nthu.edu.tw

摘要

本篇文章之目的，是以UNIX環境下的WWW系統為研究對象，針對開放CGI程式之設計權限給WWW資料提供者所衍生的系統安全問題來加以分析，並提出適當的解決之道，以便能在兼顧系統安全的考量下，讓每一位WWW資料提供者都有權限來設計自己的CGI程式。

1、簡介

隨著WWW(World Wide Web)系統的普及，提供資料的工作已不再是少數系統管理者的任務。目前大多數的WWW系統都允許每一位WWW站上的用户成為資料的提供者。長久以來廣大的資料提供者並不甘於只侷限在製作簡單的HTML（Hyper Text Markup Language）文件〔1〕，他們也很想設計一些CGI（Common Gateway Interface）程式，並配合FORM的功能來製作一些交互式的應用，如資料的登錄或查詢。

CGI程式是使用者對WWW系統作再次溝通最主要的利器。但若是CGI程式的設計權限一旦由系統管理者的手中下放到每一位資料提供者的身上，將會引發極為嚴重的系統安全問題，如檔案系統被蓄意破壞等。因此，如何針對上述問題加以改進，使得CGI程式的使用能克服安全性與普及性的兩難，即為本篇文章的重點。本篇文章是以UNIX環境下的WWW系統為研究對象，內容共分為四節：除簡介之外，第二節為分析CGI程式的安全問題；第三節將提出一個解決方案；最後一節則為結論。

2、CGI的安全問題

傳統上，WWW站上的資料區與CGI程式區是被設定在不同的區域內。資料區的權限是開放的，可由WWW站的系統管理者或一般用户自行維護資料；CGI程式區的權限是管制的，CGI程式只能由系統管理者來存放。若欲將CGI程式的設計權限開放給一般用户，較簡單的作法有三種：

1. 將CGI程式區目錄的存取權限打開。例如以指令chmod 1777 /www/cgi-bin將/www/cgi-bin的存取權限設為rwxrwxrwt，以便讓用户們在此目錄內自行存放CGI程式。
2. 為每一位WWW站上的用户開放一塊CGI程式區。例如在CERN httpd 程式的設定檔中加入Exec /user1/cgi-bin/* /home/user1/WWW/cgi-bin/* 使得用户user1在/home/user1/WWW/cgi-bin下存放的CGI程式均可被httpd執行〔2〕。
3. 為CGI程式定義一個新的MIME type，使得所有CGI程式不論存放在何處均可被執行。例如在NCSA httpd程式的設定檔中加入AddType application/x-httpd-cgi .cgi如此一來所有以cgi為副檔名的檔案不論存放在何處均可被httpd執行。

以上三種方式都會產生一個相同的安全問題：由於CGI程式一直是被httpd所執行，因此即使是一般用户的CGI程式在被執行時，執行者的角色是httpd的擁有者，而非CGI的擁有者〔3〕。我們若是仔細的考慮當指令‘/bin/rm -r /’出現在一般用户的CGI程式中，就不難理解系統可能會遭遇

到的安全危機。圖一說明了在WWW架構下，httpd程序（process）與cgi 程序之real user ID（UID）與effective user ID（EUID）變化的情形。

3、解決方案

由圖一我們可以看出安全問題的產生是因為cgi被執行時，process UID是www而非cuser或fuser。為了能使cgi的process UID能回復成cuser或fuser，一定要藉助一個set root UID的程式才能竟其功。有了此項認知後，我們接下來必須決定在WWW的運作結構中，由何者來扮演set root UID的角色。我們相信至少有下列兩種選擇：

1. httpd。當cgi被httpd呼叫時，process UID直接由www轉換成cuser或fuser。
2. 另一個cgi程式。在httpd呼叫使用者的cgi之前，先呼叫一個set root UID的cgi，然後再由其呼叫使用者的cgi，並將process UID轉換成cuser或fuser。

若以執行效率（performance）來比較，第一種方法顯然較佳。但若著眼於WWW系統的整合性與開發軟體的難易度，第二種方法應該是最佳選擇。因此，我們發展一個set root UID的程式scgi（Secure CGI），並提出新的架構如圖二。其運作步驟如下：

1. 在FORM中設定輸入後的處理程序：先交由scgi處理，然後再轉交給cgi。
2. WWW browser對FORM作回應。
3. httpd呼叫scgi。
4. scgi：
   ①seteuid（uid of HTTP_REFERER），也就是將EUID轉為FORM的UID
   ②exec（cgi）
   ③seteuid（uid of httpd）

在此有一點要特別提出說明：scgi是將EUID之值由root轉為fuser（FORM的擁有者），而非cuser（cgi的擁有者）。雖然fuser與cuser在大部份的情況下是相同的，但我們考慮到CGI程式應視為可供全體用户共用的工具，其使用權限應該是開放的；而FORM的內容應該是私有的，因此我們才對EUID的轉換作如此的設計。

4、結論

距我們提出scgi構想開始，至今已有一年多了。其間經過不斷的測試與改進，目前的運作情況非常良好。我們並且在scgi的程式中增加了對CGI input string作解碼的功能，使得後面的cgi程式的撰寫工作得以減化。

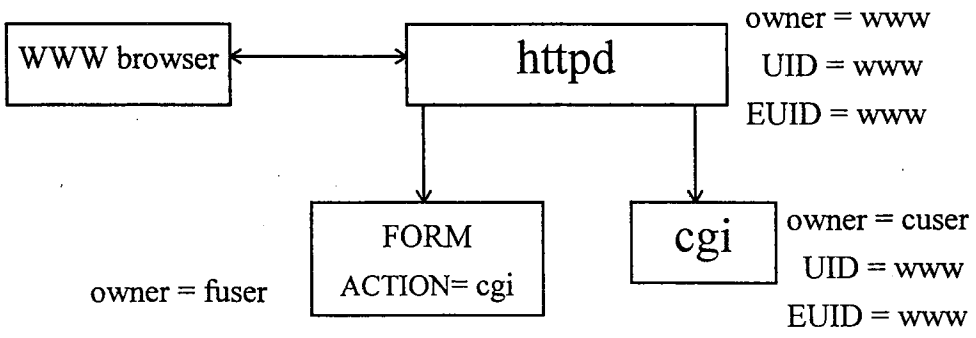
依前述的解決方案行之，整個WWW系統的安全防線將會拉到FORM檔案的擁有權上。如此一來，整個WWW的安全管制工作就得以回歸到UNIX作業系統的安全機制上。

5、參考文獻

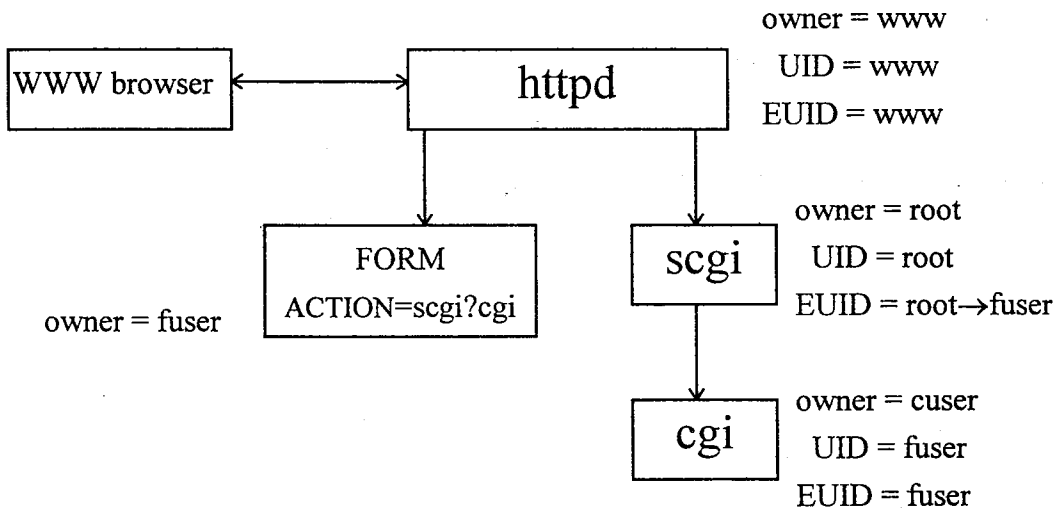
〔1〕Tim Berners-Lee，*Hyper Text Markup Language*，Internet Draft，13 July 1993。

〔2〕Tim Berners-Lee，*CERN Server User Guide*，CERN，4 March 1994。

〔3〕Time Berners-Lee，*Hypher Text Transfer Protocol*，Internet Draft，5 Nov 1993。



圖一　http 與 cgi 之 UID 與 EUID



圖二　http 、 cgi 與 scgi 之 UID 與 EUID