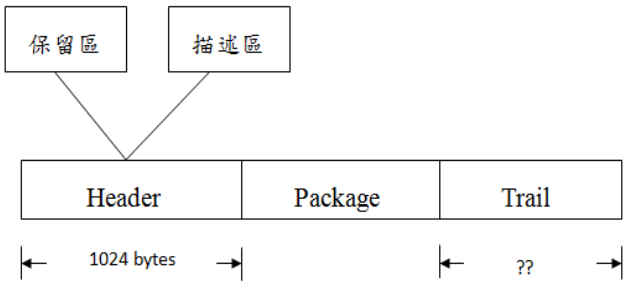
Secure Authorization & Patch Download : Applications of Public-Key Cryptography and Hash Functions

(Prof. Yeong-Sung Lin)

一、基本介紹：

1. 主旨：練習利用非對稱式加密法與可信第三方來實作 patch 檔的發布
2. 加密檔案格式：分成三個部分，包括 Header、Package、Trail。
   (1)Header：大小為 1024 bytes 。
   描述區：512 bytes。
   保留區：512 bytes。
   (2)Package：此區域存放加密過的授權碼或更新檔。
   (3)Trail：大小係依照所選定之雜湊函數而定（例如 MD5 為 16 bytes）；將 Header 及 Package 合併後，運用所選定之雜湊函數進行運算，產生雜湊值（Hash Value）放入此區域。
   如下圖所示：



圖一 加密檔案格式

3. 加密檔案傳送方式：
   設備端與原廠端須在不同主機上運作，程式本身須具備加密檔案傳送能力，不透過外部程式的輔助，以網路傳輸方式自動交換資料。

二、系統流程：

1. 作業流程一：「非對稱式金鑰加密傳輸」：
   步驟一：
   廠商人員透過系統上傳更新檔。

步驟二：

系統收到更新檔後自動通知所有設備端有 patch 檔可供更新。

步驟三：

設備端收到通知後，將授權碼使用原廠端的公開金鑰加密後，依照前述之加密檔案格式需求，發送至原廠端進行驗證。

步驟四：

原廠端收到設備端發送之授權碼後，使用本身的私密金鑰解密，進行驗證。

步驟五：

驗證無誤後，再將更新檔使用設備端的公開金鑰加密後，依照前述之加密檔案格式需求，發送至設備端進行更新。

步驟六：

設備端收到原廠端發送之更新檔後，使用本身的私密金鑰解密，以進行系統升級。

2. 作業流程二：加入「數位簽章」：

由於透過流程第一部分，可確保授權碼或更新檔之機密性與完整性，但無法達成發送方之不可否認性（Non-Repudiation），即無法保證授權碼是由設備端所發送出，或無法保證更新檔是由原廠端所發送出。第二部分流程即是要達成此項保證。

2.1 加密方

步驟一：

將加密後之授權碼或更新檔，運用所選定之雜湊函數(SHA-1、MD5、Whirlpool)進行運算，產生雜湊值。

步驟二：

將前述的雜湊值，使用本身的私密金鑰加密，以確保授權碼或更新檔的發送來源。

步驟三：

將雜湊值加密後的結果，放入 Header 之保留區，隨著加密檔案一起發送至對方。

2.2 解密方：

步驟一：

將加密檔案 Header 之保留區中的資料獨立取出，並使用對方的公開金鑰解密，得到一個雜湊值。

步驟二：

將加密檔案之 Package 部分，運用所選定之雜湊函數進行運算，產生雜湊值。

步驟三：

前二步驟中所得之雜湊值相同，方得進行後續解密動作（加密檔案之 Package 部分）；若二者不相同，則捨棄所得之檔案並顯示警告訊息。

3. 作業流程三：實作並使用 Public Key Authority：

步驟一：

請事先在 Public Key Authority 建立一個合法使用者的 IP List，利用 IP 合法性驗證使用者身分。若無第三台電腦，Public Key Authority 可建在原廠端或設備端其一，但傳輸還是必須透過網路連線機制。

步驟二：

原廠端送出 request 與任意訊息 T1 到公正的 Authority 提出申請。

步驟三：

在 Authority 得知後，將設備端的公鑰與相關資訊綁在一起，並為之簽字後發給原廠端。

步驟四：

原廠端以設備端的公鑰加密自己的 ID (IP 位置)與隨機數 N1 傳送給設備端。

步驟五：

設備端傳送 request 與任意訊息 T2 給 Authority，並經由 Authority 得到原廠端的公鑰與相關資訊 (Authority 簽字過)。

步驟六：

設備端利用原廠端的公鑰加密 challenge 對方，檢查對方是否能解開得到資訊

步驟七：

原廠端若能成功解開並回傳資訊則代表其為真，之後開始通訊則可免去上述 步驟 2 到 4

步驟八：

再次實作作業流程一。