資訊安全筆記第八週

胡樂麒

2024/5/6

1 對稱加密中的 man in the middle attack

使用對稱式加密法，讓兩人有一個共同的 key 來傳遞訊息，使中間人無法知道裡面內容，然而缺點是 a 跟 b 則必須要私下見面來給 key，並且根據攻擊的人能力不同，裡面的內容也可能遭到中間人的修改。

2 digital signature(public key mac)

使用此方法需要用 private key 來進行簽名，並且 private key 只有自己知道，因此便可以用 public key 來驗證簽名是否為真，此方法便可以解決中間人攻擊，此性質為 non-repudiation。公式:verify(p,m,σ)=1 iff σ=sign(s,m)

3 MAC

在 MAC 當中使用同一個 k 來進行 tag 跟 verify，因此當 a 和 b 在互相交換訊息，雙方互相知道 k，所以可能會造成有人發了訊息但是突然不想認帳，因此誣賴對方用了自己的 tag 來傳訊息給自己，可能會造成捏造作假的嫌疑，此性質為抵賴 (repudiation)。公式:verify(k,m,t)=1 iff t=Mac(k,m)

4 digital signature and MAC

在 MAC 中做 tag 時，使用的 key 是同一把。而在 digital signature 中 verfy 跟 sign 則是用 public 和 private 兩把 key 來做，因此 digital signature 則可以用簽名來辨認，防止 man in middle attack 或賴帳的問題。
在法律中而數位簽章與簽名同等地位。

5 RSA 數位簽名

pk: 公鑰,s: 密鑰,m= 訊息
Enc(pk,m)=m^e mod N = c Dec(s,c)=c^d mod N

1.(s,pk) gen, s=(p,q,d=e^-1 mod(p-1)(q-1)) pk=(N=pq,e)

2. σ=sign(s,m)=m^d mod N

3. verify(pk,m,σ) = m = σ^e mod N (檢查是否相等)

$\sigma^e = (m^d)^e$ mod $N = m$ mod N (d * e = 1 互為倒數)

數位簽章有好幾種作法其中 rsa 他竟可以用來加密也可以簽章，在加密中先用 publickey 加密，再用 private key 解密，在 signature 中則反過來，簽名時先用 private key 要驗證的時候再用 public key。

6 public-key infrastructure(PKI)

在一開始的對稱式加密法還有 key establishment(RSA,DH)，其中遇到 ind-cca 和 mitm 對 key 的進攻，在這裡面最大的問題是該如何讓雙方可以有一個共享的 k 並且不會被別人盜取，然而 rsa signature 的出現解決了大部分的問題，但他並非完美，因為要達成此條件必須要讓大家可以獲得正確的 public key，第一種方法是以小群體，大家一起互相交換 public key。
而當人數較多的時候，有兩種方法，其中一個是找可信度較高的組織，例如政府，透過他來收集所有人的 public key 並做成一張表，蓋上組織自己的簽名，這樣民眾便可以用政府的 public key 來驗證那張表是否出自政府 $((a,P_a),\sigma_{gov},a)$，此方法為 centralized PKI。
另外一種方法則是透過其他人的簽名來證實此人的 public key 是真的，發證書的人為 CA(certificate authority)，例如: 當 B 同時認識 A 與 C，而 A 要和 C 進行聯繫時，則 B 會給 A,C 的 public key (C,P_C,σ_{BC})，C 則會給 A(g_c,σ_c) 而前提是 A 完全相信 B。此方法稱為 chain of trust。

7 六度分隔理論

這個理論的主要概念是，任何兩個人之間的距離最多不超過六個中間人。這代表著你和世界上任何一個陌生人之間，最多只需要透過六個中間人就可以建立起連繫。這個理論恰巧可以用來呼應上面提到的 chain of trust。

8 PKI on internet

這是一種是連接網路的，由一台終端機 (root CA) 藉由控制底下的小 CA 最後來連接機器，rootCA 也會和其他 rootCA 進行混合。