Thursday, May 19, 2016

HW3

1. SYN cookie

(a) SYN cookie提供一種更嚴謹的來源監控和資源分配，不會單純地收到SYN訊息就配置資源給來源位置，如此一來攻擊者要佔用、耗竭私服器資源就必須回傳ACK訊息並記錄、回傳相對應的資料，這會讓攻擊者不容易scale up。

(b) timestamp可以對應到特定的cookie，如果沒有timestamp，攻擊者就可以重複使用同一個cookie。

(c) 記錄client address可以將cookie對應到特定的來源，如果發現某address不斷重複發送SYN訊息就可以推斷是否正在遭受攻擊。

(d) 攻擊者可以預先算出cookie內容，跳過SYN訊息，直接送出大量的ACK訊息並使伺服器為其分配資源。

2. Client Puzzle

(1) server在接收到connection request就為對方配置一塊儲存區，加上沒有記錄timestamp，推斷可能沒有機制來清理這些資訊，最後導致儲存空間用罄。攻擊者只要不斷發送connection request即可達到攻擊效果。

(2) 因為r是由client挑的，client可以重複使用相同的r，之後便無須花力氣解開p1，甚至client嘗試夠多不同的r有可能可以破解出伺服器的秘鑰k。

3. SSL/TLS

(a) (1)Server replies to *client_hello* with a server random number for each request to defend against replay attack. (2)Server will respond with *server_hello* to the false ip address and if there’s no respond, nothing will happen next. (3)attacker has to had a certificate to convince client of it’s authenticity, so as to pretend as a server.

(b) (1)a property to ensure that short-term session key won’t be compromised if the long-term private key is compromised in the future. (2)it is important because we need to make sure that our connection won’t be compromised someday if one of us had his private key stolen.

(c) (1)to lie about how to encrypt shared message(e.g, protocol version) in the first place and used a not-so-secure protocol instead once the negotiation of session key is done (2)both to double check the information and integrity of the information once again after the negotiation of session key is done

(d) (1)attacker forcing the victim to communicate in plain text, stripping https off http.
(2)server sends a http header over a https connection to inform the user that for the next *n* period of time, their connection must be conducted over https connection.

---

4. BGP Security

(1) the attacker announced 10.10.220.0/23, so then other routers will redirect to the addresses with longer prefix.

(2) (a){ 10.10.220.0/23 , {AS 999, AS 2, AS 1}}
(b)攻擊者可以利用path prepending在path前方加入周遭AS不喜歡的AS所屬的number，如此讓周遭AS選擇這條path的意願降低。或著在path加入某個AS的number，當那個AS收到這條path發現自己的number也在裡面就會放棄這條path。
(c)優點：迫使要到達某個ip的流量經過攻擊者所想要的路線。缺點：流量會經過攻擊者本身，可能會傷害到攻擊者自己。