**老師上課投影片**

CNS\_lecture8\_TLS

**攻擊SSL/TLS的論文**

|  |  |  |
| --- | --- | --- |
| 攻擊法名稱 | 攻擊方法 | 類型 |
| 統整  [Summarizing Known Attacks on Transport Layer Security (TLS)  and Datagram TLS (DTLS)] |  |  |
| Freak Attack  [A Messy State of the Union: Taming the Composite State Machines of TLS]的V-D | * 伺服器端支援RSA\_EXPORT * 客戶端實作有bug[Openssl 未特別提到版本，但2015年以前的版本應該都有疑慮]，使得客戶端用RSA，但ServerKeyExchange回傳是RSA\_EXPORT的時候，仍默默接受降級   以上條件讓攻擊者可以強迫TLS通訊使用較弱的加密，破解出加密過的資料 | 降級  實作漏洞  弱密碼設計 |
| Logjam Attack  [Imperfect Forward Secrecy:  How Diffie-Hellman Fails in Practice] | * TLS[TLS1.2以前的所有版本]同時支援DHE及DHE\_EXPORT，使得交握過程中的密鑰交換協議可降級至DHE\_EXPORT * DHE\_EXPORT使用固定的質數，使得數域篩濾法(NFS)得以預先計算。 | 降級  協定的弱點  弱密碼設計  實作問題 |
| POODLE Attack  [This POODLE Bites Exploiting The SSLv3 fallback] | * Handshake失敗，TLS的協定會下降到SSL3.0版本，而SSL3.0支援CBC mode的Block Cipher。[後續可檢查防禦機制TLS\_FALLBACK\_SCSV mechanism是否存在] * SSL3.0的CBC mode有個嚴重問題，就是padding是非決定性的，且未被MAC所涵蓋，故解密時padding的完整性無法保證。 | 協定的弱點 |
| BEAST Attack  [Here Come The Ninjas] | SSL及TLS1.0使用CBC mode的Block Cipher，IV是上個密文，可被用來做選擇明文攻擊。 | 協定的弱點 |
| Cross-Protocol Attack  [A Cross-Protocol Attack on the TLS Protocol ] | * 伺服器端支援ECDH，且使用特定橢圓曲線(secp384r1)，又客戶端支援一般的DH，使得ECDH參數可被解讀成有效的DH參數，進而與客戶端完成驗章。 * 使用的CipherSuite未被放進簽章內。[TLS1.2以前的所有版本] | 協定的弱點 |
| DROWN Attack  [DROWN Breaking TLS using SSLv2] | 利用支援SSL v2協定的伺服器端當作RSA的padding oracle，而SSL v2與TLS的RSA使用相同的Key，且SSL v2使用較弱的出口級加密，可將使用最新TLS協定的用戶端的會話解開。 | 協定的弱點 |
| RC4 Attacks  [On the security of RC4 in TLS]  [All your biases belong to us] | 使用具有多項偏離度(Bias)的串流密RC4 | 加密演算法的弱點 |
| Sweet32 Attack  [On the Practical (In-)Security of 64-bit Block Ciphers] | 使用Block Size為64 位元的Block Cipher，且使用CBC mode。 | 加密演算法的弱點 |

**一些工具**

|  |  |
| --- | --- |
| CipherScan | https://github.com/mozilla/cipherscan |
| Frankencert-cert | https://github.com/sumanj/frankencert |
| Mitmproxy | https://mitmproxy.org/ |
| Ettercap | https://ettercap.github.io/ettercap/ |