

## COMP3441/9441 Tutorial Week 9

### SSL

1. How does SSL deal with situations where the client and the server support different versions on SSL? Show how this enables a version rollback attack on SSL version 3 (v3). The SSL version 2 and 3 protocols are shown below.

SSL protocol version 2, without client authentication:

- (a)  $C \rightarrow S : C, Ver_C, Suite_C, N_C$
- (b)  $S \rightarrow C : Ver_S, Cipher, N_S, sign_{CA}\{S, K_S^+\}$
- (c)  $C \rightarrow S : \{Secret_C\}_{K_S^+}$
- (d)  $C \rightarrow S : \{N_S\}_{MasterKey}$
- (e)  $S \rightarrow C : \{N_C\}_{MasterKey}$
- (f)  $S \rightarrow C : \{SessionId\}_{MasterKey}$

where  $MasterKey = f(Secret_C, N_C, N_S)$

SSL protocol version 3, with client authentication:

- (a)  $C \rightarrow S : C, Ver_C, Suite_C, N_C$
  - (b)  $S \rightarrow C : Ver_S, Cipher, N_S, sign_{CA}\{S, K_S^+\}, (SessionId)$
  - (c)  $C \rightarrow S : \{Secret_C\}, sign_{CA}\{C, K_C^+\}, sign_C\{hash(messages(a-b))\}$
  - (d)  $S \rightarrow C : \{hash(messages(a-c))\}_{MasterKey}$
  - (e)  $C \rightarrow S : \{hash(messages(a-d))\}_{MasterKey}$
2. The version rollback attack makes attacks on SSLv2 possible even though both client and server support SSLv3. These attacks are the *downgrade attack* and the *truncation attack*. Explain how these attacks work.
  3. Client authentication is optional in SSL. What consequences does this have?
  4. Client authentication is very rarely used in practice. Why do you think it is not more prevalent, given the increased security it provides?