

COMP3441/9441 Tutorial Week 8

SPKI and Kerberos

1. Suppose that the following SPKI certificates have been issued:

- (a) (cert (issuer K1 Joe) (subject K2's Fred) (validity [10,18]))
- (b) (cert (issuer K2 Fred) (subject K3) (validity [12,20]))
- (c) (cert (issuer K4) (subject K1's Joe) (propagate) (tag A) (validity [2,16]))
- (d) (cert (issuer K3) (subject K1) (tag A) (validity [2,16]))

Show that it follows that K4 has authorized K1 to perform action A. During what time period does this authority hold?

2. The Kerberos v4 protocol is shown below. Explain what each step of the protocol does and the intention of each of the message components.

- (a) Alice (A) enters password into terminal T
 $T \rightarrow S$: Alice requests TGT, $n(T)$
 $n(T)$ = network address of T
- (b) $S \rightarrow T$: $\{K_A, TGT\}_{K_{AS}}$
 $TGT = \{A, n(T), v, K_A\}_{K_S}$
 v = validity period of TGT
- (c) Alice (A) logs into Bob (B) remotely (e.g. `rlogin`)
 $T \rightarrow S$: $A, B, TGT, \{A, n(T), timestamp\}_{K_A}$
- (d) $S \rightarrow T$: $\{B, K_{AB}, ticket_{AB}\}_{K_A}$
 $ticket_{AB} = \{A, n(T), v', K_{AB}\}_{K_{BS}}$
- (e) $T \rightarrow B$: $ticket_{AB}, \{timestamp\}_{K_{AB}}$
- (f) $B \rightarrow T$: $\{timestamp + 1\}_{K_{AB}}$

3. Design a variant of Kerberos in which the workstation generates a TGT. The TGT will be encrypted with the user's master key rather than the KDC's master key. How does this compare with standard Kerberos in terms of efficiency, security, etc.? What happens in each scheme if the user changes her password during a login session? [KPS 1]

4. Section 13.5 *Replicated KDCs* [in the textbook] explains that the KDC database isn't encrypted as a unit. Rather each user's master key is independently encrypted with the KDC master key. Suppose replication were done with a simple download (i.e. no cryptographic integrity check is performed). How could a bad guy who is a principal registered with a KDC impersonate Alice, another principal registered with that KDC? Assume he can see and modify the KDC database in transit, but that he does not know the KDC master key. [KPS 2]

Questions marked [KPS n] are taken from Kaufman et al., *Network Security*, 2nd ed., Prentice Hall, Chapter 13, Section 13, page 336.