SENG2250 System and Network Security
School of Electrical Engineering and Computing
Semester 2, 2018
Assignment 3 Report
Binbin Wang C3214157

Task 1

Q1.

There are some problems of this system.

a. The legitimacy of the reader cannot be discerned.

The tag does not have the recognition ability, so any reader can read it.

b. May can Clone the tag.

An attacker can copy a tag use to other fake things. Because the tag is outline work, and it can read at any time. Also, can reading information from a distance, means it can copy without knowing.

c. May infringe on personal privacy.

For example, a tag Implanted into personal items without knowing it, attacker can use the tag identification a person. Because it can be arbitrarily scanned at remote, and tag has uniquely identified.

Q2.

Can use the Kerberos Protocol(V5).

C: courier AS and TGS are in Server part

N: Nounce; R: Realm

C -> AS: Options, ID_C, R_C, ID_{tgs}, Times, N_1

AS -> C: R_C, ID_C, $Ticket_{tgs}$,$E_{Kc}[K_{c,tgs}$,ID_{tgs},Times, $N_1]$

$Ticket_{tgs} = E_{Ktgs}[Flags, K_{c,tgs}, R_C, ID_C, AD_C, TS_2, Times]$

C-> TGS: Options, ID_V,Times,N_2,$Ticket_{tgs}$, $Auth_C$

$Auth_C = E_{Kc,tgs}[ID_C, R_C, TS_1]$

TGS -> C: R_C, ID_C, $Ticket_V$, $E_{Kc,tgs}[K_{C,V}$, Times, N_2, R_V, $ID_V]$

$Ticket_V = E_{Kv}[Flags, K_{c,v}, R_C, ID_C, AD_C, Times]$

C -> V: Options, $Ticket_V$, $Auth_C$

$Auth_C = E_{Kc,v}[ID_C, R_C, TS_2, Subkey, Seq\#]$

V -> C: $E_{Kc,v}[TS_2$, Subkey, Seq#]

Because the client (courier) has a Reader, it has enough computing power. Also the device can connect the Internet. The server can do the AS and TGS job.

Since verification is only done at the time of delivery, time synchronization can be limited in few minutes. The server usage is not efficient at the same time and the Reader are limited, so the DDoS attack will not happen.

Q3.

We can not use PKI to verify the public keys, because tag does not have time system and it cannot access network. This protocol is based on hash chain to keep previous session security. The H_0 is the ID of tag, the H_{n-1} will save in could server.

Tag use AES

T: Tag R: Reader S: server

$H_1=h(H_0)$, $H_n=h(H_{n-1})$

T->R:E(PK, H_n)

R:check if $H_n=h(H_{n-1})$

S-> R: PK_{new}

R->T: PK_{new},$h(H_n)$

Q4.

This protocol is based on hash chain to keep previous session security. The H_0 is the ID of tag, the H_{n-1} will save in could server.

T: Tag R: Reader S: server

$H_1=h(H_0)$, Hn=$h(H_{n-1})$

Needham-Schroeder Protocol

R ->S: R,T

S->R: E(K_{rs}; K, T, H_m, E(K_{ts};K,R))

R->T:E(K_{ts};K, R)

T->R: E(K;K, H_m)

R->T: E(K;H_{n+1})

If tag desynchronies with server, can use the hash chain re-synchronize.

Task 2

use java jdk 1.8

compilation: javac C3214157.java

execution: java C3214157