Computer Security Assignment 2

Due on 12 November 2018

Released on 26 November 2018

Question 1 — **User authentication.** (5 marks) Given the online authentication protocol we have discussed in class in week 8, let the authentication server have a database of username and password pairs for all users. Moreover, for each session, the server needs to prepare two *fresh* functions f and h, where f is a normal function that translate a string to another string, and h is a one-way function (or a secure hash function). The authentication protocol runs as follows.

- $User \longrightarrow Host : UID$
- $Host$ generates random value r, function $f()$ and hash function $h()$
- $Host \longrightarrow User : r, f(), h()$
- $User \longrightarrow Host : f(r, h(password))$
- $Host$ decides whether to accept or deny UID's access based on its knowledge of r, stored $password$, $f()$ and $h()$.

After the protocol is successfully executed, $Host$ knows that it is communicating with $User$ with UID in the current session. How does the server verify that it is communicating with $User$? (2 **mark**)

If the function $h()$ is not fresh, there are possible attacks from an adversary who has full control over the network. Please describe an attack according to the scenarios when both $f()$ and $h()$ are reused for $User$. In that attack, the adversary successfully convinces the server ($Host$) that he is $User$ with UID, without the true $User$'s participation. (3 **marks**)

(Hint: $h()$ is a one-way function which means from $h(M)$ it is infeasible to compute M. $f()$ is not necessarily one-way. However, it is passible for the adversary A to store history messages that can be used for future attacks.)

Question 2 — **Denial of service.** (5 marks) The software company NikSoft is selling a new defense against DDoS attacks. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Their marketing folks are claiming that this will stop all DDoS attacks cold in the water. Is this a good solution to the problem? Why?

(Please send your answer in txt/pdf formats to chenyi_zhang@jnu.edu.cn)