TTM4137 Exam Solution Outline

12:12:12, 12.12.2012, corrections 13.12

Stig F. Mjølsnes, Joe-Kai Tsay, Simona Samardziska

Part I. Wireless Networks Security Facts

1a, 2c, 3d, 4b, 5a, 6b, 7b, 8d, 9d, 10a, 11a, 12b, 13c, 14c, 15a, 16a, 17b, 18a, 19d, 20a, 21b, 22d, 23c, 24c, 25b.

Part II. Password Based Authentication

26. Random password generation defeats a dictionary or wordlist attack.
27. Malin can set up her WiFi network interface controller (WNIC) in promiscuous mode to eavesdrop when Anne perform her login process, thereby acquire her password that is sent in cleartext.
28. Similar to the previous protocol, if Malin listens to the WiFi traffic, she can read the login values (id, v) that Anne send, and that is all she needs for impersonating Anne at the file server.
29. Client hash value computation is better if the client use the same password for access to other servers. If the hash value is computed at the server side, then an eavesdropping on the login to one server, can compromise the security of the other servers as well.
30. From the explanation given, the probability that any two employees have the same password has values is:

$$p \approx 1 - e^{-\frac{1}{2^{32}} \cdot \frac{100 \cdot 99}{2}} = 0.000001153$$

31. The probability for hash value collisions must be less than $p = 10^{-10}$, hence first, we need to solve the equation $p = 1 - e^{-\frac{1}{2^{k'}} \cdot \frac{100 \cdot 99}{2}}$ for the unknown k'. The solution can be computed by:

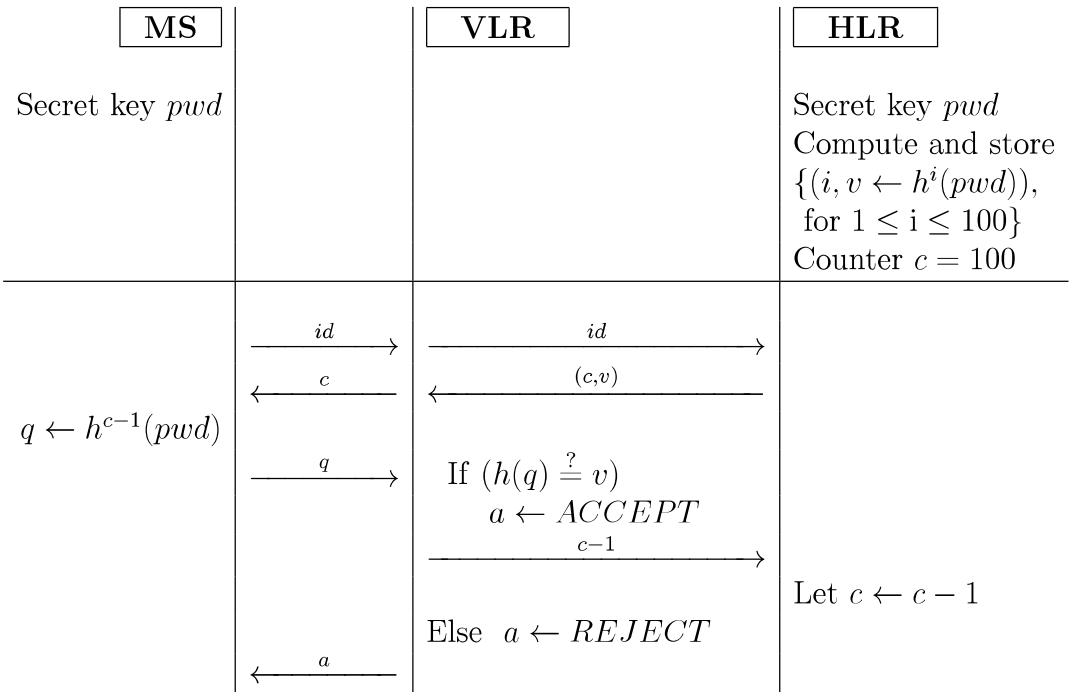
$$k' = \log_2\left(\frac{-100 \cdot 99}{2 \cdot \ln(1 - 10^{-10})}\right) = 45.49$$

Hence, for $k = \lceil k' \rceil = 46$, the probability of collision is less than 10^{-10}.

Part III. Protocols

32. The host H authenticates the user terminal U by a "Lamport onetime password scheme", thus preventing password eavesdropping.
Correctness: if U knows the password pwd, then for all c ("protocol runs") will the verification predicate be true $(h(h^{c-1}(pwd)) = h^c(pwd))$.
Security: by the oneway property of the hash function, observing the protocol triplets (id, c, q) for some c, then it is hard to compute the correct triplet for the next run $(id, c-1, v)$ such that $h(v) = q$.
33. A man-in-the-middle-attack is possible because U does not authenticate the messages from H, in other words, U has no mechanism to distinguish between messages from an attacker and the host H. Thus, Malin can send c to Anne, then receive the correct response $h^{c-1}(pwd)$ from Anne, stop the protocol with Anne, and impersonate Anne in a complete login protocol with the host. Note that, Malin can anticipate the expected c, just by listening to previous logins. But any value of c less than the previous one will also work, because Anne does not maintain the current value of c.

34. There is a lot of freedom in the answer of this question. The simplest solution is to just divide the host into two parties, the visited and the home network, without enhancing the security in any way. Q36. gives a hint on the interpretation of the function h in the mobile environment. The adaptation can be done as follows.



35. This answer will depend which protocol is constructed in Q.34. We can distinguish the following differences to the GSM authentication protocol. When the VLR sends id to the HLR, it receives back only one pair $(c, h^c(pwd))$. In GSM it may be a batch of triplets for the same user. Notice that, if the VLR has the algorithm for h it doesn't need to store the list of pairs $(i, h^i(pwd))$, for $1 \leq i \leq 100$. This is because of the counter properties of c. However, this implies that it is very easy to mount a man-in-the-middle-attack as described in Q32, which can be used to steal a call from a legitimate user. Thus, authentication of the MS to the VLR fails. The GSM key agreement part is not in our protocol, but it can be implemented as in GSM using some other function of the secret key pwd, and the counter c very similar to GSM. Again, since in this protocol there is no mutual authentication, the same man-in-the-middle-attack as in GSM can be applied in this one as well. Another difference is that the home network must be online in the process of authentication, in order to update the value from c to $c - 1$ in case of successful authentication.

36. Depends on the answer of Q34. For the protocol described here in Q34. we see that there is quite a big computational load on the MS side compared to GSM, if we assume that the cost of the h function is the same as of the A3 function, i.e., for each authentication the computational load is $c - 1$ times bigger. However, a time-memory trade-off can be done here, if instead of computing $h^i(pwd)$ all the values $(i, h^i(pwd))$, $1 \leq i \leq 100$ are stored in the MS in an ordered list. Then, after every successful authentication the expired entry can be deleted, or marked as expired. Note that this modification affects security in the sense that the man-in-the-middle-attack from Q32 can be detected. Also, at the VLR side, a similar time-memory trade-off can be made, but then, the home network must send a batch of pairs $(i, h^i(pwd))$ to the visited network. In this case, there is no need for the algorithm of h at the visited network side.

—