AARHUS UNIVERSITY - COMPUTER SCIENCE

Security Handin 3

Peter Burgaard - 201209175

May 18, 2015

QUESTION 1: if host and user is communicating via an open line, it would be very easy to intercept the UNIX-like systems pw delivery, since it is not encrypted in any way. It is thereby trivial to just deliver the intercepted pw, and the host system will have no idea that it would not be the actual user, who is logging onto their account.

For the digital signature based solution, if we are totally passive then we can't get any information from correspondence between the client and host which will grant us any access. But the can be hacked if we can make a request which gives us a random message R, which we will call R_{hack}. We then wait for our targeted user, to make a request themself, in which we switch their R_{target} with our R_{hack}. This R_{hack} will then be signed and we can take the now signed R_{hack} and return as our own request, which will grant us access to the host in our targets name.

So for these two systems, none of them would be safe, for a potential attack from a passive attack if the communication is handled on an open line. If the line was encrypted, this would not change the possibility of a passive attack, if we assume all the information for logging is packed in one file, which we can then intercept, and we have a way to veryfy this is the actual pw-file, then the login system is not safe. If these assumption are not met, then the system is safe. The digital signature system I would be assumed to be safe, if we are totally passive.

QUESTION 2: if no modification can be done, the digital signature system would be safe if we assume only the users computer can make a correct sign in their name. This is because, our ability to view this file does not change the fact that we can not produce an output the host system would view as acceptable.

With the UNIX-like system we can gain the function f, and run an exhaustive search on PW's through the function, until we get an output which matches one on the list on the server.

If on the other hand we can modify, we can now change the public key need in the digital signature system to match ours, which wil grand us access in the hacked user name.

With the UNIX-like system, we can compute f(known string), and set the f(PW) on the list, to this output, which means we have changed the password, so we can just log on our targeted users account with our own self made password.

QUESTION 3: I would prefer the digital signature system, if the communication lines were open, since it I assumes it would be more deficult for the hacker to gain access to the servers files and change the corresponding user / signature match up, than listen on a line and intercept the pw. If the encrypted line were to be used, I would prefer the pw based system.