The University of Queensland
School of Information Technology and Electrical Engineering

Semester 2, 2017

COMS3000/7003 – Tutorial 3, Answers

Q1) Consider the following challenge-response authentication protocol and find its security flaw.

Alice registers her username and secret password pA with the server.
When Alice wants to log in, she sends her username to the server.

The server sends Alice a challenge c, which is computed as follows: c = h(username)
h() is a cryptographic one-way hash function.

Alice calculates the reply r as follows: r = h(pA || c)
('||' means concatenation)

Alice sends r to the server.
The server, knowing both c and pA, also computes r and compares it with the value received from Alice. If the two values match, Alice is authenticated.

The problem is that the challenge c is the same for each login attempt. An attacker (Eve) can easily launch a replay attack by doing the following:

Eve can observe Alice's username and her reply, **r**, from the network, e.g. via eavesdropping.

Eve can now impersonate Alice by sending a login request to the server using Alice's username. She can also use the observed value **r** to respond to the server's challenge.

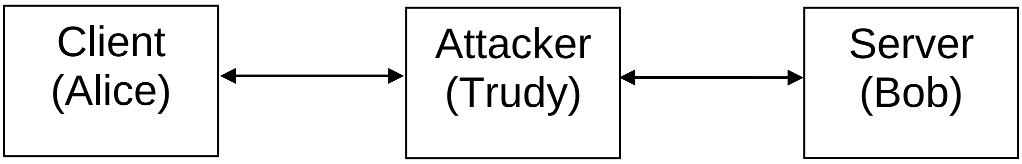
It is therefore important that the challenge ("nonce") is not reused in challenge response protocols.

Q2) Both Basic and Digest HTTP authentication are vulnerable to the so-called "man-in-the-middle" (MITM) attack. MITM attacks are a big problem for a large number of cryptographic algorithms and protocols.

The basic idea of MITM attacks is that an attacker sits between a client and a server and all the messages exchanged between the client and the server go via the attacker, which can eavesdrop and modify messages. In the case of HTTP authentication, the attacker could be a hostile or compromised web proxy. The basic problem is lack of authentication. The client thinks it is talking to the server when it is talking to the attacker. The server thinks it is talking to the client when in fact it is talking to the attacker instead.

In the HTTP protocol, a client and a server negotiate which authentication protocol to use, e.g. “basic” or “digest”. For example, the server will send a list of authentication methods it supports and, according to RFC2617, the client must select the strongest of these methods that it supports.

Given this information, explain how a MITM attack could be used to compromise the HTTP authentication protocol.



An example of an MITM attack would be to remove the strong authentication methods listed in the reply message sent by the server and only leave “Basic” authentication as an option.

This forces the client to use a weak authentication method and send the password in cleartext, which can then be observed by the attacker.

The problem of MITM attacks in the HTTP authentication protocol is described in more detail in section 4.8 of RFC2617.

Q3) Can you give an example of how a man-in-the-middle attack could be used to compromise the S/Key authentication protocol?

It is easy for an attacker to find the index n for the current password by simply sending a login request to the real server.

An attacker could set up a fake server which then uses this index n and collects the current password p_n from the user via the normal challenge response login process.

The attacker can then use p_n to log into the real server.