University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions and Answers

Lecture 8: User Authentication

Question 1

Assume that a user has authenticated to an online bank, and that the session is protected/encrypted with TLS. Describe possible threat scenarios where false transaction data get sent from the client to the server despite correct user authentication.

Answer

There are many possible ways to get false transaction data, here are two situations where this could happen:

- The user logs in and then goes to the canteen to get a cup of coffee without ending the session or locking his terminal, so somebody else can operate the client computer to send false transactions.
- A malicious Trojan in the client modifies transaction data typed by the user before sending the data to the server. This is how online banking attacks happen.

Question 2

a. What is a challenge-response authentication protocol, and what is its purpose?
b. Explain the steps of the HTTP Digest Access Authentication protocol.
c. Is it required to encrypt the HTTP-connection to make it secure to use HTTP Digest Access Authentication? Explain why / why not.
d. Can the password database at the server end be hashed/salted when using HTTP Digest Access Authentication? Explain why / why not.

Answer

a. A challenge-response protocol is an exchange of messages between two parties where one party (the verifier) challenges the other party (the applicant) to prove knowledge of a secret. The purpose of a challenge response-protocol is to avoid sending the secret in clear to the verifier when proving knowledge of the secret.
b. The HTTP Digest goes approximately as follows:
    i. The user requests a protected page
    ii. Server sends a nonce (random number) and realm name to browser
    iii. Browser window displays input fields for UserId and Password,
    iv. User fills in UserId and Password.
    v. Browser computes the response: Digest = h(UserId, Password, nonce)
    vi. Browser sends Digest + UserId + nonce + realm name to server
    vii. Server computes the same digest and compares with received Digest.
c. The HTTP connection does not need encryption to protect the user authentication. That's because the password is not sent in cleartext, it's a challenge-response protocol.

d. The password database must unfortunately store the passwords in cleartext. Otherwise the server would not be able to compute the Digest to compare with the client response.

Question 3

a. A password is normally considered to be a credential based on something you know. Discuss whether this is still the case when the password is written down.
b. Briefly explain the typical security policy requirement for password selection. You can look at the sample Password Policy document from SANS Institute at: http://www.sans.org/security-resources/policies/general#password-construction-guidelines or at UiO's requirements for acceptable and secure passwords at: http://www.uio.no/tjenester/it/brukernavn-passord/passordtjenester/hjelp/kompleksitet.html or the guidelines from NIST SP800-63B Section 5.1.1.2 Memorized Secret Verifiers https://pages.nist.gov/800-63-3/sp800-63b.html
   - What do the password policies say regarding length and complexity of passwords?
   - To what degree does the UiO password policy follow the NIST guidelines?
c. Why is it often recommended to memorize passwords, and not to write down passwords?
d. Assume that you don't agree with (c), suggest alternative methods for managing personal passwords, and discuss their security issues.

Answer

a. When writing down the password it can be considered as something you know only in the sense that you need to know where it is stored. Otherwise it must be considered as something you have, i.e. the medium where it is stored.
b. The password policies state that passwords should have sufficient minimum length and/or level of complexity.
   - The SANS policy (updated June 2014) recommends ≥ 12 characters, and to use at least one character from all 4 categories (small, capital, digit, special)
   - the UiO policy (published 14 February 2018) is based on a point system, where acceptable passwords must score at least 32 points. A relatively complex password of 8 characters would be acceptable. A password of 18 identical characters (e.g. 1111111111111111) would also be acceptable.
   - The NIST policy recommends ≥ 8 characters, and discourages enforcing "composition rules" i.e. to require characters from different categories, in contrast to most traditional password policies which do recommend enforcing composition rules. However, the NIST policy requires checking passwords for known weaknesses.
   - The new UiO policy seems to be inspired by the NIST policy regarding password/passphrase length. However, the UiO policy does not follow the NIST policy which requires checking known weaknesses in passwords.
c. A memorized password can not easily be lost or stolen, if it is truly memorized (not forgotten) and not revealed to anybody else.
d. We accumulate more and more online accounts. It is too much to expect that we memorize a strong and different password for every account. Users must be able to write them down somewhere. Storing passwords of paper is OK if you keep it safe. Storing passwords in electronic device must be done with care, i.e. the passwords should always be encrypted. If stored in cleartext the device should always be offline.

Question 4

a. Briefly define the concept of a biometric system.
b. A biometric system may operate in either verification mode or identification mode. Briefly explain the operation of both of these modes. State which of these modes is easier to implement and explain why.
c. A basic biometric system consists of four main modules. Briefly describe these modules.

Answer

a. A biometric system is an automated method of verifying or recognising a person based upon a physiological or behavioural characteristic
b. In verification mode the user claims an identity. A new biometric sample is captured and compared to the stored template corresponding to the user's claimed identity. A decision is made on the closeness of the match – access is accepted or rejected. In identification mode the user does not claim an identity. A new biometric sample is captured, and a search is conducted of the templates of all the users in the database for a match. Identification is more complex to implement since it requires 1:N matching instead of 1:1 matching required for verification.
c. The elements are
   - Sensor module: captures the biometric signal of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.
   - Feature extraction module: processes the acquired biometric signal to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.
   - Matcher module: features captured during recognition are compared against the stored templates to generate matching scores.
   - System database module: used by the biometric system to store the biometric templates of the enrolled users.

Question 5

a. Any human physiological or behavioural characteristic can be used as a biometric characteristic as long as it satisfies four basic requirements. Briefly describe these four basic requirements.
b. For the practical implementation of a biometric system some additional requirements should also be considered. Briefly describe relevant additional requirements.
c. Briefly describe the extent to which each of the following biometric types satisfies the characteristics and issues you described for parts (a) and (b).
   • Fingerprints
   • Facial recognition
   For background information, look at the article: "*An Introduction to Biometric Recognition*"
   http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Answer

a. The basic requirements are:
   - Universality: each person should have the characteristic;
   - Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
   - Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
   - Collectability: the characteristic can be measured quantitatively.

b. Additional relevant requirements are:
   - Performance: the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, the operational and environmental factors that affect the accuracy and speed;
   - Acceptability: the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
   - Circumvention: how easily can the system be fooled using fraudulent methods.
   - Safety: It might be necessary to provide safe environments for sampling biometrics.

c. Jain, Ross and Prabhakar (2004) give a table which includes the following extract. Here H, M, L stand for high, medium and low, respectively. In all cases H is the most desirable (for example, H for circumvention means that resistance to circumvention is high).

	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Cirum-vention
Facial rec.	H	L	M	H	L	H	L
Fingerprints	M	H	H	M	H	M	H

   - **Fingerprints:** A small proportion of people do not have suitable fingerprints for identification because of genetic, age, environment or occupation. Therefore universality is only medium. Fingerprints are practically unique and quite permanent. Fingerprint scanners are quite affordable and appear on many commodity devices today. Taking fingerprints is somewhat intrusive and often associated with criminal activity so is not as acceptable as some other methods.
   - **Facial recognition:** This method is non-intrusive and scores well on universality and acceptability. There are different methods to obtain an accurate quantitative sample so collectability is good. Measurements can vary considerably with lighting and viewing angle which detracts from permanence. Moreover, facial measurements on their own provide a questionable basis for identification, so uniqueness and performance are rated low. This also affects circumvention, particularly if the subject does not cooperate (for example by presenting a different viewing angle).

Question 6

a. The score *s* quantifies the similarity between the input sample and the stored sample. Explain how the score *s* and the threshold *T* are used to determine mate pairs and non-mate pairs between the samples.
b. The threshold *T* can be tuned to provide the optimal balance between FMR (False Match Rate) and FNMR (False Non-Match Rate). Explain roughly the principle for adjusting threshold *T* as a function of the costs associated with false accept and false reject.

Answer

a. Pairs of biometric samples generate score *s*, where $s \geq T$ dictates mate pairs (i.e., belonging to the same person), and thus accept. Pairs of biometric samples where $s < T$ dictates non-mate pairs, and thus reject.
b. High *T* value gives high FNMR and low FMR, which is good in case of high cost of false accept (false match). Low *T* value gives high FMR and low FNMR, which is good in case of high cost of false reject (false non-match).

Question 7

Several governments have national authentication frameworks. The Norwegian framework "*Rammeverk for Autentisering og Uavviselighet*" (RAU) can be accessed at http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
The ISO29115 **Entity authentication assurance framework** can be accessed at the INF3510 wiki: https://wiki.uio.no/mn/ifi/INF3510-2018/

a. To what degree are authentication assurance levels of RAU and ISO29115 compatible?
b. RAU does not explicitly focus in identity registration, whereas ISO29115 does. Give a possible explanation for why RAU does not focus on identity registration.
c. Discuss whether RAU covers user authentication for e.g. EU citizens to access Norwegian e-Government services.
d. The eIDAS regulation to be implemented in the EU in 2018 only provides three different LoA (Levels of Assurance) for authentication, see EU Regulation 2015/1502 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
Why did the EU decide to have only three levels of authentication assurance?
e. What are the terms used to denote each LoA in eIDAS?

Answer

a. They both have 4 levels which are more or less compatible.
b. In Norway the Person Register is considered a reliable source of registered identities, so it was considered unnecessary to cover registration in RAU.
c. Since RAU does not cover the registration of identities it is not directly applicable to EU citizens. RAU only applies to people who are already registered in the national Person Register (Folkeregisteret).
d. The lowest AAL (Authentication Assurance Level) in previous frameworks was never used, and would anyway be inadequate for cross-border authentication to e-government services, so only the three highest AALs (LoAs) are used in eIDAS.
e. eIDAS uses the term LoA (Level of Assurance) with the same meaning as AAL (Authentication Assurance Level). In eIDAS the three LoAs are called 'Low', 'Substantial' and 'High'. Criteria for each level are described in "Guidance on Levels of Assurance" available at:
https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents