Information Systems Security: exercises on security of IP networks

Diana Berbecaru

< diana.berbecaru @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

AY 2023-2024

Outline

- **questions (authentication) – from previous practical exercises**
  - reusable password, OTP, symmetric/asymmetric CRA
- **short problem(s)**
- **questions + discussion on:**
  - authentication of network access and network access protocols
    - EAP
    - RADIUS
    - IEEE 802.1x

Problem 2

Assume Alice has two databases: a trusted storage (that an attacker cannot read and modify), and an untrusted storage (that an attacker can read and modify). Assume Alice can use:

1) H : a secure cryptographic hash function, like SHA256

2) || : the concatenation function

Alice creates and stores four files, F1, F2, F3, F4 in the untrusted storage. Alice also computes and stores a hash of each file (content) in the untrusted storage:

h1 = H(F1), h2 = H(F2), h3 = H(F3), h4 = H(F4)

Then, Alice calculates h_{chain} and stores it in the trusted storage:

h_{chain}= H(h1 || h2 || h3 || h4)

Let's assume Bob modifies F3.

Problem 2 – questions

- **can Alice detect the modification done by Bob?**
  - A. Yes, Alice recomputes h3 = H(F3) and sees that it doesn't match with the stored h3
  - B. Yes, Alice recomputes h_{chain} and sees that it doesn't match with the stored h_{chain}
  - C. No, Alice cannot detect the modification because the attacker can change both F3 and H(F3)

Problem 3

Assume Alice has one trusted storage (that an attacker cannot read and modify), and an untrusted storage (that an attacker can read and modify). Assume Alice can use two functions:

1) H, a secure cryptographic hash function, like SHA256

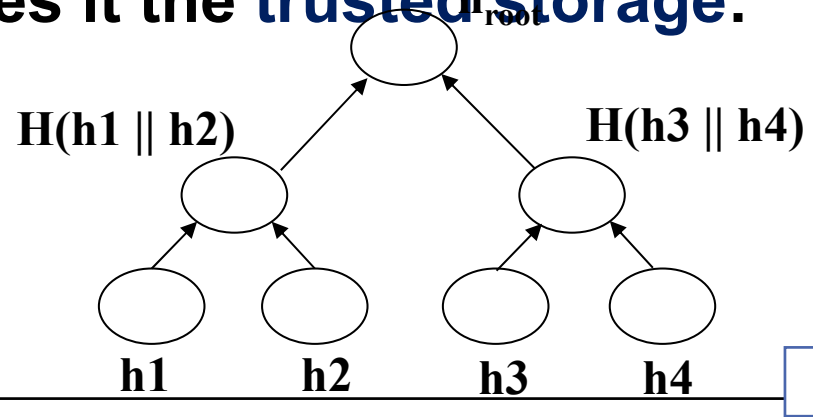
2) || , the concatenation function

Alice creates and stores four files (F1, F2, F3, F4) in the untrusted storage. Alice also computes a hash on each file (content):

$h1 = H(F1), h2 = H(F2), h3 = H(F3), h4 = H(F4)$

Then, Alice calculates h_{root} and stores it the trusted storage:

$h_{root} = H(H(h1||h2)||H(h3||h4))$



Let's assume Bob modifies F3.

Problem 3 – questions

- **can Alice detect the modification done by Bob?**
  - A. Yes, Alice recomputes h3 = H(F3) and sees that it doesn't match with the stored h3
  - B. Yes, Alice recomputes h_{root} and sees that it doesn't match with the stored h_{root}
  - C. No, Alice cannot detect the modification because the attacker can change both F3 and H(F3)

Questions
(Security of IP networks)

Question 1

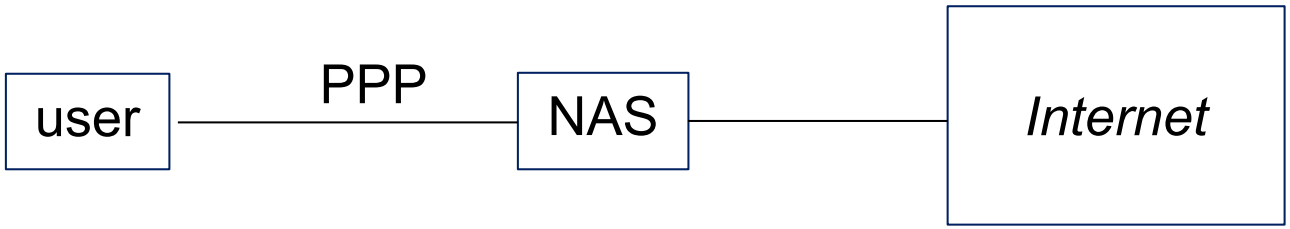
- **which protocol can be exploited for user authentication in dial-up, wireless, or virtual links (you can select multiple choices)?**
  - A. RADIUS
  - B. EAP
  - C. DIAMETER
  - D. CHAP

Question 2

- **at which level in the OSI stack is exploited EAP (Extensible Authentication Protocol) to support authentication?**
  - A. L2 (data link layer)
  - B. L3 (network level)
  - C. L7 (application level)
  - D. L4 (transport level)

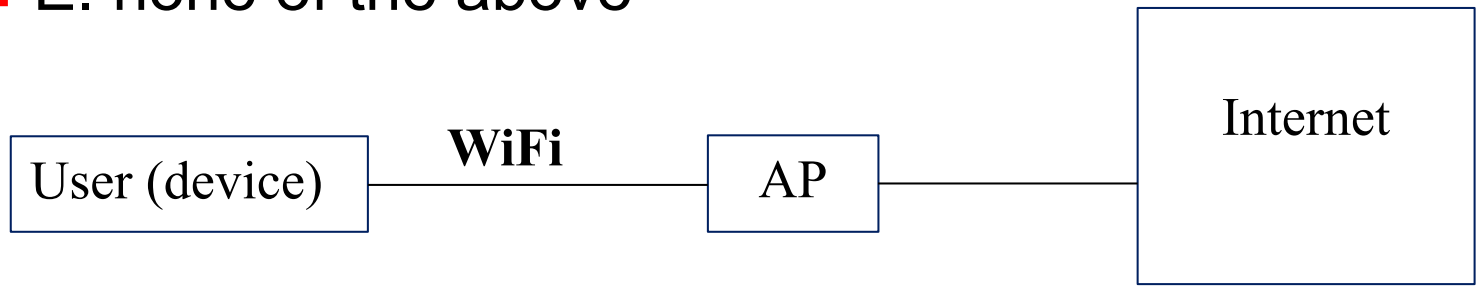
Question 3

- **Assume that we have a small company which uses a NAS supporting EAP, PAP, CHAP. Look at the picture and tell which methods and protocol(s) can be used to authenticate a user (device) with the NAS to provide it access to Internet:**
  - A. RADIUS
  - B. PAP
  - C. CHAP



Question 4

- **Assume we have small hotel that uses an Access Point (NAS) supporting EAP, CHAP. Take a look at the picture below and indicate which methods can be used to authenticate a user (device) with the AP to provide access to Internet:**
  - A. EAP-TLS
  - B. CHAP
  - C. Username and password and EAP
  - D. RADIUS
  - E. none of the above



Question 5

- **EAP transports authentication messages between a user (supplicant) and a NAS:**
  - A. before the IP channel is established. Thus, EAP uses its own encapsulation protocol because IP packets are not available
  - B. after the IP channel is established. Thus, EAP packets are encapsulated inside IP packets
  - C. none of the above

Question 6

- **EAP can transport authentication messages between a user and NAS (Network Access Server):**
  - A. only for PPP channels
  - B. for any L2 protocol, such as PPP, 802.11 (wi-fi), 802.3 (Ethernet), 802.5 (token ring)
  - C. only for 802.11 (Wi-fi) and 802.3 (Ethernet)

Question 7

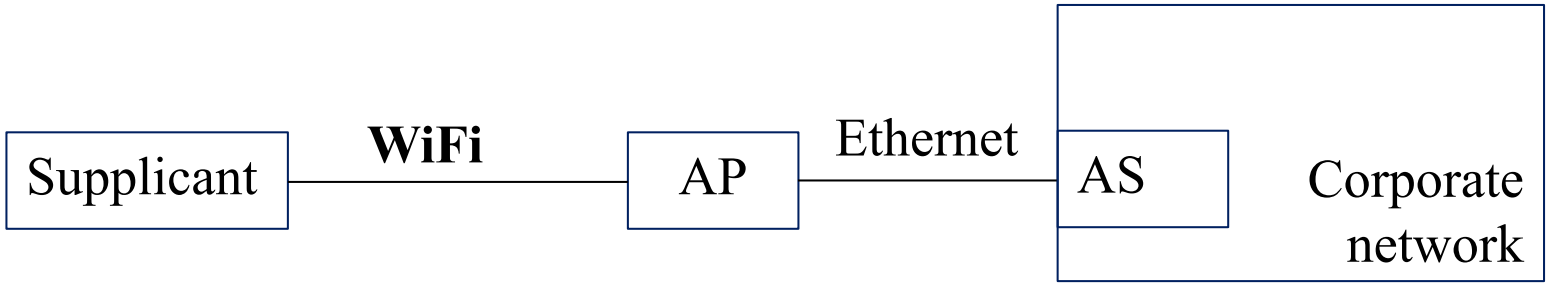
- **What is an EAP method (e.g. EAP-TLS, EAP-TTLS, EAP-SRP, AKA-SIM)?**
  - A. it's a variant to allow EAP to be exploited in other (upper level) protocols
  - B. it's the method used by EAP to perform user authentication
  - C. it's the method used by EAP to transfer the messages of a specific (user) authentication protocol
  - D. none of the above

Question 8

- **RADIUS is a network authentication protocol that:**
  - A. is used for communication (client-server schema) between a user (supplicant) and a NAS
  - B. is used for communication (client-server schema) between a NAS and a backend Authentication Server (AS)
  - C. supports user authentication via PAP, CHAP, and EAP
  - D. supports user authentication only via EAP
  - E. may act as a proxy towards other AS

Question 9

- **Assume we have a corporate network which has an Authentication Server (AS) in place, and uses a APfor network access control. Take a look at the picture below and indicate the protocol(s) typically used for the communication between AP and AS during authentication of supplicants:**
  - A. RADIUS
  - B. PAP
  - C. CHAP



Question 10

- **RADIUS implements the following security properties**
  - A. authentication and integrity of requests, where the RADIUS requests are protected with a digital signature
  - B authentication and integrity of requests, where the RADIUS requests are protected with a keyed-digest
  - C. authentication and integrity of responses, where the RADIUS responses are digitally signed by the RADIUS server
  - D. authentication and integrity of responses, where the RADIUS responses are protected with a keyed-digest
  - E. authentication of the server, through the calculation of an authenticator via keyed-digest

Question 11

- **RADIUS implements the following security properties:**
  - A. confidentiality of the data in the RADIUS request by encrypting the data with an algorithm that can be negotiated
  - B. confidentiality of the data in the RADIUS request by masking the (user) password (with an XOR operation)
  - C. confidentiality of the data in the RADIUS response by encrypting the data with an algorithm that can be negotiated
  - D. confidentiality of the data in the RADIUS response by masking the password (with an XOR operation)
  - E. protection from replay of RADIUS response, by using a sequence number in the RADIUS response
  - F. protection from replay of RADIUS response, by binding the response to a specific request via a Request Authenticator

Question 12

- **Consider an architecture in which we have: a supplicant (user), a NAS, and a RADIUS server. If the RADIUS server and the user have a shared secret (named "secret"), does this mean that a (malicious) user can create a fake RADIUS response?**
  - A. yes, because the user knows the secret
  - B. no, because in the construction of the RADIUS response it is used also a Request Authenticator generated by the NAS
  - C. no, because NAS and the RADIUS server have also a "secret" that the user does not know (used in protecting the RADIUS response)

Question 13

- **Assume a company uses RADIUS to authenticate users and Wi-Fi access-points and switches enabled with support for 802.1x. What is the main role of the Wi-Fi access points and switches and what needs to be done to allow them to work when new user authentication protocols appear (and are supported by EAP)?:**
  - A. allow to perform authentication of the users connecting to the AP or switch by exploiting EAP
  - B. encapsulate the EAP messages received from the users (supplicant) into RADIUS messages sent to the AS
  - C. must be updated if new user authentication protocols appear and are supported by EAP
  - D. no change is needed if new user authentication protocols appear and are supported by EAP