Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Heiko Niedermayer
Dipl.-Inform. Ralph Holz
Dipl.-Inf. Ali Fessi

# Exercises for lecture „Netzsicherheit“
# Assignment 5, WS09/10

| | |
|---|---|
| Hand.out: | Thursday January 7th 2010 |
| Deadline: | Wednesday January 20th 2010 |
| Exercise course: | Thursday January 28th 2010 |

## Task 1: Internet Key Exchange v2 (IKEv2)

a) IKE_SAs, CHILD_SAs:
   a. Explain the difference between IKE_SA and CHILD_SA.
   b. What is the reason that the IKE_AUTH exchange contains the additional payloads ($SA_{i1}$, $TS_i$, $TS_r$) resp. ($SA_{r2}$, $TS_i$, $TS_r$)?

b) Diffie-Hellman Exchange:
   - Argue why the DH exchange, $KE_i$ ($=g^i$) and $KE_r$ ($=g^r$), in IKE_SA_INIT is not sufficient to authenticate the other communication partner.
   - What is then the purpose of the Diffie-Hellman exchange?

c) Random numbers $N_i$ and $N_r$:
   - Argue why the initiator (or the responsder respectively) has to include the random number $N_r$ ($N_i$) in its calculation of the AUTH payloads.
   - What is the purpose of the random numbers $N_i$ and $N_r$ in addition to the generation of keying material?

d) AUTH Payload:
   - What cryptographic methods can be used to compute the „AUTH Payload“ during the IKE_AUTH exchange?
   - Argue why it is not possible for a Man-In-The-Middle attacker to modify the cryptographic algorithms selected for the protection of the IKE messages without the initiator or responder noticing the change.

## Task 2: SSL/TLS

a) For many applications it is sufficient and reasonable that only the TLS Server authenticates towards the TLS client and the client does not authenticate itself. What are the reasons?
b) How do client and server calculate the Premaster Key (TLS Handshake Protokol)?
c) How can the client in the TLS Handshake Protocol be sure of the identity of the server
   - in case of the RSA variant of TLS for the Premaster Secret?
   - In case of the Diffie-Hellman variant for the Premaster Secret?
d) What are the changes in TLS V1.0 in comparison to SSL V3.0?

**Task 3: Link Layer Security - Extensible Authentication Protocol (EAP)**

Figure 1 shows the general message flow of the authentication with the EAP protocol. This is independent of the particular EAP method (like EAP-TLS). A RADIUS server is used as authentication server.

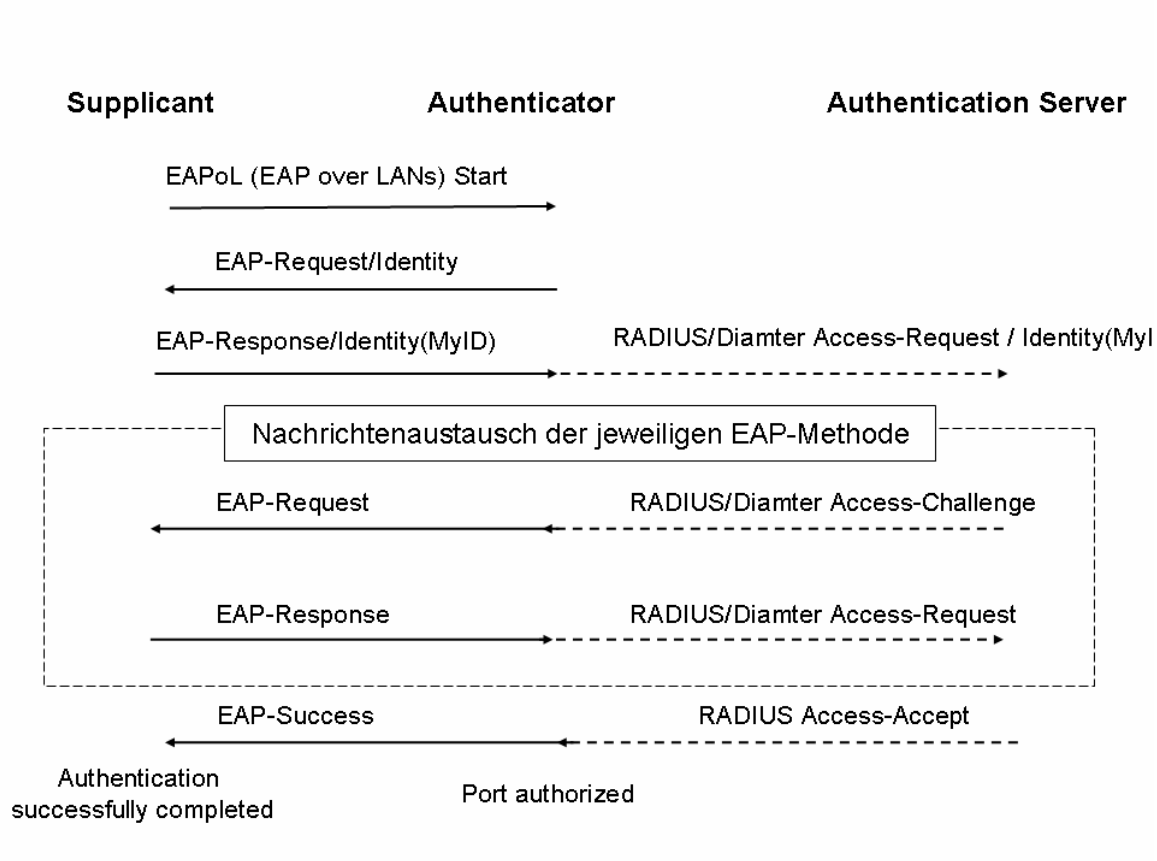


**Figure 1: EAP generic message exchange with RADIUS server**

a) Describe the authentication dialog when Supplicant, Authenticator and Authentication Server use the EAP-MD5 method.
   Note 1: see RFC 3748 "`PPP Extensible Authentication Protocol (EAP)"', Section 3.4 "`MD5-Challenge"'.
   Note 2: The placeholder "Nachrichtenaustausch der jeweiligen EAP-Methode" in Figure 1 needs to be replaced with 2 messages for your solution.
b) Argue why EAP-MD5 is vulnerable to dictionary attacks.
c) Argue why this attack is not possible when EAP-TTLS or PEAP are used.
   Note: Read the article "TTLS and PEAP Comparison", downloadable under http://www.opus1.com/www/whitepapers/ttlsandpeap.pdf for a good overview on these two methods.
d) Search on the Internet for the keywords "`EAPOL Start Attack"' und "`EAPOL Logoff Attack"'. Describe these attacks that are possible despite using a secure EAP method.

--- turn page ---

**Task 4: SSH weaknesses**

SSH uses algorithms for encryption and authentication that can be assumed secure. However, so-called Timing attacks are still possible. Consider this, SSH as well as Telnet send a packet for each character that is typed at the console (Interactive mode).

a) How can attackers use this to gain security-relevant information?
b) A number of related problems are discusses in the paper "Timing Analysis of Keystrokes and Timing Atacks on SSH" by Dawn X. Song et al. (Hint: Google Scholar, USENIX). Read the sections 1 and 2.What kind of weaknesses are introduced?
c) What are the attacks that can use the weaknesses?
d) In December 2009 the LRZ found out that a variety of "typing error domains", e.g. *.lrz-munchen.de, were registered and that on all its subdomains there are running SSH daemons that interact with the user to get its inpu and then refuse the login. Argue: Is is possible to learn SSH passwords in that way? How can a user detect such a fraud when the user was already logged on to a LRZ computer with SSH? Why does this fail when the user was not yet logged into the LRZ?