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

Übung zur Vorlesung „Netzsicherheit“
Übungsblatt 5, WS09/10

Ausgabe:	Do 7. Jan. 2010
Abgabe:	Mi 20. Jan. 2010
Besprechungstermin:	Do 28. Jan. 2010

Aufgabe 1: Internet Key Exchange v2 (IKEv2)

a) IKE_SAs, CHILD_SAs:
   a. Erklären Sie den Unterschied zwischen eine IKE_SA und CHILD_SA.
   b. Aus welchem Grund welchen beim IKE_AUTH Austausch zusätzlich die Payloads (SA_{i1}, TS_i, TS_r) bzw. (SA_{r2}, TS_i, TS_r) mit übertragen?

b) DH-Austausch:
   - Begründen Sie, warum der DH-Austausch, KE_i ($=g^i$) und KE_r ($=g^r$), bei IKE_SA_INIT noch nicht ausreicht, um den Kommunikationspartner erfolgreich zu authentisieren.
   - Welche Rolle spielt dann der DH-Austausch?

c) Zufallszahlen N_i und N_r:
   - Begründen Sie, warum der Initiator (bzw. der Responder) die Zufallszahl N_r (bzw. N_i) in die Berechnung des AUTH Payloads mit einbeziehen muss.
   - Welche Rolle spielen die Zufallszahlen N_i und N_r zusätzlich für die Generierung des Schlüsselmaterials?

d) AUTH Payload:
   - Mit welchen kryptographischen Verfahren kann der „AUTH Payload“ bei IKE_AUTH berechnet werden?
   - Begründen Sie, warum es einem Man-In-The-Middle-Angreifer nicht möglich ist, die kryptographischen Algorithmen für den Schutz der IKE-Nachrichten zu verändern, ohne dass der Initiator oder der Responder das merkt.

Aufgabe 2: SSL/TLS

a) Begründen Sie, warum es in vielen Anwendungen sinnvoll (bzw. ausreichend) ist, wenn sich nur der TLS Server gegenüber dem TLS Client authentisiert und der Client nicht.
b) Wie wird der Premaster Key beim TLS Handshake Protokol berechnet?
c) Wie kann sich der Client bei dem TLS Handshake Protokol von der Identität des Servers vergewissern
   - bei der RSA-Variante der Berechnung des Premaster Secret?
   - und bei der Diffie-Hellman Variante der Berechung des Premaster Secret?
d) Welche Änderungen wurden bei TLS V1.0 im Vergleich zu SSL V3.0 vorgenommen?

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

Abbildung 1 zeigt den allgemeinen Nachrichtenablauf bei der Authentisierung mit dem EAP-Protokoll unabhängig von der verwendeten EAP-Methode. Als Authentisierungsserver wird ein RADIUS-Server verwendet.

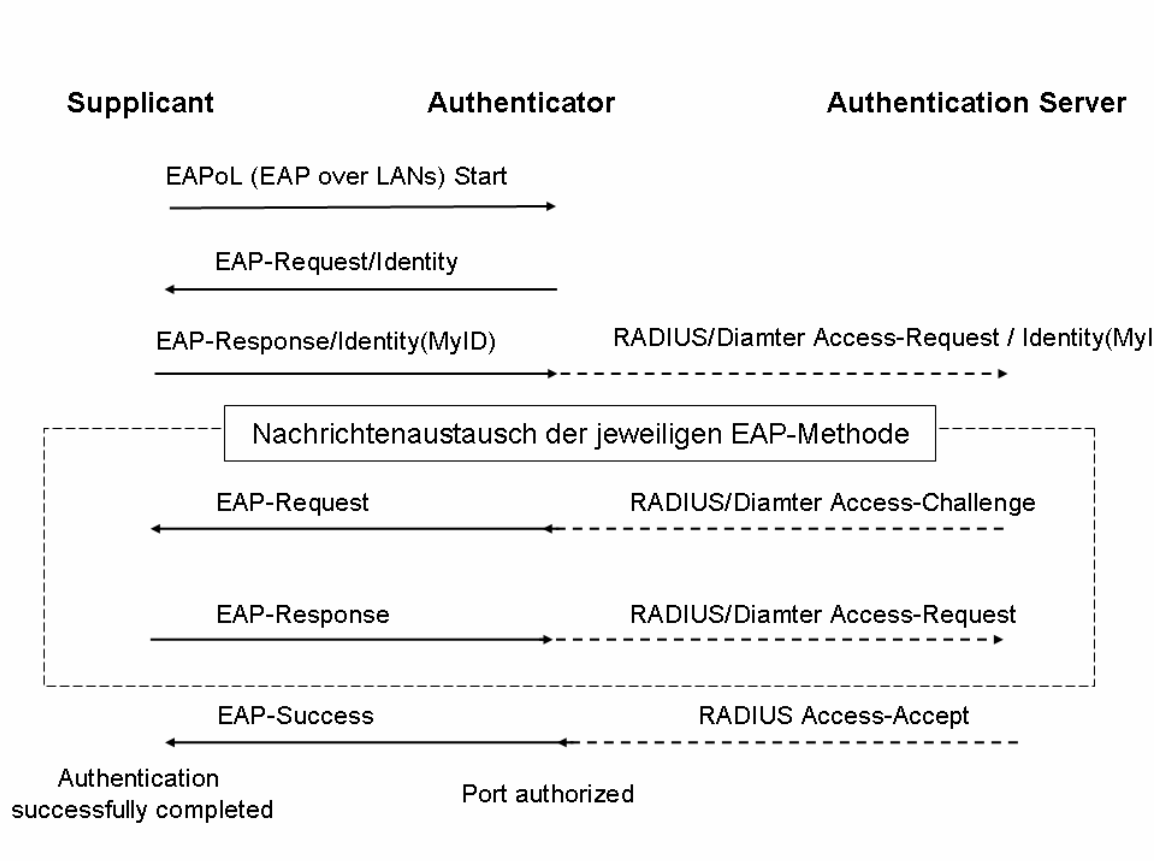

Abbildung 1: EAP generischer Nachrichtenaustausch mit einem RADIUS-Server

a) Beschreiben Sie den Authentisierungsdialog zwischen Supplicant, Authenticator und Authentication Server bei der EAP-MD5-Methode.
   Hinweis 1: siehe RFC 3748 "`PPP Extensible Authentication Protocol (EAP)'", Section 3.4 "`MD5-Challenge'".
   Hinweis 2: Der Platzhalter "`Nachrichtenaustausch der jeweiligen EAP-Methode'" in Abbildung 1 ist mit genau 2 Nachrichten zu ersetzen.
b) Begründen Sie, warum EAP-MD5 gegen Wörterbuch Angriffe anfällig ist.
c) Begründen Sie, warum dieser Angriff mit der Anwendung von EAP-TTLS oder PEAP nicht mehr möglich ist.
   Hinweis: Lesen Sie dazu den Artikel "`TTLS and PEAP Comparison'" unter http://www.opus1.com/www/whitepapers/ttlsandpeap.pdf der einen sehr guten Überblick über die verschiedenen Methoden gibt.
d) Recherchieren Sie im Internet kurz nach den Begriffen "`EAPOL Start Attack'" und "`EAPOL Logoff Attack'". Beschreiben Sie diese Angriffe, die trotz der Anwendung einer sicheren EAP-Methode möglich sind.

--- bitte wenden ---

Aufgabe 4: SSH-Schwachstellen

SSH verwendet Algorithmen für Verschlüsselung und Authentisierung, die allgemein als sicher angesehen werden. Dennoch sind sog.Timing-Angriffe möglich. Beispielsweise sendet SSH wie auch Telnet im Interactive Mode jedes eingegebene Zeichen in einem eigenen Packet.

a) Wie können Angreifer daraus sicherheitsrelevante Informationen ableiten?
b) Weitere derartige Probleme werden in dem Paper "Timing Analysis of Keystrokes and Timing Atacks on SSH" von Dawn X. Song et al. (Tipp: Google Scholar, USENIX) angesprochen. Lesen Sie dort die Abschnitte 1 und 2. Wie sehen die genannten Schwachstellen aus?
c) Welche Angriffe werden dadurch ermöglicht?
d) Im Dezember 2009 stellte man fest, dass verschiedene "Tippfehler-Domains", z. B. *.lrz-munchen.de, registriert worden sind und dort auf allen Subdomains SSH-Daemons liefen, die User-Eingaben entgegennahmen und dann den Login ablehnten. Begründen Sie: Ist es dem Angreifer so möglich, die SSH-Passworte abzugreifen? Wodurch kann ein Nutzer gewarnt sein, falls er vorher schon auf einem der richtigen LRZ-Rechner per SSH eingeloggt war? Warum ist das nicht möglich, wenn er noch nie auf einem LRZ-Rechner eingeloggt war?