Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2024/2025
Übungsblatt 12

Besprechung: Do, 30.01.2024 um 14:00 Uhr

Aufgabe 1: (T) Network-Security & 802.1X

Zur Absicherung von Netzen existieren verschiedene Verfahren. Eine sehr einfache, aber effiziente Möglichkeit, Netztraffic zu separieren, stellt der Einsatz von Virtual LANs (VLANs) dar. Eine im WLAN-Umfeld häufig anzutreffende Maßnahme ist der Einsatz von 802.1X.

a. Erläutern Sie knapp den Aufbau eines VLAN-Tags. Beschreiben Sie kurz die Priorisierung. Welche Prioritätseinstufung schlagen Sie für Video- bzw. IP-Telefonie vor?

b. 802.1X ist ein in WLAN- und VLAN-Infrastrukturen häufig verwendeter Network Access Control-Mechanismus. Sie benötigen in einem Besprechungsraum am LRZ Internet-Zugang über das dort zur Verfügung stehende, 802.1X-gesicherte WLAN. Welche erste Nachricht sendet der Supplicant üblicherweise, wenn der Authenticator nicht bekannt ist?

c. Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants auf Ihrem Notebook an den WLAN-Access Point?

d. Skizzieren Sie die weitere Kommunikation zwischen ihrem Notebook, dem WLAN-Access Point und dem RADIUS-Server generell. Welchen großen Vorteil bietet die Verwendung von EAP-TLS? Was ist hierbei jedoch zwingende Voraussetzung?

Aufgabe 2: (T) Firewalls und Intrusion Detection

a. Welche Firewall-Techniken lassen sich im Allgemeinen unterscheiden? Beschreiben Sie die jeweilige Technik und zeigen Sie mindestens einen sinnvollen Einsatzzweck auf.

b. Erstellen Sie exemplarisch Firewall-Regeln, um die folgenden Anforderungen zu erfüllen. Achten Sie dabei auch auf Vollständigkeit Ihres Regelwerks unter Berücksichtigung maximaler Sicherheit:

   - Der Zugriff auf den Firmen-eigenen Webserver soll von extern per HTTPS möglich sein
   - Die Administration des Webservers erfolgt von dedizierten Managementstationen (IPs: 10.10.18.5 und 10.10.18.200) per ssh
   - Verbieten Sie explizit den Telnet-Zugang auf den Webserver aus dem internen LAN

- Die Security-Policy verbietet den Mitarbeitern des Kunden unter anderem den Aufruf von Jobsearch-Seiten

Ihre Firewall besitzt die externe IP-Adresse 212.34.128.12. Ihr Webserver besitzt die IP-Adresse 10.10.19.6 und befindet sich in einer DMZ. Das interne LAN die Adressen 10.10.18.0/24. Welche zusätzliche Konfiguration an Ihrer Firewall müssen Sie für den Zugriff auf den internen Webserver durchführen?

Erstellen Sie Ihre Firewallregeln in folgendem Tabellenschema:

Nr	Source	Dest	Protocol	Source-Port	Dest-Port	Action

c. Welche grundsätzlichen Erkennungstechniken findet man bei einem Netz-basierten Intrusion Detection System? Nennen Sie Vor- und Nachteile.

d. Intrusion Detection Systeme lassen sich umgehen. Beschreiben Sie mindestens eine mögliche Evasiontechnik.

Aufgabe 3: **(H)** PPTP, MS-CHAPv2 und 802.1x

In der Vorlesung wurde das Point-to-Point-Tunneling Protocol (PPTP) erläutert und dessen Sicherheitseigenschaften betrachtet. Bruce Schneier zeigt in einem Paper Schwachstellen des Protokolls auf. Betrachtet wird darin insbesondere die Authentifizierungsmöglichkeit auf Basis von MS-CHAPv1.

a. Beschreiben Sie in Stichpunkten den Unterschied zwischen Voluntary Tunneling und Compulsory Tunneling.

b. Microsoft besserte das Challenge/Response-Verfahren (MS CHAP) nach. Daraus entstand MS-CHAPv2. Skizzieren Sie den Ablauf von MS-CHAPv2. Welche Schwachstellen wurden in Version 2 im Vergleich zu Version 1 beseitigt und welche nicht. Begründen Sie kurz Ihre Antworten.

c. Gegeben sind

- die 16-Byte Challenge AB12CD34EF56AB12CD34EF56AB78AABB,
- die Peer Authenticator Challenge 159753AFEDAABBCCDDEEFFAADEFA3579
- der Benutzername itsecusr
- das Passwort itsecusr

Berechnen Sie hierzu die jeweiligen Werte, die bei der Kommunikation von Client und Server im Rahmen von MS-CHAPv2 ausgetauscht werden. Beachten Sie dabei folgende Vereinfachungen:

(i) Für die Berechnung des NT-Hash ersetzen Sie einfach die 4-höherwertigen Bits durch Null

(ii) DES wird ersetzt durch eine XOR-Verknüpfung

(iii) MD4 wird ersetzt durch MD5

Die Parameter werden jeweils konkateniert an eine Hashing-Funktion übergeben, d.h. ohne Leerzeichen, Zeilenumbrüche etc.

d. Sie versuchen Zugang zu einem 802.1x gesicherten WLAN aufzubauen. Welche Nachrichten werden zwischen Supplicant, Authenticator und Authentifizierungsserver ausgetauscht bei Verwendung von EAP-TLS? Beschränken Sie sich bei Ihrer Antwort auf die Authentifizierungsphase, d.h. lassen Sie Phasen wie WLAN-Assoziierung und IP-Adressaushandlung mittels DHCP unberücksichtigt.

Aufgabe 4: **(H)** Wired Equivalent Privacy (WEP)

Besonders in WLAN-Netzen werden an die Sicherheit hohe Anforderungen gestellt. Ein erster Schritt die Vertraulichkeit sicherzustellen war Wired Equivalent Privacy (WEP).

a. Beschreiben Sie textuell den Ablauf von WEP (Verschlüsselung)

b. Gegeben sind

   - die Nachricht $M = 27$
   - das Generatorpolynom $x^4 + x + 1$
   - der Initialisierungsvektor IV = F59CE7
   - der Key = 3FC9AB082A

   (i) Berechnen Sie die CRC-32 der Nachricht M

   (ii) Berechnen Sie den Ciphertext

c. Oftmals wird zur Absicherung von WLAN-Umgebungen vorgeschlagen, das SSID-Broadcasting abzuschalten und die Nutzung des WLANs nur Geräten mit bestimmten MAC-Adressen zu erlauben. Ist das Ihrer Ansicht nach sinnvoll? Begründen Sie kurz ihre Antwort.

Aufgabe 5: **(H)** WiFi Protected Access (WPA)

Leider zeigt sich bald, dass die Sicherheitsaspekte von WEP unzureichend waren. Verbesserung versprach sich die IEEE durch Definition von WiFi Protected Access (WPA), insbesondere WPA-TKIP.

a. Beschreiben Sie knapp den Integritätscheck-Algorithmus *Michael*. Der Schlüssel werde mit K^* bezeichnet, der unverschlüsselte Datensatz mit A. Welche Werte nutzt *Michael* für die Berechnung? Welche Bestandteile hat der Wert D, der dem RC4-Algorithmus als Eingabe übergeben wird?

b. Um sich vor Replay-Angriffen zu schützen, wurde in WPA-TKIP ein TKIP Sequence Counter (TSC) eingeführt. Beschreiben Sie in Stichpunkten diesen Wert. Was passiert nach jeder Übertragung damit?

c. Auf Empfängerseite wird der TSC geprüft. Was passiert, wenn der Wert des TSC kleiner oder gleich dem beim Empfänger gespeicherten TSC-Wert ist?

d. Mit WPA-TKIP wurde eine Schlüsselhierarchie eingeführt. Beschreiben Sie knapp die einzelnen Hierarchiestufen.

e. Beschreiben Sie den Ablauf eines WPA Chop-Chop-Angriff! Nennen Sie wichtige Voraussetzungen/Annahmen. Welche Nachrichtenteile sind dem Angreifer trotz passivem Sniffing unbekannt und bilden den Ausgangspunkt des Angriffs?