Informationssysteme
Semesterwoche 12

A) Technologien und Konvergenz

1. Welche Anforderungen stellt die Vision einer permanenten IP Verbindung an das Internet, auch wenn man sich örtlich bewegt?
→ Eine mobile/öffentliche IP Adresse für jedes Gerät
→ Allgegenwärtiges Netzwerk
→ Ein Location Management
→ Caching Strategien

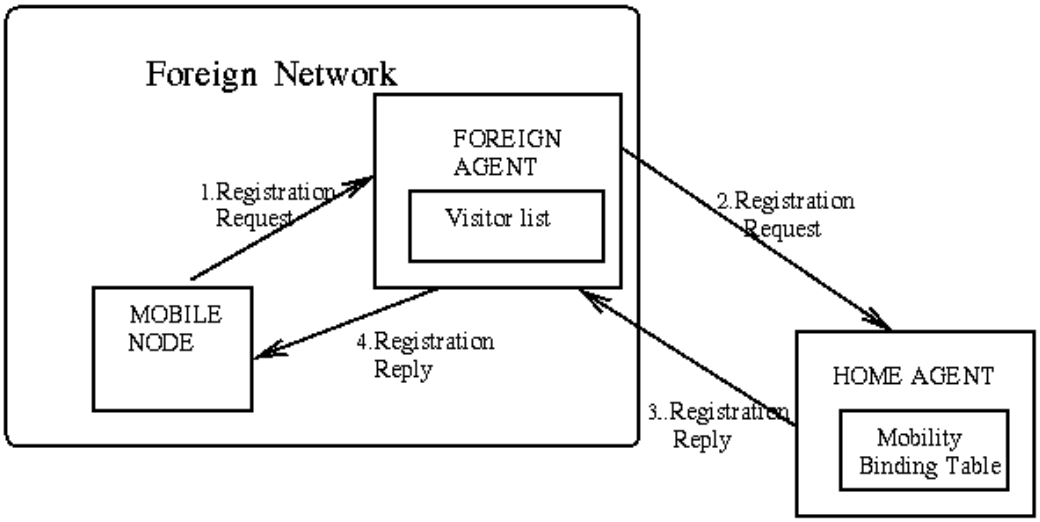
2. Skizzieren Sie die Abläufe im GPRS Netz für die Prozeduren GPRS Attachement und GPRS PDP Context Activation.
→ Siehe Links bzw. Folie 14/15.
http://en.wikipedia.org/wiki/GPRS_Core_Network
http://en.wikipedia.org/wiki/GPRS

Ist die Datenverbindung auf der Luftschnittstelle chiffriert? Wie wird die Datenverbindung zwischen dem SGSN und dem GGSN geschützt?
→ Die Verbindung zwischen Mobiltelefon und dem SGSN ist verschlüsselt..
→ Die Verbindung zwischen SGSN (Serving GPRS Support Node) und GGSN (Gateway GPRS Support Node) ist geschützt mit einem Tunnelling-Mechanismus (IP over IP).

3. Welche vier grundlegenden Netzkonfigurationen von WLAN Ausrüstungen kennen Sie? Formulieren Sie den Einsatz in eigenen Worten.
→ Ad-Hoc: 2 oder mehr Devices verbinden sich gegenseitig in einer Ad-Hoc Session.
→ Infrastructure: Mehrere Devices verbinden sich mit einem Access Point.
→ Bridging: Zwei Netzwerke werden über ein bidirektionalen WLAN-Link verbunden.

4. Welche WLAN Sicherheitsmechanismen gelten heute als unsicher? Zwischen welchen Einsatzbereichen unterscheidet das Wi-Fi Forum bei ihrem WPA Standard?
→ Als unsicher gelten folgende Mechanismen: Versteckte SSID, Statische MAC Reservierung (Whitelists), statische WEP-Verschlüsselungen (d.h. ohne EAP).

5. Erklären Sie den Vorgang von Mobile IP anhand einer Skizze und dem Registrieungsprozess



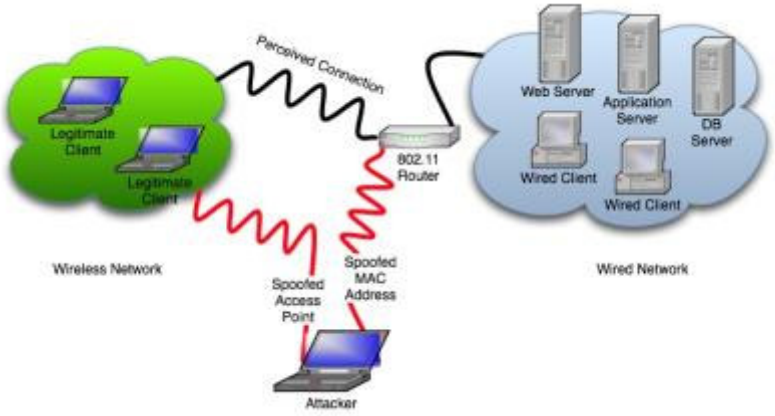
(Siehe auch Folie 45)

B) Netzwerke

1. Welche Sicherheitslücken kann ein Netzwerk haben, welche Schäden können auftreten?
➔ Fehlerhaft konfigurierte Firewall (offene Ports, zugelassene Applikationen)
➔ Fehlender physikalischer Schutz von Netzwerkgeräten.
➔ Fehlende Komplexität bei der Passwortwahl.

➔ Missbrauch der Geheimhaltung
➔ Datenmissbrauch
➔ Datendiebstahl
➔ Datenverlust
➔ Sabotage
➔ Ressourcenzugriff /-diebstahl
➔ Spionage

2. Erklären Sie eine MITM-Attacke
➔ Bei einem Man-In-The-Middle-Angriff (MITM-Angriff) versucht der Angreifer zwischen die beiden Kommunikationspartnern zu gelangen und dabei mit seinem System die komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern zu übernehmen.
So kann er die Informationen nach Belieben einsehen und sogar manipulieren. Der Clou des Angriffs besteht darin, dass den Kommunikationspartnern das jeweilige Gegenüber vorgetäuscht werden kann, ohne dass sie es bemerken.



http://de.wikipedia.org/wiki/Man-In-The-Middle-Angriff

3. Was ist der Unterschied zwischen einem Virus und einem Wurm:
➔ Ein Virus infiziert Dateien sodass die Schadensfunktion mit dem Ausführen der entsprechenden Dateien gestartet wird.
➔ Ein Wurm versucht sich aktiv selber weiter zu verbreiten.
http://de.wikipedia.org/wiki/Computervirus
http://de.wikipedia.org/wiki/Computerwurm

4. Was ist sicherheitstechnisch die Schwachstelle bei der symmetrischen Verschlüsselung.
➔ Der Schlusselaustausch. Dieser kann aber über ein sicheres Verfahren (asymmetrische Verschlüsselung wie RSA) gesichert werden.
http://de.wikipedia.org/wiki/Schl%C3%BCsselverteilungsproblem
http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem

5. Bei der Public-Key-Verschlüsselung können auch mehrere Public-Keys (von verschiednen Personen) benutzt werden, um eine Datei zu verschlüsseln. Jede der Personen kann alleine mit ihrem jeweiligen privaten Schlüssel die Nachricht entschlüsseln. Was ist der Vorteil den diese Möglichkeit bietet?
➔ Jeder kann den öffentlichen Schlüssel zum Verschlüsseln verwenden. Nur der Besitzer des privaten Schlüssels kann entschlüsseln.
http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem

6. Was ist der Vorteil eines Hash im Vergleich zu einer verschlüsselten Datei?
➔ In der Kryptologie werden kryptologische Hashfunktionen zum Signieren von Dokumenten oder zum Erzeugen von Einweg-Verschlüsselungen verwendet.

→ Hashes werden zum Verschlüsseln von Passwörtern verwendet, da diese niemals wieder in Klartext umgewandelt werden müssen.
→ Hashwerte können niemals zurückgewandelt werden.
http://de.wikipedia.org/wiki/Hashfunktion

7. Warum ist bei einer Firewall das Logging wichtig?
→ Im Firewall-Log können Unregelmässigkeiten (z.B. wiederholte Angriffsversuche) festgestellt werden.