Sicherheit moderner Netzwerke

Kapitel 2: Sicherheit: Typische Angriffe

* Verteidigung vor einem Angriff allgemeine Vorgehensweise: Prevention, Detection, Repsonse
* Typen von Malware:

1. Virus: Code der an einer anderen ausführbaren Datei anhängt; meistens wird End-Nutzer Initiierung benötigt; kann zu spezifischer Zeit aktiviert werden
2. Wurm: Code der sich reproduziert; verlangsamt Netzwerke; laufen ohne Host und brauchen nach Infizierung keine Teilnahme vom (bösen) Nutzer
3. Trojanisches Pferd: führt schädlichen Code aus während es sich als neutrale/gute Software ausgibt; Unterschied zu Virus ist, dass es an Bildern, Audios oder Spielen hängt und nicht an ausführbaren Dateien
4. Logic Bomb: benutzt einen Trigger um den Code zu aktivieren; Trigger kann Datum, Zeit, Programme oder auch die Erkennung eines Nutzers sein
5. Ransomware: nimmt einen Computer als „Geisel“ bis eine Bezahlung gemacht wird; arbeitet indem Daten im Computer mit einem unbekannten Schlüssel verschlüsselt werden
6. Backdoors und Rootkits: Backdoors umgehen die normale Authentifizierung zu einem System; Rootkit bringt das System dazu eine Backdoor zu erstellen; Angreifer nutzen Backdoor um Computer remote zu steuern

* Email und Browser Attacken:

1. Spam: Form von Junk Mail; kann schädliche Links oder Malware senden
2. Spyware: Software mit der man Informationen über die Aktivitäten eines Nutzers erhalten kann
3. Adware: lässt nervige Pop-Ups erscheinen; die Malware kann die Interessen des Nutzers analysieren und es kann dann Pop-Ups in Bezug auf die Interessen senden
4. Scareware: bringt den Nutzer mit Pop-Ups dazu spezifische Aktionen aufgrund von Furcht auszuführen
5. Phishing: Email, die aussieht als ob sie von einer vertrauenswürdigen Quelle wäre; Ziel ist es den Nutzer dazu zu bringen Malware zu installieren oder persönliche Daten abzugeben
6. Spear Phishing: ist eine auf die Zielperson ausgerichtete Phishing-Mail
7. Vishing: entspricht Phishing aber mit Sprachkommunikation; auch vorbereitete Aufnahmen können genutzt werden
8. Pharming: Täuschen eine Nutzers indem eine Webseite so erstellt wird, dass sie legitim und wie ihr Original erscheint, um den Nutzer dazu zu bringen sensible Daten anzugeben
9. Whaling: Phishing-Angriff der Ziele mit hohem Wert innerhalb einer Organisation angreift
10. Plugin: erlauben die Entwicklung von interessanten Grafiken und Animationen, um das Aussehen einer Webseite zu optimieren
11. SEO Poisoning: nutzt SEO um eine gefährliche Webseite weiter oben in den Suchergebnissen anzeigen zu lassen
12. Browser Hijacker: Malware welche den Nutzer weiterleitet zu Webseiten, welche Kunden des Kriminellen gehören, die diesen dafür bezahlt haben

* Arten von Cyber Attacken:

1. Man-in-the-middle: Angreifer greift in Kommunikation zwischen Computern ein um Daten zu stehlen; Daten können auch manipuliert werden und Falschinformationen können eingegeben werden
2. Zero-Day Attacke: Angriff der Schwachstellen nutzt, die für den Softwareentwickler unbekannt sind
3. Keyboard Logging: Software welche die Eingaben auf einer Tastatur speichern und an den Angreifer senden (z.B. per Mail)

* Kabellose und mobile Angriffe:

1. Grayware: Anwendungen, die auf störende Weise agieren; kann nicht erkennbare Malware versteckt beinhalten
2. SMiShing: kurz für SMS Ühishing; bringt das Opfer dazu eine Webseite zu besuchen oder ein Nummer anzurufen; auf Webseite kann automatisch eine Malware heruntergeladen werden
3. Rogue Access Points: ein Access Point der in einem sicheren Netzwerk ohne Authorisierung installiert wird; kann auf zwei Wege eingerichtet werden:
4. RF Jamming: unterbricht die Übertragung einer Radio- oder Satellitenstation sodass das Signal nicht sein Ziel erreicht
5. Bluejacking: senden von unauthorisierten Nachrichten zu einem anderen Bluetoothgerät
6. Bluesnarfing: Angreifer kopiert die Informationen des Opfers von seinem Gerät

* Anwendungsangriffe:

1. Cross-site scripting (XXS): Schwachstelle wird in Webanwendungen genutzt um schädliche Skripte zu injiziieren
2. Code Injection Agriff: Schwachstellen in Datenbanken wird genutzt um diese anzugreifen
3. Buffer Overflow: Daten werde geändert, sodass sie den Speicherbuffer überschreiben; kann zu Crash, Datenänderung oder privilege escalation führen
4. Remote Code Execution: über Schwachstelle wird schädlicher Code ausgeführt und Angreifer kann Kontrolle über den PC des Opfers übernehmen

* Wie man sich gegen Anwendungsnagriffe verteidigen kann:

1. Solid code schreiben
2. Jeder Input außerhalb einer Funktion sollte als feindlich angesehen werden
3. Jeden Input validieren, wenn er feindlich ist
4. Betriebssystem und Software immer aktuell halten

* Weitere bekannte Gefahren:

1. Stealth virus: kann seine Veränderungen verstecken sodass sie nicht von Anti-Virus Programmen entdeckt wird
2. Killer packet („Tschernobyl-gram“): sorgt für einen Crash des Opfers
3. Mail bomb: Email mit großen Anhängen, um die Mailbox des Opfers zu fluten (heutzutage nicht mehr so gefährlich)
4. dDOS (distributed DOS attacks): Netzwerkressourcen negativ beeinflussen durch Ausschöpfen oder Überlastung der Kapazitäten

* Echo/Chargen-Angriff: Echo-Befehl befiehlt Zielserver identische Kopie der erhaltenen Daten zurück an Quellserver zu senden; Angreifer sendet große Menge an Echo-Anfrage-Pakete an Zielserver; Zielserver kann mit endloser Anzahl an Echo-Anfrage überflutet werden
* Ping of Death: Angreifer sendet große Anzahl an Ping-Anfragen an Zielserver; ab bestimmten Punkt wird verfügbare Netzwerkkapazität des Servers verbraucht
* Smurf-Angriff: angreifer sendet Ping-Anfrage an IP-Broadcast-Adresse eines großen Netzwerks; Anfrage wird an jeden Host weitergeleitet; jeder Host sendet Antworten an Zielserver weil in Ping-Anfrage die Adresse des Zielservers als Quelle angegeben wird, wodurch Kapazität des Zielservers überlastet wird
* Fraggle: wie Smurf-Angriff aber anstatt von ICMP werden UDP Pakete genutzt
* ICMP port unreachable flood: zufällige Ports werden mit UDP Paketen geflutet sodass die Meldung „ICMP port unreachable“ ausgegeben wird
* Tear drop-Attacke: Angreifer manipuliert Segmente einer Nachricht, sodass sie sich überlappen oder übermäßige Daten enthalten; Zielserver ist mit Nachricht verwirrt und evt. Nicht in der Lage die Nachricht wieder zusammenzusetzen
* Memcached DDoS Reflection Angriff: Memcached ist ein Datenbank Caching System; es hat einen außergewöhnlichen Verstärkungsfaktor (210 byte request kann 100 MB response triggern); auf ungeschützem Server schickt Memcached die Daten auf jeden der fragt, auch gespoofte IP Adressen
* SYN-Flood: Drei-Wege-Handschlag wird ausgenutzt; Ziel wird mit falschen SYN Paketen geflutet; Flut nutzt Zielressourcen aus; dagegen kann mit einem zufälligen drop von unvollständigen Verbindungen gehandelt werden
* Stealth SYN Angriff: nach jedem SYN Paket wird ein RST Paket durch welches UNIX keine Logeinträge generiert; der Angriff wird nicht geloggt
* Adress-Spoofing: Pakete die von A gesendet werden, werde über Angreifer an B weitergeleitet; erlaubt „Man in the Middle Attack“; dagegen kann mit Überwachung der ARP-Tabellen der Netzwerkteilnehmer vorgegangen werden
* DNS-Spoofing: Angreifer fälscht Zuordnung zwischen IP-Adresse und Domänen-Namen; Angreifer täuscht vor bestimmter Webserver zu sein und kann so sensible Informationen ermitteln; dagegen kann mit Überprüfung via private und public key vorgegangen werden
* Firewalking: offene ports eine Firewall und hosts hinter einer Firewall finden; können dann als Brückenkopf für weitere Angriffe dienen; dagegen kann vorgegangen werden, indem ausgehende ICMP TTL Exceeded Nachrichten geblockt werden

Kapitel 3: Sicherheitsarchitekturen

* Firewall: trennt internes Netz einer Organisation vom Rest des Internts; manche Pakete dürfen passieren, andere nicht
* Aufgaben einer Firewall:
  + Denial-of-Service-Angriffe abwehren
  + Illegalen Zugriff auf oder Manipulation von internen Daten verhindern
  + Nur autorisierten Zugriff auf internes Netz erlauben
* Drei Arten von Firewalls:
  + Zustandslose Paketfilter
  + Zustandsbasierte Paketfilter
  + Anwendungs-Gateways
* Zustandslose Paketfilter: Router betrachtet jedes Paket für sich; Entscheidung für Weiterleitung basiert auf: Quell- und Ziel-IP, TCP/UDP-Quell und Zielportnummer, TCP-SYN und ACK-Bits
* Zustandsbehaftete Paketfilter: liest den Verbindungsaufbau- und -abbau mit, kann bestimmen ob ein- und ausgehende Pakete „sinnvoll“ sind; Timeout für inaktive Verbindungen in der Firewall
* Circuit Level Gateways: zerstört ankommende TCP Verbindung und baut eine neue mit dem internent Host auf; interne Host ist somit nicht von außen angreifbar; dazu werden auch die externen TCP Verbindungen überprüft ob sie sich richtig verhalten
* Application Level Gateways: beenden nicht nur externe TCP Verbindungen, sondern inspizieren auch Anwendungs-Verkehr und lässt nur Payloads durch die keine schädlichen Inhalt haben (sind also Proxies)
* Distributed Firewalls: jeder Host hat seine eigene Instanz der Firewall; werden zentral gemanaged; fällt eine Firewall sind andere Hosts noch geschützt im Gegensatz zu einer Standard Firewall
* Anwendungs-Gateways: Pakete warden basierend auf Anwendungsdaten untersucht
* Grenzen von Firewalls und Gateways: IP-Spoofing; wenn mehrere Anwendungen Spezialregeln brauchen, j´hat jede ein eigenes Gateway; Client-Software muss wissen wie man das Gateway kontaktiert; Filter verwenden oft eine „Alles-oder-Nicht“-Regel für UDP; Abwägung zwischen Kommunikationsmöglichkeiten vs. Sicherheitslevel
* Zwei policies: Lax policy (erlaube alles, was nicht explizit verboten ist); Paranoid (verbiete alles, was nicht explizit erlaubt ist)
* Intrusion-Detection-Systeme (IDS): Deep Packet Inspection (DPI): betrachtet Paketinhalt und vergleicht z.B. ob Zeichenketten vorkommen die in bekannten Viren vorhanden sind; erlaubt das Erkennen von Port-Scanning, Netzwerk-Mapping und DoS-Angriffe
* DeMilitarized Zone (DMZ): Zone zwischen „wildem“ Internet und geschützten Intranet; Isolierung der Systeme mit Zugang nach Außen; Genaue Überwachung des Verkehrs; Server in DMZ kann von sich aus keine Verbindung zum LAN aufbauen; gehackter Server in DMZ kann nicht das LAN kompromittieren

Kapitel 4: Ende-zu-Ende Sicherheit

* Anforderungen an eine sichere Verbindung: Vertraulichkeit (kein Abhören), Integrität (Daten vor Veränderung geschützt), Nichtabstreitbarkeit (Urheber ist eindeutig), Authentizität (fremder Datensatz wird erkannt)
* Welche Sicherheitsfunktionalitäten bietet SSL (Secure Sockets Layer) an:

1. Authentisierung des HTTPS Secure-Servers im SSL-Handshake (asymmetrisches Krypto-Verfahren, Public-Key-Verfahren
2. Verschlüsselung der Datenübertragung über SSL-Records (symmetrisches Kryptoverfahren)
3. Sicherstellung der Integrität der übertragenen Daten über SSL-Records (Hashfunktion zur Integritätsprüfung)

* Handshake:

1. Client baut TCP-Verbindung zum Server auf
2. Client baut dann SSL-Session auf und Server authentifiziert sich mit einem Zertifikat
3. Client erzeugt, verschlüsselt und verschickt Master Secret an Server, daraus werden Schlüssel für Kommunikation abgeleitet

* Cipher Suite: Kombination die aus asymmetrischen algorithmus, symmetrischen Algorithmus und Hashfunktion bezeichnet wird, die beim Verbindungsaufbau zwischen Client und Server vereinabrt wird
* Verkürzter Handshake: Wiederaufnahme einer Session; Anhand der Session ID wird versucht mit „altem“ Master Secret weiterzumachen; neue Schlüssel werden aber errechnet
* Status nach dem Handshake: Session ID als Name der SSL-Verbindung; Cipher Suite mit je einem Public-Key-Algorithmus, einem symmetrischen Verschlüsselungsalgortihmus, einem Hashalgorithmus und einem gemeinsamen Master Secret; ein Schlüssel für den Datenverkehr von Client zu Server und umgekehrt
* Schlüsselableitung: Client und Server verwenden Master Secret um vier Schlüssel zu erzeugen: Schlüssel für Verschlüsselung Client -> Server und Server -> Client, MAC-Schlüssel Client -> Server und Server -> Client
* Zertifikat: Authentisierung des öffentlichen Schlüssels durch Zertifikat; Zertifikat enthält Domainname, Ablaufdatum des Schlüssels, Instanz welche die Vertrauenswürdigkeit bestätigt hat; durch Zertifikat authentisiert sich Client gegenüber Server und andersrum
* Root-/ Stamm-Zertifikat: Zertifikat der Zertifizierungsstelle; wird bedingungslos vertraut; Anhand dem Stammzertifikat kann ein Browser feststellen, ob das Zertifikat wirklich von der angegebenen Zertifizierungsstekke ausgestellt wurde
* Validierung eines Zertifikats: OSCP (online Certificate Status Protocol); mit Validierung wird Identität bestätigt, ohne dass beteiligte Kommunikationspartner vorab Authentifizierungsinformationen austauschen müssen
* MAC (Message Authentication Code): kryptografische Prüfsumme; beinhaltet neben Datensatz auch geheimer symmetrischer Schlüssel von Sender und Empfänger; kann nur von Sender und Empfänger berechnet und verifiziert werden
* Schwachstellen von SSL:

1. Zertifizierungsstelle (keine echte Kontrolle; erst wenn etwas bekannt ist verliert die Stelle ihr Vertrauen)
2. Schlüsselerzeugung (einige Zertifizierungsstellen erzeugen auch das Schlüsselpaar; sollte aber nur auf eignen Rechner erzeugt werden)
3. Prüfung der Zertifikate (Browser akzeptieren auch ein ungültiges Zertifikat wenn sie keine Antwort der Zertifizierungsstelle erhalten)
4. Schwache Verschlüsselung

* IPSec (Internet Protocol Security): Protokoll-Suite für gesicherte Kommunikation über IP-Netze
* Einsatzszenarien von IPSec: VPN in unterschiedlichen Ausprägungen (Gateway-zu-Gateway, Host-zu-Host, Host-zu-Gateway)
* Bestandteile von IPSec-VPNs: kryptografischer Schutz der übertragenen Daten, Zugangskontrolle, Datenintegrität, Verschlüsselung, Authentifizierung von Schlüsseln)
* Ziele von IPSec: Vertraulichkeit, Authentizität, Integrität
* Methoden von IPSec: zusätzlicher Header mit MAC; Verschlüsselung
* IPSec basiert auf der Security Association (SA) zwischen zwei Kommunikationspartnern
* Parameter einer SA: Art der gesicherten Übertragung; Verschlüsselungsalgorithmus; Schlüssel; Dauer der Gütligkeit der Schlüssel
* 2 Betriebsarten von IPSec: Tunnel-Modus (Verbindung zwischen zwei Routern); Transport-Modus (Verbindung zwischen zwei Endsystemen)
* Tunnel-Modus:

1. Gesamtes IP-Paket wird vollständig eingekapselt und geschützt
2. Neuer zusätzlicher IP-Header
3. Typisch zwischen IPSec-Routern zur Verbindung von Unternehmensstandorten
4. Kommunikationsbeziehung (originaler IP-Header) bleibt verborgen

* Transport-Modus:

1. Original IP-header bleibt erhalten
2. IPSec Header werden zusätzlich eingefügt
3. Kommunikationsbeziehung (originale IP\_header) ist sichtbar
4. Typisch zwischen zwei Clienten oder Client – IPSec-Router

* Security Association: Idee: im Header nur minimale Info für IPSec; SA ist eindeutig bestimmt durch Security Parameters Index, Ziel IP-Adresse und Sicherheitsprotokoll; jede Sa ist undirektional; SA führt zur SAD
* SA Database (SAD) enthält:

1. Authentifikationsverfahren, Modi und Schlüssel für AH-Protokoll
2. Verschlüsselungsverfahren, Authentifikationsverfahren, Modu und Schlüssel für ESP-Protokoll
3. Lebensdauer der Schlüssel bzw. der SA
4. IP-Adressen der SA-Teilnehmer

* Security Policy Database (SPD): Regeln welche definieren, welche SA im IP Verkehr genutzt werden sollen; jeder Host oder Gateway hat seine eigene SPD
* Authentication Header im Tunnelmodus: gesamtes IP-Paket wird in neues IP-Paket gepackt und geschützt; geeignet für alle VPN-Verbindungen
* Authentication Header im Transportmodus: IP-Header bleibt erhalten und wird mit Rest geschützt; nur geeignet für Host-Host Verbindungen
* Encapsulating Security Payload-Protocl (ESP): ESP-Header (ähnlich AH) nicht verschlüsselt um Auswertung zu ermöglichen
* AH und ESP unabhängig voneinander: AH bietet Authentifikation, ESP bietet Verschlüsselung; oft ist AH ausreichend; ESP ist aufwendiger; AH einfacher als ESP
* Geräte die AH Transportmodus nutzen nennt man IPSec Hosts; Gerät die AH Tunnelmodus nutzen nennt man IPSec Gateways
* IPSec Design Regeln:

1. Ist einer der IPSec Endpunkte ein Gateway -> Tunnelmodus
2. Sind beide IPSec Endpunkte Hosts -> Transportmodus
3. Wenn gesamtes IP-Paket und Header geschützt werden soll -> Tunnelmodus
4. Wenn AH und ESP gemeinsam eingesetzt werden: AH ist äußeres Protokoll, ESP inneres; gemeinsame Modus für beide nutzen

* IPSec Probleme und Schwachstellen:

1. Komplexität der Einstellungen
2. Administration der SPD
3. Verwalten der Parameter
4. Durch NAT erhält IPSec-Paket neue IP-Adresse und anderen Quell-Port; wird IPSec-Paket verändert wird es ungültig -> Lösung: Erweiterung NAT-Traversal: ESP-Pakete werden in UDP-Pakete verpackt und über Port 4500 verschickt, dann können NAT-Router ohne Probleme Adressen und Ports umschreiben

Kapitel 5: Mobilfunk-Netze – Grundlagen und GSM

* Unterschiede zwischen Mobilfunknetz und Festnetz:

1. Teilnehmerauthentifizierung (MN: eigenes Verfahren/ FN: Trust by wire)
2. Mobilitätsverwaltung (MN: Heimat- und Besuchsdatenbank/ FN: durch Rufnummer definiert (ortsbezogene Rufnummer))
3. Mobilität der Teilnehmer (MN: Gespräch wird weitergereicht (Handover)/ FN: Teilnehmer können während des Gesprächs die Funkzelle wechseln)

* GSM (Global System for Mobile Communications): 1. Internationaler Standard für digitale Mobilfunknetze
* IMEI (International Mobile Station Equipment Identity): 15-stellige Seriennummer des Mobilen Gerätes
* SIM-Karte (Subscriber Identity Module): Identität des Nutzers im GSM-Netz; mit PIN geschützte Authentifikation; enthält Prozessor und Schlüssel für die Verschlüsselung der Daten; Location Area der letzten Verbindung
* IMSI (International Mobile Subscriber Identity): weltweit eindeutige Nummer; Zuordnung zu einem Land und Betreiber; benötigt für Zuordnung des Teilnehmers zu einem Ort
* Blockschaltbild einer SIM-Karte: Zugriff auf die Daten im EEPROM nur über den Prozessor; Dateisystem mit Zugriffsrechten; Zugriff erfordert vorher PIN-Eingabe; weitere Applikationen möglich mit SIM Application Toolkit
* MSC (Mobile Switching Centre): Schnittstelle zwischen Funknetz und Telefonnetz; für bestimmtes Gebiet zuständig; Aufgaben: Steuerung des Gesprächaufbaus und -abbaus; Vermittlung der Sprachkanäle; Lokalisierung der Teilnehmer; Steuerung des Handover
* Home Location Register (HLR): enthält Daten wie IMSI, gebuchtes Dienstprofil, Adresse des Visitor Location Registers und Gebührendaten
* Visitor Location Register (VLR): Einbuchen des Teilnehmers bei Aufenthalt in der Location Area eines VLR; enthält Daten wie IMSI, Temporary Mobile Subscriber Identity und Location Area Identification
* Authentication Center (AuC): enthält geheimen Schlüssel der Teilnehmer; Schlüssel für die Nutzdatenverschlüsselung
* Radio-Ressource-Layer (RR-Layer): Steuerung des Funkkanals; Messungen der Funkstrecke; Leistungsregelung; Aktivieren der Verschlüsselung
* Handover: Weiterreichen der bestehenden Verbindung von einer Funkzelle zur nächsten
* Grundprinzip der Sicherheit bei GSM:

1. Authentifizierung des Nutzers durch SIM-Karte/PIN zur SIM-Karte
2. Authentifizierungsverfahren: Challenge/Response
3. SIM-Karte enthält: Initialisierungsschlüssel Ki, Authentifikationsalgorithmus A3, Verfahren A8 zur Generierung der Schlüssel Kc für Daten
4. Verschlüsselungsalgorithmen: A3 (im ROM der SIM-Karte, nicht kopierbar); A8 (im ROM der SIM-Karte, nicht kopierbar); A5 (Verschlüsselung der Nutzdaten mit Sitzungsschlüssel Kc)

* GSM-Schwachstellen:

1. Nur einseitige Authentifizierung (Handy kann nicht überprüfen ob mit richtigem Netz verbunden)
2. Man-in-the-middle Angriff (starkes Mobilfunksignal an Handy -> Handy bucht sich ein -> Abfangen der IMSI -> Ausschalten der Verschlüsselung -> SMS und Signalisierung sind nicht verschlüsselt)
3. Problem SS7 (Internationales Signalisiersystem für Telefonie; Lokalisierungsdaten werden unverschlüsselt übertragen; Betreiber können Standorte der Nutzer abfragen; Zugriff auf SS7 über dubiose Kanäle kaufbar)

* GSM-Angriffsvektoren:

1. Modem/Baseband
2. Roving Bug
3. COO-Ortung
4. IMSI/LAI im Klartext
5. Störfunk
6. Stille SMS
7. Location Leaks und SS7

* GPRS (General Packet Radio Service): Paketvermittlung mit virtuellen Verbindungen; Neue Struktur für Funkkanäle definiert; Neues Codierschema
* Erhöhung der Datenrate von GPRS mit EDGE (Enhanced Data Rates für GSM Evolution)

Kapitel 6: Mobilfunk-Netze, LTE & weitere Entwicklung

* LTE (Long Term Evolution): Mobilfunkstandard der 4. Generation; höhere Datenraten und Flexibilität aufrgund von steigendem Bandbreitenbedarf
* Anforderungen an Funkkanal bei LTE: Nutzung unterschiedlich breiter Kanäle; sehr effiziente Modulation; Adaptives Verfahren zum Ausgleich schwankender Funkstrecken
* Modulationsverfahren OFDM (orthogonal Frequency Division Multiplexing): Signal wird gleichzeitig auf viele Subträger moduliert; gute Anpassung an verfügbare Bandbreite und Störverhalten
* eNodeB (evolved NodeB) Funkteil eines LTE-Netzes: Steuerung der Luft-Schnittstelle; User Management und Aufteilung der Ressourcen auf Luft-Schnittstelle an mehrere Teilnehmer; Sicherstellung von QoS-Attributen für einzelne Verbindungen; Mobilitätsmanagement
* LTE-Netzarchitektur, EPC (Evolved Packet Core) als neue Struktur des Netzes
* EPC Elemente:

1. MME (Mobility Management Entity): Mobility Management; Authentifizierung; Steuerung der IP-Tunnel zwischen eNodeB und Gateway; Unterstützung des Handover
2. SAE (Service Architecture Evolution-Gateway): unterteilt in
3. S-GW (Serving Gateway): steuert Nutzverkehr in bestimmten Gebiet; Weiterleitung der Nutzdaten vom eNodeB zum PDN-GW
4. PDN-GW (Packet Data Network Gateway): Übergang vom LTE-Netz zum Internet; Vergabe von IP-Adressen an Endgeräte; Aufbau und Verwaltung der IP-Tunnel für Nutzdaten
5. HSS (Home Subscriber Server): Authentifizierung und Autorisierung der Nutzer; enthält geheimen Schlüssel der Nutzer
6. PCRF (Policy and Charging Rules Function): Überwachung und Begrenzung des IP-Verkehrs mithilfe von Policies

* Neue Funktionen von LTE Advanced:

1. Carrier Aggregation, Frequenzband-übergreifende Nutzung eines Endgeräts
2. Verbesserte Nutzung von Multi-Antennentechniken
3. Unterstüzung von Relay Nodess