Aufgaben XVI Netzwerktechnik Lösung

Aufgabe 1: Mit welchem asymmetrischen Schlüssel kann man signieren? Von wem muss er stammen?
Antwort: Nur einer darf etwas signieren, der Inhaber des privaten Schlüssels! Er signiertes so, dass alle anderen es mit seinem öffentlichen Schlüssel auf Unversehrtheit der Nachricht und Korrekten Absender prüfen kann. Dazu hat er seinen öffentlichen Schlüssel weitergegeben und/oder veröffentlicht. Beim Verschlüsseln ist es genau anders herum, mit dem öffentlichen Schlüssel kann jeder eine Nachricht für den Inhaber des Schlüsselpaares verschlüsseln und nur der Inhaber des privaten Schlüssels kann entschlüsseln. Für eine gegenseitige Kommunikation mit Verschlüsselung und/oder Signatur sind für jeden Beteiligten ein Schlüsselpaar nötig!
Aufgabe 2: Wie heißen die Verschlüsselungsverfahren bei WLAN? Kann man WLAN auch ohne Verschlüsselung betreiben? Welche rechtlichen Fragen wirft es auf?
Antwort: WEP, WPA, WPA2, WPA3. Die letzten beiden gelten (noch!) als sicher. Man kann auch unverschlüsseltes LAN anbieten. Bei Hotels u.ä. dient ein nachgeschalteter Proxy zum Steuern des Zugriffes. Nur Inhaber eines PIN's können (evtl. zeitlich begrenzt) die Verbindung nutzen. Früher galten harte rechtliche Bedingung für die Benutzung eines Internetanschlusses für den Inhaber. Das ist jetzt gelockert, so dass der Inhaber nicht mehr direkt für die Nutzung über ein freies WLAN in Haftung genommen werden kann.
Aufgabe 3: Der Windowsizewert beträgt 88. Es wurden 22 Pakete empfangen. Das nächste kommt nicht. Wieviel Pakete kann der Empfänger trotzdem noch empfangen haben und wie geht es weiter?
Antwort: 65 Pakete. 88-22 -1(klemmt), Wenn die ersten 22 bestätigt sind: 87 Pakete. Nicht der Empfänger fordert es nach. Da der Absender nur ACK's für 22 Pakete empfangen hat, sendet er Paket 23 von sich aus nach einem Timeout für Bestätigungen nochmals ab. Der Empfänger kann dann mehrere Pakete mit einmal bestätigen (über ackn mit Wert für empfangene Bytes). Dann wird das Fenster beim Sender und Empfänger weiter geschoben, so daß der Senderpuffer weitere zu sendene Daten enthält.
Aufgabe 4: Ordnen Sie folgenden Aktionen die zugehörigen kryptographischen Hilfsmittel zu!
„Arbeitstier" der Verschlüsselung: Symmetrische Verschlüssellung
Verschlüsseln beim Verbindungsaufbau: öffentlicher Schlüssel des Empfängers
Beglaubigung des öffent. Schlüssels: Zertifikat, ausgestellt von einer Certification Authority
Testen der Signatur einer eMail: öffentlichen Schlüssel des Absenders
Oberste Beglaubigungsstätte: Trust Center, Certification Authority
Aufgabe 5: Nennen Sie den öffentlichen Bereich an IPv6 und IPv4 Adressen? Wie lauten die privaten Adressbereiche?
Aufgabe 6: Mit welchen Protokollen wird IP unterstützt? Nennen Sie einige Typen vom IP-Nachrichtensteuerprotokoll!
Antwort: Durch ICMPv6 und ICMPv4, Fehlermeldungen, Echo (Ping, Traceroute) sowie NDP und ARP.
IPv6: 1- Destination Unrecheable, 2-Paket to Big, 3-Time Exceeded, 128+129-Echo Request/Reply, 133+134 RA Solicitation/Advertisement, 135,136: Neighbor Solicitation/Advertisement
Ipv4: 0+8 Echo Request/Reply, 3-Fehler, 11-Code 0 TTL abgelaufen
Aufgabe 7: Wann ist eine Verbindung kollisionsfrei? Kann ein Switch das für alle Übertragungen garantieren?
Antwort: Bei Vollduplex und Punkt-zu-Punkt-Verbindung. Kollisionen ist bei der gemeinsamen Nutzung mehrerer Sender auf einem gemeinsamen Medium typischerweise verbreitet und wird mit CSMA/CD (bei Kollisioserkennung oder sonst:), mit CSMA/CA „bekämpft". Kollisionen können bei Broadcast oder Multicast oder bei der Notfallumschaltung in eine Hub auch vorkommen. Die Pakete gehen dabei (evtl./wahrscheinlich) verloren und das muss durch höhere Schichten entweder korrigiert oder ignoriert werden. Das Internet bietet halt nur eine unsichere Verbindung an…..

Aufgabe 8: Nennen Sie die Unterschiede zwischen Multicast, Broadcast und Anycast! Welche Cast's gibt's noch und woran erkennt man jede einzelne?
Antwort: Multicast ist eine Verbindung von Einem zu Einigen/Mehreren, Broadcast von Einen zu Allen und Anycast von Ein zu Ein aus Einigen, also eine Unicast-Verbindung. Sonst gibt es noch Unicast mit Ein zu Einem und GeoCast von Einem zu Einem nahgelegenen. Uni-, Multi- und Broadcast haben je einen eigenen Adressbereich (Wiederholen Sie bitte diese für IPv6 und IPv4!), während Any- und Geocast von Routern organisiert werden. (IPv6 soll dafür auch eigenen Adressbestandteile definieren, die haben ja genug Adressen…..)