

Aufgabe 1

- Erläutern Sie das TCP Sliding Window Verfahren und welche Vorteile sich gegenüber anderen Verfahren ergeben!
- Erklären Sie auch die Funktion und Wirkungsweise von Duplicate Acknowledgements und Selective Acknowledgements (SACK)!
- Können SACKs immer verwendet werden?

Antwort

- Definiert Sendefenster mit Anzahl der Pakete
 - Pakete werde ohne vorheriges ACK gesendet
- Vorteile:
 - Schnellers senden gegenüber normalem Verfahren
- Duplicate ACK weißt auf Fehler hin
 - Letzes richtig empfangenes Paket wird mehrfach geACKt ^^
- Selective ACK
 - Gruppierung von mehreren ACK in einem ACK-Paket
 - Übertragung der erfolgreichen Pakete

Aufgabe 2

- Erläutern Sie die Begriffe: Scope (DHCP), Realm, Policy, Supplicant und ASN.1!

Antwort

- Scope - Adressbereich der vom DHCP-Server vergeben wird
- Realm - Arbeitsbereich/Domäne
- Policy - Einträge in einer Datenbank zur Rechteverwaltung
- Supplicant - Rechner der sich authentifizieren soll/will
- ASN.1 - Beschreibungssprache für Protokollspezifikation

Aufgabe 3

- Beschreiben Sie kurz den Begriff Zustandsraumexplosion!
- Nennen und beschreiben Sie Methoden, um das Problem der Zustandsraumexplosion zu lösen oder zu umgehen!

Antwort

- Bei großen Zustandsautomaten entstehen sehr viele mögliche Zustände die unterschiedlich aufgerufen werden können.
- Ab 10^9 zu viele Zustände, um alle Zustände in realistischer Zeit auf Konformität prüfen zu können.
- Nur bis 10^7 (kleine Protokolle) realistische vollständige Prüfung möglich
- Teilweises Testen
- Testen auf definierte Zustände - Partitionierung
- zufälliges Testen von Zuständen und Transitionen

Aufgabe 4

In dem E-Mail Postfach das Sie nutzen, sind noch 10 MB Speicherplatz verfügbar. Sie schreiben eine E-Mail mit einer PDF-Datei (8 MB) als Anhang und möchten diese in Ihrem Postfach abspeichern. Beim Speichern wird Ihnen ein Fehler signalisiert der besagt, dass nicht genug Speicherplatz zur Verfügung steht, um die E-Mail zu speichern.

- Begründen und erläutern Sie warum es zu diesem Fehler kommt!
- Wie viel Speicherplatz verbraucht die E-Mail mindestens?

Antwort

- Durch MIME!
 - Erzeugt Overhead durch Kovertierung
- ca. 1/3 mehr als ohne MIME mit base64

Aufgabe 5

Wieso kann durch einen TCP SYN-Flooding Angriff ein Server lahm gelegt werden?

- Erklären Sie kurz, wie durch SYN-Cookies diese Art von Angriff verhindert werden kann!
- Welche Informationen werden dazu im Cookie gespeichert?

Antwort

- Zu viel Speicher wird allokiert...
 - Ressourcenknappheit
 - Keine Anfragen können mehr angenommen werden

- Funktion:
 - SYN
 - SYN,ACK,COOKIE
 - ACK, COOKIE
- Erst nach Empfang des SYN-Cookies vom Client wird Speicher allokiert
- Cookie beinhaltet
 - Session-ID
 - Max-Segmentsize
 - Zeitstempel
 - Ports
 - Geheimer Wert vom Server

Aufgabe 6

- Es gibt drei Anwendungsarten/Anwendungsszenarien für VPNs.
 - Nennen Sie diese!
- IPSec kennt zwei Modi für die Datenübertragung.
- Welcher Modus wird für welches VPN-Anwendungsszenario genutzt?
 - Begründen Sie Ihre Aussage!

Antwort

- Arten:
 - Site-to-Site
 - * Netze über Router verbinden
 - Site-to-End
 - * Netz mit Clientrechner
 - End-to-End
 - * Zwei Clientrechner
 - * Remote-Service
- Modi:
 - Transportmode:
 - * End-to-End Schutz
 - * Direkt Verbindungen von Rechnern
 - Tunnelmode:
 - * Geschützt durch ein drittes Netz routen
- Zusatzinfo...
 - AH - Authentifizierung

- * Sicherstellen des richtiger Kommunikationspartner
- * Inhalt unverfälscht
 - AH/ESP - Verschlüsselung
- * Inhalt vor Zugriff durch unberechtigte geschützt

Aufgabe 7

Skizzieren Sie einem Message Sequence Chart (MSC) zu Aufgabe 1 in dem 5 TCP-Segmente gesendet werden. In dem MSC sind vier Alternativen zu unterscheiden:

1. Alle Segmente werden fehlerfrei übertragen und bestätigt.
2. Das zweite Segment geht verloren.
3. Segment zwei und Segment vier gehen verloren.
4. Das Acknowledgement für das fünfte Segment geht verloren.

Hinweis: Verwenden Sie keine vereinfachte Form des MSC, sondern die vollständige Form wie in ITU-T Z.120 beschrieben.

Antwort