

Vertiefung Rechnertechnik und -netzwerke

Übungsaufgaben – 19. Juni 2012

Aufgabe 1: Routing

Ein Unternehmen verwendet für seinen Standort A das Netz $192.168.65.0/24$, für Standort B das Netz $192.168.66.0/24$. Der Rechner mit der untersten verfügbaren IP-Adresse ist jeweils für die Verbindung zur Außenwelt zuständig; alle anderen TCP/IP-fähigen Geräte sind entsprechend konfiguriert.

Beide Standorte werden nun über eine PPP-Verbindung miteinander verbunden.

Der Rechner $192.168.65.1$ („Firewall A“) erhält dadurch die zusätzliche IP-Adresse $192.168.0.65$, der Rechner $192.168.66.1$ („Firewall B“) die zusätzliche IP-Adresse $192.168.0.66$.

Der Rechner $192.168.66.17$ soll auf dem Drucker $192.168.65.101$, TCP-Port 631, drucken können. Auf beiden Firewall-Rechnern wird IP-Forwarding aktiviert.

- Welche Routing-Tabellen müssen in welcher Weise angepaßt werden?
- Skizzieren Sie eine Firewall-Konfiguration, die bewirkt, daß außer dem genannten Druckvorgang keine Verbindungen zwischen beiden Netzen zustandekommen.
- Was ändert sich, wenn die PPP-Verbindung an Standort A nicht an $192.168.65.1$, sondern an einem anderen Rechner, z. B. $192.168.65.2$ ankommt?

Aufgabe 2: File Transfer Protocol (FTP)

Eine FTP-Dateiübertragung arbeitet nicht mit nur einer, sondern mit zwei TCP-Verbindungen: Die direkt aufgebaute TCP-Verbindung (Server-Port: 21) dient nur zur Steuerung; für die eigentliche Dateiübertragung wird eine zweite TCP-Verbindung aufgebaut. Dabei kann man zwischen zwei grundsätzlich verschiedenen Modi wählen:

- Aktives FTP:** Der Client öffnet einen zufälligen Port und teilt dem Server seine IP-Adresse und die Port-Nummer mit. Der Server baut daraufhin die zweite TCP-Verbindung zum Client auf.
- Passives FTP:** Der Server öffnet einen zufälligen zweiten Port und teilt dem Client seine IP-Adresse und die zweite Port-Nummer mit. Der Client baut die zweite TCP-Verbindung zum Server auf.

- Inwieweit handelt es sich bei FTP um eine Verletzung des Schichtenprinzips?
- Begründen Sie, weshalb man aktives FTP nicht mehr verwenden sollte.
- Kann man FTP über SSH tunneln? Wenn ja, wie? Wenn nein, warum nicht?

Aufgabe 3: ElGamal-Verschlüsselung

Dieses Public-Key-Verschlüsselungsverfahren arbeitet ähnlich wie der Diffie-Hellman-Schlüsselaustausch. Wie bei allen Public-Key-Verschlüsselungsverfahren gilt:

- Alice erzeugt einen öffentlichen und einen geheimen Schlüssel.
- Bob verwendet den öffentlichen Schlüssel von Alice, um einen Klartext m zu verschlüsseln.
- Alice verwendet ihren geheimen Schlüssel, um den verschlüsselten Text wieder zu entschlüsseln.

Beim ElGamal-Verfahren gilt:

- Alice und Bob einigen sich auf einen gemeinsamen Modulus p und eine gemeinsame Basiszahl g .
- Der geheime Schlüssel von Alice ist eine Zahl a ; der zugehörige öffentliche Schlüssel ist $g^a \pmod{p}$.
- Um eine Nachricht m zu verschlüsseln, wählt Bob eine zufällige Zahl b . Zur Verschlüsselung wird m mit $(g^a)^b$ multipliziert (alles mod p). Zusätzlich zur verschlüsselten Nachricht überträgt Bob den Wert g^b an Alice.
- Da Alice die Zahl a kennt, kann sie $(g^a)^b = (g^b)^a$ berechnen, die verschlüsselte Nachricht dadurch dividieren (alles mod p) und auf diese Weise entschlüsseln.

- Demonstrieren Sie die ElGamal-Verschlüsselung am Beispiel $p = 17$, $g = 3$, $a = 6$, $m = 9$, $b = 5$. (Musterlösung: Wikipedia)
- Erklären Sie den Zusammenhang mit dem Diffie-Hellman-Schlüsselaustausch.
- Warum darf Bob nicht b an Alice übertragen, sondern nur g^b ?