1 Netzwerk und Internetsicherheit

1.1 Computernetzwerk

- Zwei oder mehrere Computer, die durch ein Übertragungsmedium miteinander verbunden (vernetzt) sind, bilden ein Computernetzwerk.
- Es gibt Relais Knoten für die Vernetzung da nicht jeder Knoten mit jedem anderen verbunden werden kann (zuviele Verbindungen nötig)

1.2 Adressing und Routing

- Knoten besitzen Adresse
- Mit Pfadangabe können dann Pakete über das Netzwerk verschickt werden
- Jeder Knoten besitzt Routingtabelle = Tabelle wo hingeschicket werden kann
- Forwarding = Prozess der Datenweiterleitung mit Informationen aus dem Routing
- Das eigentliche zusammengefasst: Naming = Name für Knoten oder Dienst/ Adressing = Adresse für Knoten oder Dienst / Routing = Bestimmung des Pfades den Daten durch das Netzwerk nehmen / Forwarding = weiterleiten von Daten von einem Netzwerksegment ins nächste

1.3 Schichtenmodell

- Es hat sich herausgestellt, dass zur Beherschung der Komplexität von Netzwerken Schichten gleicher Funktionalität nützlich sind.
- Schicht ist eine Dienstschnittstelle an die höhere Schicht
- Protokoll zum Austausch von Nachrichten
- jedes Gerät hat eine MAC Adresse und eine IP-Adresse
- beim Austausch werden Pakete übertragen

1.4 IP unter der Lupe

- IP ist Konvergenzprotokoll = überbrückt unterschiedlichste Netzwerktechhnologien / ermöglicht einheitlichen Zugriff für höhere Schichten

1.5 Netzwerksicherheit

- Netzwerksicherheit = Sicherheit aller an das Netzwerk angeschlossenen Geräte abhängig von den Schutzzielen.
- Bit und Linklayer = Schichten 1 & 2: physikalische Verbindung zwischen zwei Netzwerkgeräten - Nur einzelne Segmente können geschützt werden (z.B.) verschlüsseltes WLAN
- Network Layer Schicht 3: - Vermittlungsschicht unabhängig von dem gewählten Linklayer - IP-Adresse -Internetprotokoll IPv4 - IPv6 /Ipsec (ist ein VPN) - Alle Geräte inklusive Router sind beteiligt- Probleme mit NATs = Network Adress Translator
- Transport-Layer 4: bekanntes Beispiel TLS Transport Layer security = https - beseitig Ipsec Probleme (passiert NATs)- nur direkt zwischen den komunizierenden Geräten
- Schicht 7: Application Layer - Beispiel: Email - (EzE) Ende zu Ende Sicherheit - bei Email ist EZE über mehrere Hosts verteilt

1.6 Email unter der Lupe

- Drei wichtige Bestandteile: Anwendungsprogramm(Outlook etc.) - Mailserver - SMTP (Simple Mail Transfere Protokoll)
- Funktionsweise: Anwendungsprogramm sendet an eigenen Mailserver - dieser speichert in eigene Warteschlange - öffnet TCP Verbindung als Client vom Empfängermailserver - Nachricht wird über - Empfängermailserver empfängt Nachricht und speichert sie- Empfänger liest irgendwann die Mail
- Übertragung wird in der Regel geschützt - Obwohl die Mails selbst in Klartext auf den Mailservern und Clients liegen.

3SMTP Client versendet

1.7 Protokoll-Entwurf

- Wie der Computer Hallo sagt: TCP-Verbindungsanforderung (links) / TCP-Verbindungsbestätigung(recht
  GET http://www... (links) / sendet Datei (rechts)
- Für Sicherheit: Bei Verbindung feststellen ob Anfrage nicht mit gefälschter IP versendet wurde. (Beispielsweise könnte Angreifer mit gefälschter IP 1000 Anfragen schicken DOS)
- IPsec (Schutzziel Vertraulichkeit): Sender verschlüsselt (IP Payload) - (Schutzziel Authentifizierung:) Zielhost kann Quell-IP authentifizieren
- IPsec besteht aus 3 Protokollbestandteilen: 1. Authentication-Header-Protokoll(AH) 2. Encapsulation-Security-Protokoll ESP 3. Internet Key Exchange IKE

1.8 Security Association SA

- Aufbau einer logischen Verbindung namens 'Security Association' (SA)
- Verbindung auf der Netzwerkschicht
- wird für AH und ESP benutzt
- Eigenschaften: uni-direktional /SA eindeutig bestimmmt durch: Sicherheitsprokoll(AH oder ESP)/ Quell IP/ 32 Bit Verbindungsid
- 2 Betriebsmodi: Transportmodus (direkte Verbindung zwischen zwei Hosts) / Tunnel-Modus - Tunnel zwischen zwei Hosts - andere Hosts benutzen ihn
- für Kommunikation von A und B wird eine SA von A nach B benötigt und eine SA von B nach A benötigt

1.9 Was hat AH (Authentication Header) zu bieten?

- Quellen-Authentifizierung/ Datenintegrität/ keine Vertraulichkeit - AH-Heaeder liegt zwischen Daten und IP-Header
- gewährt Datenintegrität und Quellen-Identifizierung - aber keine Vertraulichkeit

1.10 Was hat ESP (Encapsulating Security Payload) zu bieten?

- bietet Vertraulichkeit/ Hostauthentifizierung / Datenintegrität
- Daten und ESP-Trailer sind verschlüsselt
- viel blabla welches unwichtig scheint...

1.11 SA - Management

- ESP oder AH werden für Übertragung verwendet -aber wie baut man die Verbindung auf?
- Möglichkeiten: 1. manuelle Konfiguration (selbstständige Eingabe der Verschlüssungsparameter 2. Automatische Konfiguration - Beispiel (IKE = Internet Key Exchange)

1.12 IKE

- Gegenseitige Authentifizierung
- Aushandeln der Parameter
- Aufbau und halten der Verbindung
- benutzt Zertifikate oder shared secrets für den Verbinundsaufbau
- Zwei Versionen IKEv1 und IKEV2 (2 scheint super wichtig zu sein)

1.13 Was die IP alles erlaubt

- Jeder Host kann mit jedem anderen Host komunizieren
- jede Art von Dienst möglich
- Vor- und Nachteile - Angriffe(Denial of Service, Einbrechen in Systeme, Missbrauch von Daten)

1.14 Was machen Firewalls?

- Filtern und untersuchen Datagramme (Hauptsächlich Paketheader (Inhalt würde tiefergehen DPI = Deep Packet Inspection))
- Firewalls werden in den Netzwerk-Datenpfad gesetzt
- typischerweise an den definierten Netzübergängen (zwischen unterschiedlichen Sicherheitsbereichen)
- Firewall erlaubt Durchgang oder blockiert (Einzelne Pakete - bzw. Fluss von Pakten (package flow))
- Firewalls blocken sowohl angreifer von außen ab - als auch die Weiterleitung von Viren von Innen.
- Firewalls inspezieren die Pakte anhand von Filterregeln (dann aktion pass - bzw. block)
- Policiy-Rules implizieren eine Verkehrsfulssrichtung (Ausgehender Verkehr - eingehender Verkehr)

1.15 Firewall Typen

- Nur Ip Layer (seit 2014 nicht mehr im Einsatz)
- checkt Layer 4 Tcp und IP header - checkt unter anderem die Semantic ... sehr verbreitet (2014)
- Deep Packet Inspection - checkt weiter als Layer 4 bis in die Applikationsdaten hinein
- Zustandslose/stateless
- Zustandsbehaftete/stateful: behält einen Zustand für eine Verbindung für beispielweise TCP ICMP ...
- Unterschied zwischen stateless und stateful - bei stateful gilt wer reinkommt darf auch beantwortet werden

1.16 Was ist eine Middlebox?

- Eine Mittelbox ist alles was zwischen einem Quellhost und einem Zielhost liegt und andere Aufgaben erfüllt als ein normaler Router
- Beispiele: Firewall, NAT (Network Adress Translator), Quality of Service Packet markers, Transportverzörgerer und vieles mehr...

1.17 Middlebox Konfiguration

- Grundsätzliche Konfiguration: Erlaube ausgehende Verbindungen (statisch) blockiere eingehende Verbindungen (statisch)
- TCP wird von Firewalls bevorzugt da zustandsbehaftetes Protokoll
- UDB blockiert oder nur sehr begrenzt zugelassen (Nur für DNS domain name server)

1.18 Layout 1: Zwei Arm Mittelbox

- eine Firwall zwischen dem Intenert und dem Firmennetz
- billigste Lösung aber kommt einer rein hat er kompletten Zugriff!

1.19 Layout 2: DMZ = Demilitarised Zone

- Standard Rangehensweise
- Externer Webserver FTP Server in DMZ durch Firwall gesichert
- Internes Netzwerk nochmal durch eigene Firwall gesichert

1.20 Sonstige Layouts

- Nur eine Middlebox für inneres Netzwerk (fast so sicher wie standardlösung)
- Schlechte Lösung zwei interne netzwerke mit jeweils eigener Firwall
- bessere Lösung zwei interner Netzwerke die durch selbe Middlebox geschützt werden