TelNet:

Voller Name: Teletype Network

Entwickelt am 1969 für das ARPNET.

Ziel: Rechenzeit, Anwendungen und Datenbanken remote nutzen können wurde 1974 zum ersten Mal eingesetzt

Virtueller zugriff auf einen anderen Computer

Bidirektionale, textbasierte Kommunikation Verbindung zwischen zwei PCs

Abzuraten weil es 100% offen ist

RDP:

Remote Desktop Protokoll

Netzwerkprotokoll für fernzugriffe auf normalerweise Windows PCs

Von Microsoft entwickelt im Jahr 1998

Basiert auf Citrix Technik Multiwin

Verfügbar ab WindowsNT 4.0 bzw. Windows XP SP-1

Gibt eine Visuelle Datenübertragung

Minimum an Input wird an gesteuertem Gerät gesendet und Minimum an Ausgabe (Bsp. Framebuffer/Output der Grafikkarte) wird an das Steuernde Gerät gesendet

Konkurrenz zu dem VNC-Protokoll das Open source ist

VNC:

Virtual Network Computing

Existiert seit dem 90er Jahren

RDP ähnliches X11 Protokoll

Unterschiedliche Umsetzung Art die auf dasselbe hervor geht

VNC ist wegen Remote Framebuffer platformunabhängig

TeamViewer

Seit 2015 auf dem Markt und wurde ständig verbessert

Basiert auf VNC

FunFact: Das unternehmen wollte unnötige Fahrten zu seinen Kunden vermeiden

Ist eine Fernwartungssoftware

Verfügbar auf den Meisten gängigen Betriebssystemen

Benötigt Teamviewer an den beiden Geräten

TCP/UDP Verbindung via Port 5938

End to End Verschlüsselung mit RSA und AES

SSH:

Secure Shell

Entwickelt 1995 von Tatu Ylönen(Finne)

Grund: Angriff auf Uni. Helsinki

RSH, rlogin und Telnet sind plain-text Fernzugriffs-Protokolle aus der Prä-Internet-Zeit

Funktionen:

Sichere verschlüsselte verbindung

Eigentlich nur Dienst zur Verschlüsselung von TCP-Verbindungen

Öffentlich: Die Existenz einer ssh verbindung

Anzahl der Pakete

Frequenz des Datenaustauschs

Verschlüsselt: Paket Inhalt

Verbindung:

1. Aufbau TCP Verbindung
   1. Auch Websocket-Verbindung möglich
2. Host identifiziert sich mit RSA- DSA- o. ECDSA-Zertifikat
3. Symmetrische Verschlüsselung der Verbindung
4. Authentifizierung des Clients
   1. Public/Private-key
   2. Passwort
   3. MFA Möglich bei aktueller Version

Pro verbindung gibt es einen Channel, Mehrere Verbindungen zum Host möglich

Paketaufbau:

1. Paketlänge (4 Bytes) (Offen)
2. Paddingmenge (1 Byte) (Verschlüsselt)
3. Inhalt/Payload (Verschlüsselt)
   1. Andere Protokolle möglich
   2. Komprimierung möglich
4. Padding (Verschlüsselt)
   1. Zufällige Bytes für Sicherheit
5. Nachrichtenauthentifizierungscode (Offen)
   1. Verifizierung der Integrität des Pakets