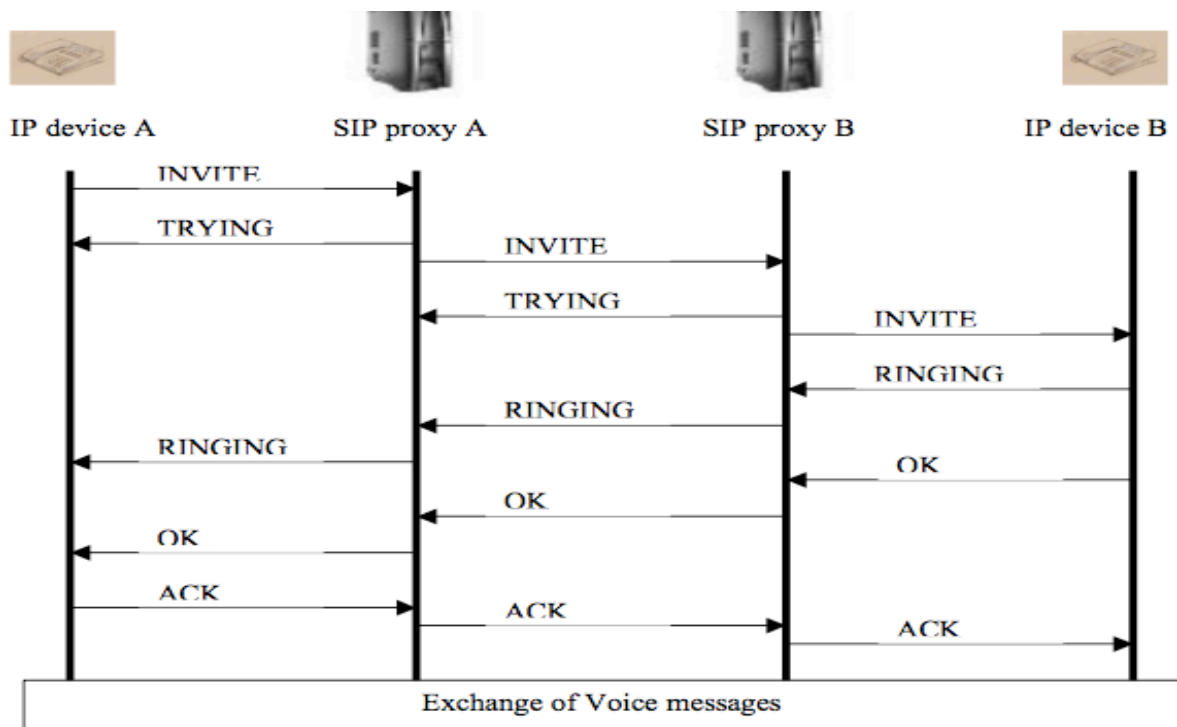


## IT-Sicherheit in Netzwerken – Praktische Aufgaben 4

Um Informationsflusssicherheit garantieren zu können, muss der Kommunikationsfluss zwischen den verschiedensten Schichten des so genannten hybriden ISO/OSI 7 Schichtenmodels geschützt werden. Dabei müssen ggf. die genutzten Kommunikationswege einer jeden einzelnen Anwendung neu betrachtet werden. Im Rahmen der Veranstaltung IT-Sicherheit in Netzwerken haben wir bereits die Internet Protokolle angesehen, wie IP, TCP, UDP und ICMP.

Um sichere Netzwerke zu garantieren, werden in der Regel Proxies (Hilfsprogramme) verwendet. Proxy Server werden benutzt, um Netzwerk Richtlinien (Network Policies) zu implementieren und damit Sicherheitsstrategien für Dienste (Services) im Web bereitzustellen. Üblicherweise ist der Web Proxy nicht für die Client-Anwendung transparent: Der Proxy muss konfiguriert werden. Die Konfiguration kann dabei manuell oder durch ein automatisiertes Script vorgenommen werden. Die Verwendung eines Proxys kann der Benutzer oftmals umgehen, indem die Client-Anwendung neu gestartet wird. Ausgenommen wenn der Proxy anstelle eines NAT Routers benutzt wird, um eine gemeinsame Internet-Verbindung oder LAN-Verbindung aufzubauen.

Im Folgenden soll die Anwendung Telefonieren im Internet (Voice over IP, VoIP) betrachtet werden; d.h. der zu schützende Verbindungsauf- und abbau zweier Teilnehmer A und B ist zu untersuchen. Dabei ist zu ermitteln, welche Gefahren drohen und welche Schwachstellen zu schützen sind, um die Entwicklung eines sicheren Proxys für die Nutzung von VoIP zu ermöglichen. Der Verbindungsaufbau bei VoIP ist im unter Anwendung des so genannten Session Initiation Protocols (SIP) ist im folgenden Diagramm dargestellt. Teilnehmer A ruft Teilnehmer B an. Der Teilnehmer A benutzt Proxy Server A und Teilnehmer B entsprechend Proxy Server B.



Die Spezifikation von SIP erlaubt die Verwendung von TCP und UDP (neben weiteren anderen Protokollen).

1. Beschreiben Sie in eigenen Worten den gesamten Ablauf einer VoIP-Verbindung. Geben Sie dabei die anzusprechenden Schichten im hybriden TCP/IP 7 Schichtenmodell in Abhängigkeit jeweiligen Rechner der Teilnehmer A und B bzw. der möglicherweise verwendeten Intermediates an, wenn Teilnehmer A den Teilnehmer B anruft. Als Darstellung genügt eine durchnummerierte Liste, die die entsprechenden angesprochenen Schichten und darin nötigen Informationen zum Verbindungsaufbau und -abbau in Abhängigkeit der verwendeten Protokolle wiedergibt.
2. Diskutieren Sie Vor- und Nachteile von TCP und UDP als Transportschicht, um SIP Nachrichten zu senden.
3. Auf welchen Ebenen und in welchen Situationen ist es möglich die Verbindung über VoIP unter Anwendung von SSL/TLS zu schützen? Können Sie die unterschiedlichen Aufgaben und Rollen der Clients und der Server unter Berücksichtigung des SSL/TLS Protokolls für die „Objekte“ im oben gegebenen Sequenzdiagramm beschreiben?
4. Was muss für die Anwendung von SSL/TLS auf der Transportebene zusätzlich verlangt werden?
5. Fassen Sie zusammen: Welche bekannten Sicherheitsprobleme zur Gewährung von Informationsflusssicherheit wiederholen Sie bei der Einführung neuerer Technologien im Vergleich zu der Absicherung einer Ethernet-Verbindung.
6. Unter <http://www.voip-info.org/> finden Sie verschiedene OpenSource Software, um eine VoIP-Verbindung nutzen zu können.
  - a. Installieren Sie eine Version, die zu Ihrem Betriebssystem passt.
  - b. Konfigurieren Sie den jeweiligen Client Proxy, so dass Sie mit einem Kommilitonen kommunizieren können.
  - c. Testen Sie auch, ob Ihre Verbindung sicher ist, indem Sie versuchen ein Gespräch auf Ihrem Rechner aufzuzeichnen und es erneut versuchen (unverschlüsselt ?) auf Ihrem Rechner abzuhören.
  - d. Was ist also bei der Konfiguration von Clients zusätzlich zu beachten? Welche Sicherheitsvorkehrungen müssen beide Teilnehmer A und B in Übereinkunft treffen?

Nach Durchführung dieser Aufgaben sind Sie in der Lage bei neuen Anwendungen

- Gefahren, die die Informationsflusssicherheit gefährden könnten, entlang der verwendeten Protokolle für eine hybride TCP/IP ISO/OSI 7 Schichtenarchitektur zu identifizieren,
- die Schwachstellen, insbesondere in Hinblick auf neue Protokolle für moderne Anwendungen, zu finden und zu bewerten,
- eine (informationsfluss-)sichere Spezifikation für Protokolle moderner Anwendungen zu liefern und
- eine die (zusätzlichen) Funktionalitäten benötigter Proxies anzugeben.