CS7344 Homework 1

Name: Bingying Liang
ID: 48999397

Sep 10 2023

1. You set up a communication channel between two medieval castles by letting a trained raven repeatedly carry a scroll from the sending castle to the receiving castle, 160 kilometers away. The raven flies at an average speed of 40 km/h, and carries one scroll at a time. Each scroll contains 1.8 terabytes of data. Calculate the data rate of this channel when sending.

   See section 1.9 for metric units.

   (a) 1.8 terabytes of data;

   Solution:

   $\because$ The raven flies at an average speed of 40 km/h, and carries one scroll at a time.
   Each scroll contains 1.8 terabytes of data

   $\therefore$ Just fly one time

   $$\therefore \text{Data rate} = \frac{\text{Amount of Data}}{\text{Time}} = \frac{1.8 \text{ terabytes}}{\frac{160km}{40km/h} \times 1} = \frac{1.8 \times 10^3 \times 8 \text{ gigabits}}{4 \times 60 \times 60 \text{ seconds}} = 1 \text{ Gbps}$$

   (b) 3.6 terabytes of data.

   Solution:

   $\because$ The raven flies at an average speed of 40 km/h, and carries one scroll at a time.
   Each scroll contains 1.8 terabytes of data

   $\therefore$ Just fly three times

   $$\text{Data rate} = \frac{\text{Amount of Data}}{\text{Time}} = \frac{3.6 \text{ terabytes}}{\frac{160km}{40km/h} \times 3} = \frac{3.6 \times 10^3 \times 8 \text{ gigabits}}{4 \times 60 \times 60 \times 3 \text{ seconds}} \approx 0.67 \text{ Gbps}$$

2. Which of the OSI layers and TCP/IP layers handles each of the following:

   (a) Dividing the transmitted bit stream into frames.

   Solution: OSI layers: This task is managed by the Data Link Layer (Layer 2). The Data Link layer is responsible for creating a reliable link between two directly connected nodes, and this involves framing, which is the process of dividing the data stream

into frames.
TCP/IP layers: In the TCP/IP layers, this is handled by the equivalent of the Link layer. In the TCP/IP model's terminology, this layer is typically combined with the Physical layer and is referred to as the Network Access/Link Layer.

(b) Determining which route through the subnet to use.

Solution: OSI layer: This responsibility belongs to the Network Layer (Layer 3). This layer is concerned with determining the best path to route data from the source to the destination, which may involve multiple hops across different networks.
TCP/IP layer: This corresponds to the Internet Layer. In the TCP/IP model, the Internet layer is responsible for addressing, packaging, and routing functions.

3. Mobile phone network operators need to know where their subscribers' mobile phones (hence their users) are located. Explain why this is bad for users. Now give reasons why this is good for users.

Solution:

Why This is Bad for Users:

(a) Privacy Concerns: Knowing a user's location can provide insights into their habits, routines, interests, and relationships. Continuous tracking can result in a comprehensive profile of a user's life.

(b) Data Security: If there's a breach in the operator's database, the location data of users could be accessed by malicious actors. This data can be used for various nefarious purposes, including stalking, blackmailing, or even burglary when they know you're away from home.

(c) Potential Misuse: Governments or law enforcement could potentially request access to this data without the user's knowledge or consent, leading to surveillance and potential infringement on civil liberties.

(d) Targeted Advertising: Knowing a user's location allows companies to push location-based advertisements. While this could sometimes be seen as a benefit (in the ”good for users” section), it can also be intrusive and unwanted by many users.

(e) Battery Drain: Continual location tracking, especially with high accuracy, can deplete a mobile phone's battery more rapidly.

Why This is Good for Users:

(a) Emergency Services: In the event of an emergency, location data can be invaluable. If someone calls for an ambulance or police, their location can be pinpointed immediately, potentially saving lives.

(b) Better Connectivity: Operators use this data to understand where to build new towers or optimize existing ones. Knowing where users commonly are helps improve network coverage and signal strength.

(c) Location-based Services: Many modern smartphone apps provide services based on your location, such as weather updates, restaurant recommendations, or navigation. Without location data, these services wouldn't be as effective or accurate.

(d) Fraud Detection: For services that monitor unusual activity (like banking apps), an unexpected location can be a signal of potential fraud, triggering alerts or security checks.

(e) Optimized Experience: As mentioned in the negative section, targeted advertising can be seen as a positive by some users. If you walk into a shopping mall, you might receive discounts or promotions related to stores in that mall, providing a personalized experience.

(f) Lost Device Tracking: If you lose your phone or it gets stolen, having location services can help you locate and potentially recover your device. In conclusion, while there are legitimate concerns about location tracking by mobile operators, there are also clear benefits. It's a balance between privacy and convenience, and users should be aware of both sides to make informed decisions about their location settings.

4. An image is 3840*2160 pixels with 3 bytes/pixel. Assume the image is uncompressed. How long does it take to transmit it over a 56-kbps modem channel?

Solution:

$\because$ The image is 3840×2160 pixels with 3 bytes/pixel

$\therefore$ Image size $= 3840 \times 2160 \times 3 \times 8 = 199065600$ bits

$\because$ transmit it over a 56-kbps modem channel

$$\therefore \text{Time} = \frac{\text{Image size}}{\text{Transmission Rate}} = \frac{199065600 \text{ bits}}{56 \text{ kbps}} = \frac{199065600 \text{ bits}}{56,000 \text{ bps}} \approx 3554.7429 \text{ seconds}$$

5. Go to IETF's Web site, www.ietf.org, to see what they are doing. Pick a project you like and write a half-page report on the problem and the proposed solution.

Solution:

Project: TLS 1.3
Problem: Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL) and is used to encrypt data transmitted over networks, such as data sent via HTTPS. Previous versions of TLS (especially 1.0 and 1.1) had various vulnerabilities, which made encrypted data susceptible to eavesdropping and tampering. Over the years, as these vulnerabilities were discovered, the urgent need for a more secure protocol became evident. The older versions were prone to attacks like the BEAST, CRIME, and POODLE, which threatened online data security.

Proposed solution: IETF, in its ongoing effort to ensure the security and stability of internet protocols, worked on TLS 1.3 as the newest version of the TLS protocol. Some of the key features and improvements proposed for TLS 1.3 included:

(a) Reduced Handshake Time: Unlike previous versions which required two round-trips to complete the handshake, TLS 1.3 reduced this to only one, thereby speeding up the connection establishment.

(b) Removal of Outdated Cipher Suites: Many old and insecure cryptographic algorithms, like DES, RC4, and even AES-CBC, were removed. This made the protocol leaner and more secure.

(c) Forward Secrecy as Default: TLS 1.3 mandates forward secrecy, which means even if the private key is compromised in the future, past communications remain secure.

(d) Introduction of 0-RTT (Zero Round Trip Time Resumption): This allows the client and server to remember previous sessions and thereby eliminate round-trips entirely for subsequent connections. However, this feature also brought new challenges, such as potential replay attacks.

(e) Encrypted Handshake: Unlike previous versions where some parts of the handshake were sent in clear, TLS 1.3 proposed that most of the handshake process be encrypted, providing more privacy.

Conclusion: TLS 1.3, as proposed by the IETF, aimed to enhance security by eliminating vulnerabilities present in older versions and introducing features that speed up secure communication. Adoption of TLS 1.3 was a significant step towards a more secure internet. However, like any technology, it was essential to monitor and adapt as new challenges arose.