# Social Engineering
# Denial of Service

Security spring 2019

# Social Engineering principles

- Reprocity
  - People tend to return a favour (good cop/bad cop)
- Commitment and consistency
  - Brainwashing – ”I’ll sign up later” vs. ”No thanks I prefer not making money”

# Social Engineering principles

- Social proof
  - The others do so
- Authority
- Linking
  - What would others do or think
- Scarity
  - Limited time

# Social Engineering vectors

- Vishing
  - Voice phishing
- Phishing
  - Homophone for *fishing*
  - Spear phishing uses highly customized content
  - Water holing uses knowledge about favourite sites
- Smishing
  - SMS phishing
- Impersonation

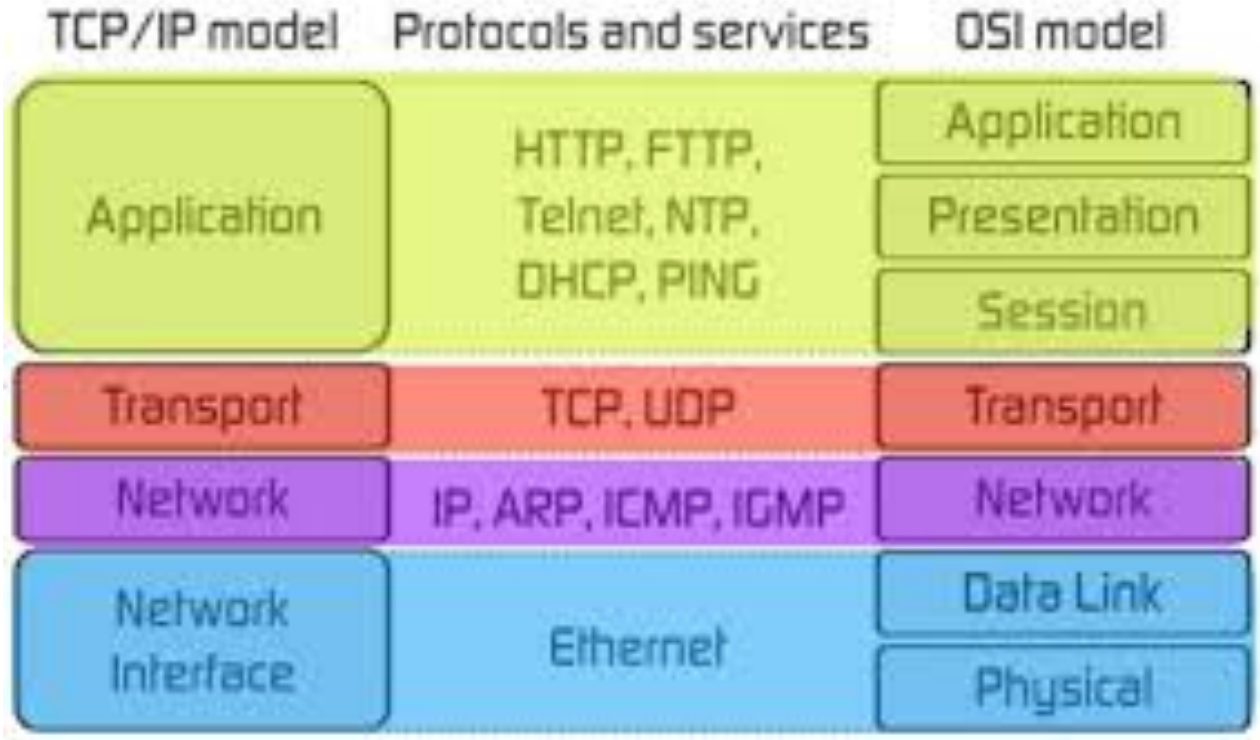
# SMTP

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.com
S: 250 smtp.example.com, I am glad to meet you
C: MAIL FROM:<bob@example.com>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.com>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

# Denial of Service

- Crash Service
- Flood Service
- Distributed attacks

- Application layer attacks
- Network layer attacks



# Denial of Service DoS

- Degradation of Service
- Denial of Service Level II
  - Make the service block as a defense mechanism
- Distributed Denial of Service DDoS
- HTTP POST DoS attack
- Internet Control Message Protocol Attack
- Permanent DoS attacks *phlashing*
  - Destroy Server e.g. By updating firmware

# Denial of Service

- Amplification

**UDP-based Amplification Attacks**

| Protocol | Bandwidth Amplification Factor |
|---|---|
| Memcached | 50000 |
| NTP | 556.9 |
| CharGen | 358.8 |
| DNS | up to 179 [52] |
| QOTD | 140.3 |
| Quake Network Protocol | 63.9 |
| BitTorrent | 4.0 - 54.3 [53] |
| SSDP | 30.8 |
| Kad | 16.3 |
| SNMPv2 | 6.3 |
| Steam Protocol | 5.5 |
| NetBIOS | 3.8 |

# Denial of Service

- Elastic cloud services
- Blackholing – sinkholing
- ISP based prevention
- DoS Defense System (DDS) based defense
- Firewalls
- Routers
- Upstream filtering