UDP and TCP

Level 0x02: Sockets

Quick Overview

- UDP / TCP Background
- Demo
- Takeaways

View Source CTF

- Online CTF - https://ctf.viewsource.me/
  - Categories include reverse engineering, pwn, cryptography, forensics, web, and misc.
  - Join our Discord: https://discord.gg/mVAzUJrpyf
  - Infra sponsored by goo.gle/ctfsponsorship
  - Starts: Saturday Sept 23, 2023 12PM NOON EST
  - Ends: Sunday Sept 24, 2023 12PM NOON EST
- Student Division:
  - 1st Place - $250
  - Only teams composed of middle school, high school, or undergraduate students are eligible for Student division prizes. Register with your school email and choose the Student division in your profile.

Florida Tech Cyber Class

- Too late to join this one
- 4 of our students joined
- Plus more West Shore students not in CS club

- Future Activities
  - TBA Spring CTF with mentoring in-person
  - 1-week Summer Camp
    - 5 full days
    - Paid for by NSA grant

BECOME A CYBER-SUPERSTAR IN 10 WEEKS USING HACKABLE TOYS

Sept. 14–Nov. 16 | Two hour weekly classes

Free course offered at Florida Tech

APPLY HERE

Florida Tech
Ruth Funk Center (Esports)
150 W. University Blvd., Melbourne, FL 32901

Each participant will:

- **Have a chance to win a 4-year scholarship to Florida Tech, worth $80,000 over 4 years.**
- **Receive a certificate of completion of cybersecurity training.**
- **Learn skills related to ethics in cybersecurity, web exploitation and cryptographic attacks.**

Do you have what it takes to become the next generation cyber-superstar? Come join us for an exciting adventure and discover the secrets of the cyber world! In this 10-week course that meets once a week after school. You will learn and apply coding and problem-solving skills about how to hack and protect against cyberattacks on the web and smart devices, such as Alexa and ring doorbell cameras! Experience the thrill of using hackable toys like remote control cars, Game Boy emulators and Raspberry Pis to get you on a path to a potential cybersecurity career.

Participation Requirements: No prior coding/hacking knowledge or skills required, must be willing to attend two hours a week for 10 weeks, must be able to work in groups

FLORIDA TECH

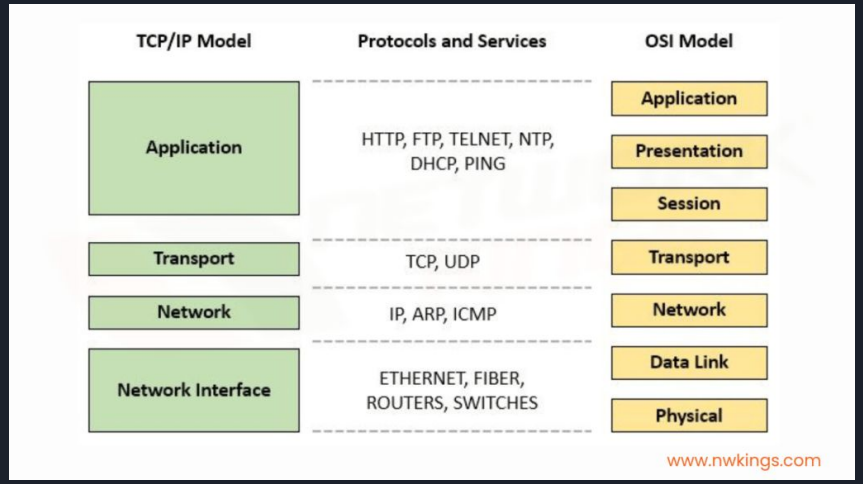
Zammis Clark
aka Slipstream aka Raylee

- Hacked VTech servers in 2015
  - Stole info on 6 million children - but sent it all to the media to expose VTech
  - VTech got fined $650,000
- Hacked Nintendo
  - Leaked source and documentation on Nintendo games and consoles
- Hacked Microsoft in 2017, stole 43,000 files
- Due to autism, face-blindness, prison won't help him
  - Didn't serve his 18 month sentence (2019)
- Hacked North Korea in 2015
  - Stole Red Star OS (North Korean Linux) - never seen by anyone outside of Korea

"Chaotic Good" - a reddit user

Transport Layer

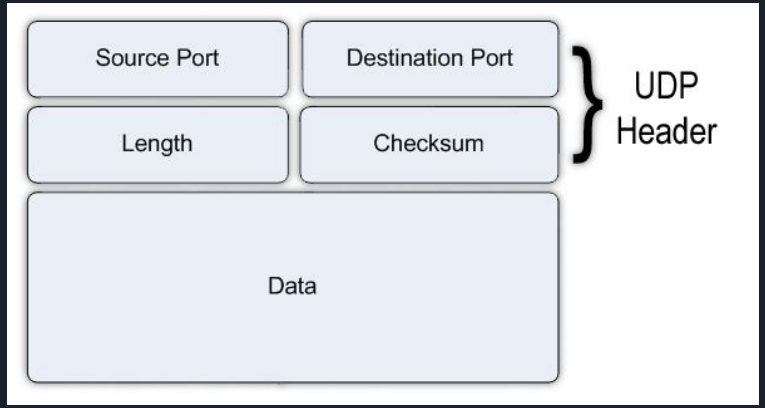
- Lower layer
  - Wired ethernet
  - Wireless LAN
- Network
  - IPv4
  - 192.168.1.100
- ***Transport***
  - ***UDP***
  - ***TCP***
- Application
  - Software you build on top of the network




Want to hear a funny UDP joke?
Um, okay?
You may not get it, and I really won't care.
.....
www.NeweggBusiness.com
Design: Dana Choi

UDP - RFC 768

- User Datagram Protocol
- Ports are 0 - 65535
  - 0 - 1024 are well known ports
  - Ephemeral = i don't care which one
  - Destination is the important one
- Length is: 8 - (depends ~65,507)
- Pros
  - No connection / overhead
  - Checksum for packet integrity
  - Fast
- Cons
  - You may drop packets
  - Packets may appear out-of-order

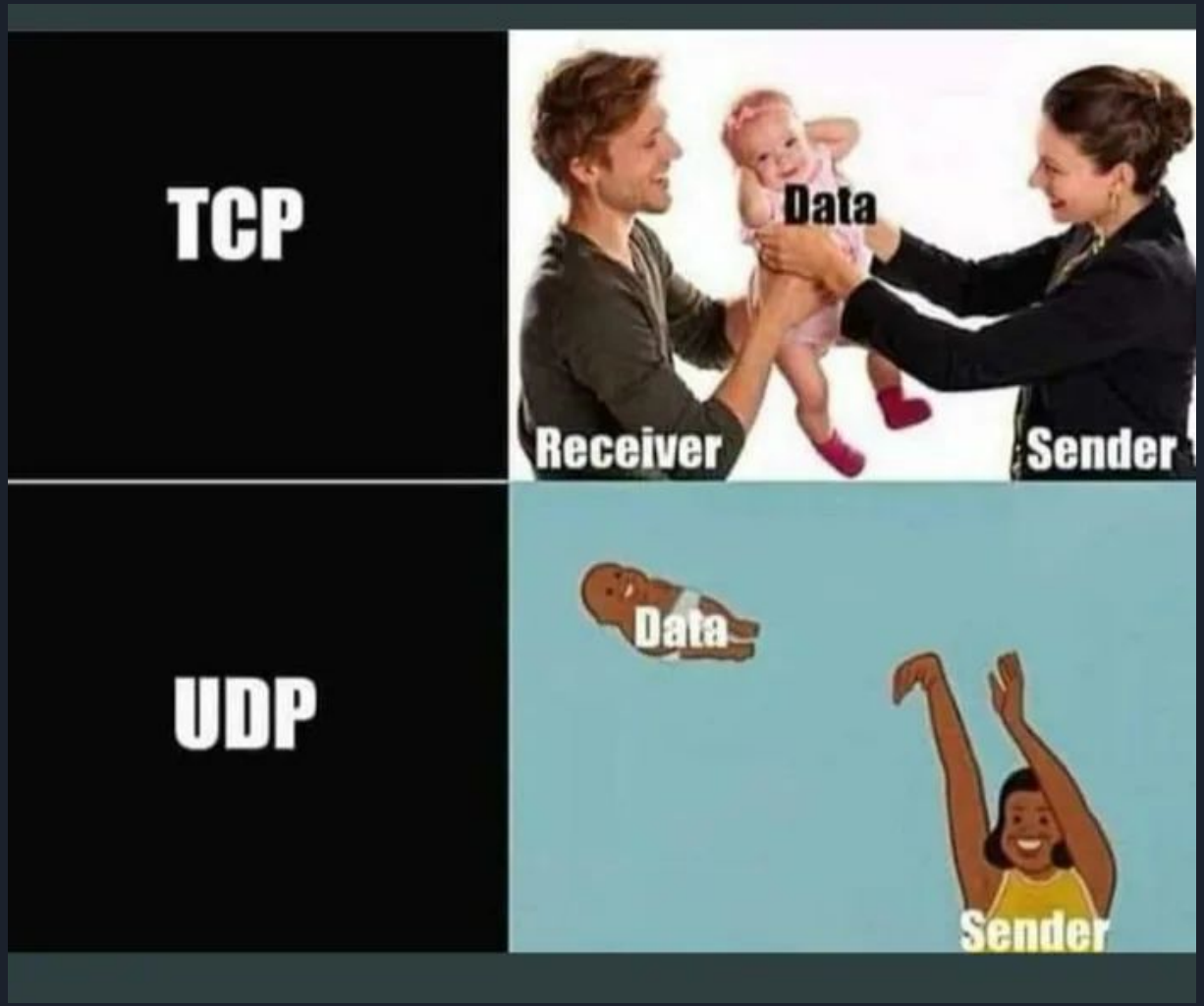


How to send and receive UDP

- Netcat / Shell
  - Send:
    `echo “hello” | nc -u server.com port`
  - Receive:
    `nc -l -k -u port`
- Python

```
print("UDP target IP:", destIp)
print("UDP target port:", destPort)
print("message:", message)

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) # UDP
sock.sendto(bytes(message, "utf-8"), (destIp, destPort))
```

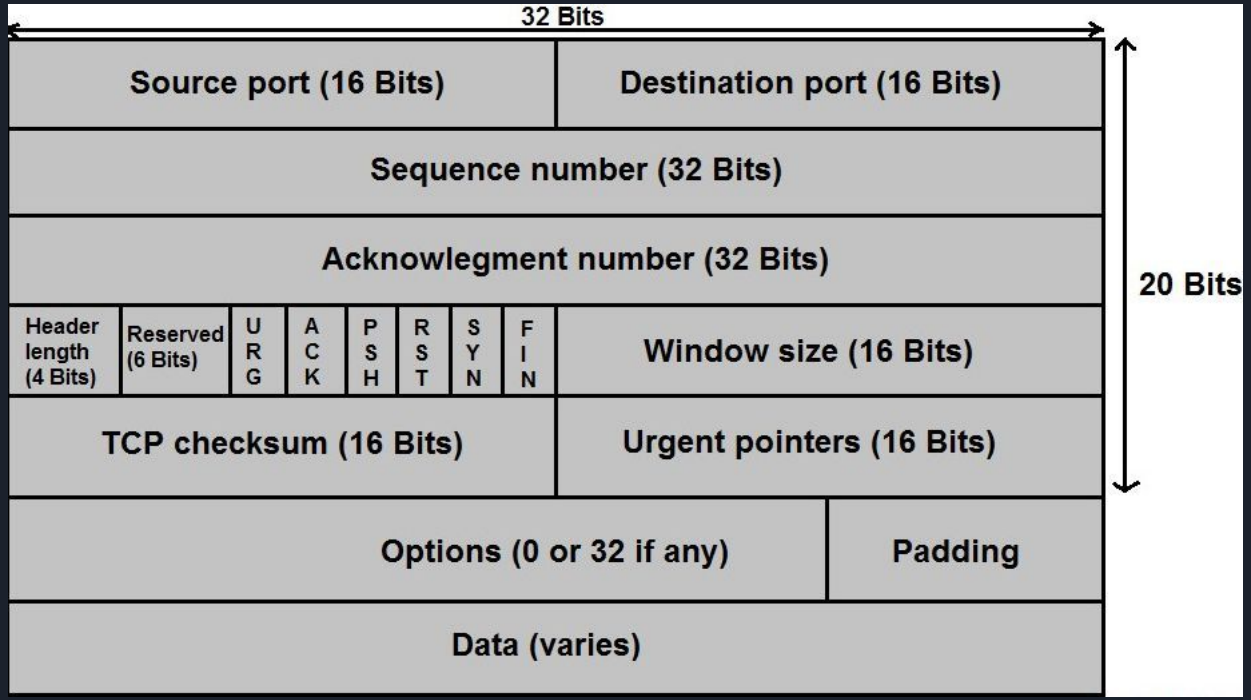

TCP
Data
Receiver
Sender
UDP
Data
Sender

TCP - RFC ~~793 -> 879 -> 2873~~ ... -> 9293

Packets Ordered ->

Retry on failure ->

Flow control ->



Where is the Size?

How to send and receive TCP

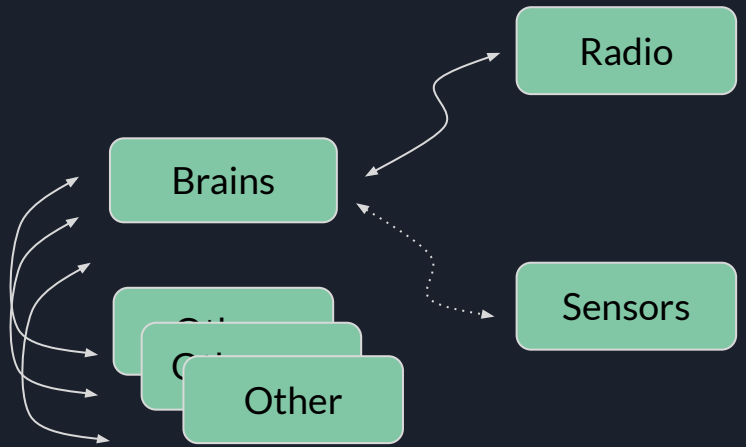
- Netcat / Shell
  - Send:
    ```
    echo “hello” | nc server.com port
    ```
  - Receive:
    ```
    nc -l -k port
    ```
- Python

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM) # TCP
sock.connect( (destIp, destPort) )
sock.sendall(bytes(message, "utf-8"))
sock.close()
```

Demo / Wireshark

- Captured pcap
  - Sudo tcpdump -i eth0 -w test.pcap
  - Can open later in WireShark
- Wireshark Filters
  - ip.proto == udp
  - Ip.proto == tcp
  - tcp.port == 1234
  - Right click, follow xyz stream
- **`tshark`** - wireshark for the CLI

War Story



- Brains computer ran out of communication ports
- “We can just switch between 2 of the minion computers”

1. Brains gets status from Radio
2. Radio sends back status
3. Brains unplugs radio, plugs in sensor
4. Brains TCP/IP stack sends ACK for Radio to Sensors
5. … FAIL

Additional Concerns

- So which one?
  - Speed = UDP (voice and video transmission, game data)
  - Allowed to be slow / retry = TCP (web, file transfer)
  - Some applications USE BOTH!
- Security
  - Hubs vs Switches
  - Wi-fi
  - SSL Sockets
  - VPN
  - SSH Tunnels

Internet Noise...

```
Sending a really really really long long long mesage 99, gosh, seems like it will never end.  then sleeping 0 ms aaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaa
Done
U%V}u9V'~11 /0+,
/5
8


GET / HTTP/1.1
Host: 64.227.11.12
Accept: */*
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 zgrab/0.x

uqQ]"qZ4f~T4QjUI%gt/+
/5
.


^C
user@wildcat-practice-ctf:~/scratch/TCP_Simple_Demo$
```

Attributions

- https://www.theverge.com/2019/3/28/18286027/microsoft-nintendo-vtech-security-hack-breach-researcher-guilty
- https://www.nknews.org/2015/01/hacker-claims-to-have-cracked-north-koreas-intranet/
- Code snippets from stackoverflow