Scapy

Bo Li

What is Scapy

- **Scapy** is a packet manipulation tool for computer networks.

- forge or decode packets, send them on the wire, capture them, and match requests and replies

- Handle tasks

    - scanning, tracerouting, probing, unit tests, attacks, and network discovery.

Introduction of Python

- This is an **int** (signed, 32bits) : `42`
- This is a **long** (signed, infinite): `42L`
- This is a **str** : `"bell\x07\n"` or `'bell\x07\n'` (" $\Longleftrightarrow$ ')
- This is a **tuple** (immutable): `(1,4,"42")`
- This is a **list** (mutable): `[4,2,"1"]`
- This is a **dict** (mutable): `{ "one":1 , "two":2 }`

http://www.secdev.org/conf/scapy_csw05.pdf

Introduction of Python

No block delimiters. Indentation **does** matter.

```
if cond1:
    instr
    instr
elif cond2:
    instr
else:
    instr
```

```
while cond:
    instr
    instr
```

```
try:
    instr
except exception:
    instr
else:
    instr
```

```
def fact(x):
    if x == 0:
        return 1
    else:
        return x*fact(x-1)
```

```
for var in set:
    instr
```

```
lambda x,y: x+y
```

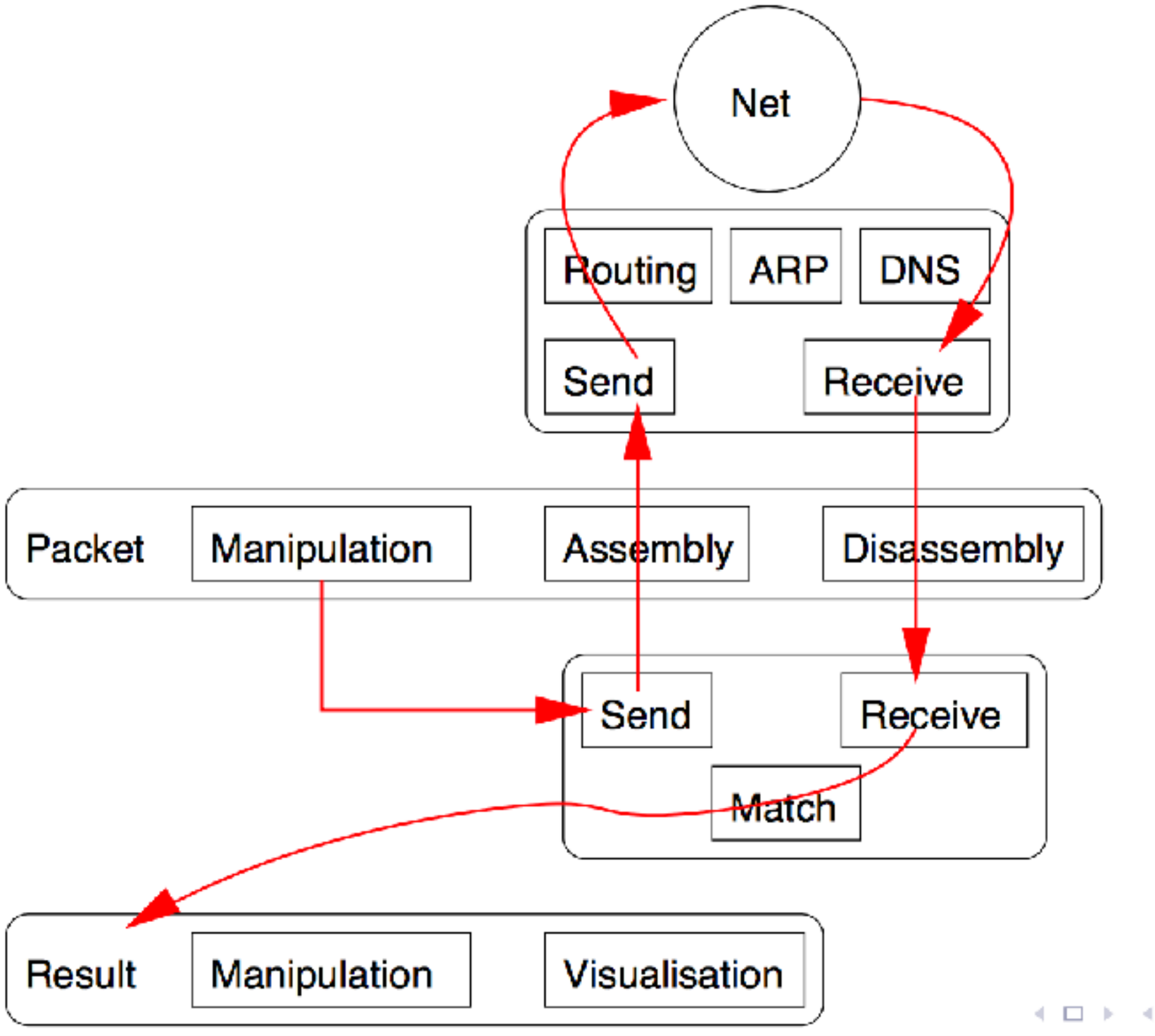
EADS CCR

http://www.secdev.org/conf/scapy_csw05.pdf

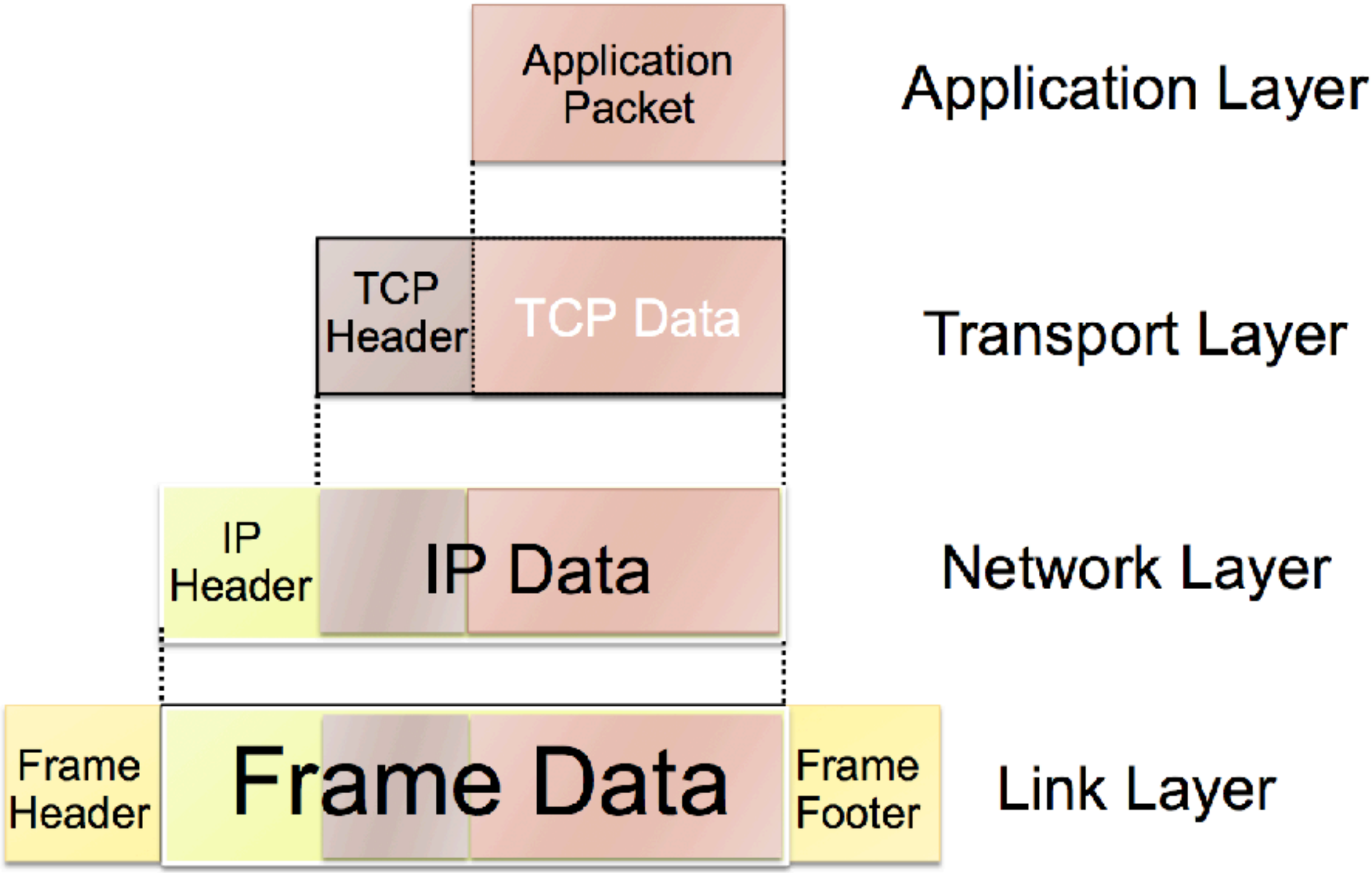
Recap of Last Class

- server_address = ('localhost', 10001)
- **sock.connect(server_address)**
- try:
- …
- while True:
- **data = sock.recv(4096)**
- …
- finally:
- **sock.close()**

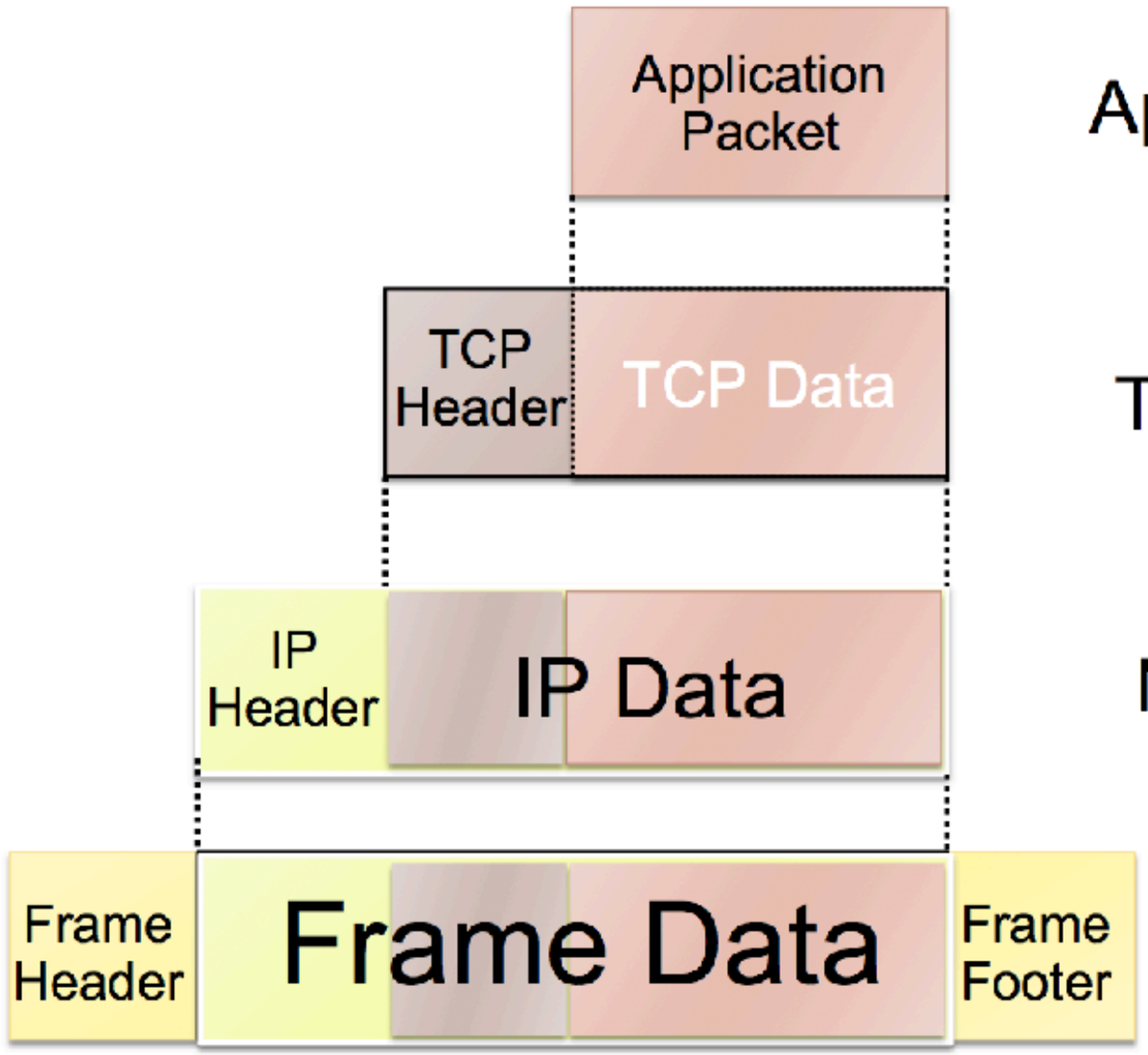
Scapy


Net
Routing
ARP
DNS
Send
Receive
Packet
Manipulation
Assembly
Disassembly
Send
Receive
Match
Result
Manipulation
Visualisation

Network Layer



Layers scapy works on



Application Layer `"GET / HTTP/1.0\r\n\r\n"`

/

Transport Layer `TCP(dport=80)`

/

Network Layer `IP(dst="127.0.0.1")`

/

Link Layer `Ether()`

Construct packet

- Combine different layers
  - default: system default
- Example:
  - a = Ether()/IP()/TCP()/“GET / HTTP/1.0**\r\n\r\n**"

Send and Receive

- Send only
  - send() — send package(s) at **Network** layer
  - sendp() — send package(s) at **Link** layer
- Send & receive
  - sr() — send and receive package(s) at **Network** layer
  - sr1() — send and receive **one** package at **Network** layer
  - srp() — send and receive package(s) at **Link** layer

Two ways of using Scapy

- Console
    - sudo scapy
- With in Python script
    - from scapy.all import *

Examples

- Get DNS request
  - a = sr1(IP(dst=“8.8.8.8")/UDP()/ DNS(rd=1,qd=DNSQR(qname="www.google.com")))
- TCP ping
  - ans,unans=sr(IP(dst="192.168.1.*")/TCP(dport=80,flags="S"))
  - ans.summary(lambda(s,r) : r.sprintf("%IP.src% is alive"))
- More on:
  - http://www.secdev.org/projects/scapy/doc/usage.html#simple-one-liners

Any Questions?