IP Spoofing

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

IP Spoofing

IP Spoofing is to spoof the source IP address of an IP packet.

```
from scapy.all import *
# you can spoof the source address
print("Sending spoofed udp packets.....")
ip = IP(src="1.2.3.4", dst = "127.0.0.1")
udp = UDP(sport = 8888, dport=9999)
data = "TTTTTTT\n"
pkt = ip/udp/data
pkt.show()
send(pkt)
```

IP Spoofing

The IP packet with a spoofed source IP address will still be routed to the destination IP address.

IP spoofing itself is not harmful. But it is used for other attacks

- SYN Flood Attacks
- DNS Cache Posioning Attacks
- TCP session Hijacking
- TCP RST attacks
- ...

Who Should Stop IP Spoofing?

Ideally routers since they are working on level 3. But not all of them stop IP spoofing.

- Performance Overhead
  - `check(dst_ip)` is now `check(src_ip) and check(dst_ip)`.
- They (especially those away from the edge) do not know the ground truth
  - Routings are very dynamic.

Preventations

Filtering at the edge of the network (i.e., gateways).

- *ingress filtering*: discard an incoming packet from an extneral network but with an internal source IP address.
- *egress filtering*: discard an outgoing packet from an internal network but with an external source IP address.