

Port scanning

~ confidentiality



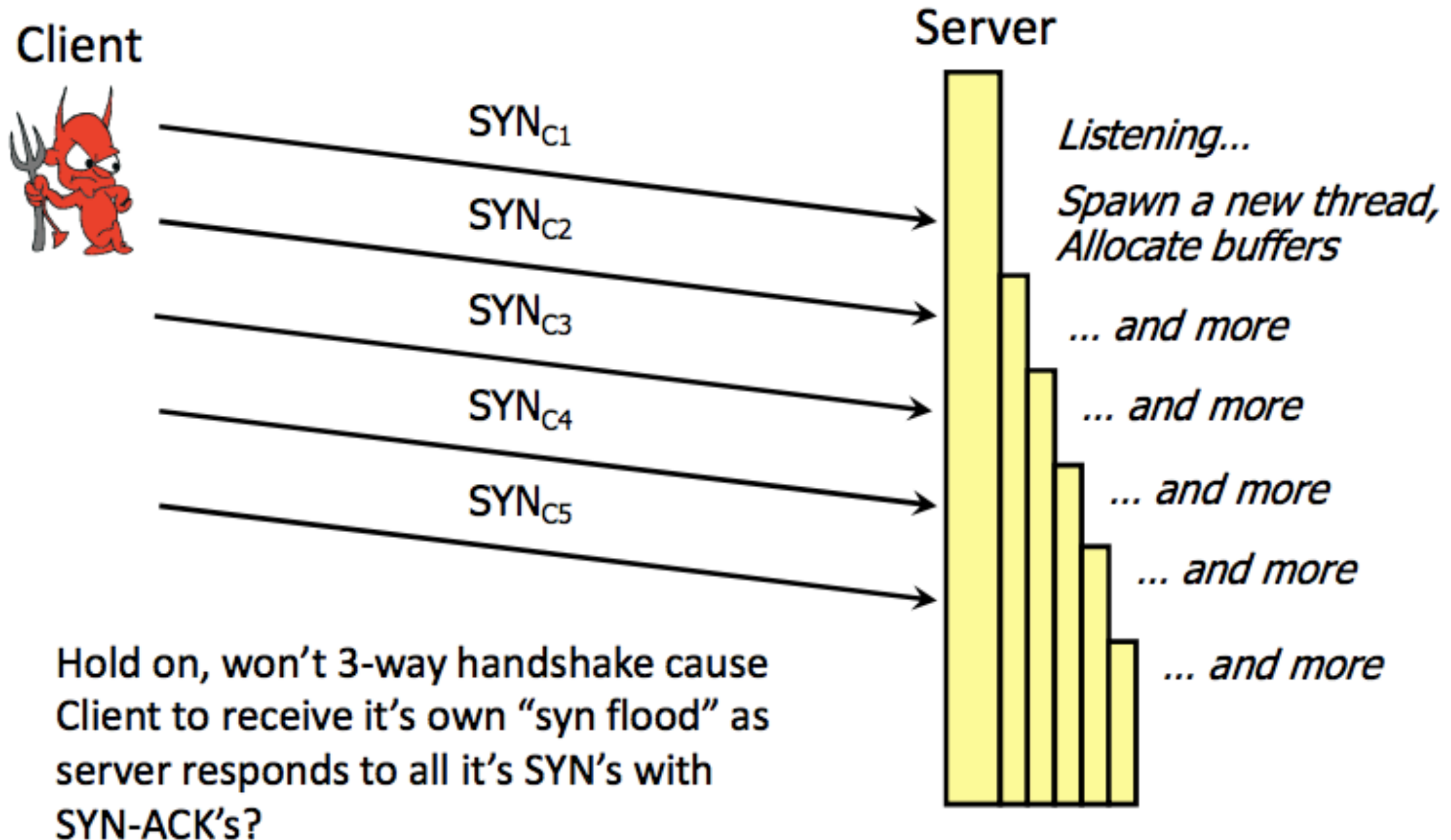
- ➔ Using the “3-way” handshake, an attacker can scan for all open ports for a given host

e.g. `nmap`

```
... 549.4... 192.168.2... 192.168.2... TCP 66 51467 → 8001 [SYN] Seq=0 Win=64240 Len=0 MSS=...  
... 549.4... 192.168.2... 192.168.2... TCP 54 8001 → 51467 [RST, ACK] Seq=1 Ack=1 Win=0 Len=...
```

TCP-syn flooding

availability



Note asymmetric effort between attacker client and victim server