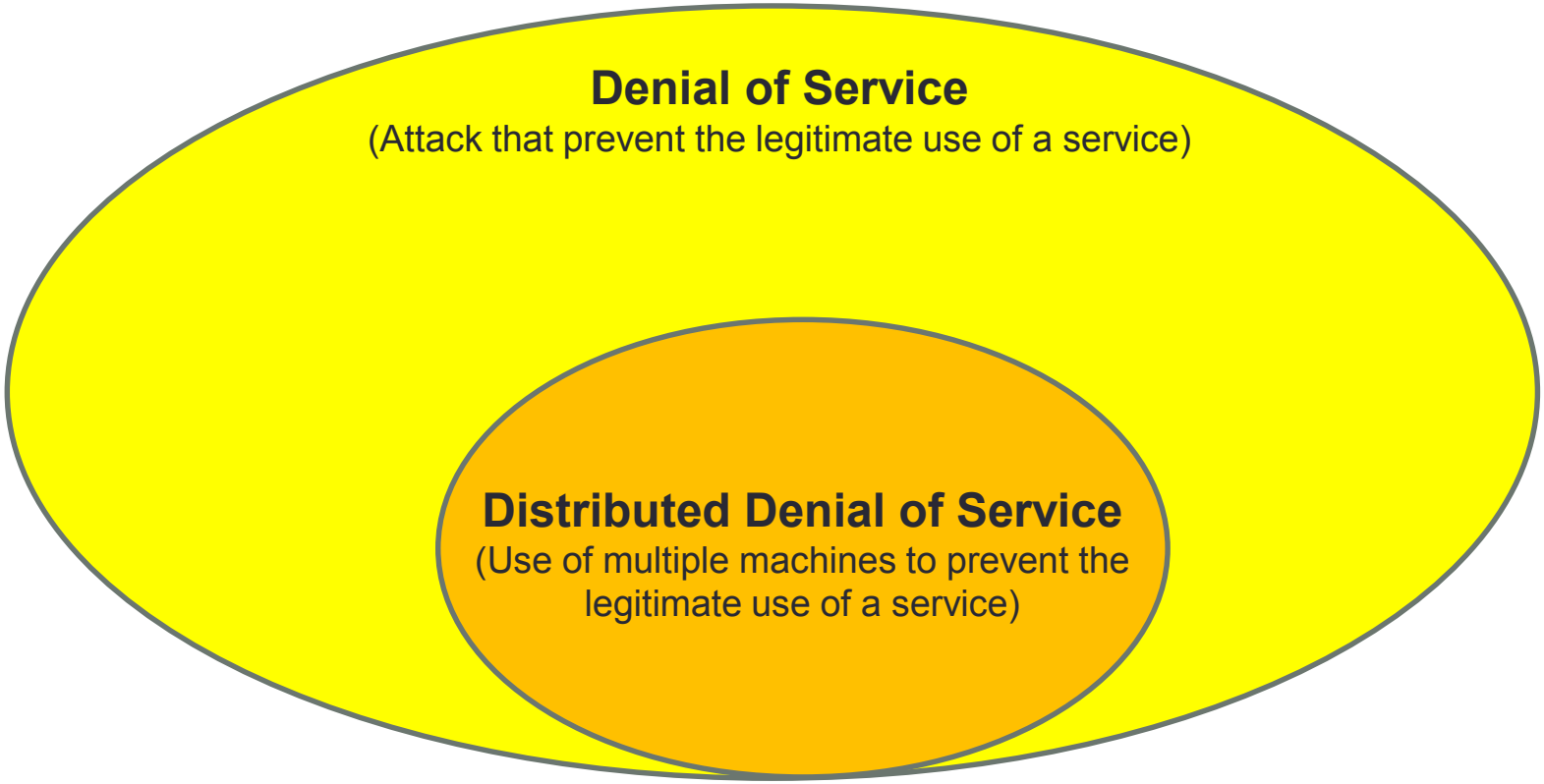
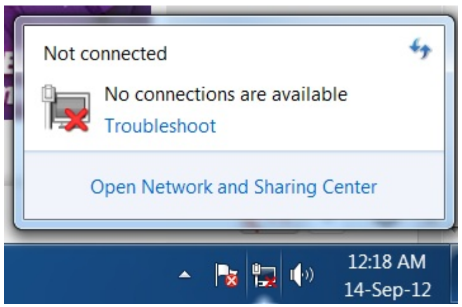
NETWORK SECURITY PRACTICES – ATTACK AND DEFENSE

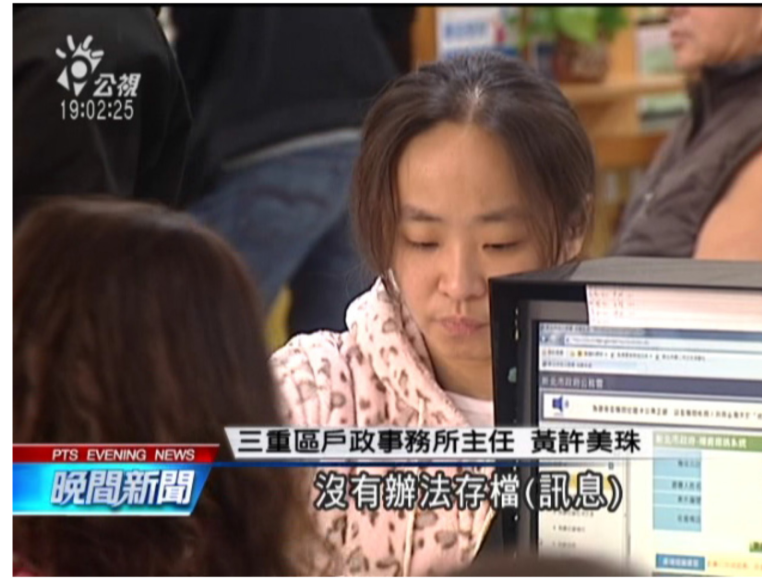
(Distributed) Denial of Service

Overview

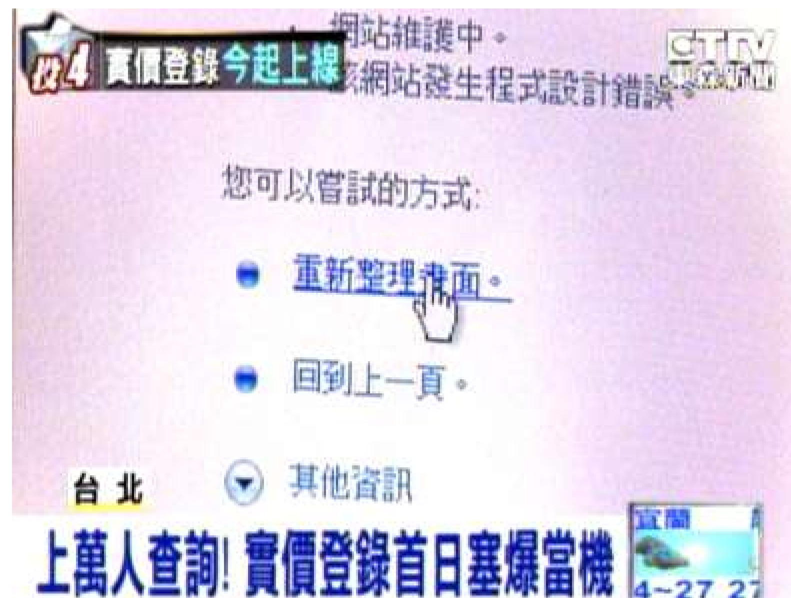

Denial of Service
(Attack that prevent the legitimate use of a service)
Distributed Denial of Service
(Use of multiple machines to prevent the legitimate use of a service)

Overview

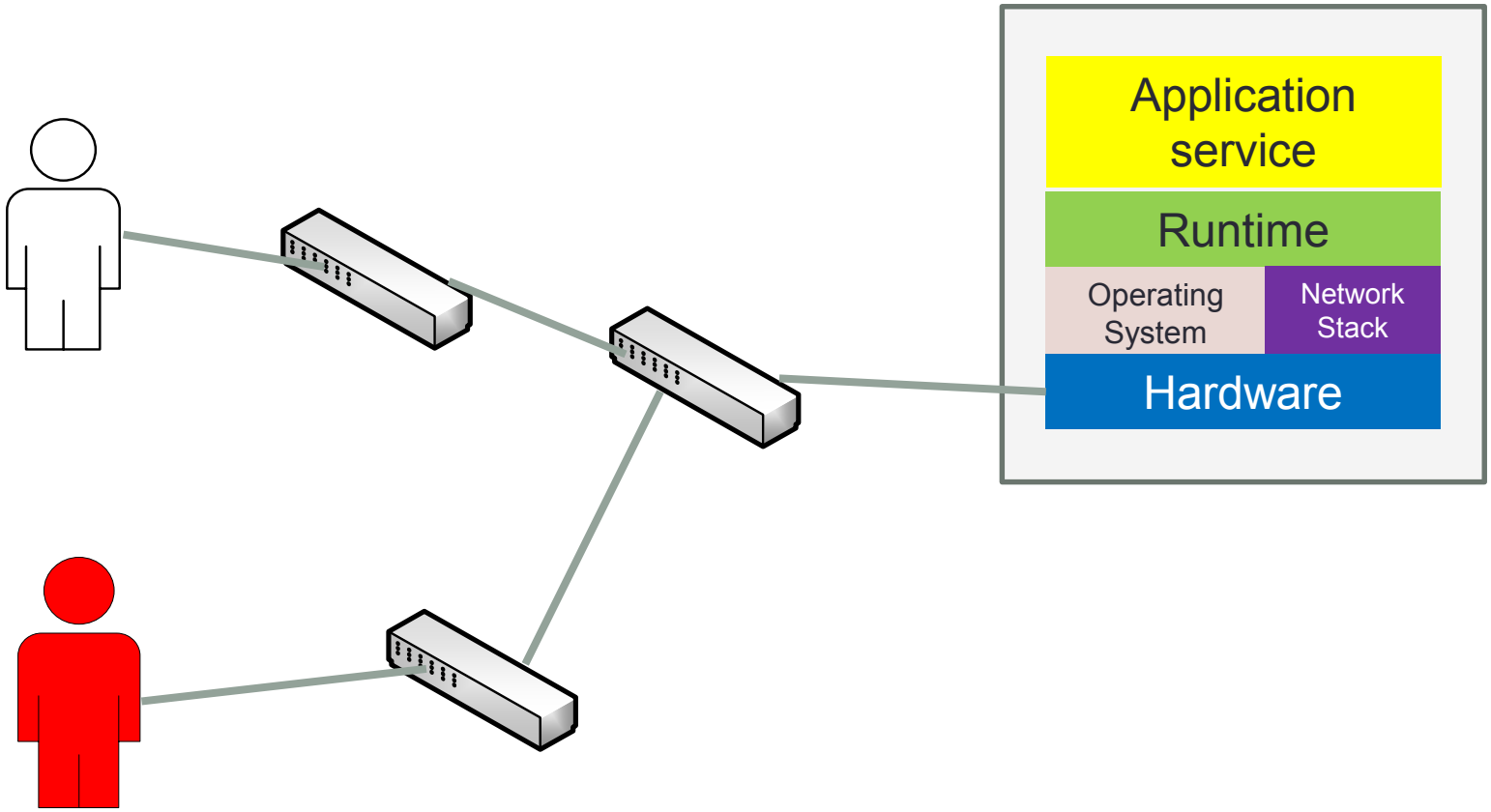

Not connected
No connections are available
Troubleshoot
Open Network and Sharing Center
12:18 AM
14-Sep-12


公視
19:02:25
PTS EVENING NEWS
晚間新聞
三重區戶政事務所主任 黃許美珠
沒有辦法存檔(訊息)


LIVE
部山區易有局部的
台南縣
最新
高鐵訊號異常 平均每班次延40分
9:26
高雄氣爆
管線交會 中油曾順便檢測榮化管

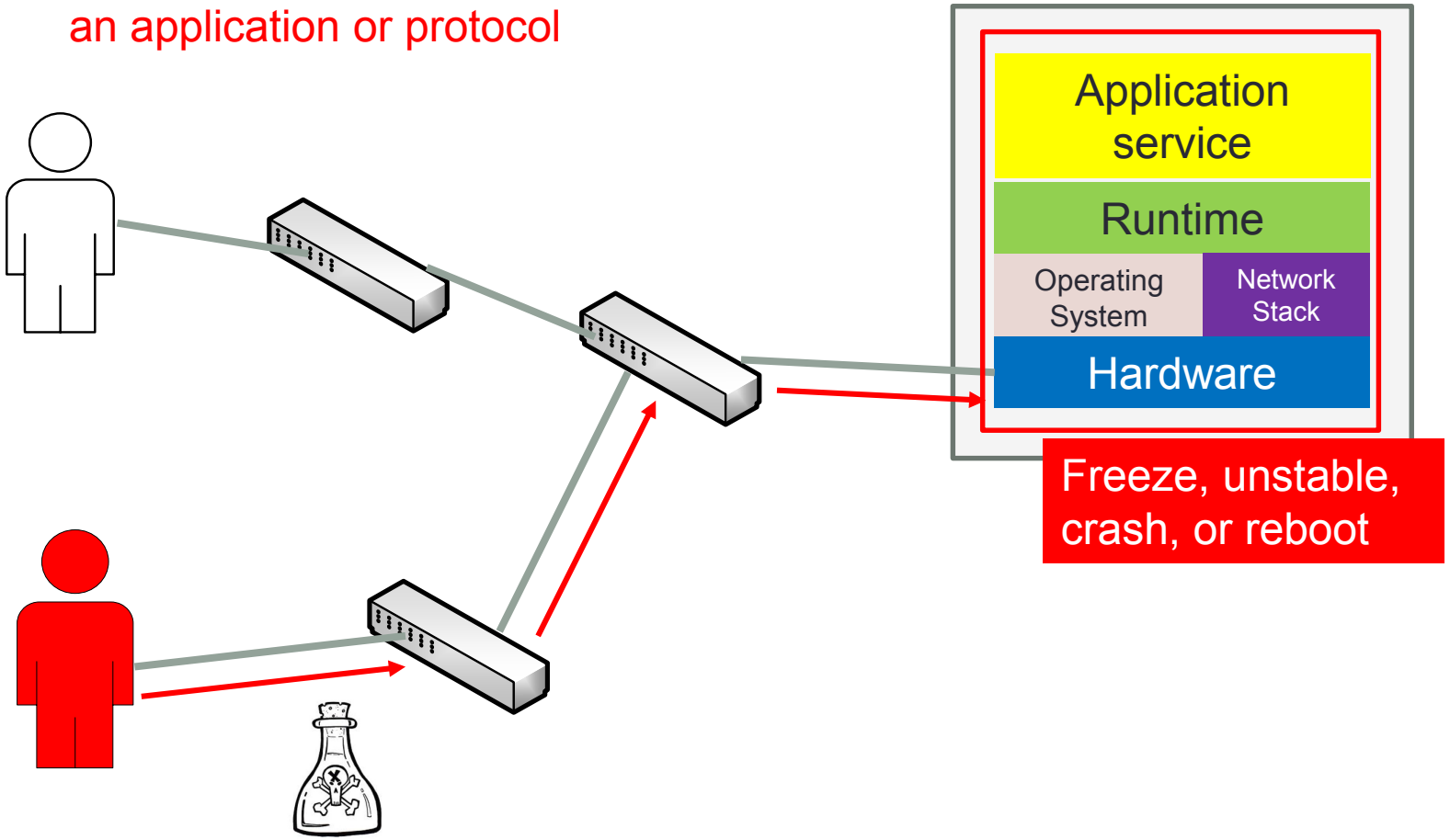

網站維護中。
實價登錄今起上線
您可以嘗試的方式:
重新整理畫面。
回到上一頁。
其他資訊
台 北
上萬人查詢! 實價登錄首日塞爆當機
宜蘭
4~27

DoS Attack


Application service
Runtime
Operating System
Network Stack
Hardware

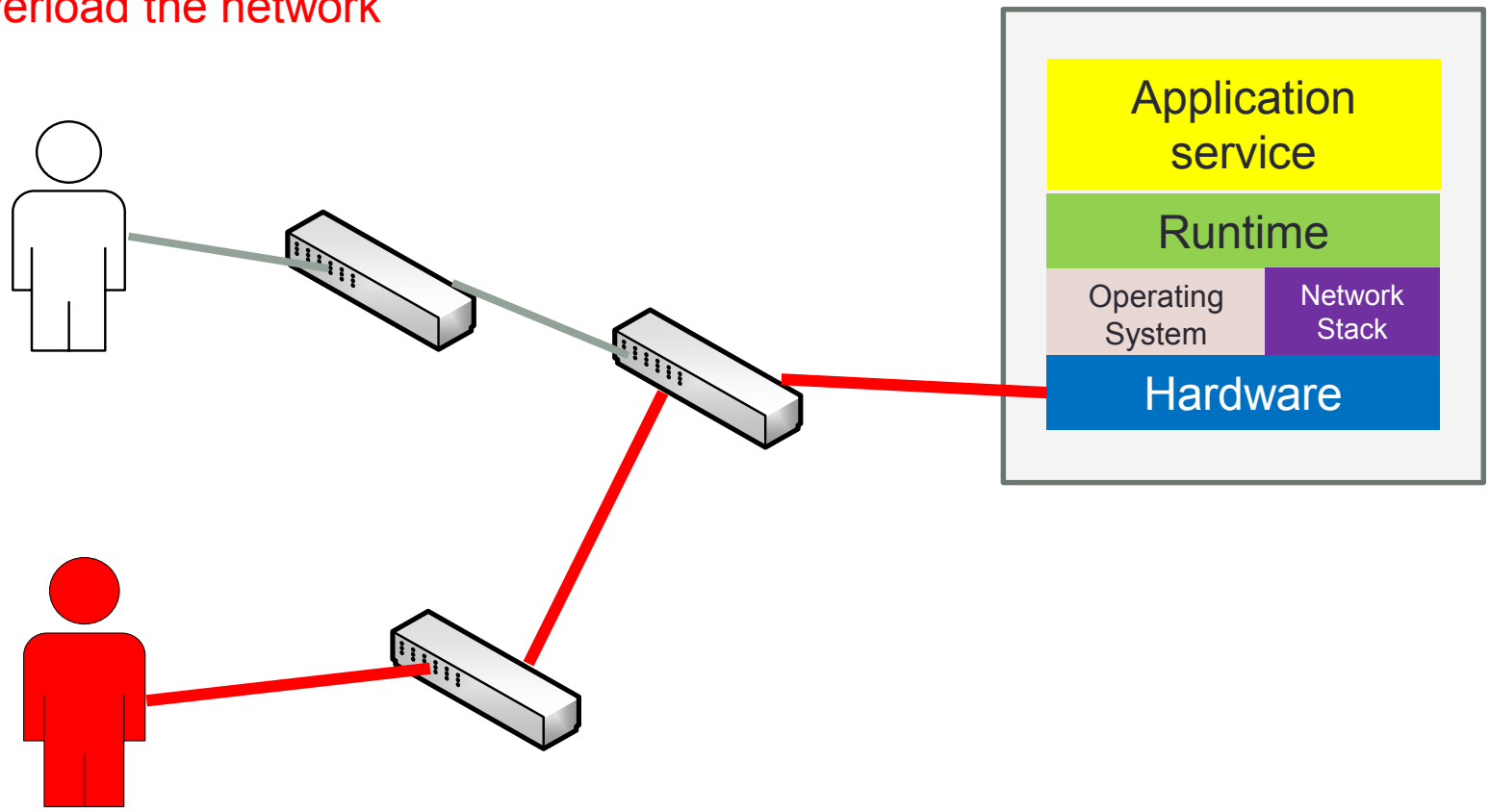
DoS Attack

Malformed request consuming an application or protocol



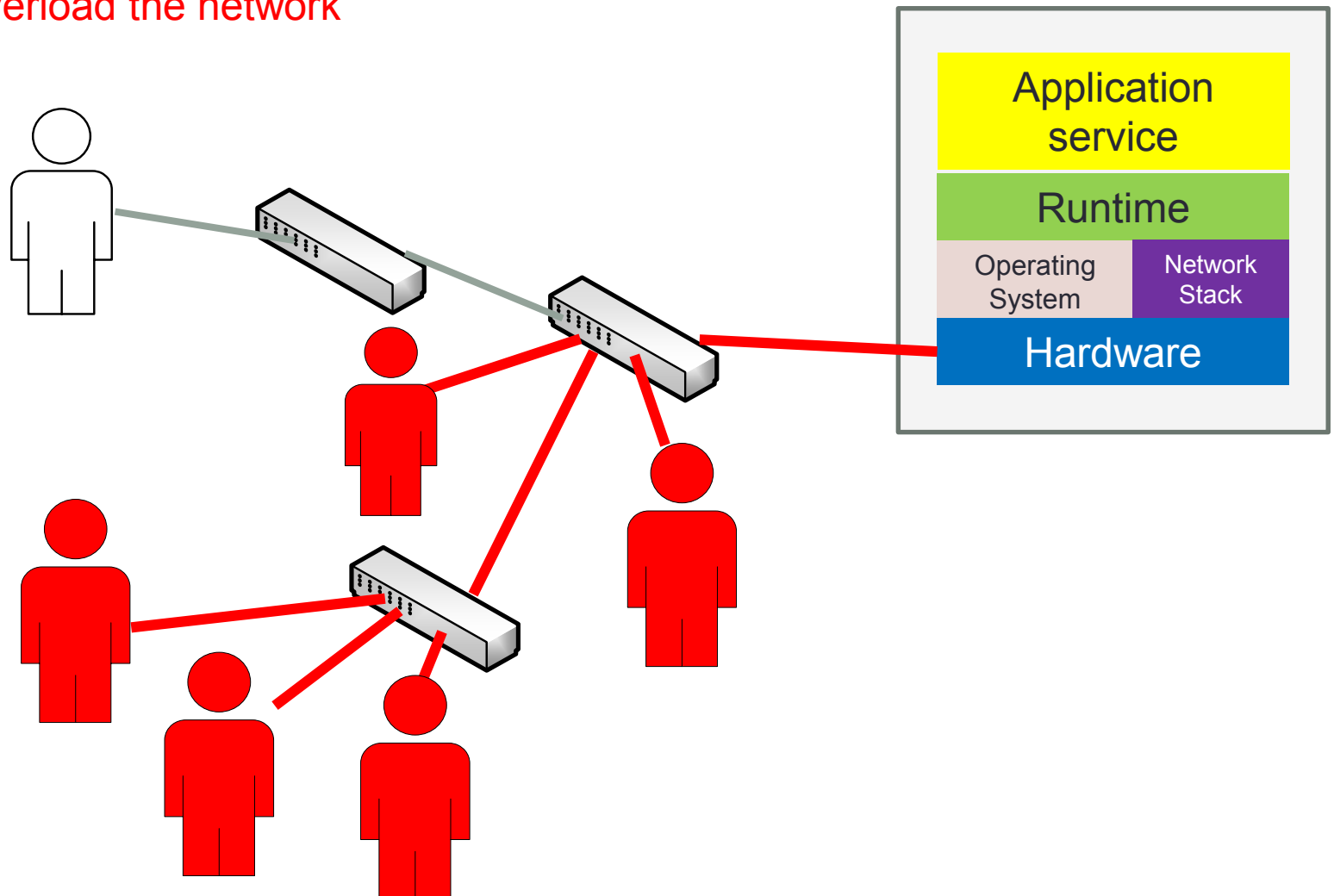
DoS Attack

Overload the network

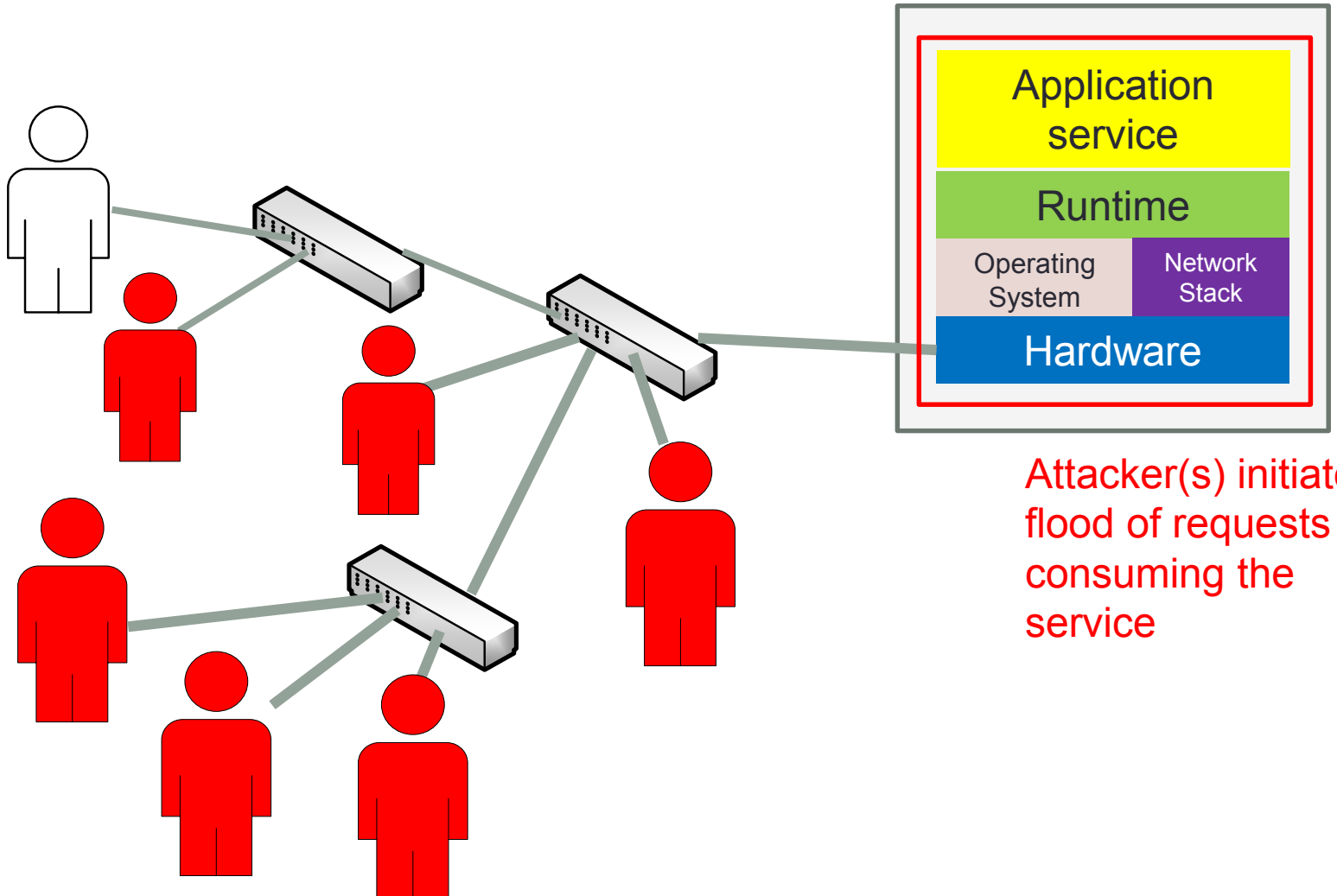


DDoS Attack

Overload the network

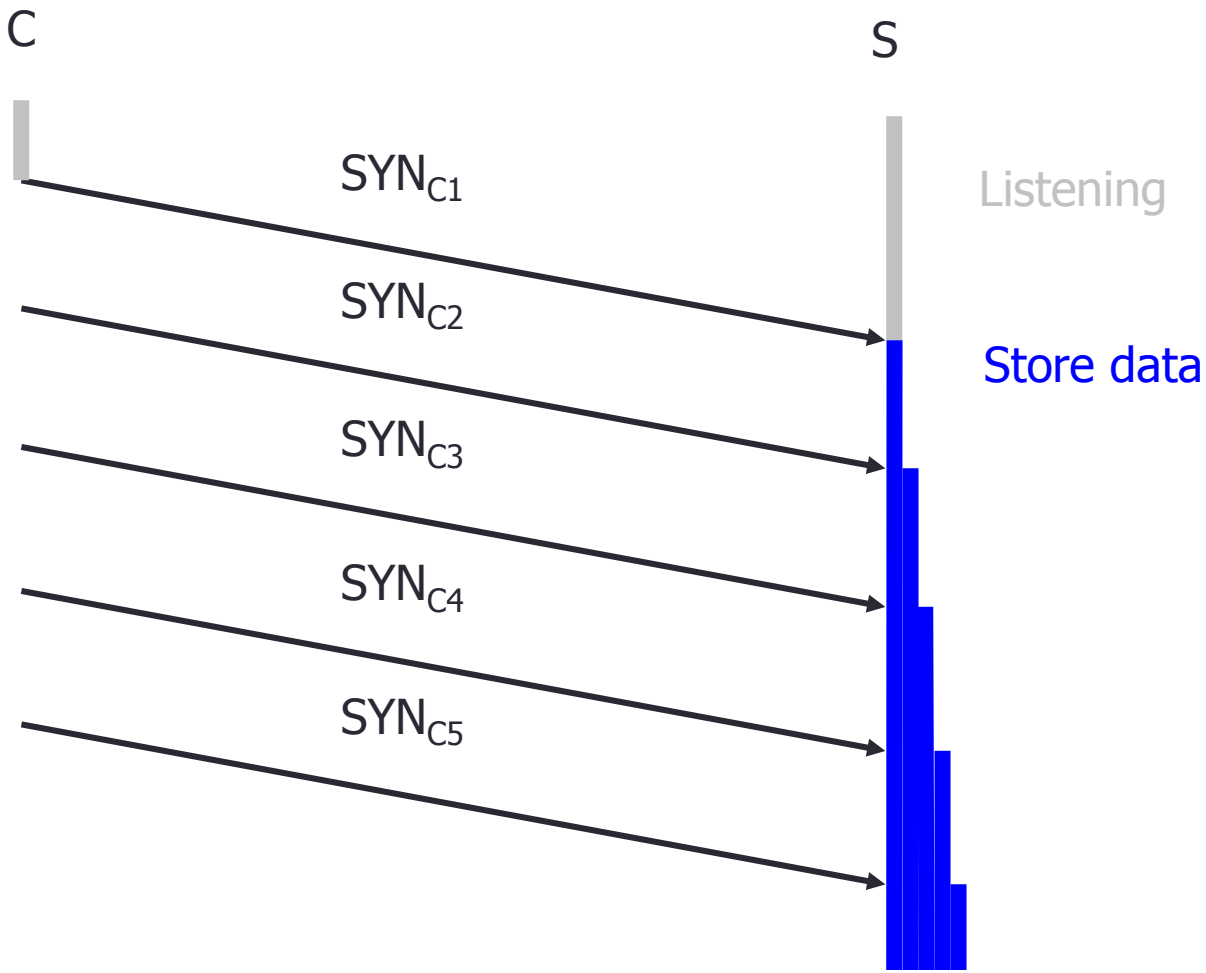


DDoS Attack



Attacker(s) initiate flood of requests consuming the service

TCP SYN Flooding

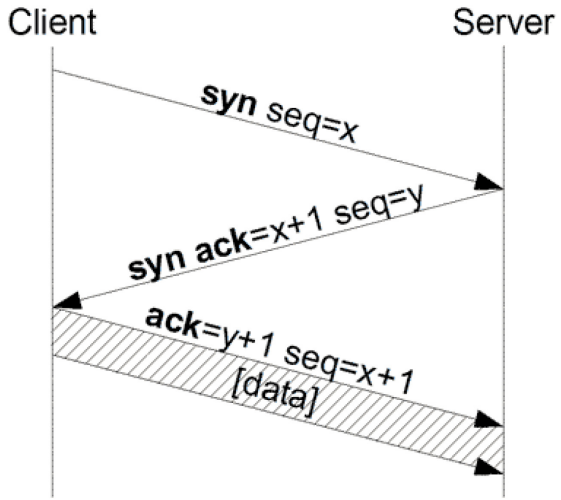


TCP SYN Flood

- Attacker sends many connection requests
  - Spoofed source addresses
- Victim allocates resources for each request
  - Connection requests exist until timeout
- Resources exhausted $\Rightarrow$ requests rejected
  - Asymmetric allocation of resources for the server and the client
  - Many implementations in 1996 for half-open connections queue is 8 entries long with expire time 3 minutes
- No more effective than other channel capacity-based attack today
  - SYN Cookies
  - Limiting new connections per source per timeframe is not a general solution

SYN Cookies

- After receiving SYN from client, server creates an entry in the SYN queue to record information such as maximum segment size (MSS) and other TCP options
- SYN Cookies: Encode the record in the initial *sequence number* (*seq*) of the SYN+ACK packet. Discard the entry.
  - Make it the client's responsibility to keep the record
- The client replies with ACK (*seq+1*). The server deduces the MSS from *seq*.



Why are DDoS attacks possible?

- Internet security is highly interdependent
  - Each host depends on the state of security in the rest of global Internet
- Internet resources are limited
  - Not enough resources to match the number of users
- Resources are not collocated
  - End networks only have small amount of bandwidth compared to abundant resources of network

Why are DDoS attacks possible?

- Accountability is not enforced
  - Source address spoofing
- Control is distributed
  - Networks run according to local policy
  - Difficulties in investigating cross-network traffic behavior

DDoS Attack Phases

- Recruiting
  - multiple agents (slaves, zombies) machines
- Exploiting
  - utilize discovered vulnerability
- Infecting
  - plant attack code
- Using
  - send attack packets via agents

DDoS Attacks

- Amplifier
  - NTP
    - http://openntpproject.org/
  - DNS
    - http://openresolverproject.org/
  - Chargen
  - SNMP
- Reflector
  - echo

NTP

- Network Time Protocol
  - Used to synchronize clock over the network
  - NTP daemon (ntpd)
  - Over UDP on Port 123
- Use *monlist* command to ask a remote ntp server to return a list of the last 600 hosts who have connected to that server

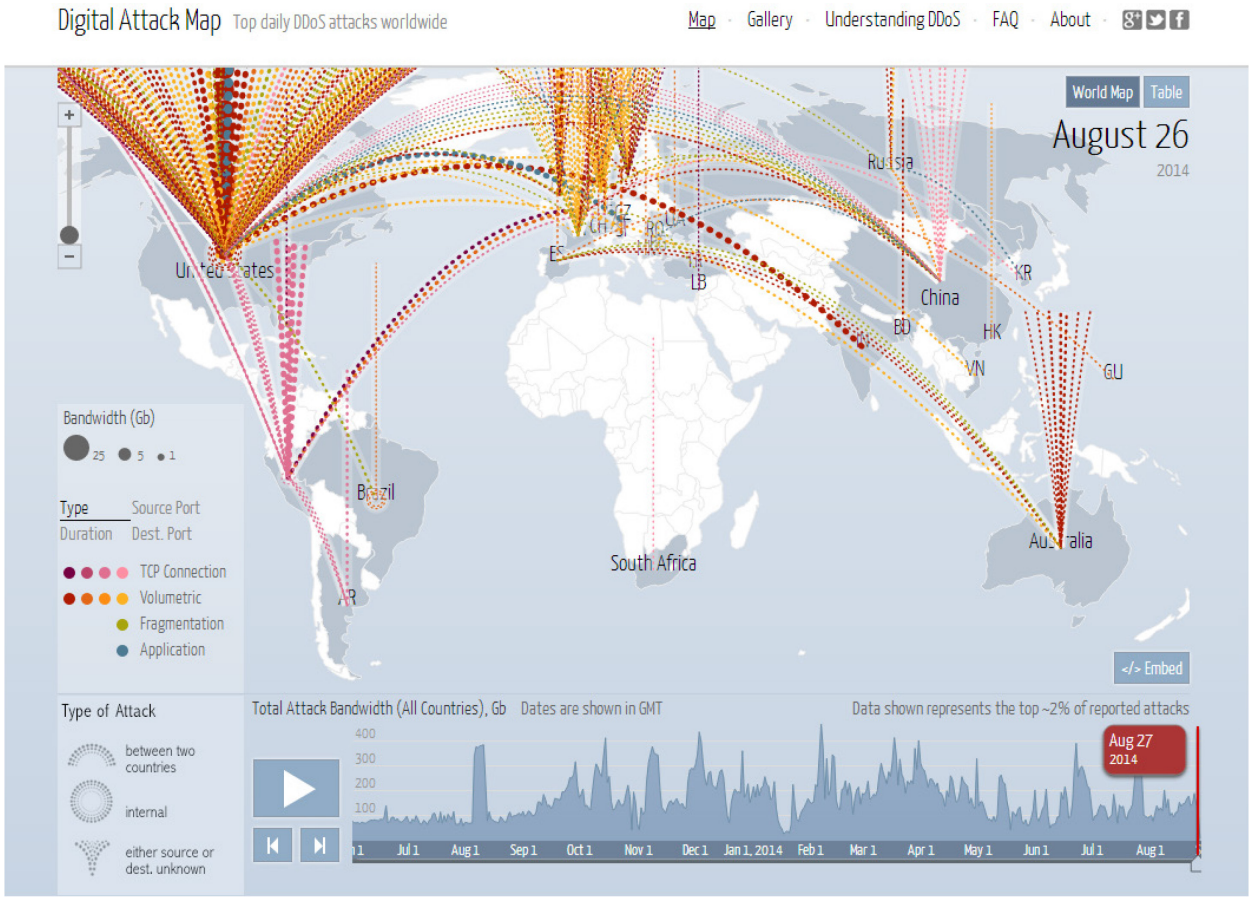
```
[root@sense ~]# ntpdc -n -c monlist 127.0.0.1
remote address          port local address      count m ver code avgint  lstint
===============================================================================
127.0.0.1              41301 127.0.0.1              1 7 2      0       0        0
220.135.58.124           123 140.113.88.151      2133 4 4    1c0    1024      656
118.163.81.61            123 140.113.88.151      2147 4 4    5d0    1024      750
[root@sense ~]#
```

DNS

- Domain Name Server
  - Hierarchical distributed naming service
- A DNS can play two roles
  - Authoritative server
    - Provide information of zones (≈domains)
  - Recursive resolver
    - Serve as a cache between *authoritative servers* and *stub resolver* (the client)

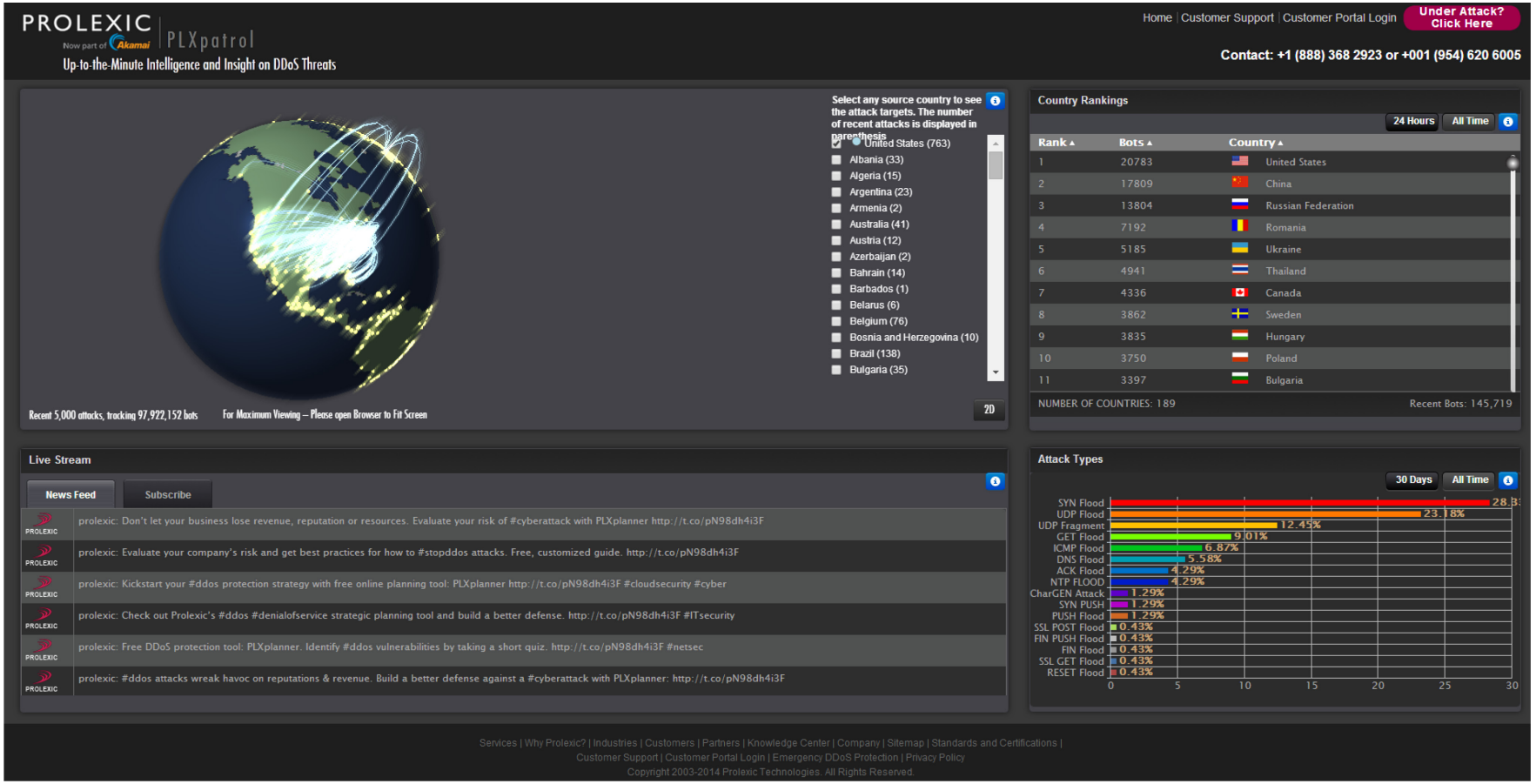
DDoS Attack Defense

- http://www.digitalattackmap.com/



DDoS Attack Defense

- http://www.prolexic.com/plxpatrol/



DDoS Attack Defense

- Patch vulnerable servers
- Ingress / egress filter / BCP38
  - Drop packets with spoofed / illegitimate source address
  - Can be evaded via reflection
- Restrict traffic amplification
  - Unicast Reverse Path Forwarding (RFC 2827)
    - Ensures that a packet must be received on the interface that the router would use to forward the return packet
    - In practice ISPs have multiple upstream transit connections and it's not unusual for a packet to return to the source address through a different ingress interface
  - …

DDoS Defense Challenges

- Distributed response needed at many points on Internet
  - Attacks target more than one host
  - Wide deployment of any defense system cannot be enforce because Internet is administered in a distributed manner
- Economic and social factors
  - Distributed response system must be deployed by parties that do not suffer direct damage from DDoS attacks
  - Many good distributed solutions will achieve only sparse deployment

DDoS Defense Challenges

- Lack of detailed attack information
  - Attacks are only reported to government
    (it is believed making this knowledge public damages the business reputation of the victim network)
- Lack of defense system benchmarks
  - Currently no benchmark suite of attack scenarios that would enable comparison between defense systems
- Difficulty of large-scale testing
  - Defenses need to be tested in a realistic environment
  - Lack of large-scale testbeds

Summary

- Route
  - Denial-of-service: bandwidth and latency
    - e.g. SYN Flood, Smurf
  - Tampering with route
    - E.g. ARP spoofing, man-in-the-middle, DNS poisoning, DoS,…
- Data
  - Packet headers and payloads
  - Confidentiality of data
    - E.g. Sniffing
  - Integrity of data
    - E.g. data forgery, replay, session hijacking, …
- Authentication and encryption → more states to maintain
  - Performance, reliability, and manageability

Spoofer Project: State of IP Spoofing

- http://spoofer.cmand.org/index.php

Summary:

Data Range: *Fri Feb 11 08:16:52 EST 2005 to Wed Sep 17 12:45:40 EDT 2014*
Total Tests: *22907*
Unique IPs tested: *18193*
Unique Routed Prefixes tested from: *9874*
Unique ASes tested from: *3099*