Security 11: Proxies and similar

i.g.batten@bham.ac.uk

Firewalls: Not Enough

- Firewalls restrict access to services (or, more accurately, to ports on which services run).

- Provide no checking of correct behaviour inside protocol.

- Provide no protection against tunnelling, variant ports, etc, etc.

- Can block access to external services, but not very well (I just run my VPN/ssh/etc server on port 80)

NAT: Not Enough

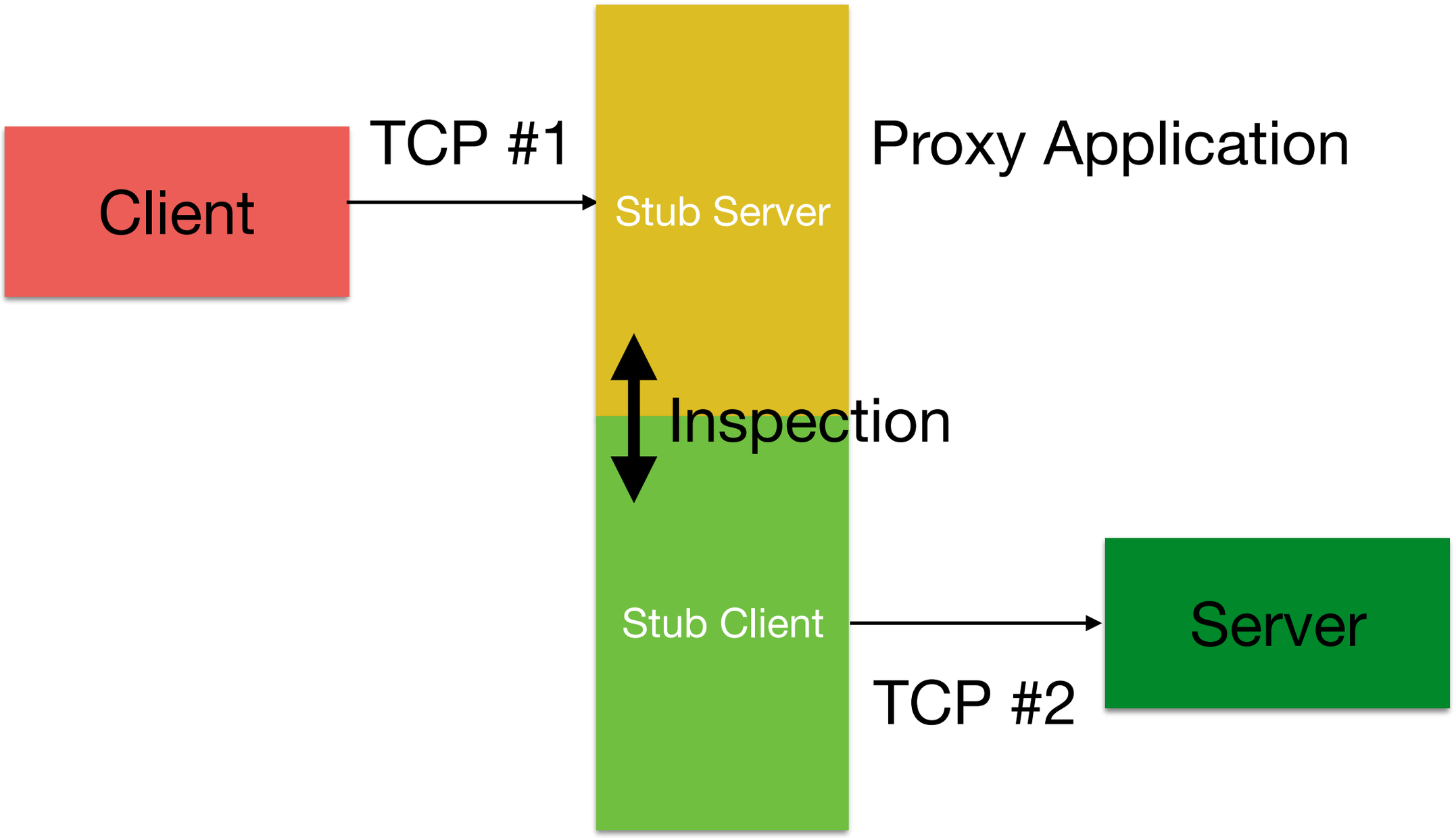
- Provides no outbound security at all
- Provides some inbound security
- No checks on protocol operation

Proxies

- Old technology: “fwtk” (confusingly, firewall toolkit) made available by TIS in 1993

- Extremely effective when used carefully

Basic Premise



Security Concept

- Stub server supports enough of the protocol to receive commands and check them for legality and plausibility (state, “usual size”, etc)
- Stub client supports enough of the protocol to send commands and receive responses
- Both are simple, clear, auditable code (you hope)
- Shields messy, attackable, complex, privileged origin server from attacker

SMTP exchange

```
igb986@cs.bham.ac.uk... Connecting to smart1.bham.ac.uk. via relay...
220 smart1.bham.ac.uk ESMTP Exim 4.82 Tue, 17 Feb 2015 14:21:15 +0000
>>> EHLO mail.batten.eu.org
250-smart1.bham.ac.uk Hello mail.batten.eu.org [147.188.192.250]
250-SIZE 104857600
250-8BITMIME
250-PIPELINING
250 HELP
>>> MAIL From:<igb@batten.eu.org> SIZE=128
250 OK
>>> RCPT To:<igb986@cs.bham.ac.uk>
>>> DATA
250 Accepted
354 Enter message, ending with "." on a line by itself
>>> .
250 OK id=1YNj1X-0000U8-G7
igb986@cs.bham.ac.uk... Sent (OK id=1YNj1X-0000U8-G7)
Closing connection to smart1.bham.ac.uk.
```

HTTP Exchange

```
wget -d -v http://www.batten.eu.org/~igb/fdsfasfs

Resolving www.batten.eu.org (www.batten.eu.org)... 2a00:7b80:3019:12::579c:4928, 128.204.195.144
Caching www.batten.eu.org => 2a00:7b80:3019:12::579c:4928 128.204.195.144
Connecting to www.batten.eu.org (www.batten.eu.org)|2a00:7b80:3019:12::579c:4928|:80... connected.
```

```
GET /~igb/fdsfasfs HTTP/1.1
User-Agent: Wget/1.14 (solaris2.11)
Accept: */*
Host: www.batten.eu.org
Connection: Keep-Alive
```

```
HTTP/1.1 404 Not Found
Server: nginx/1.0.15
Date: Tue, 17 Feb 2015 14:24:55 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
```

Vectors…

- Mail server looks up supplied hostname (in some cases) and supplied email addresses (eventually)

- If those somehow trigger buffer overruns or similar (there was such an attack recently) then the receiver's SMTP daemon can be taken over by attacker

- Similarly HTTP: reverse lookups of addresses, lookups of URLs, calls to namei(), possible shell processing for cgi-bin, etc, etc, etc.

In and Out

- Proxies can be used both inbound and outbound
- Inbound proxies cannot make assumptions about client knowing the proxy is there.
- Outbound proxies can use modified version of protocol, as clients can be configured to know.

Example: Web proxying

- Outbound web proxying is used in place of NAT.
- Client connects to proxy, passes URL, proxy fetches content, sends content back.
- Makes tunnelling **much** harder: tunnelled data must look like plausible HTTP.
- Proxy can do content filtering, virus scanning, logging, etc, etc.

Web Proxying

- 1995—2005, Web Proxying also offered **caching**.
- Repeated requests for same content served from cache to save bandwidth, improve performance.
- Benefits now very limited, most caching turned off by 2010.

Web Proxying

- With configuration, proxy is known to client.
- For use without configuration, outbound “transparent proxying” involves NAT-ing packets destined for outside to proxy, and delivering (somehow) the intended destination so proxy can make onward connection.
- Popular in mobile phone networks.

Encryption

- Web proxies struggle with encryption.
- Solution #1: “CONNECT” operation allows client to make arbitrary connection through proxy which is relayed, byte-for-byte.
- End to end encryption
- Breaks security model: useful for avoiding NAT, but not for secure environments.

Encryption

- Solution #2: Certificate Forgery
  - Proxy performs man in the middle attack by creating certificate on the fly for requested site, so proxy has access to plaintext.
  - Used for content filtering in schools, etc.

Inbound Proxies

- For HTTP, proxy can check for syntactically correct protocol and scan for obvious attacks, passing only sanitised requests to internal servers.

- Can also do basic access control in one place, when “origin servers” cannot be trusted to do it right.

- Proxy can also scan content for sensitive material (“Data Leakage Protection”)

Inbound Proxies

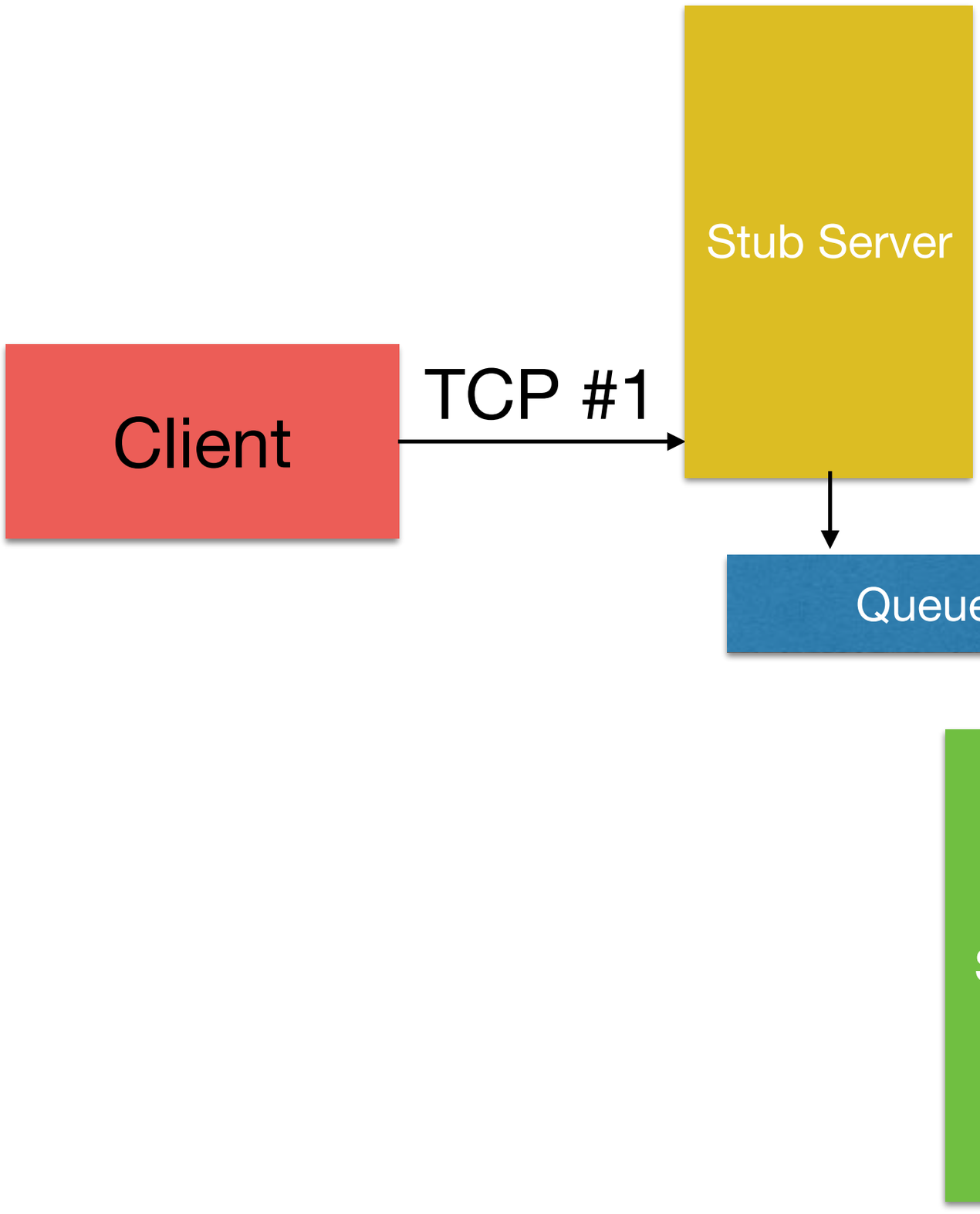
- Inbound proxy can also be used to unify namespace, so “www.my.dom.ain/some/URL” can be serviced on different machines for different URLs without exposing this fact to user.

Mail

- Young people use IM, Twitter, Snapchat, etc.
- Business and government functions with email.
- So email is the bare minimum needed

Mail Proxies

- Key point: mail is not real time
- Allows far more paranoid architecture



Stub server drops messages in queue, stub client fetches them and sends them to real server

Mail Gateways

- Any attack on internal server has to be embedded in messages
- But protocol is generated only by stub client
- Very hard to get chosen protocol operations through

Mail precautions

- Often stub server has no list of addresses, so will accept mail to any address. Errors are sent back asynchronously.

- But can check addresses for correct format, to avoid embedding of buffer overruns (etc) into addresses.

- Can limit number of addresses, rate, etc, etc.

Queue Precautions

- Queue can include virus scanning, etc.
- There are known attacks on virus scanners (for example, “compression bombs”)
- But scanner is not exposed to attacker, and has no path to either Internet or inside systems
- Bi-directional mail is usually done with two such set-ups, one in, out out.

Data Diodes

- “Outside, Queue, Inside” can be generalised
- “Data Diodes” are a popular concept in multi-level secure (protectively marked) environments.
- Usually custom built, but basic idea is same: bring data to staging area, then transmit onwards
- In extreme cases, can require physical re-wiring (accept for an hour, forward, repeat)

Voice

- Serious problem: voice is business critical and cannot be relayed with delay
- Has slowed adoption of voice over IP: keeping the voice in a completely separate infrastructure is attractive for security in buildings with existing cable plant.
  - And in 2017, who cares about fixed line telephony anyway?

Session Border Controllers

- Phone registers with central call server
- SBC keeps track of registrations
- Allows incoming signalling from call server, with protocol inspection proxy-style
- Allows incoming media stream once signalling is in correct state
- Also implements (for example) lawful intercept, codec translation, dealing with NAT…

VoIP Issues

- Of course, it's very difficult indeed to examine a stream of 8KHz, 8-bit samples and test to see if it is real voice or some other protocol being tunnelled.

- Hence very popular solution is to have VoIP on a separate VLAN, to keep traffic away from computers.

VoIP issues

- For historical reasons, operators of VoIP networks are often liable to perform intercept when equivalent scenarios within non-voice ISPs would be carried out by law enforcement at law enforcement's expense.

- VoIP networks also need good overload control and 999/911 prioritisation.

- So SBCs are specialised, and able to name their own price.

Ian’s Prediction

- VoIP as a customer proposition is dead, because it’s a replacement technology for analogue fixed line voice, which is also dead.
- Customers wanting fixed line voice may find it is handled with VoIP inside telco network, but it will be traditional POTS/ISDN to the customer.
- 4G voice is again VoIP inside telco network, but customer doesn’t see this.
- So need to bring voice through main Internet gateway will reduce, not grow.
- **I could well be wrong.**

Remember

- StuxNet was a suite of malware (probably) written by the US government, which targeted industrial controllers operating centrifuges.

- Centrifuges are the current best technology for separating fissile U235 from inert U238, to enrich Uranium either for nuclear power use or for weapons use.

- Stuxnet modified control programs to drive the centrifuges in an unstable way, to ruin their main bearings.

Stuxnet

- The equipment in question was air gapped from the outside world: the only route to the controllers was via “sneaker net”: USB memory sticks, floppy drives, software updates on flash.

- It was still possible to infect the controllers.

- Proxies and Data Diodes protect against some network attacks, but are not perfect.

Summary

- Proxies can protect against some outbound issues (DLP, downloading of viruses)
- Proxies hugely improve security on inbound services, especially when inbound servers are complex, privileged and old
- Data Diodes useful in classified environments
- Still can be bypassed by sufficiently resourceful attacker.