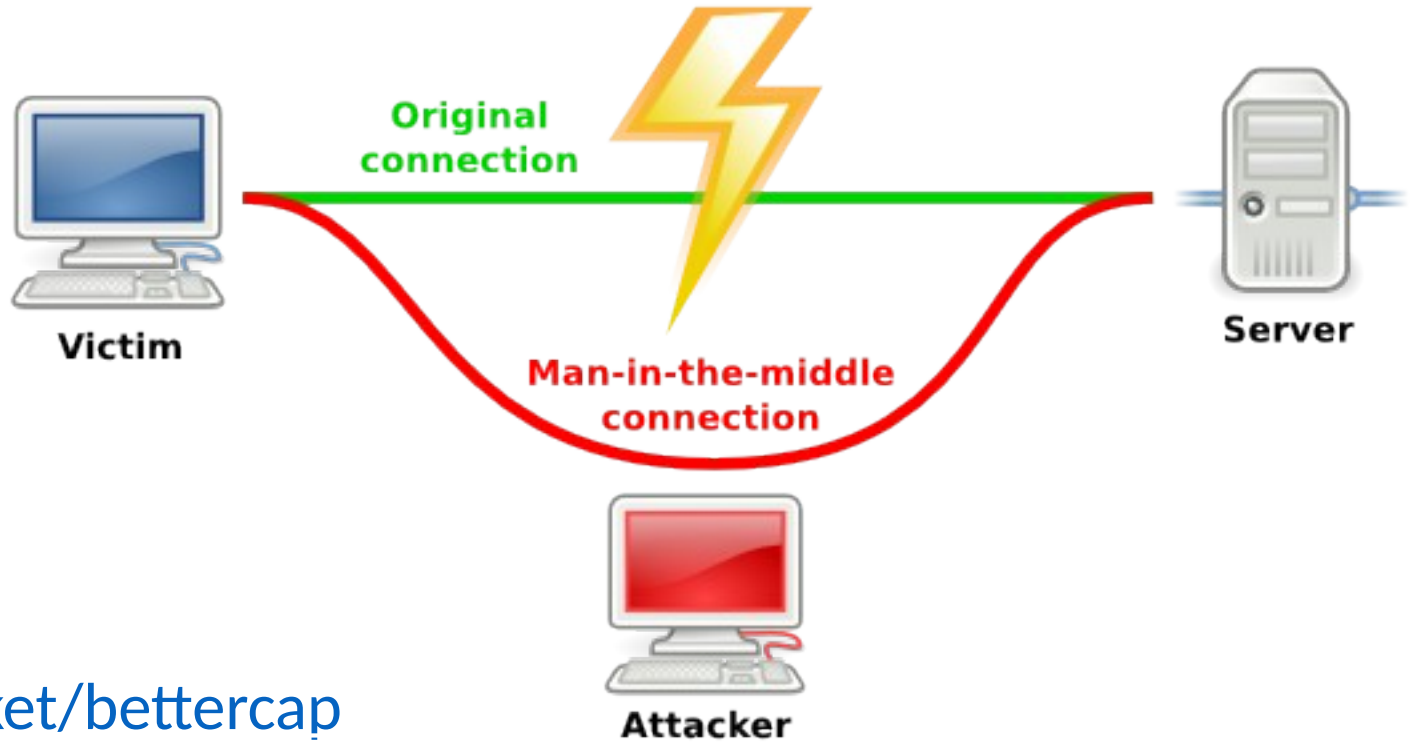
BetterCap
a MitM framework

Eva Sarafianou
April 2016

BetterCap

- A Man-in-the-Middle framework
- Written by Simone Margaritelli in Ruby
- Fully compatible with GNU/Linux,
- Mac OS X and OpenBSD platforms
- Modular - Easily extensible
- Site: www.bettercap.com
- Github: https://github.com/evilsocket/bettercap



BetterCap

We will:

- talk about:
  - ARP Spoofing
  - DNS Spoofing
  - SSLstrip & HSTS bypass
  - Code Injection

- run Demos

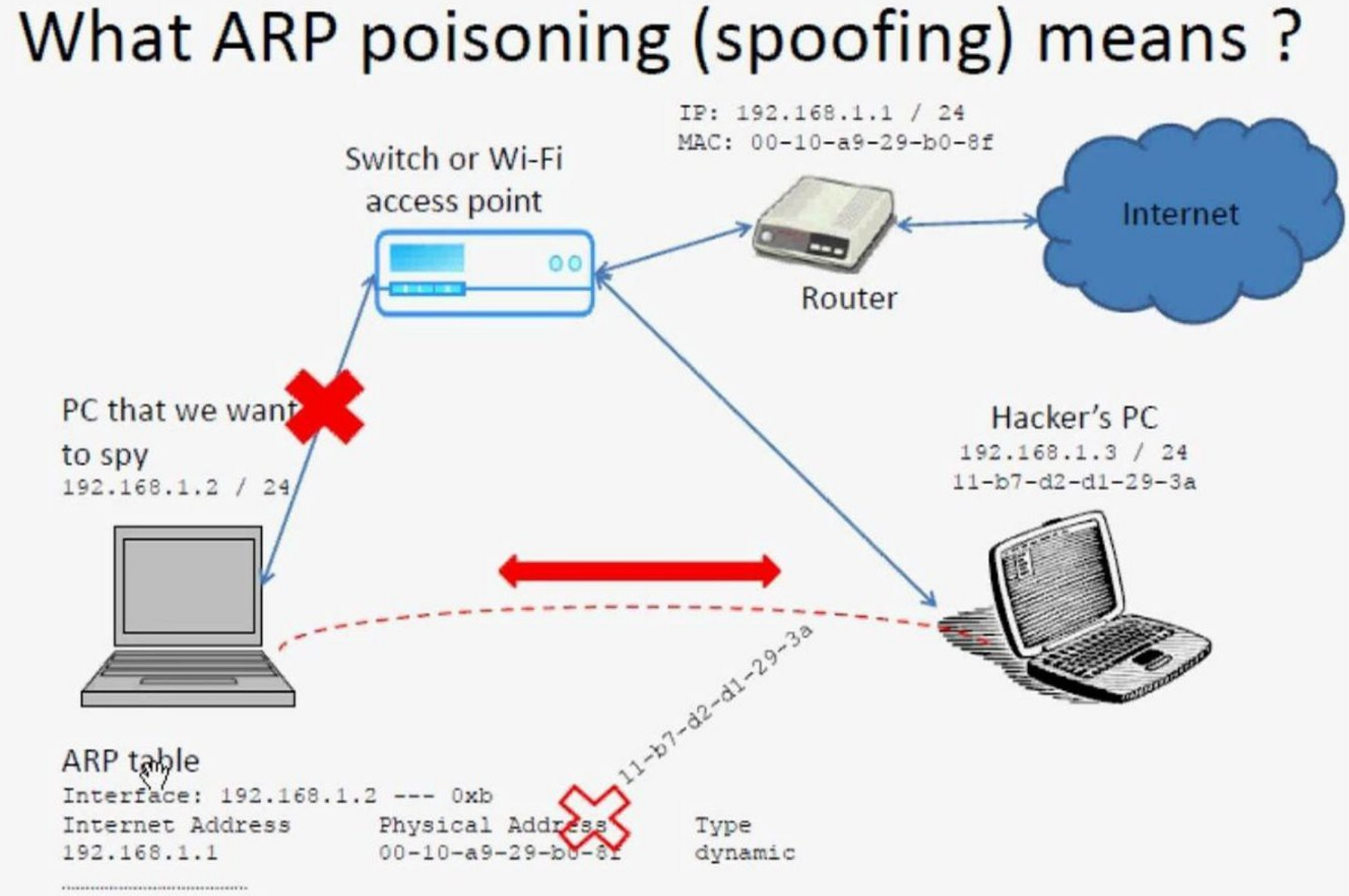
ARP Protocol

Resolves IP address to MAC address
Needed to find which host is the destination of a packet

ARP table: entries of MAC address ↔ IP address

```
bulbasaur@bulbasaur:~$ sudo arp
[sudo] password for bulbasaur:
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.11             ether   74:86:7a:0e:3b:8f   C                     eth0
gateway                  ether   dc:02:8e:f3:41:b8   C                     eth0
```

ARP Spoofing

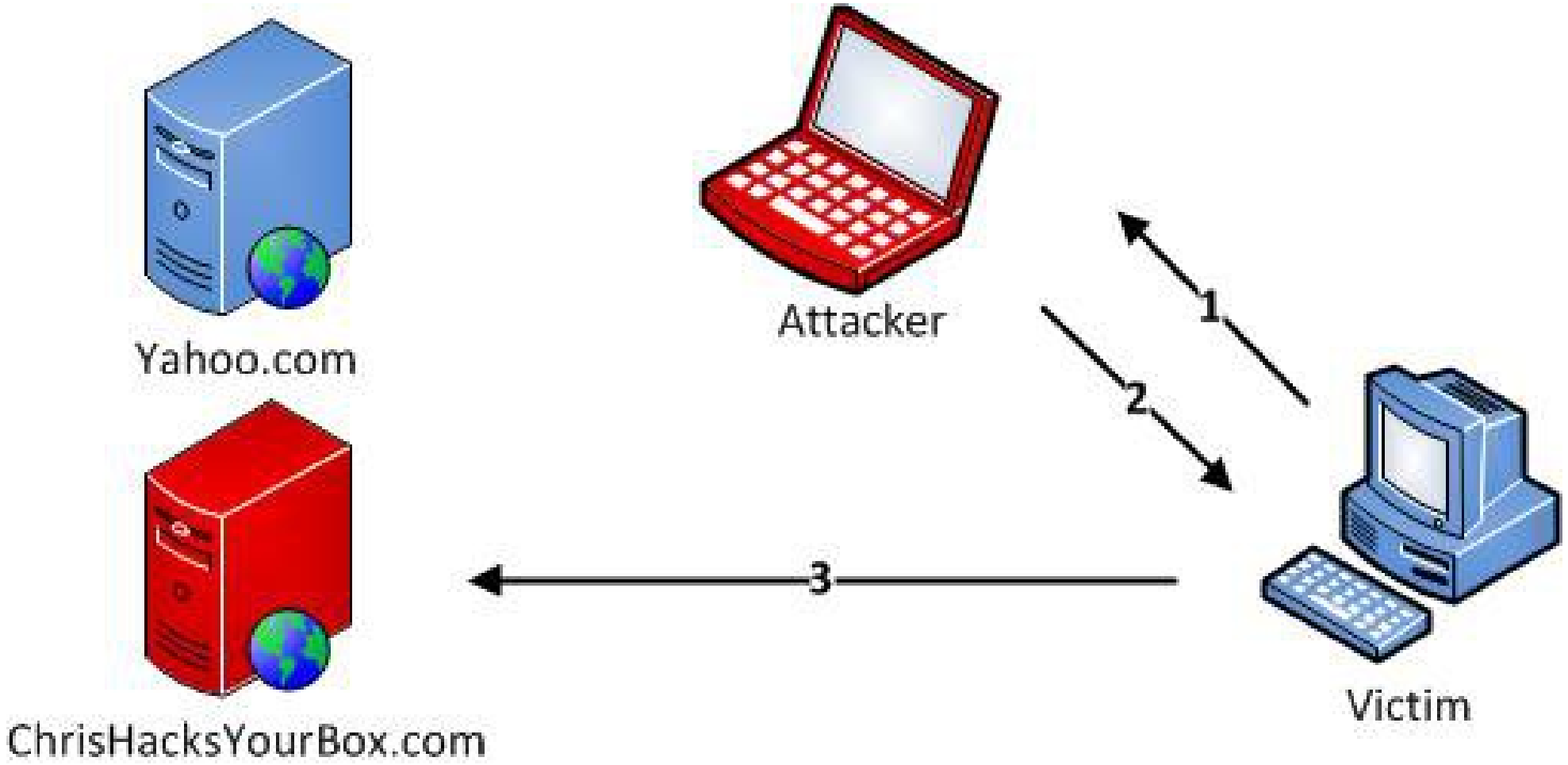


Normal DNS communication

- Internet only understands addresses such as 74.125.95.103
- DNS → associates IPs with hostname e.g. google.com →64.233.166.94
- Query/response type format

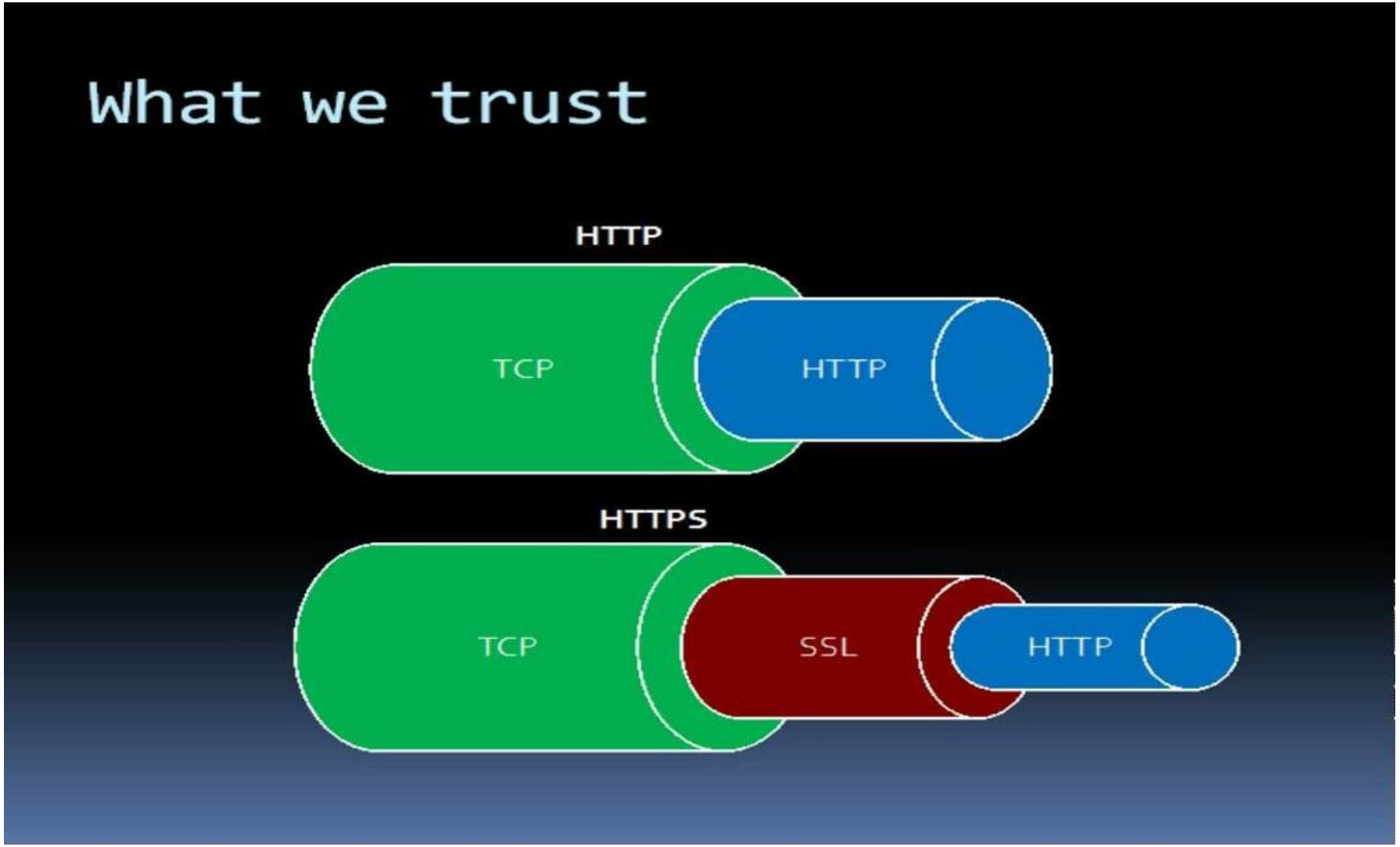
DNS Spoofing

1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as result



Live demo

HTTP vs HTTPS/SSL connection



HTTPS/SSL connection

Web Browser

Connect to HTTP Site on 80

Redirect to HTTPS Site

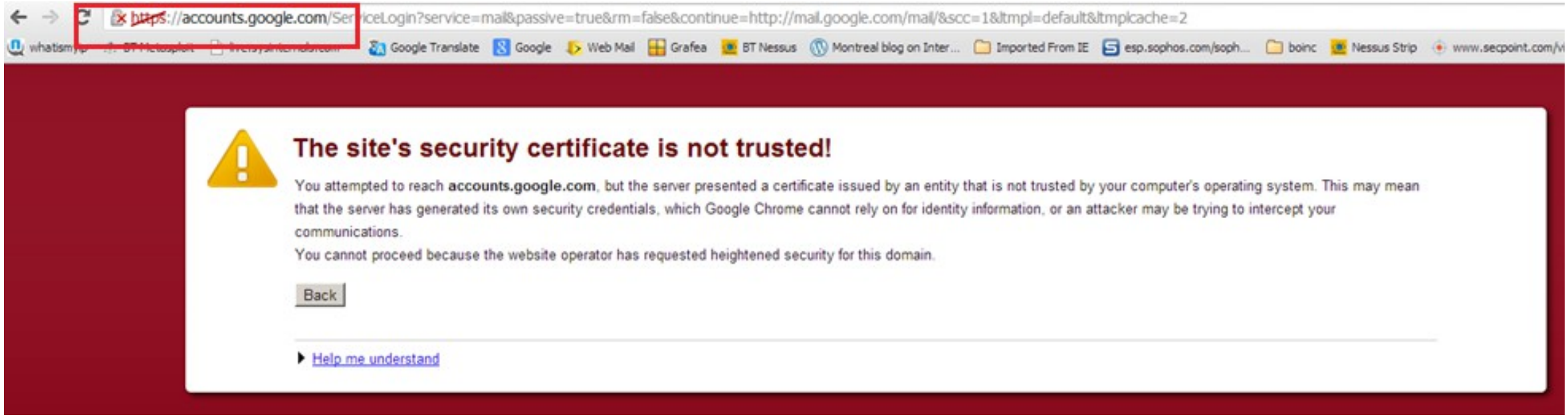
Connect to HTTPS Site on 443

Provide Server Certificate

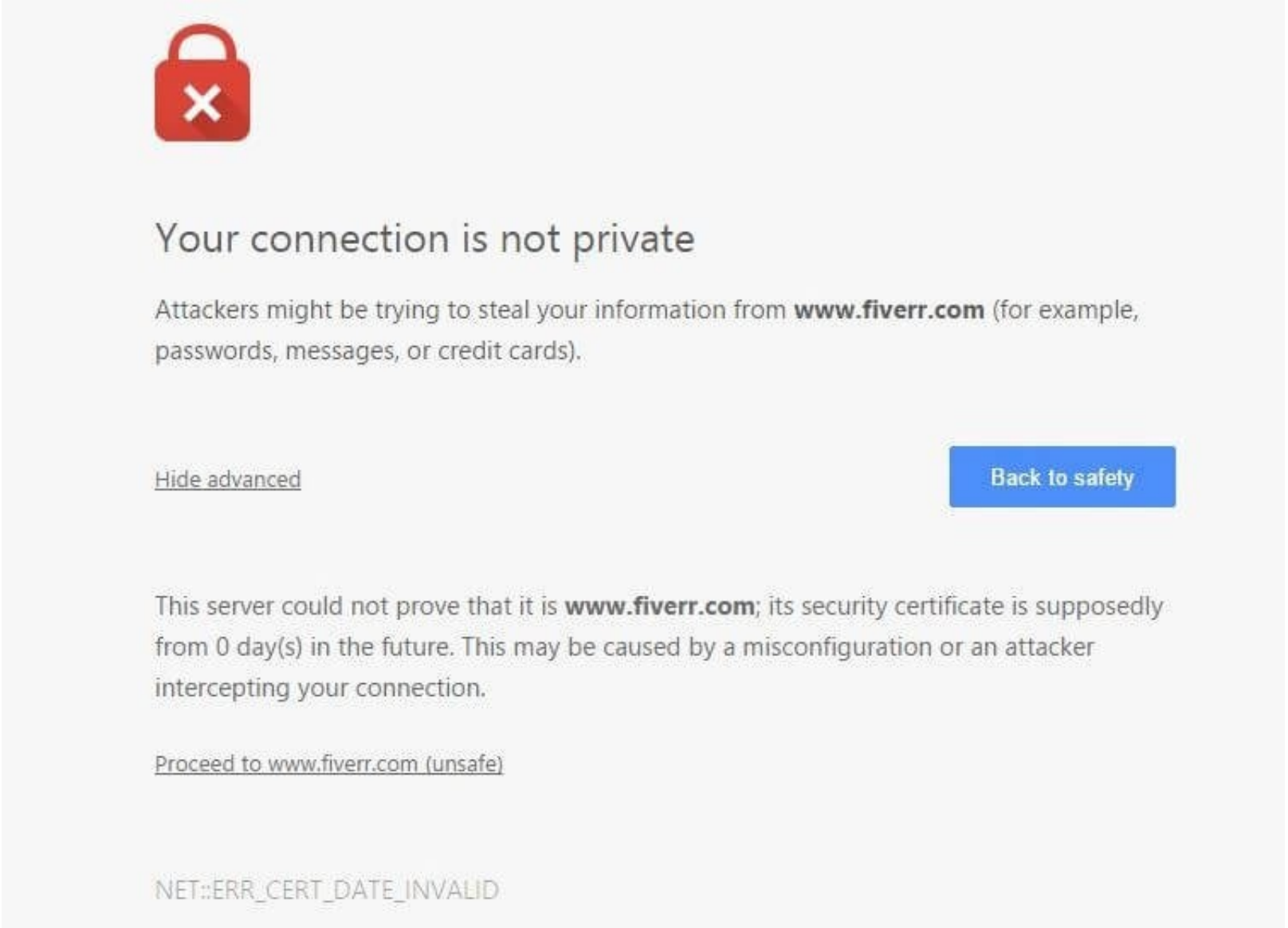
Communication Begins

Web Server

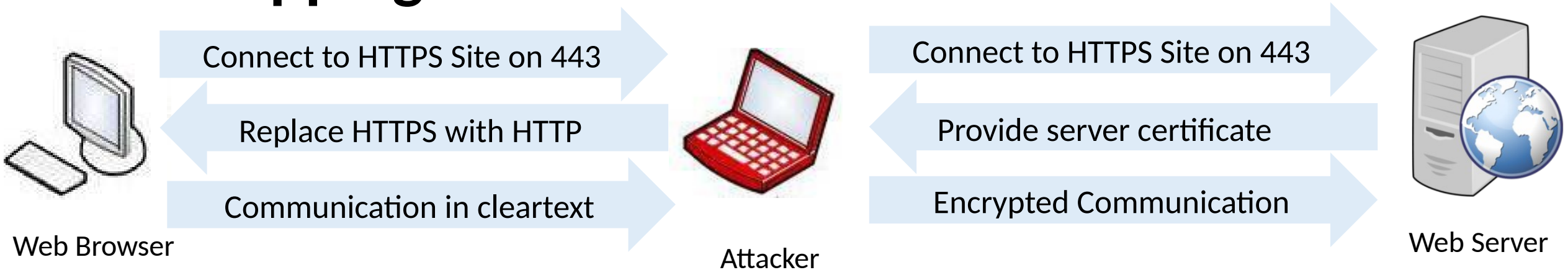
HTTP vs HTTPS/SSL connection



HTTP vs HTTPS/SSL connection



SSL stripping



Defeats the “bridge” between non-encrypted and encrypted communications → defeats https

A page would normally look like:
… Login …

During a SSL stripping attack its HTML code will be modified as:
… Login …

HSTS & HSTS bypass (sslstrip2)

HSTS

- A solution to sslstrip
- Web browsers interact with web servers using only secure HTTPS connections
- HSTS policies have been prebuilt into major browsers

HSTS bypass

- Downgrade HTTPS links to HTTP
- Prepend some custom subdomain name to them

A page would normally look like:
… Login …

Using HSTS bypass attack:
… Login …

Can we HSTS bypass using BetterCap?

Yes!
Server Name Indication (SNI) → multiple HTTPS websites served off the same IP address with multiple certificates

At TLS negotiation: server's decision for the correct certificate → attacker detects it

BetterCap’s HTTPS proxy
- detects the upstream server host
- spoofs the correct certificate

But!
NEED access to the victim's pc → add BetterCap's certificate to victim's browser trusted certificates → unreasonable assumption

Injecting Javascript/HTML/CSS

Live demo

Commands we used

Arp spoofing
sudo bettercap -T 192.168.1.2 -X

Dns spoofing
sudo bettercap -T 192.168.1.2 –dns dns.conf

Getting credentials from http
sudo bettercap 192.168.1.2 --proxy -P POST

Getting credentials from https:
sudo bettercap -T 192.168.1.2 --proxy –proxy-https -P POST

Css injection
sudo bettercap -T 192.168.1.2 -X --proxy --proxy-module injectcss --css-file site.css

Js injection
sudo bettercap -T 192.168.1.2 -X --proxy --proxy-module injectjs ––js-file myjs.js

Thank you :)

Questions?

eva.sarafianou@gmail.com