Communication Vulnerabilities

Dr Rosanne English

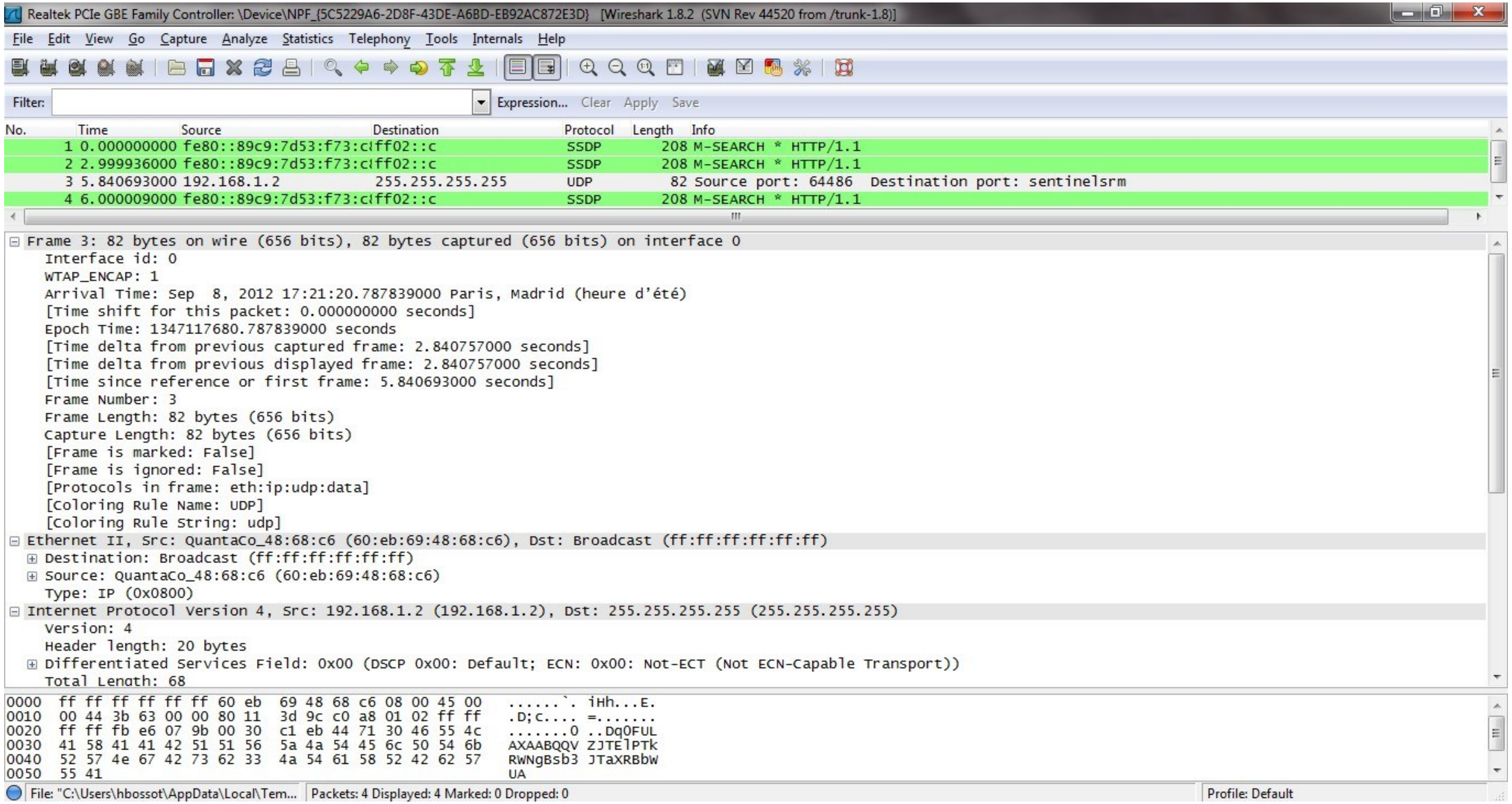
Packet Sniffing

- The attacker can snoop information as it passes through a network the attacker is on

Packet Sniffing - Switches

- A list of which relates connections to nodes
- Can overload switches and put them into ‘promiscuous mode’

WireShark


Realtek PCIe GBE Family Controller: \Device\NPF_{5C5229A6-2D8F-43DE-A6BD-EB92AC872E3D} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Filter:
Expression...
Clear
Apply
Save

```
No.   Time        Source                   Destination      Protocol  Length Info
    1 0.000000000 fe80::89c9:7d53:f73:c(ff02::c          SSDP        208 M-SEARCH * HTTP/1.1
    2 2.999936000 fe80::89c9:7d53:f73:c(ff02::c          SSDP        208 M-SEARCH * HTTP/1.1
    3 5.840693000 192.168.1.2              255.255.255.255  UDP          82 Source port: 64486  Destination port: sentinelsrm
    4 6.000009000 fe80::89c9:7d53:f73:c(ff02::c          SSDP        208 M-SEARCH * HTTP/1.1
```

```
⊟ Frame 3: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Sep  8, 2012 17:21:20.787839000 Paris, Madrid (heure d'été)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1347117680.787839000 seconds
    [Time delta from previous captured frame: 2.840757000 seconds]
    [Time delta from previous displayed frame: 2.840757000 seconds]
    [Time since reference or first frame: 5.840693000 seconds]
    Frame Number: 3
    Frame Length: 82 bytes (656 bits)
    Capture Length: 82 bytes (656 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
⊟ Ethernet II, Src: QuantaCo_48:68:c6 (60:eb:69:48:68:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: QuantaCo_48:68:c6 (60:eb:69:48:68:c6)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 68
```

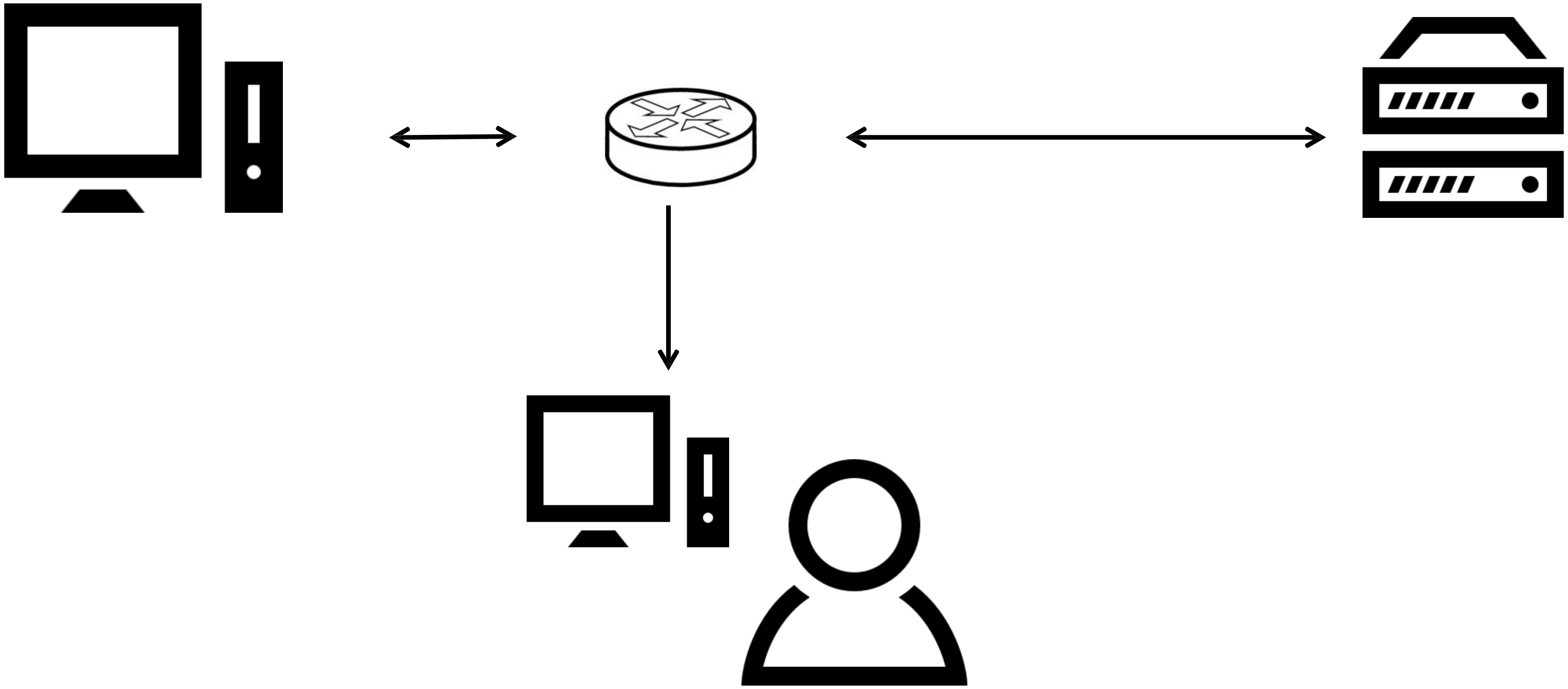
```
0000  ff ff ff ff ff ff 60 eb  69 48 68 c6 08 00 45 00   ......`. iHh...E.
0010  00 44 3b 63 00 00 80 11  3d 9c c0 a8 01 02 ff ff   .D;c.... =.......
0020  ff ff fb e6 07 9b 00 30  c1 eb 44 71 30 46 55 4c   .......0 ..Dq0FUL
0030  41 58 41 41 42 51 51 56  5a 4a 54 45 6c 50 54 6b   AXAABQQV ZJTElPTk
0040  52 57 4e 67 42 73 62 33  4a 54 61 58 52 42 62 57   RWNgBsb3 JTaXRBbW
0050  55 41                                              UA
```

File: "C:\Users\hbossot\AppData\Local\Tem... | Packets: 4 Displayed: 4 Marked: 0 Dropped: 0 | Profile: Default

Image used under Creative Commons Licence from: wireshark image

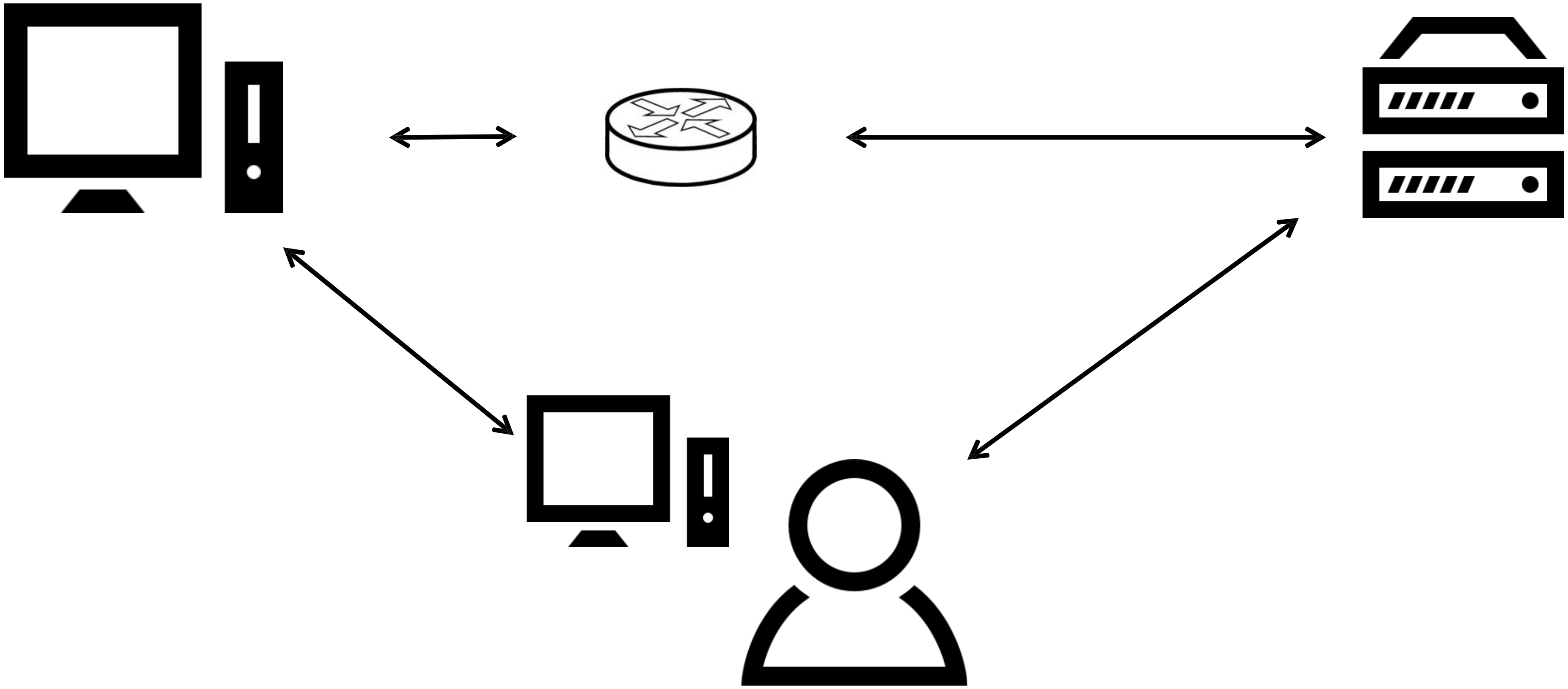
Packet Sniffing

The process of monitoring communications across a network
Attacker must be on the network to monitor packets
Generally requires either a hub or for a switch to be in ‘promiscuous’ mode



Machine in the Middle (MITM)

The process of spoofing client to server and server to client such that communications between parties can be monitored and potentially changed



Spoofing

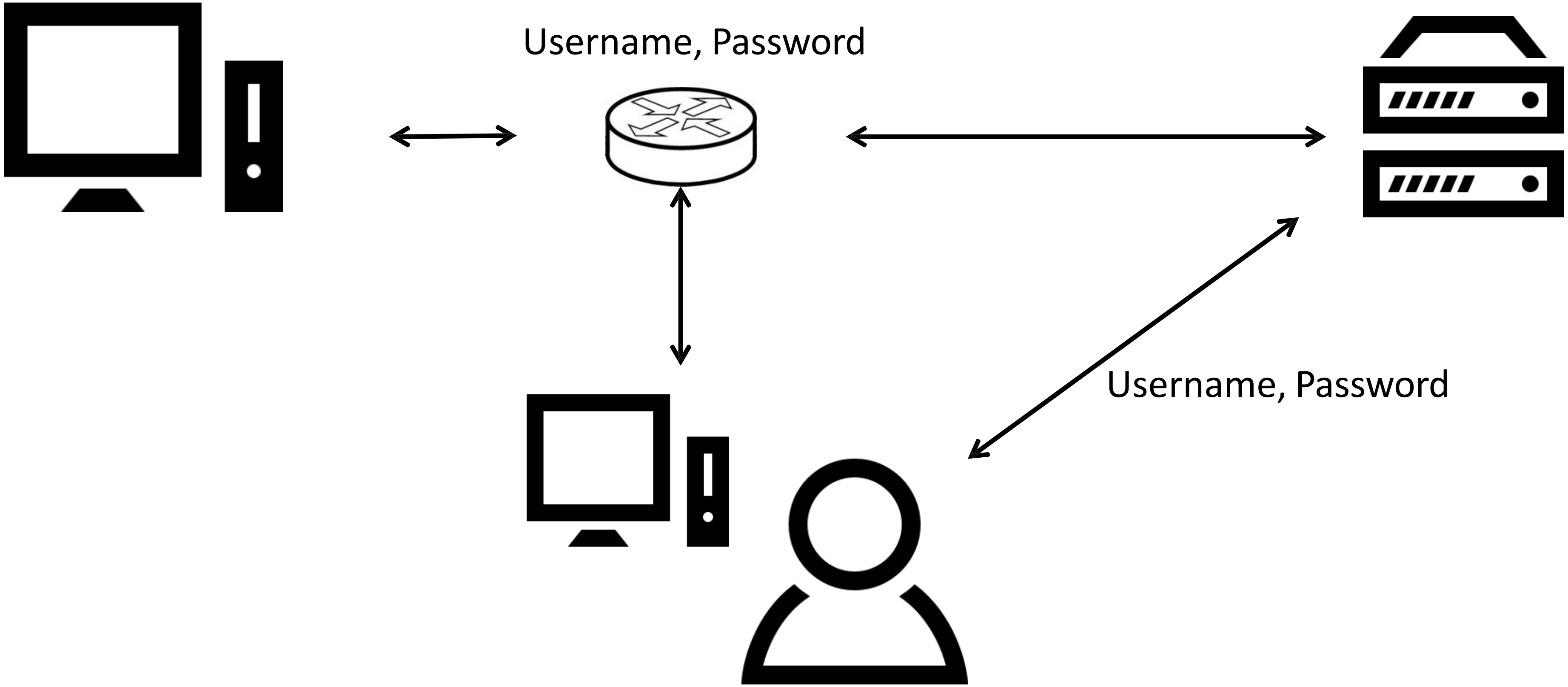
- In a LAN – Address Resolution Protocol spoofing
  - ARP maps IP addresses to MAC addresses
  - Change the map of an IP to the attacker’s MAC
  - Tools such as Ettercap

Spoofing

- In a LAN – Address Resolution Protocol spoofing
  - ARP maps IP addresses to MAC addresses
  - Change the map of an IP to the attacker's MAC
  - Tools such as Ettercap
- On the internet – DNS Protocol
  - Requires Domain Name Server entry to be replaced with attackers IP

Replay Attack

A replay attack involves the monitoring of information from client to server such as a username and password, and replaying this to the server at a later time in order to spoof the client



Dr Rosanne English