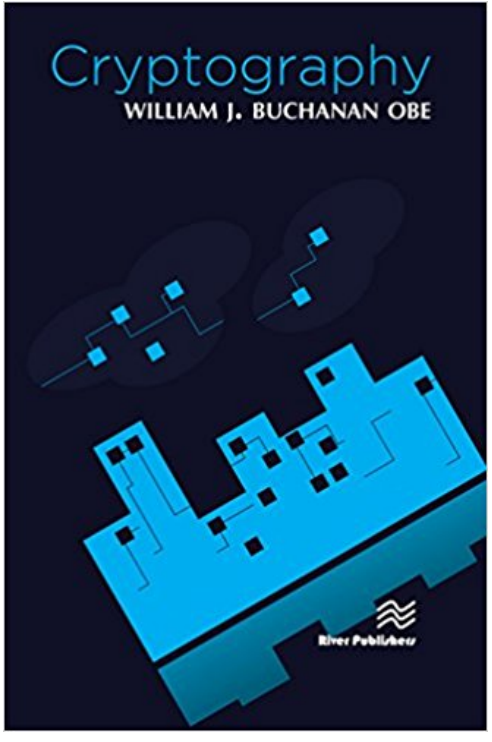
Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

http://asecuritysite.com/encryption
http://asecuritysite.com/unit06



Overview

No	Date	Subject	Lab
1	**17 Jan 2020**	Ciphers and Fundamentals Unit	Lab [Link] Demo [Link]
2	**24 Jan 2020**	Symmetric Key Unit	Lab [Link] Demo [Link]
3	**31 Jan 2020**	Hashing and MAC Unit	Lab [Link]
4	**7 Feb 2020**	Asymmetric (Public) Key Unit	Lab [Link]
5	**14 Feb 2020**	Key Exchange Unit	Lab [Link]
6	**21 Feb 2020**	Guest lecture	Mini-project/Coursework [Link]
7	**28 Feb 2020**	Trust and Digital Certificates Unit	Lab [Link]
8	**6 Mar 2020**	Tunnelling Unit	Lab [Link]
9	**13 Mar 2020**	Test 1 (Units 1-5) [Study guide]	
10	**20 Mar 2020**	Blockchain Unit	Lab [Link]
11	**27 Mar 2020**	Future Cryptography Unit	Lab [Link]
12	**3 April 2020**	Tokens, Authorization and Docker Unit	Lab [Link]
13	**10 April 2020**	Trusted Hosts Unit	
Easter Break			
14	**Week beginning 27 April 2020 (TBC)**	Test 2 (Units 6-10)	
15	**Week beginning 4 May 2020 (TBC)**	Coursework Hand-in [Draft]	

Overview

No	Date	Subject	Lab
	(TBC)		

e-Security Test 1

[Back] The test will run on 15 March 2019. This page defines some of the areas you may want to focus your study. Remember to **check back regularly** for any updates.

Sample Exam Questions | Sample Exam Paper | Main Study Guide

Sample Exam Questions

There will be **four main questions** in the exam: Symmetric Key (Unit 2), Hashing (Unit 3), Public Key (Unit 4), and Key Exchange (Unit 5).

1. Symmetric Key

Key principles: Salting, AES, ECB, CBC, Key entropy.

- Computing power increases each year. Outline the challenge this gives when protecting encrypted data. [Ref: Symmetric Key]
- What are the possible advantages of using stream ciphers over block ciphers? [Ref: Symmetric Key]
- The AES method is recommended by NIST for symmetric key encryption. What are the main stages involved in the AES process? [Ref: Symmetric Key]
- Bob encrypts his data using symmetric key encryption and sends it to Alice. Every time he produces the ciphertext it changes, and he is worried that Alice will not be able to decipher the cipher text. He encrypts "Hello" and gets a different cipher stream each time. Why does the cipher text change? [Ref: Symmetric Key]
- Bob is sending encrypted data to Alice, and Eve is listening. After listening for a while, Eve is able to send a valid encrypted message to Alice. By outlining ECB, discuss how this might be possible. [Ref: Symmetric Key]
- Bob is using a password to generate a 128-bit encryption key. Explain why the key space is unlikely to be 2128, and why key entropy could be used to measure the equivalent key size. [Ref: Symmetric Key]
- Bob says that the number of bytes used for the cipher text will change directly with the number of bytes used in the plain text. Alice disagrees and says that most encryption methods involve having block sizes. Who is correct? Explain why. [Ref: Symmetric Key]
- With block encryption, how do we know where the ciphered data actually ends? Does it just use an end-of-file character or a NULL character? [Ref: Symmetric Key]
- Alice says she is confused that Bob is sending her the same message as a cipher, but every time the cipher text changes. Apart from using the shared encryption key, what does Alice use to decipher the cipher text? [Ref: Symmetric Key]
- Why would Eve have an aversion to salt? [Ref: Symmetric Key]

Overview

No	Date	Subject	Lab

Analysis of Next Generation Cryptography

[Home] **Note: This is a draft, and is likely to be subject to change.**

Requirements

You are requested to investigate, build a prototype, and evaluate one of the following:

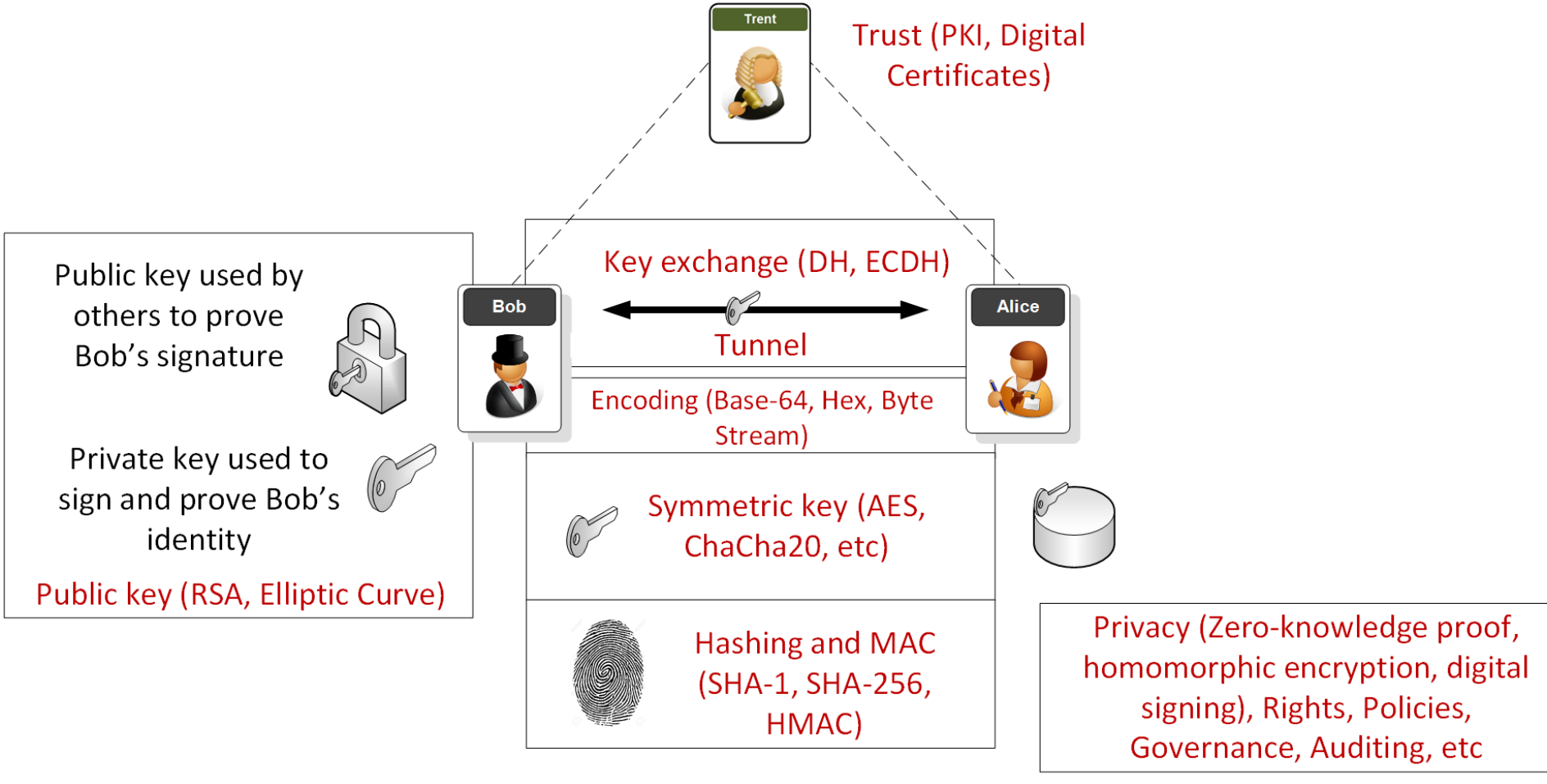
- **Zero-knowledge proof (ZKP) methods**. This involves using cryptography to allow users to prove shared knowledge without having to reveal the original information. This might involve passing knowledge of a password, without actually revealing the password.
- **Homomorphic encryption**. This involves processing encrypted data and can be partial homomorphic encryption (where a few mathematical methods can be implemented) or full homomorphic encryption.
- **Light-weight cryptography**. This involves cryptography methods that supports encryption which are suitable for IoT devices. This is normally opmitized in terms of reducing processing requirements, memory utilization and energy drain.
- **Quantum-robust cryptography**. Quantum computers are likely to crack existing public key methods, and thus we need to move toward public key methods which are quantum robust.
- **Key Distribution Centres**. The complexity of handling keys is an increasing challenge for many companies. Within a KDC, we can implement methods which will generate encryption keys for users. This topic will involve investigating possible methods that could be used.
- **Blockchain integration**. Many applications are moving towards storing data on a blockchain and in using smart contracts. This area will investigate new areas of improving the security and/or performance of blockchain related methods.

There are many different methods involved in each of these areas, so while your literature review might have a relatively wide scope, you might want to focus in on one or more methods for your implementation and evaluation. You may also pick another related area, but this would have to be approved by your tutor.

- Why would Eve have an aversion to salt? [Ref: Symmetric Key]

(TBC)

Overview


Trent
Trust (PKI, Digital Certificates)
Public key used by others to prove Bob's signature
Private key used to sign and prove Bob's identity
Public key (RSA, Elliptic Curve)
Bob
Key exchange (DH, ECDH)
Tunnel
Alice
Encoding (Base-64, Hex, Byte Stream)
Symmetric key (AES, ChaCha20, etc)
Hashing and MAC (SHA-1, SHA-256, HMAC)
Privacy (Zero-knowledge proof, homomorphic encryption, digital signing), Rights, Policies, Governance, Auditing, etc

Qualys. SSL Labs

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

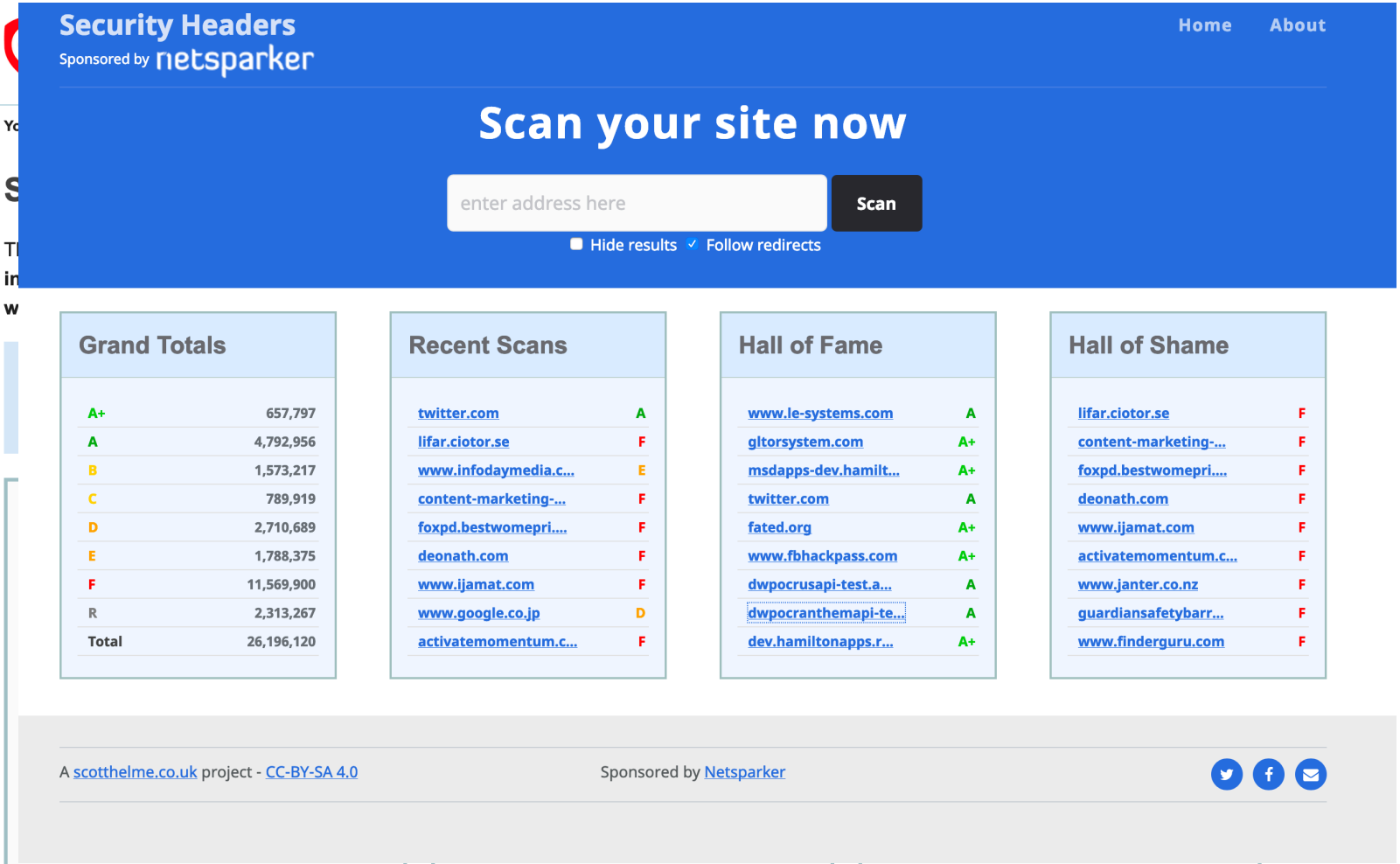
Hostname: Submit

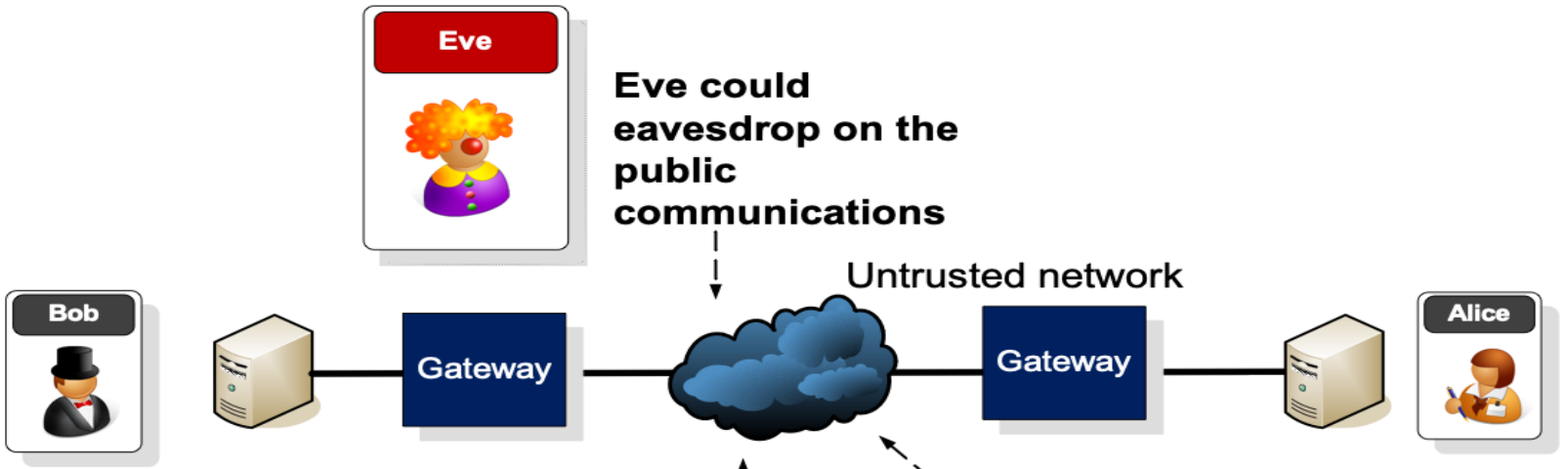
Do not show the results on the boards

Recently Seen	
www.yaklink.com	
billiardunderground.org	
ha.homenetwork.biz	
srv-web02.imageware.ch	
evisa.gov.ge	
www.theleveluppleague.com	Err
sportclinic.it	
edpnet.net	
bungholio.ch	
trade.eurocarparts.com	

Recent Best	
forachange.co.il	A+
auth.touchsurgery.com	A+
www.chegaga.de	A+
ps-metro-fsd-mm-10-0-fsd-mm- ...	A
callback.datinglab.net	A
www.rivanov.nl	A
www.ioffice.kz	B
afficheo.com	B
popuplabor-bw.de	B
mobile.imageware.ch	B

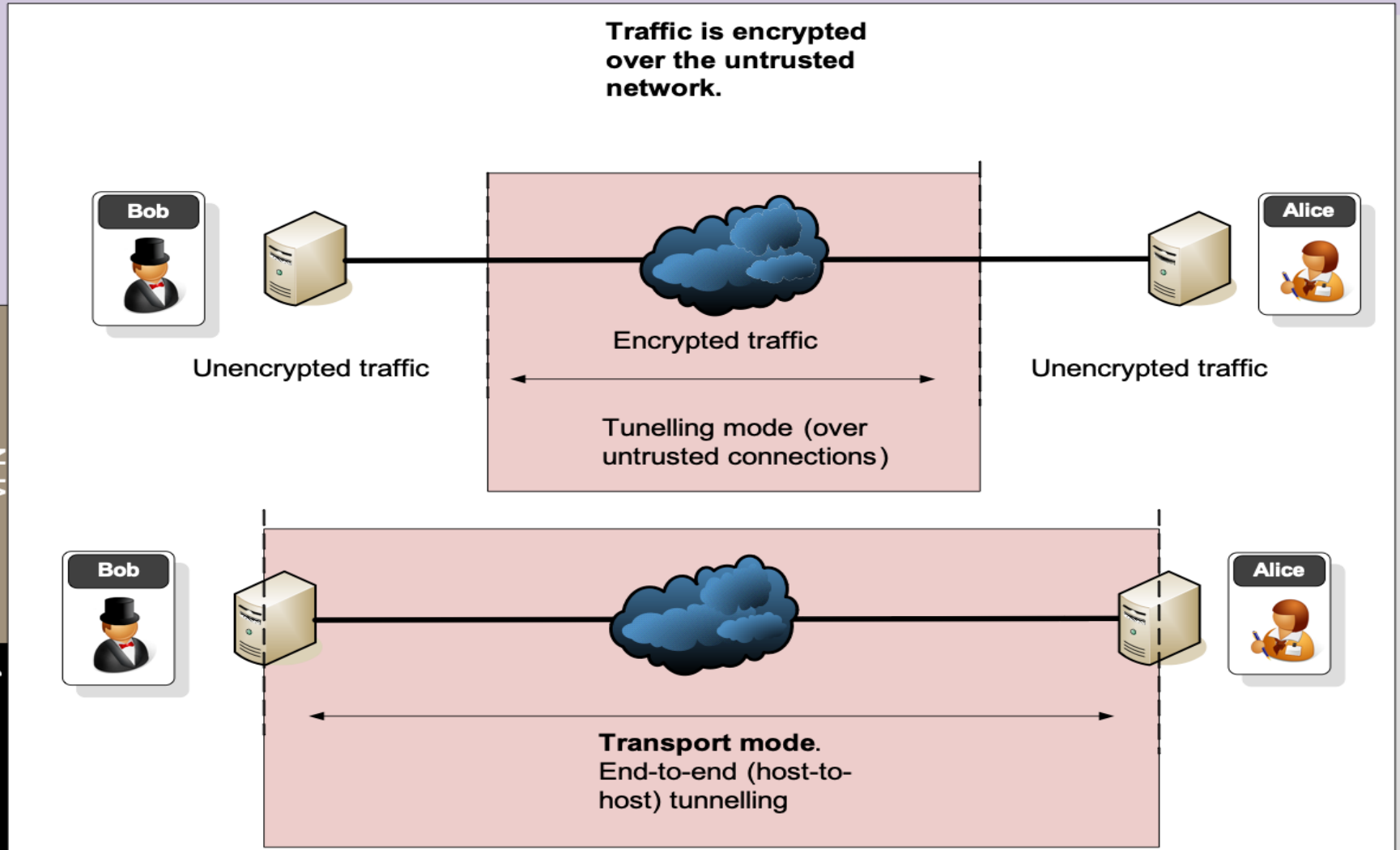
Recent Worst	
chepai.alltobid.com	F
mail.frende.no	F
mitpfa.dk	F
ow-analytics.com	F
mft.imageware.ch	T
selfservice.kvk.nl	F
www.migrosmagazin.ch	F
www.vkekk.lt	F
www.preiswerte-werbeartikel. ...	F
bbapp.toddmorton.net	T


Security Headers
Sponsored by netsparker
Home
About
Scan your site now
enter address here
Scan
Hide results
Follow redirects
Grand Totals
A+ 657,797
A 4,792,956
B 1,573,217
C 789,919
D 2,710,689
E 1,788,375
F 11,569,900
R 2,313,267
Total 26,196,120
Recent Scans
twitter.com A
lifar.ciotor.se F
www.infodaymedia.c... E
content-marketing-... F
foxpd.bestwomepri.... F
deonath.com F
www.ijamat.com F
www.google.co.jp D
activatemomentum.c... F
Hall of Fame
www.le-systems.com A
gltorsystem.com A+
msdapps-dev.hamilt... A+
twitter.com A
fated.org A+
www.fbhackpass.com A+
dwpocrusapi-test.a... A
dwpocranthemapi-te... A
dev.hamiltonapps.r... A+
Hall of Shame
lifar.ciotor.se F
content-marketing-... F
foxpd.bestwomepri.... F
deonath.com F
www.ijamat.com F
activatemomentum.c... F
www.janter.co.nz F
guardiansafetybarr... F
www.finderguru.com F
A scotthelme.co.uk project - CC-BY-SA 4.0
Sponsored by Netsparker

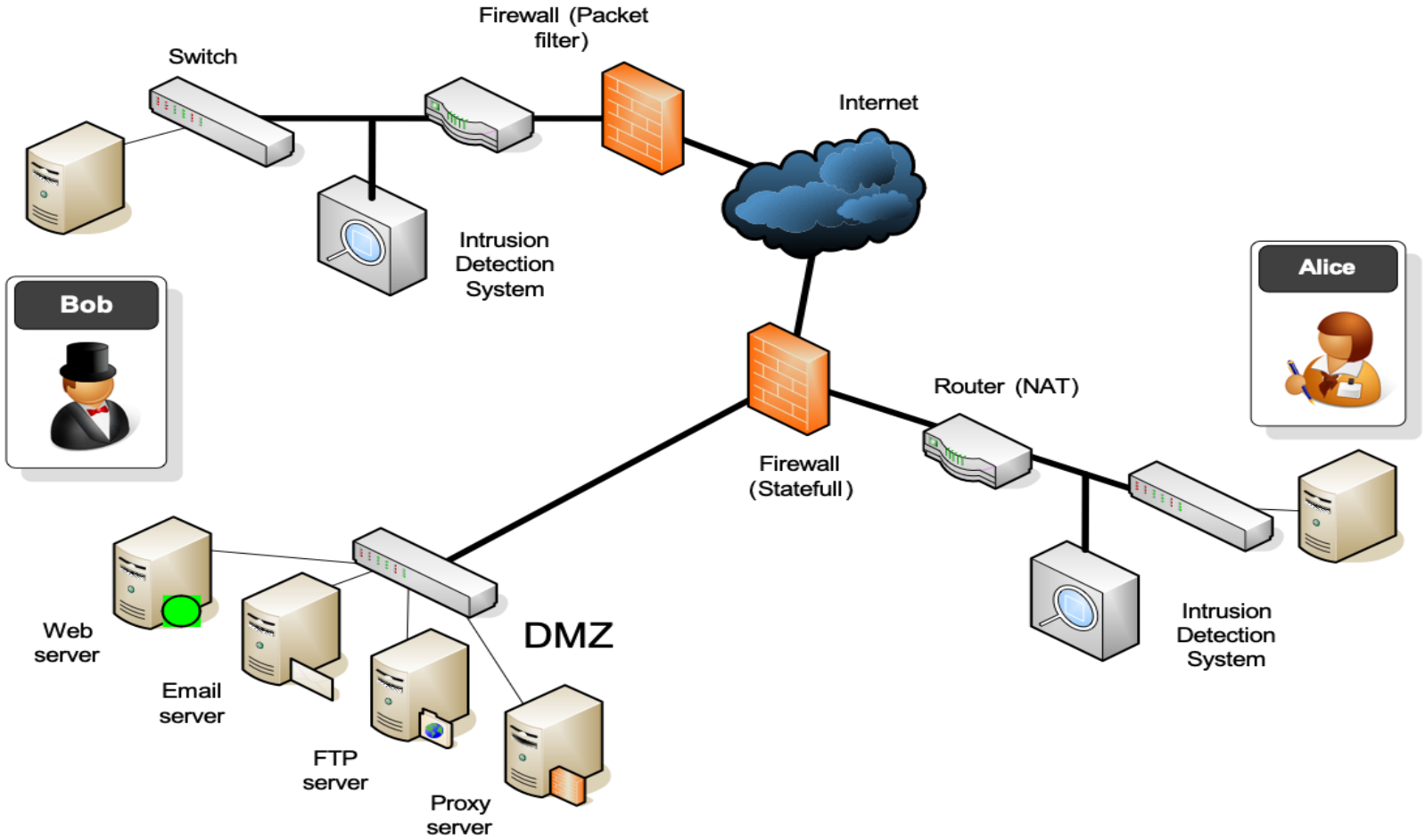


What is required is:

- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

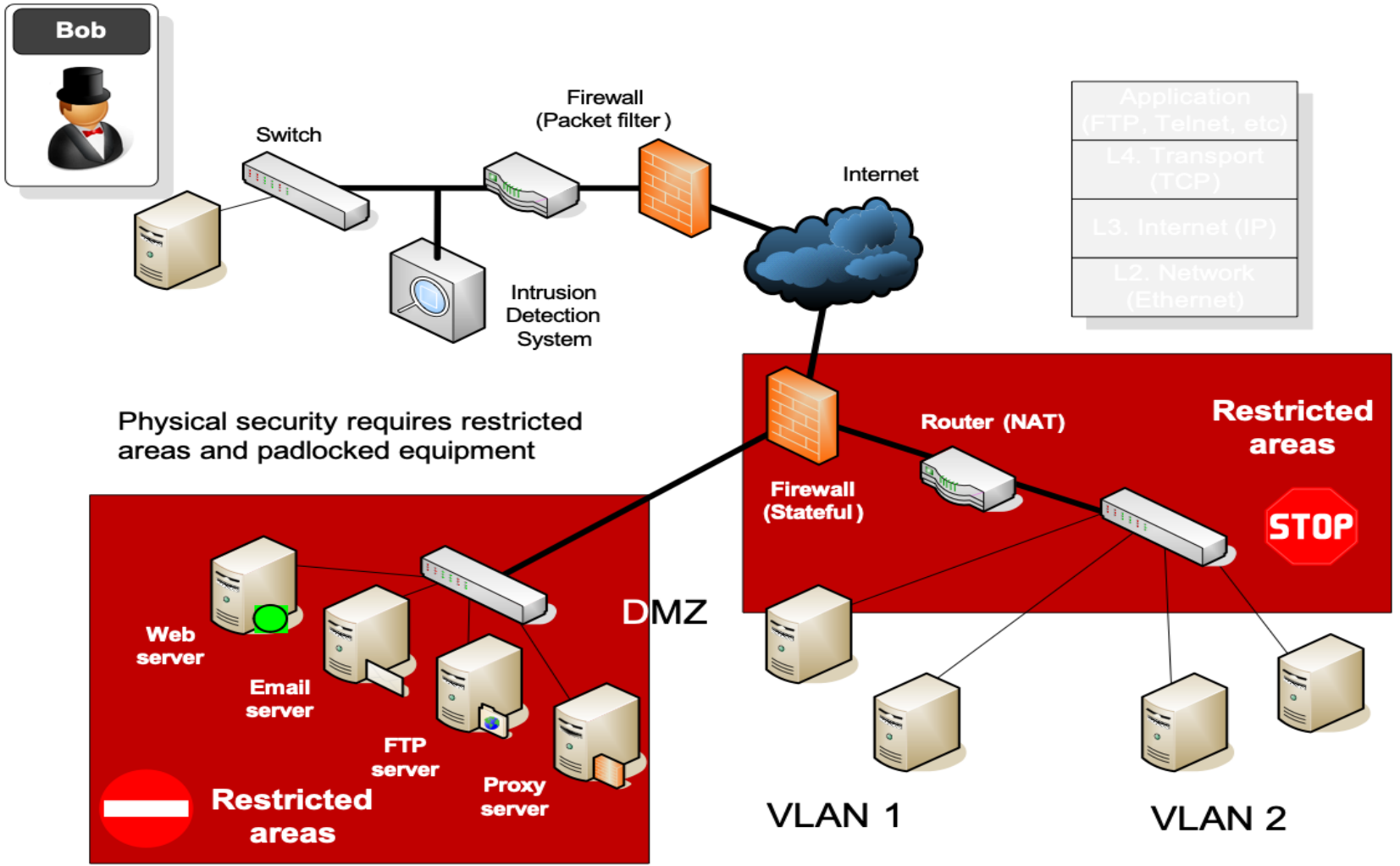


Tunnelling mode or transport mode

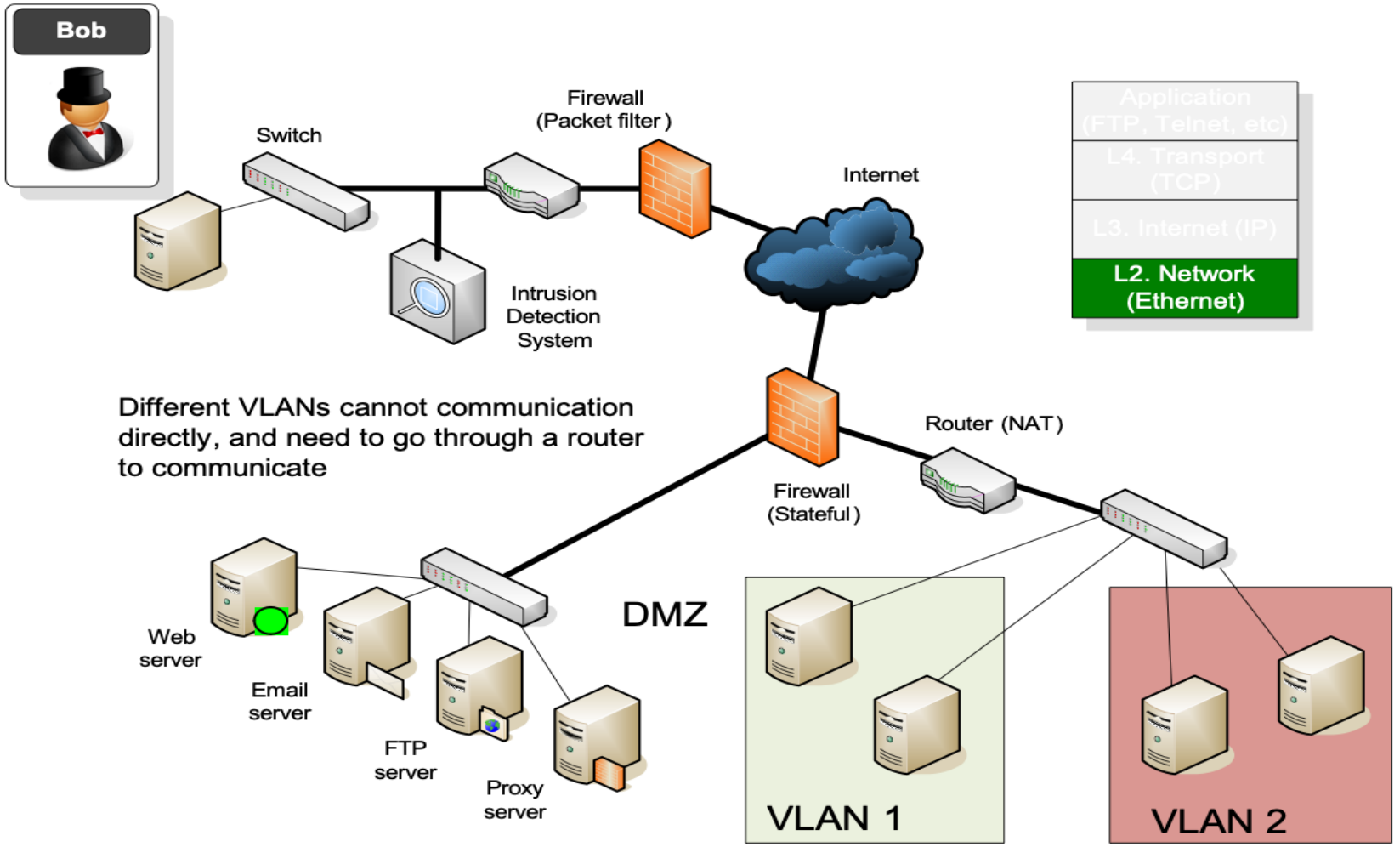


Author: Prof Bill Buchanan

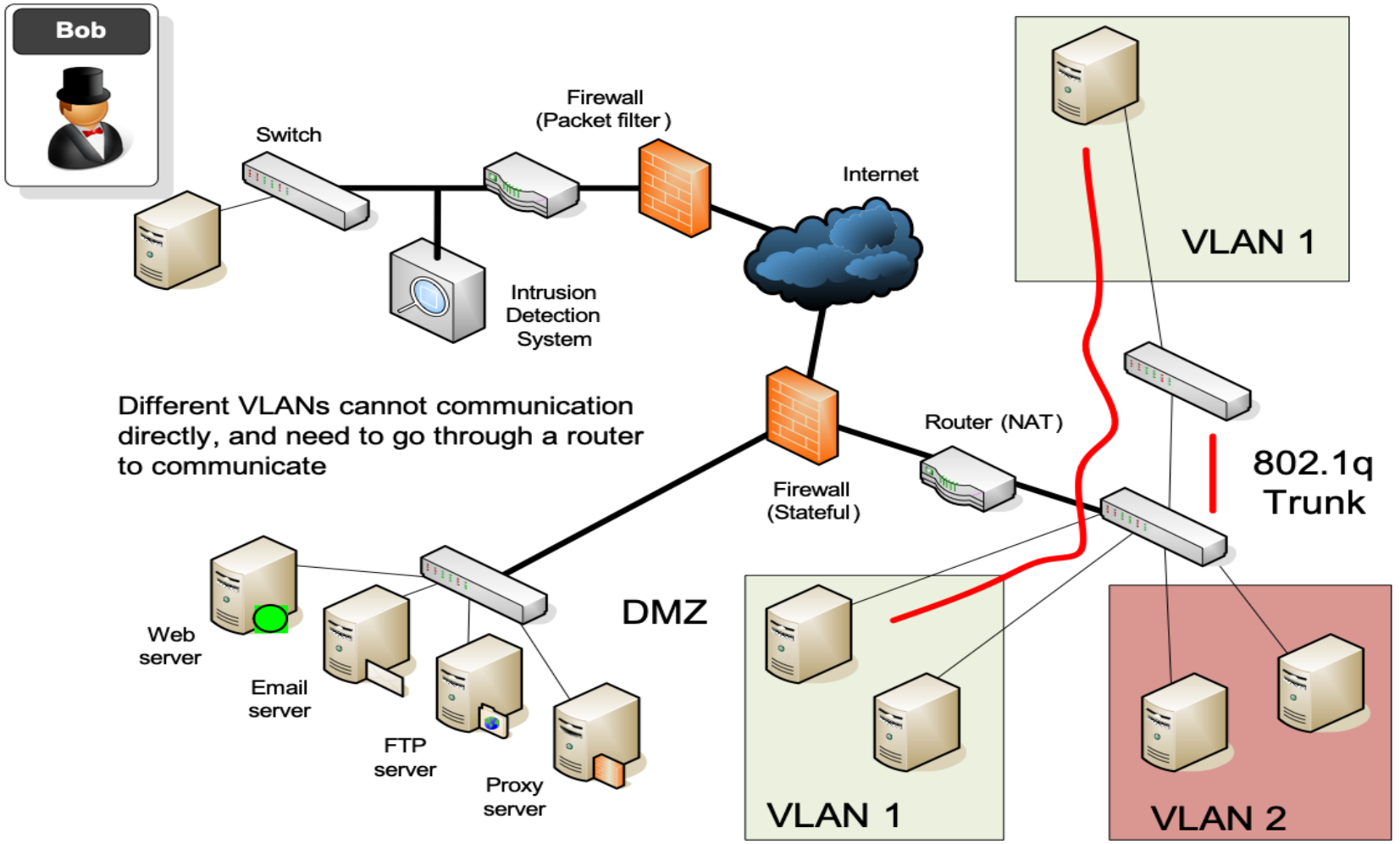
Example Infrastructure



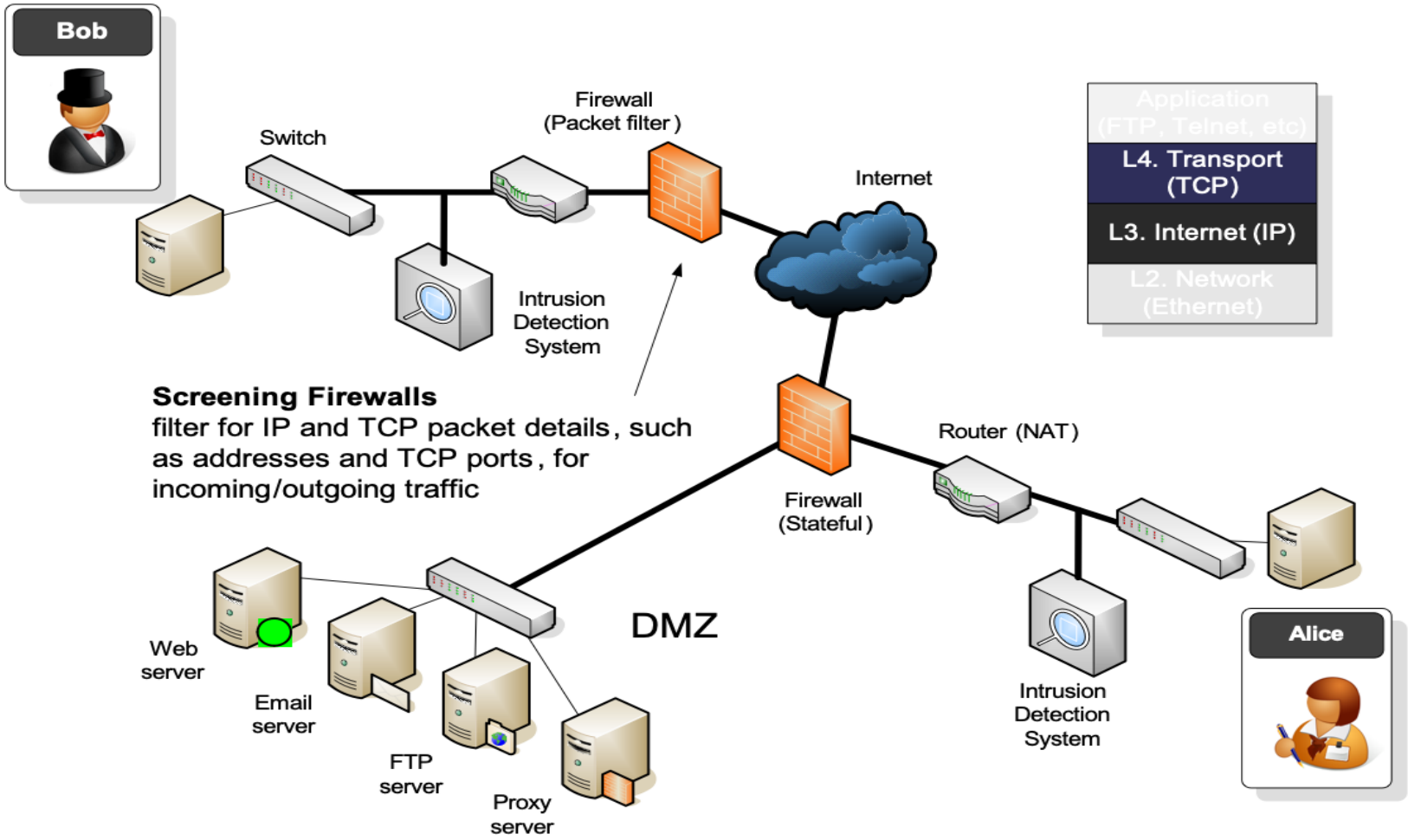
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



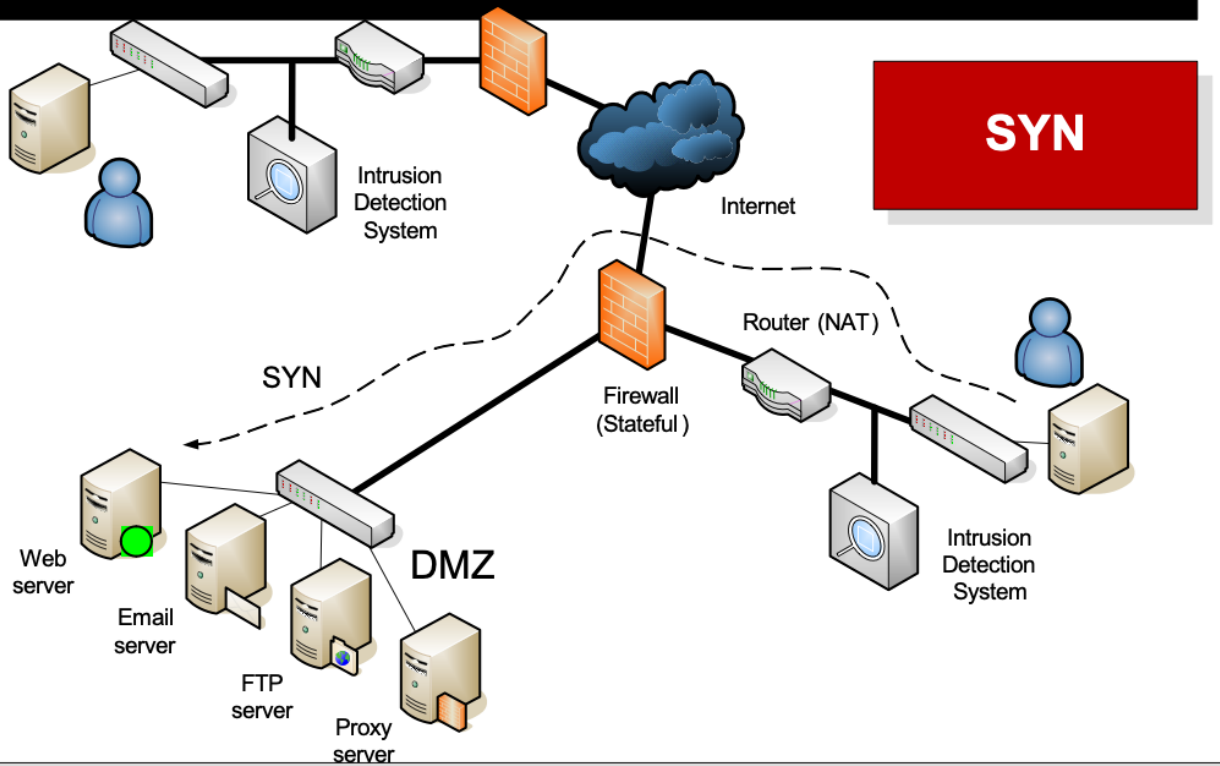
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Originator		Recipient
1. CLOSED		LISTEN
2. SYN-SENT	**<SEQ=999><CTL=SYN>**	**SYN-RECEIVED**
3. ESTABLISHED	<SEQ=100><ACK=1000><CTL=SYN,ACK>	SYN-RECEIVED
4. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED
5. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED

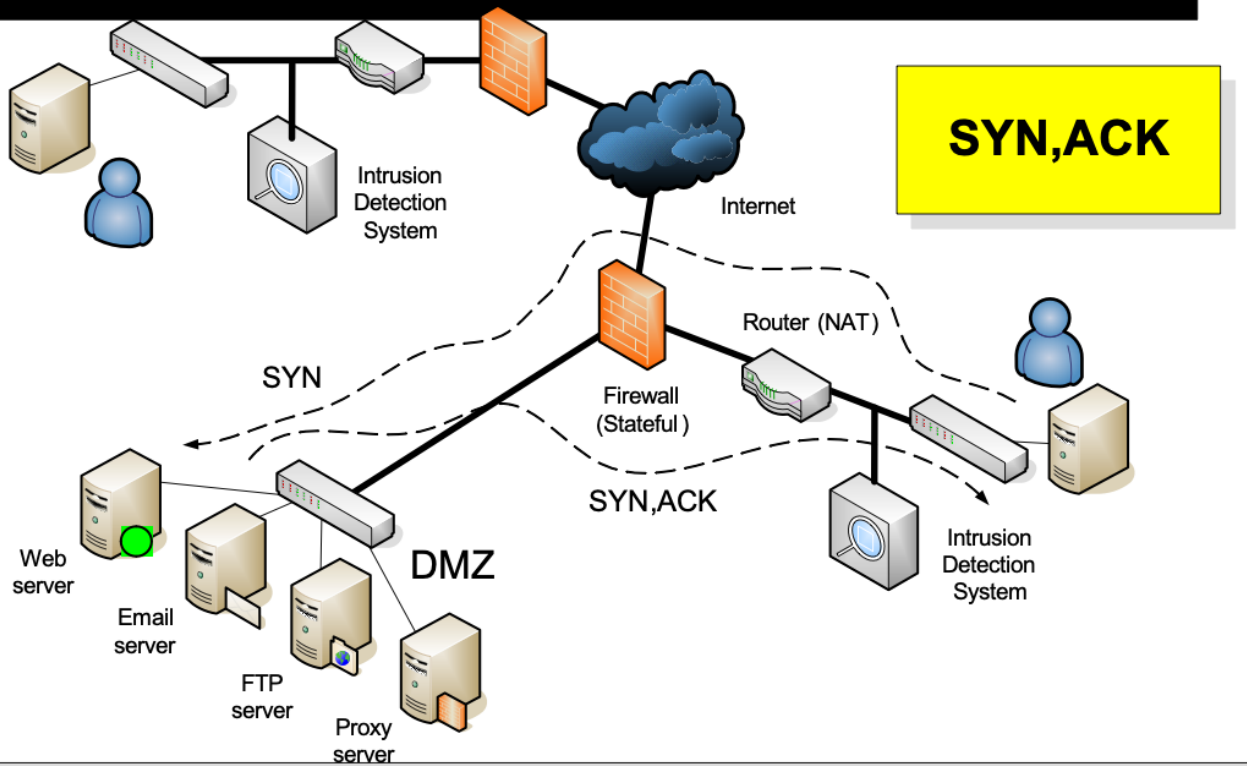
SYN



Originator		Recipient
1. CLOSED		LISTEN
2. SYN-SENT	<SEQ=999><CTL=SYN>	SYN-RECEIVED
3. ESTABLISHED	**<SEQ=100><ACK=1000><CTL=SYN,ACK>**	**SYN-RECEIVED**
4. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED
5. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED

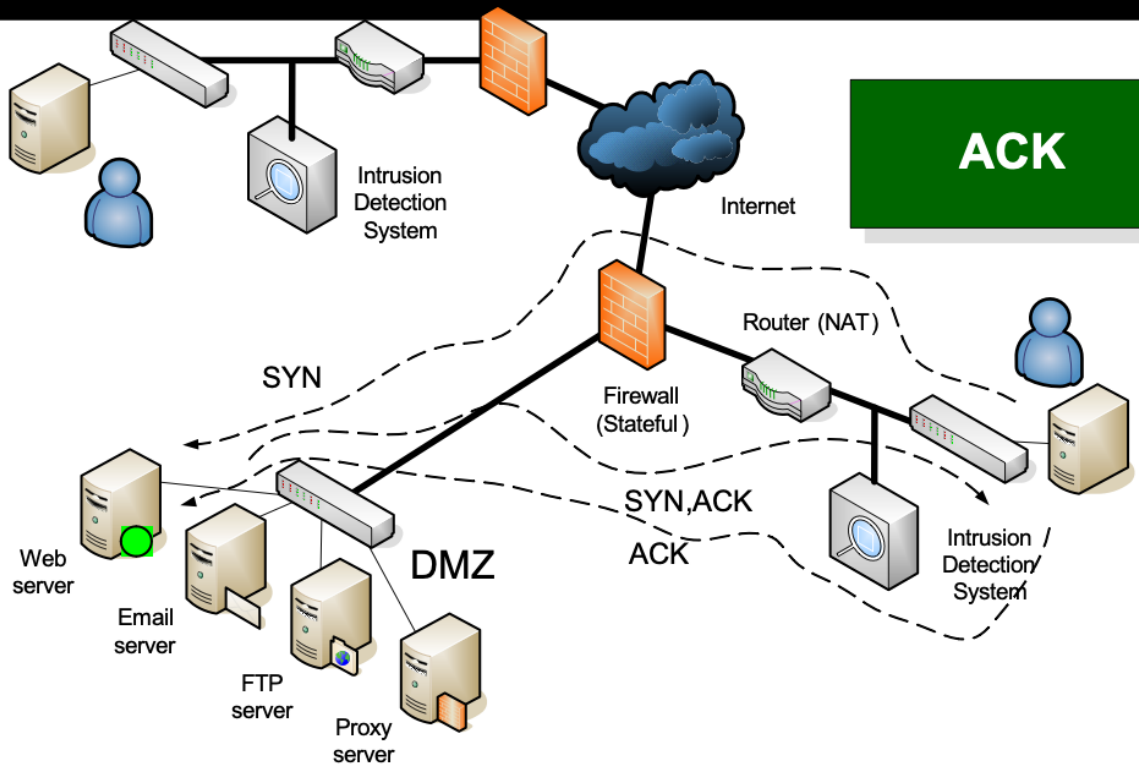
SYN

SYN,ACK



Originator		Recipient
1. CLOSED	LISTEN	
2. SYN-SENT	<SEQ=999><CTL=SYN>	SYN-RECEIVED
3. ESTABLISHED	<SEQ=100><ACK=1000><CTL=SYN,ACK>	SYN-RECEIVED
4. ESTABLISHED	**<SEQ=1000><ACK=101><CTL=ACK>**	**ESTABLISHED**
5. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED

SYN
SYN,ACK
ACK

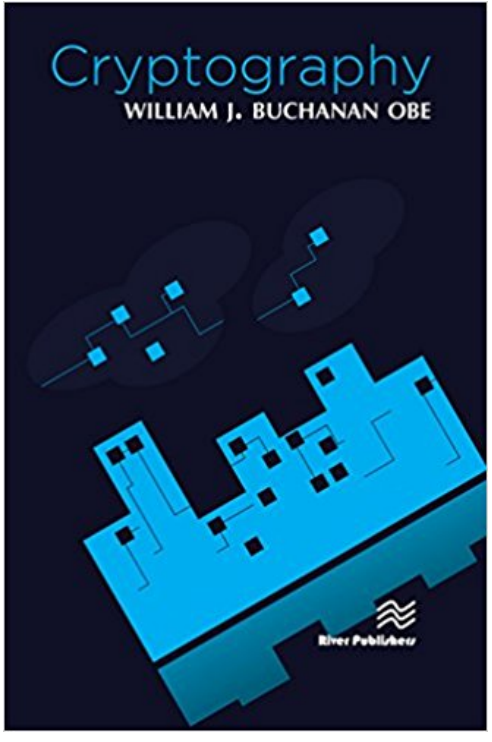


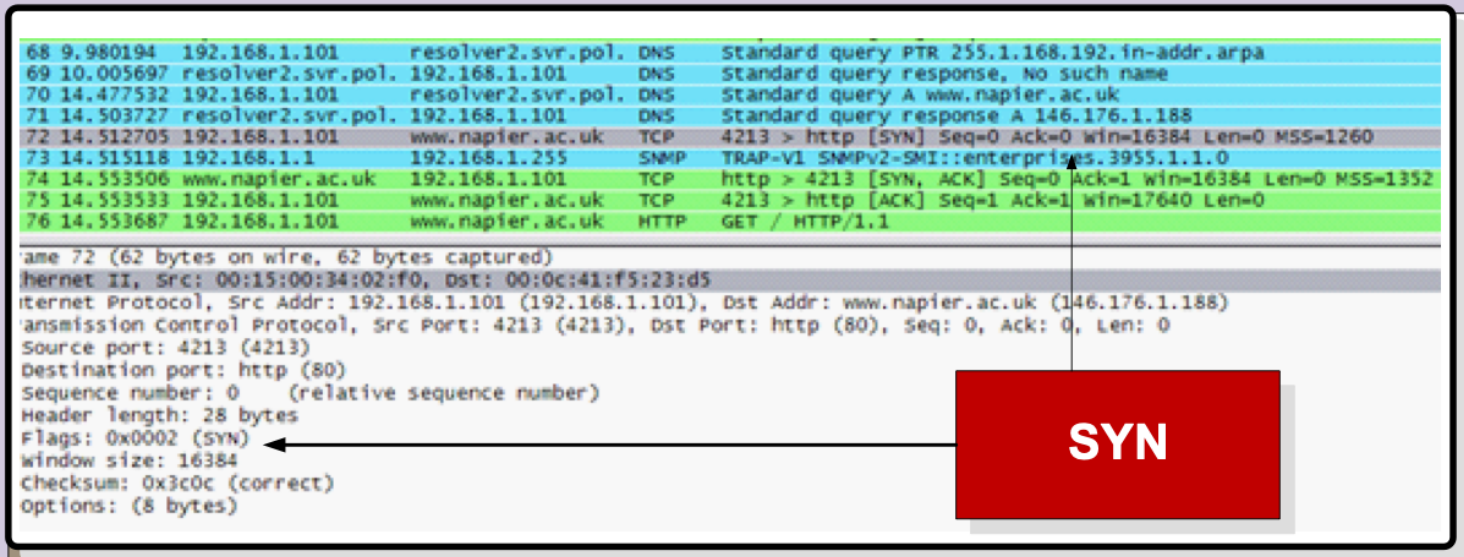
Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

http://asecuritysite.com/encryption
http://asecuritysite.com/unit06





Stateful fi

Network Security

www.napier.ac.uk?

DNS server

146.176.1.188

SYN
Src Port=4213, Dest Port=80

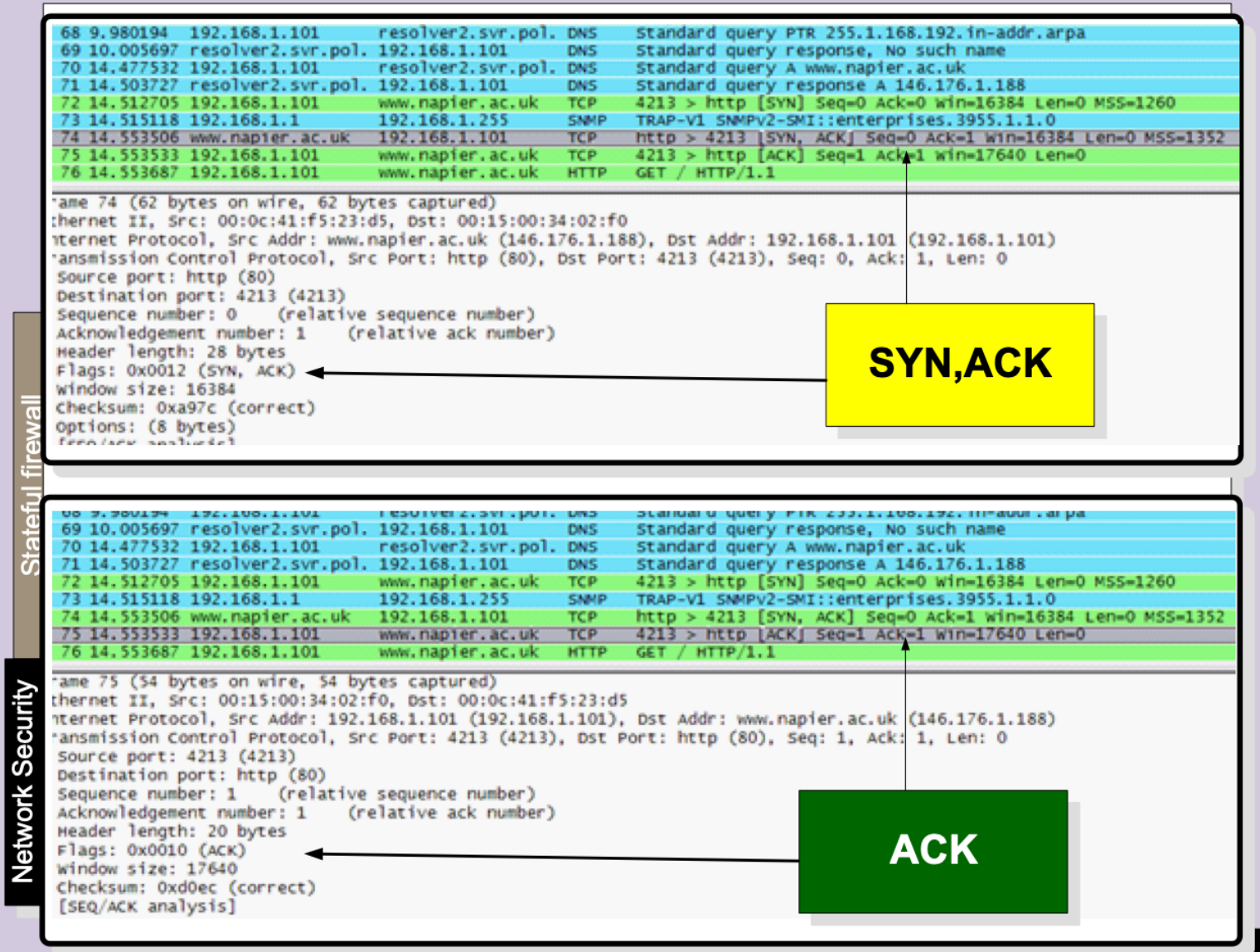
TCP port=4213

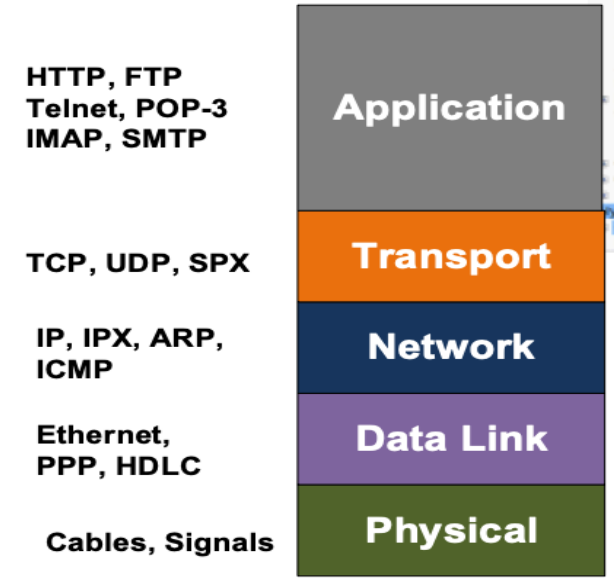
TCP port=80

192.168.1.101

146.176.1.188

Client-server (SYN)


Stateful firewall
68 9.980194 192.168.1.101 resolver2.svr.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.svr.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.svr.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.svr.pol. 192.168.1.101 DNS Standard query response A 146.176.1.188
72 14.512705 192.168.1.101 www.napier.ac.uk TCP 4213 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
73 14.515118 192.168.1.1 192.168.1.255 SNMP TRAP-V1 SNMPv2-SMI::enterprises.3955.1.1.0
74 14.553506 www.napier.ac.uk 192.168.1.101 TCP http > 4213 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1352
75 14.553533 192.168.1.101 www.napier.ac.uk TCP 4213 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
76 14.553687 192.168.1.101 www.napier.ac.uk HTTP GET / HTTP/1.1
ame 74 (62 bytes on wire, 62 bytes captured)
thernet II, Src: 00:0c:41:f5:23:d5, Dst: 00:15:00:34:02:f0
nternet Protocol, Src Addr: www.napier.ac.uk (146.176.1.188), Dst Addr: 192.168.1.101 (192.168.1.101)
ansmission Control Protocol, Src Port: http (80), Dst Port: 4213 (4213), Seq: 0, Ack: 1, Len: 0
Source port: http (80)
Destination port: 4213 (4213)
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 28 bytes
Flags: 0x0012 (SYN, ACK)
Window size: 16384
Checksum: 0xa97c (correct)
Options: (8 bytes)
SYN,ACK
Network Security
69 10.005697 resolver2.svr.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.svr.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.svr.pol. 192.168.1.101 DNS Standard query response A 146.176.1.188
72 14.512705 192.168.1.101 www.napier.ac.uk TCP 4213 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
73 14.515118 192.168.1.1 192.168.1.255 SNMP TRAP-V1 SNMPv2-SMI::enterprises.3955.1.1.0
74 14.553506 www.napier.ac.uk 192.168.1.101 TCP http > 4213 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1352
75 14.553533 192.168.1.101 www.napier.ac.uk TCP 4213 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
76 14.553687 192.168.1.101 www.napier.ac.uk HTTP GET / HTTP/1.1
ame 75 (54 bytes on wire, 54 bytes captured)
thernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
nternet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
ansmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
Source port: 4213 (4213)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x0010 (ACK)
Window size: 17640
Checksum: 0xd0ec (correct)
[SEQ/ACK analysis]
ACK

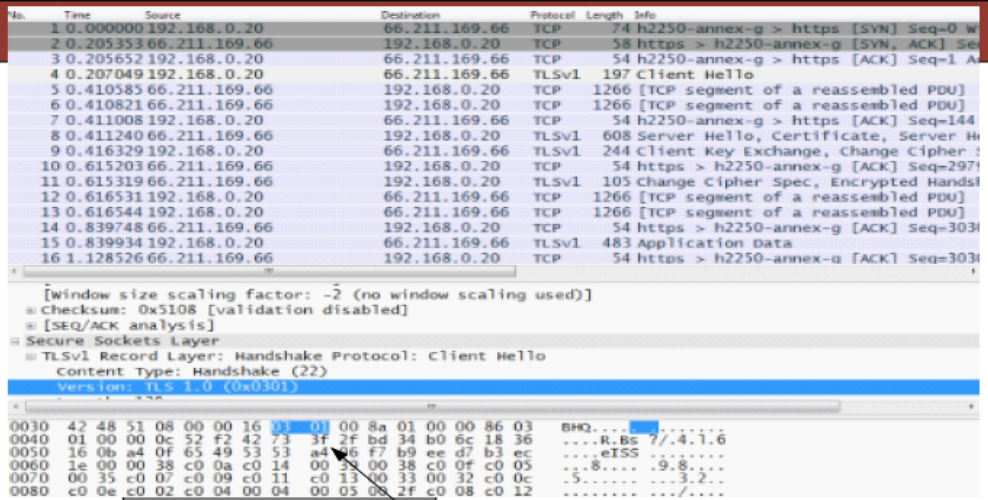


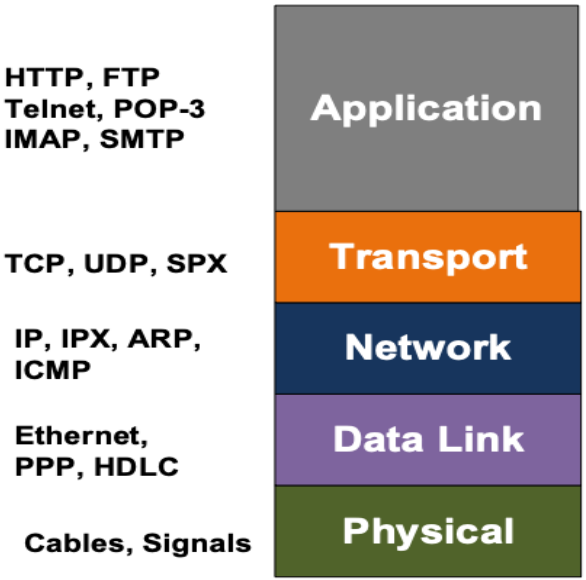

```
    4 0.000602 192.168.75.132      192.168.75.1      TCP      78 http > mgcp-gateway [SYN, ACK] Seq=0 Ack=1 W
    5 0.000681 192.168.75.1        192.168.75.132    TCP      66 mgcp-gateway > http [ACK] Seq=1 Ack=1 Win=66
    6 0.000835 192.168.75.1        192.168.75.132    HTTP    475 GET / HTTP/1.1
    7 0.055477 192.168.75.132      192.168.75.1      TCP    1514 [TCP segment of a reassembled PDU]

⊞ Destination: Vmware_0f:71:a3 (00:0c:29:0f:71:a3)
⊞ Source: Vmware_c0:00:08 (00:50:56:c0:00:08)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 461
  Identification: 0x011e (286)
⊞ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
⊞ Header checksum: 0xe036 [validation disabled]
  Source: 192.168.75.1 (192.168.75.1)
  Destination: 192.168.75.132 (192.168.75.132)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: mgcp-gateway (2427), Dst Port: http (80), Seq: 1, Ack: 1, Len: 409
  Source port: mgcp-gateway (2427)
  Destination port: http (80)
  [Stream index: 0]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 410    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
⊞ Flags: 0x018 (PSH, ACK)
  Window size value: 16652
  [Calculated window size: 66608]
  [Window size scaling factor: 4]
⊞ Checksum: 0xf834 [validation disabled]
⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
⊞ [SEQ/ACK analysis]
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.15 Version/10.01\r\n
```

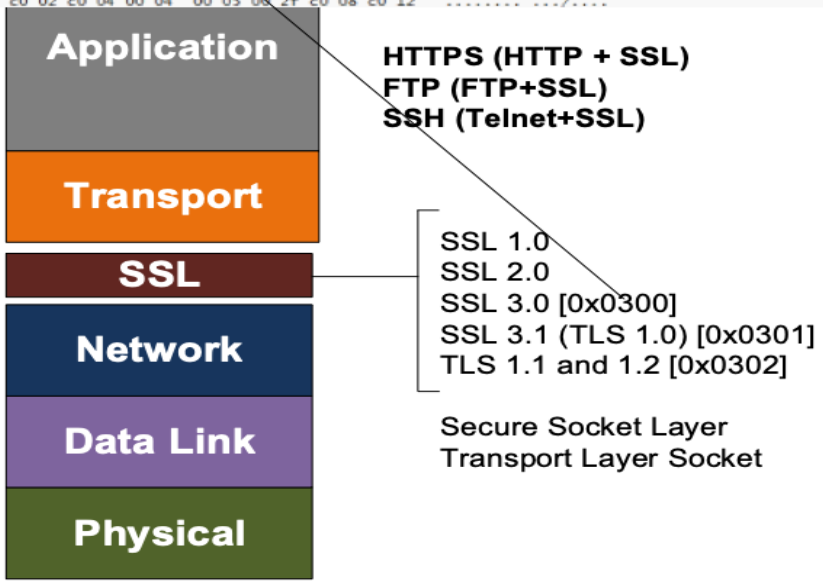
Author: Prof Bill Buchanan

Ports

HTTP	80	HTTPs	443
TELNET	23	SSH	22
SMTP	25	SMTPs	465
POP-3	110	POP-3s	995







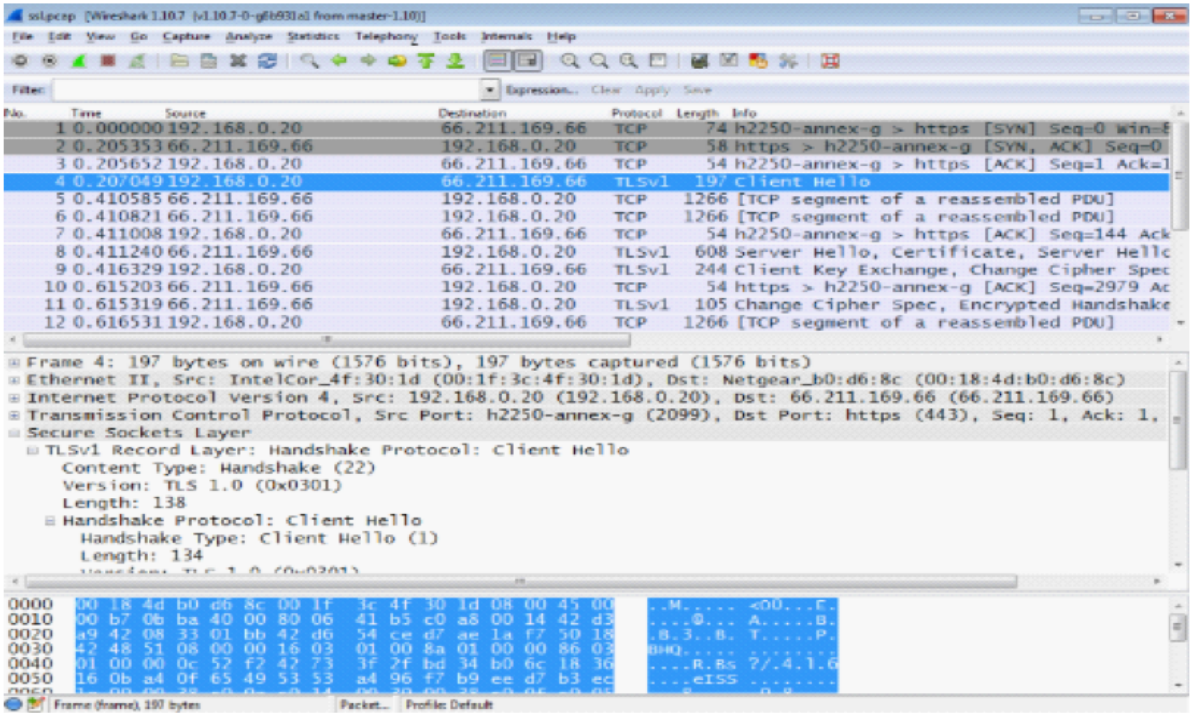
Author: Prof Bill Buchanan

TCP [SYN] to Port 443

TCP [SYN,ACK] from Port 443

TCP [ACK] to Port 443

Client Hello (Start of Handshake)



Application

Transport

SSL

Network

Data Link

Physical

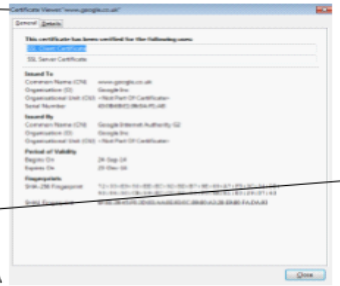
Author: Prof Bill Buchanan

192.168.0.20

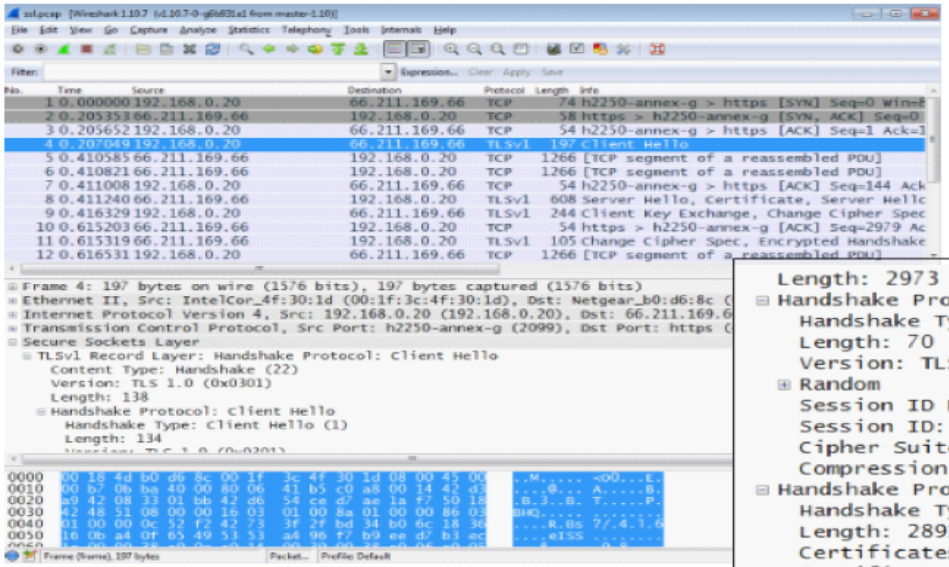
Client Hello

66.211.169.66

```
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 138
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 134
  Version: TLS 1.0 (0x0301)
  Random
  Session ID Length: 0
  Cipher Suites Length: 56
  Cipher Suites (28 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
```

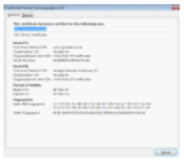


Server Hello



```
Length: 2973
Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 70
  Version: TLS 1.0 (0x0301)
  Random
  Session ID Length: 32
  Session ID: ed2175399c8f02d916e58afdbbd46317564a98a1d985632a...
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Compression Method: null (0)
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 2891
  Certificates Length: 2888
  Certificates (2888 bytes)
```

Author: Prof Bill Buchanan



192.168.0.20

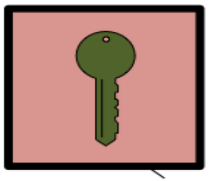
Client Hello

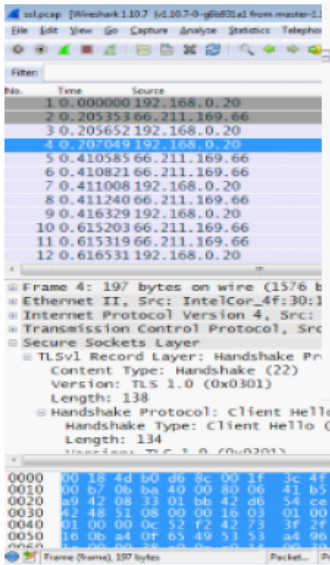
66.211.169.66

Server Hello

Client Key Exchange

Public key

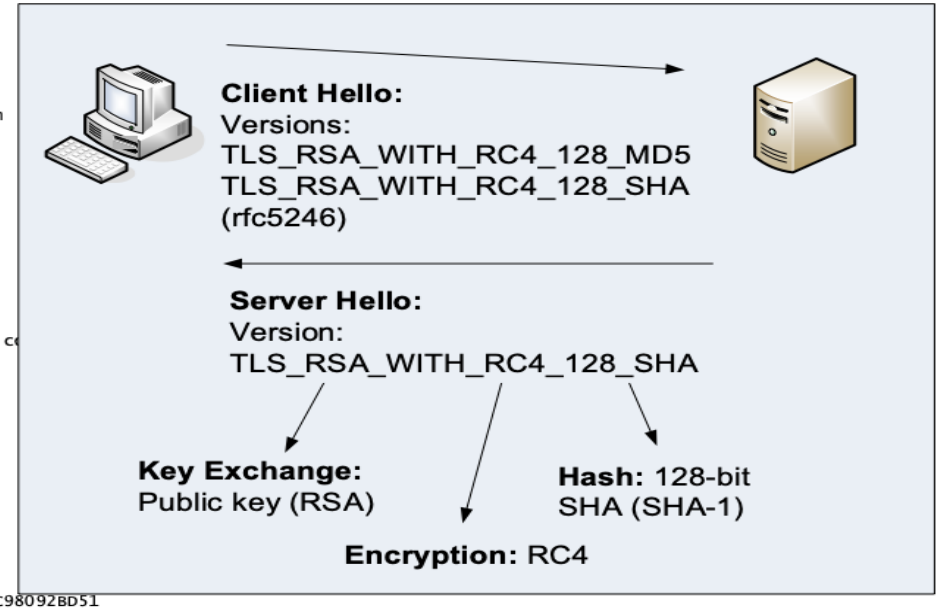




```
    [Window size scaling factor: -2 (no window scaling used)]
  ⊞ Checksum: 0x2a30 [validation disabled]
  ⊞ [SEQ/ACK analysis]
Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 134
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      ⊟ RSA Encrypted PreMaster Secret
          Encrypted PreMaster length: 128
          Encrypted PreMaster: 07d26b83aa8129bd8c48462627a1d3f67f34e2745959fce2...
  ⊟ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
```

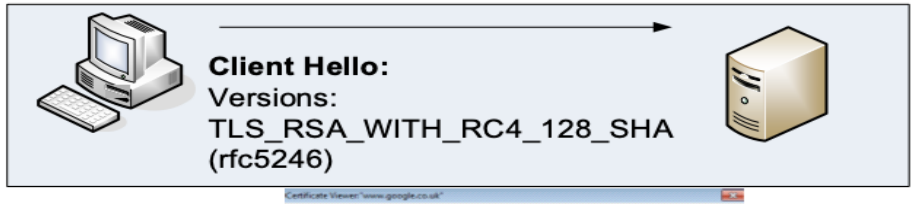
Author: Prof Bill Buchanan

```
billbuchanan@Bills-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIISVyALWN+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
---
SOx4I5L0D0jZYqKfJuImGcFwdIETqOEpCmkhJfGNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.c
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
---
SSL handshake has read 3719 bytes and written 446 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 9D92CEC32FA9F86C6D902081EE186C4FC68234FFF7B903D6621A86C98092BD51
    Session-ID-ctx:
    Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd   ...PS=.... ..S..
    0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db   .......V...6.V..
    0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97   +..V....4.r!.|..
    0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac   *.. .....W(:.g..
    0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84   }...m......@._..
    0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3   .;.........k6.W.
    0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02   .... ...k.Nz..m.
    0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25   0.....I.1k0....%
    0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45   b..3.%."2.T..v.E
    0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d   :`.....}..G )...
    00a0 - 6f 5a b4 f2                                       oZ..

    Start Time: 1413136351
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
```




```
TLS_RSA_WITH_AES_256_CBC_SHA256
Key: RSA Enc: AES_256_CBC  Hash: SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
Key ex: DH_DSS Enc: 3DES_EDE_CBC Hash: SHA
```

Author: Prof Bill Buchanan

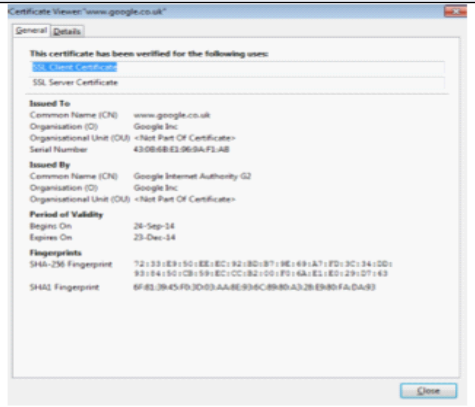


Server Hello:
Version:
TLS_RSA_WITH_RC4_128_SHA

Key Exchange:
Public key (RSA)

Encryption: RC4

Hash: 128-bit
SHA (SHA-1)



Session key

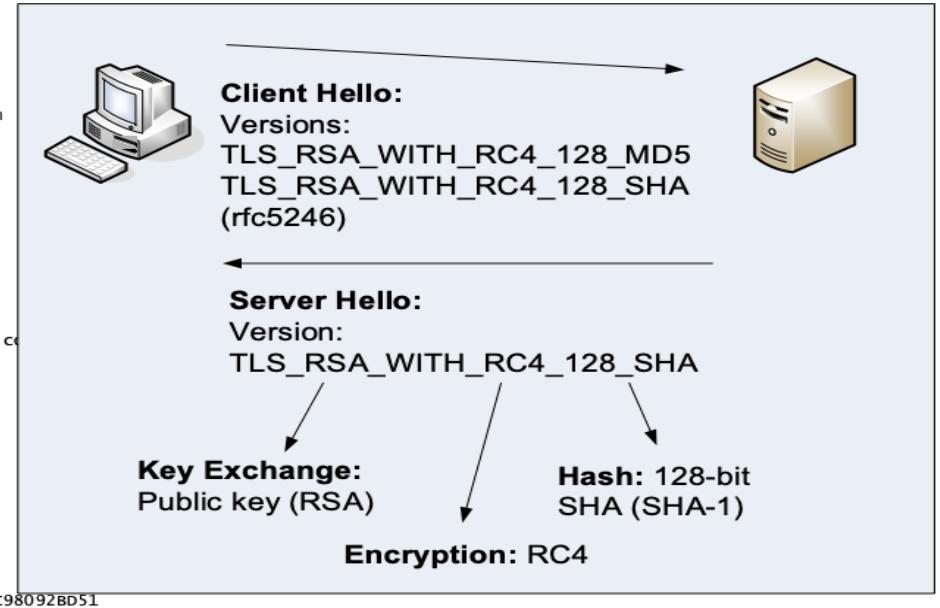
Public key

Private key

Tunnel created (RC4, Hash: SHA-1)

Author: Prof Bill Buchanan

```
billbuchanan@Bills-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIISVyALWN+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
---
SOx4I5L0D0jZYqKfJuImGcFwdIETqOEpCmkhJfGNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.c
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
---
SSL handshake has read 3719 bytes and written 446 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 9D92CEC32FA9F86C6D902081EE186C4FC68234FFF7B903D6621A86C98092BD51
    Session-ID-ctx:
    Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd   ...PS=.... ..S..
    0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db   .......V...6.V..
    0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97   +..V....4.r!.|..
    0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac   *.. .....W(:.g..
    0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84   }...m......@._..
    0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3   .;.........k6.W.
    0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02   .... ...k.Nz..m.
    0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25   0.....I.1k0....%
    0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45   b..3.%."2.T..v.E
    0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d   :`.....}..G )...
    00a0 - 6f 5a b4 f2                                       oZ..

    Start Time: 1413136351
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
```




```
TLS_RSA_WITH_AES_256_CBC_SHA256
Key: RSA Enc: AES_256_CBC  Hash: SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
Key ex: DH_DSS Enc: 3DES_EDE_CBC Hash: SHA
```

Author: Prof Bill Buchanan

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

while True:
  sock = socket.socket()
  sock.bind(('', 444))
  sock.listen(5)
  context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
  context.load_cert_chain(certfile="mycert.pem")
  context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1  # optional
  context.set_ciphers('AES256+ECDH:AES256+EDH')
  while True:
    conn = None
    ssock, addr = sock.accept()
    try:
      conn = context.wrap_socket(ssock, server_side=True)
      handle(conn)
    except ssl.SSLError as e:
      print(e)
    finally:
      if conn:
        conn.close()
```

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

while True:
  sock = socket.socket()
  sock.bind(('', 444))
  sock.listen(5)
  context = ssl.create_default_context(ssl.Purpose.CLI
  context.load_cert_chain(certfile="mycert.pem")
  context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1
  context.set_ciphers('AES256+ECDH:AES256+EDH')
  while True:
    conn = None
    ssock, addr = sock.accept()
    try:
      conn = context.wrap_socket(ssock, server_side=Tr
      handle(conn)
    except ssl.SSLError as e:
      print(e)
    finally:
      if conn:
        conn.close()
```

```
import socket, ssl


HOST, PORT = '10.214.0.96', 443

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

def main():

    sock = socket.socket(socket.AF_INET)

    context = ssl.create_default_context(ssl.Purpose.SERVER_AUTH)
    context.check_hostname = False
    context.verify_mode=ssl.CERT_NONE


    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1

    conn = context.wrap_socket(sock, server_hostname=HOST)

    try:
        conn.connect((HOST, PORT))
        handle(conn)
    finally:
        conn.close()

if __name__ == '__main__':
    main()
```

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

while True:
  sock = socket.socket()
  sock.bind(('', 444))
  sock.listen(5)
  context = ssl.create_default_conte
  context.load_cert_chain(certfile="
  context.options |= ssl.OP_NO_TLSv1
  context.set_ciphers('AES256+ECDH:A
  while True:
    conn = None
    ssock, addr = sock.accept()
    try:
      conn = context.wrap_socket(sso
      handle(conn)
    except ssl.SSLError as e:
      print(e)
    finally:
      if conn:
        conn.close()
```

```
import socket, ssl
```

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
8	0.002270000	10.221.0.7	10.221.0.7	TLSv1.2	1364	Server Hello, Certificate, Se
9	0.002277000	10.221.0.7	10.221.0.7	TCP	66	60770 > https [ACK] Seq=279 A
10	0.003070000	10.221.0.7	10.221.0.7	TLSv1.2	192	Client Key Exchange, Change C
11	0.003530000	10.221.0.7	10.221.0.7	TLSv1.2	308	New Session Ticket, Change Ci
12	0.003693000	10.221.0.7	10.221.0.7	TLSv1.2	110	Application Data
13	0.003714000	10.221.0.7	10.221.0.7	TLSv1.2	110	Application Data
14	0.004240000	10.221.0.7	10.221.0.7	TCP	66	60770 > https [FIN, ACK] Seq=
15	0.041712000	10.221.0.7	10.221.0.7	TCP	66	https > 60770 [ACK] Seq=1585

```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 62
    Version: TLS 1.2 (0x0303)
  ⊞ Random
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 22
  ⊞ Extension: renegotiation_info
```

```
0060  d3 e6 2a 6c fd cf 62 3f  47 fc 8d d3 8e 00 c0 30   ..*l..b? G.....0
0070  00 00 16 ff 01 00 01 00  00 0b 00 04 03 00 01 02   ........ ........
0080  00 23 00 00 00 0f 00 01  01 16 03 03 03 6b 0b 00   .#...... .....k..
0090  03 67 00 03 64 00 03 61  30 82 03 5d 30 82 02 45   .g..d..a 0..]0..E
00a0  a0 03 02 01 02 02 09 00  83 74 d7 0e 41 d4 ac 8e   ........ .t..A...
```

```
if __name__ == '__main__':
    main()
```

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla

August 2018

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla
August 2018

The Transport Layer Security (TLS)

Abstract

This document specifies version 1.3 of t
(TLS) protocol. TLS allows client/serve
over the Internet in a way that is desig
tampering, and message forgery.

This document updates RFCs 5705 and 6066
5246, and 6961. This document also spec
TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track docu

This document is a product of the Interr
(IETF). It represents the consensus of
received public review and has been appr
Internet Engineering Steering Group (IES
Internet Standards is available in Secti

Information about the current status of
and how to provide feedback on it may be
https://www.rfc-editor.org/info/rfc8446.

Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates

Marc Fischlin Felix Günther

Cryptoplexity, Technische Universität Darmstadt, Germany
marc.fischlin@cryptoplexity.de, guenther@cs.tu-darmstadt.de

February 2, 2017

Abstract. We investigate security of key exchange protocols supporting so-called zero round-trip time (0-RTT), enabling a client to establish a fresh provisional key without interaction, based only on cryptographic material obtained in previous connections. This key can then be already used to protect early application data, transmitted to the server before both parties interact further to switch to fully secure keys. Two recent prominent examples supporting such 0-RTT modes are Google's QUIC protocol and the latest drafts for the upcoming TLS version 1.3.

We are especially interested in the question how replay attacks, enabled through the lack of contribution from the server, affect security in the 0-RTT case. Whereas the first proposal of QUIC uses state on the server side to thwart such attacks, the latest version of QUIC and TLS 1.3 rather accept them as inevitable. We analyze what this means for the key secrecy of both the preshared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie–Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

Replayable 0-RTT data presents a number of security threats to TLS-using applications, unless those applications are specifically engineered to be safe under replay (minimally, this means idempotent, but in many cases may also require other stronger conditions, such as constant-time response). Potential attacks include:

- Duplication of actions which cause side effects (e.g., purchasing an item or transferring money) to be duplicated, thus harming the site or the user.

- Attackers can store and replay 0-RTT messages in order to re-order them with respect to other messages (e.g., moving a delete to after a create).

- Exploiting cache timing behavior to discover the content of 0-RTT messages by replaying a 0-RTT message to a different cache node and then using a separate connection to measure request latency, to see if the two requests address the same resource.

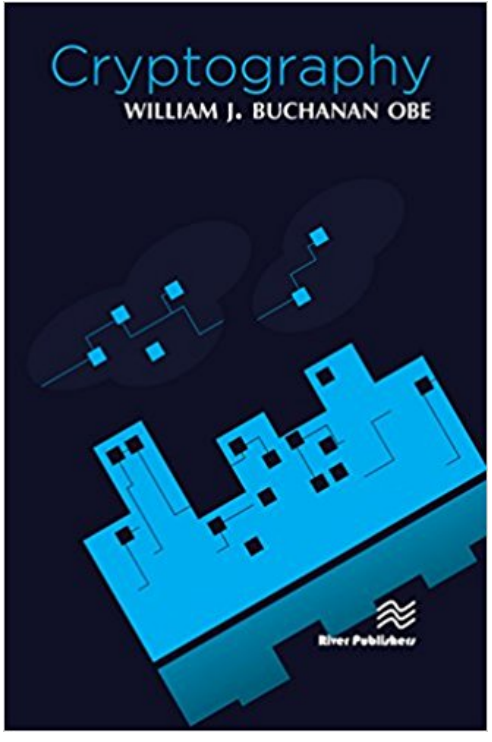
inevitable. We analyze what this means for the key secrecy of both the preshared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie–Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

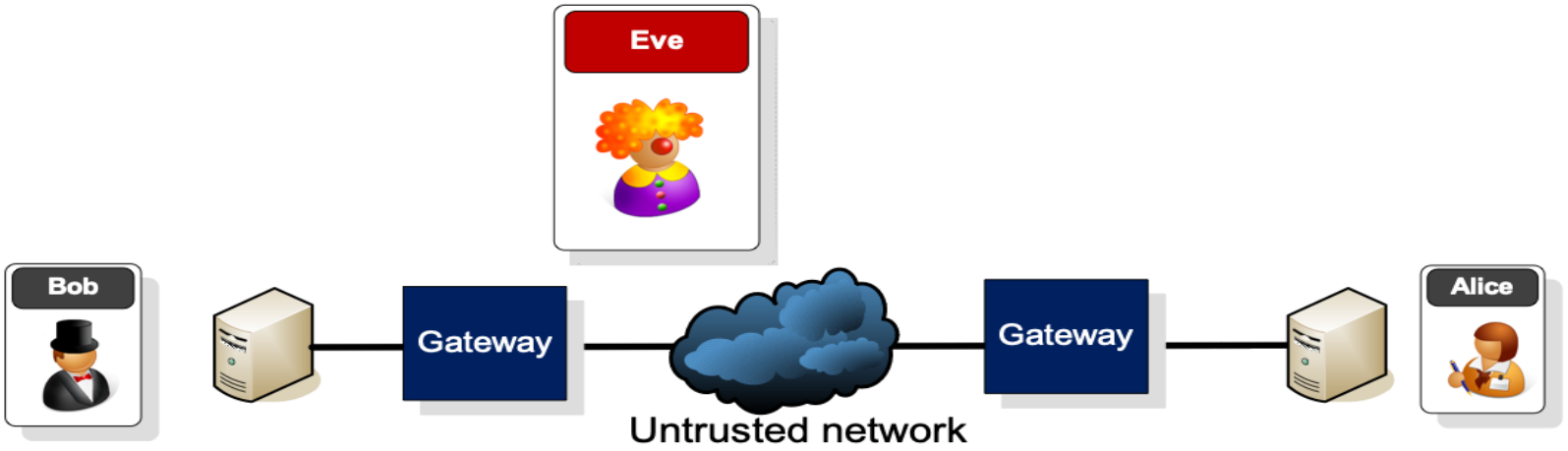
Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

http://asecuritysite.com/encryption
http://asecuritysite.com/unit06





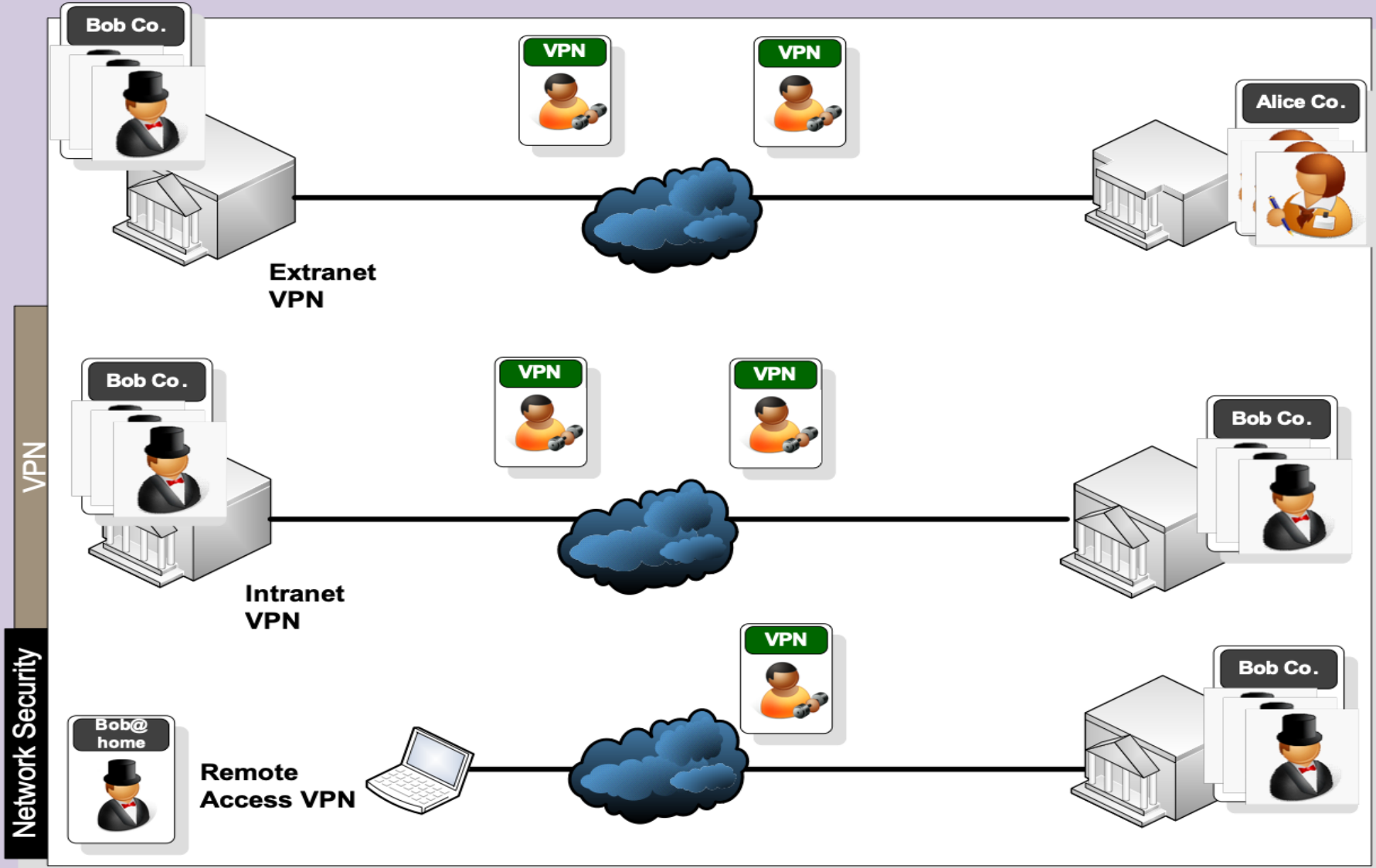
What is required is:

- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

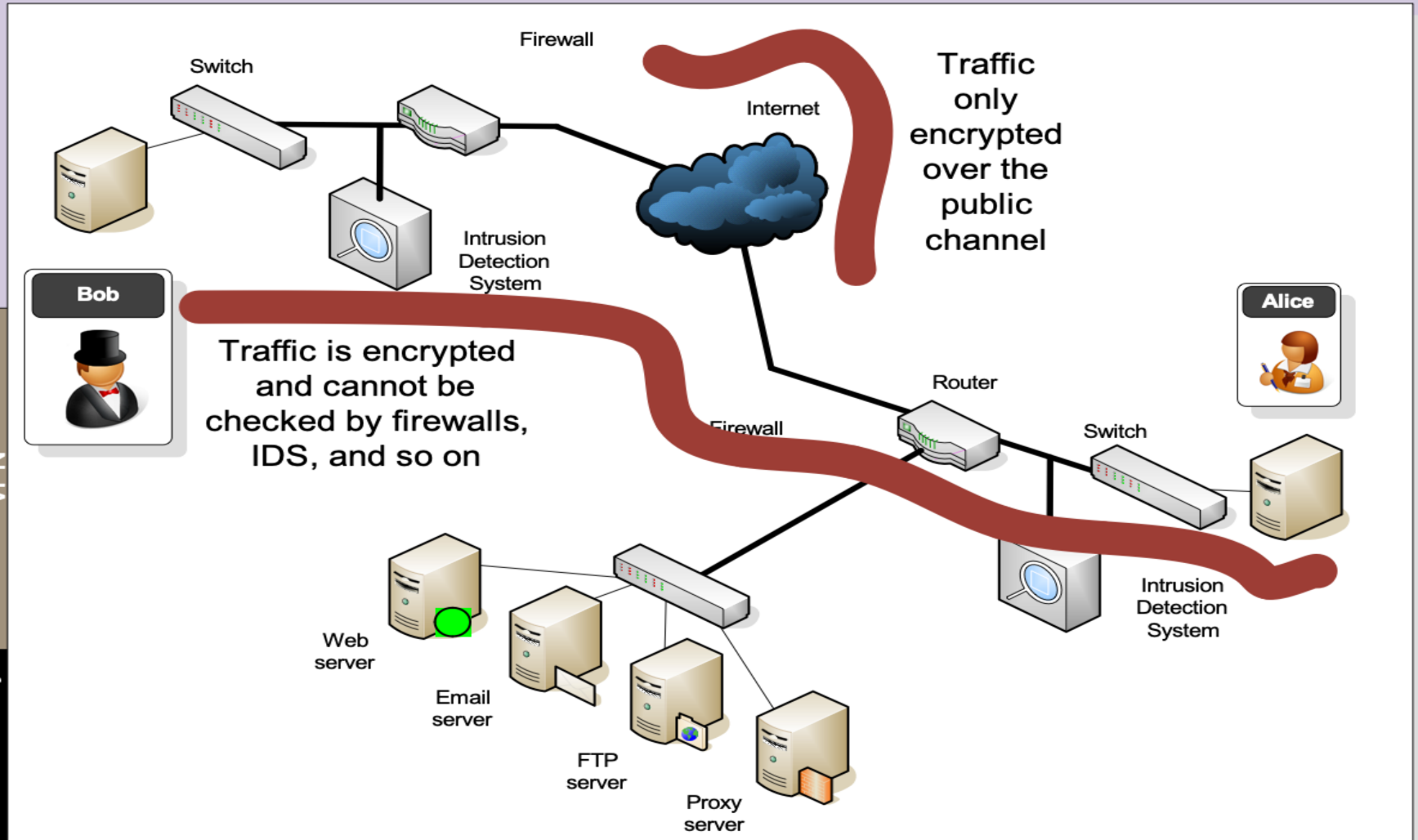
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

L2TP (Layer 2 Tunneling Protocol). Works at Layer 2 to Forward IP, IPX and AppleTalk (RFC2661). Cisco, Microsoft, Ascent and 3Com developed it. User and machine authentication, but no encryption (but can be used with L2TP over IPSec).

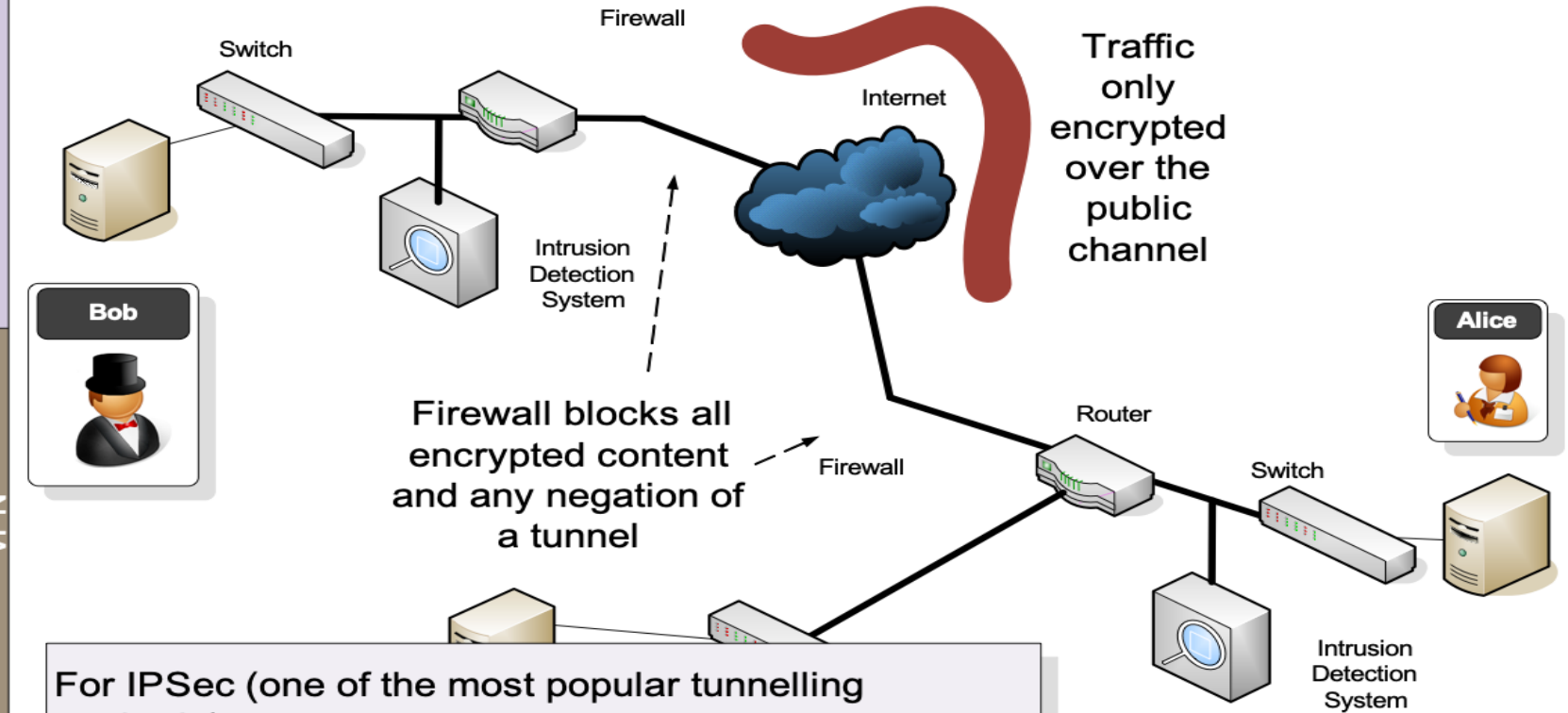
IPSec. An open standard. Includes both encryption and Authentication.


Bob Co.
VPN
VPN
Alice Co.
Extranet
VPN
Bob Co.
VPN
VPN
Bob Co.
Intranet
VPN
VPN
Bob@
home
Remote
Access VPN
Bob Co.
VPN
Network Security

VPN types



Tunnelling mode or transport mode

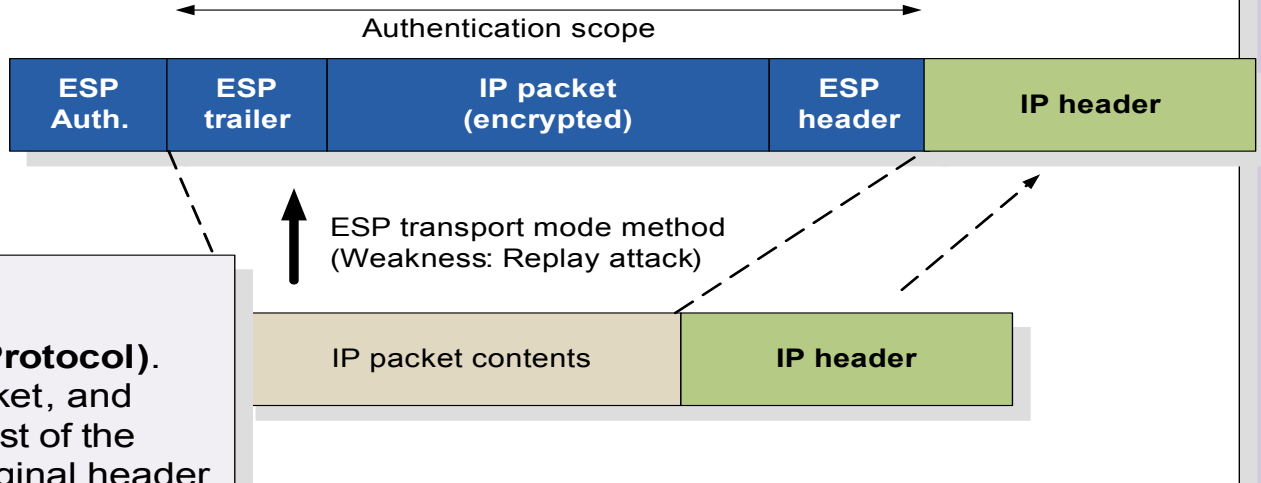


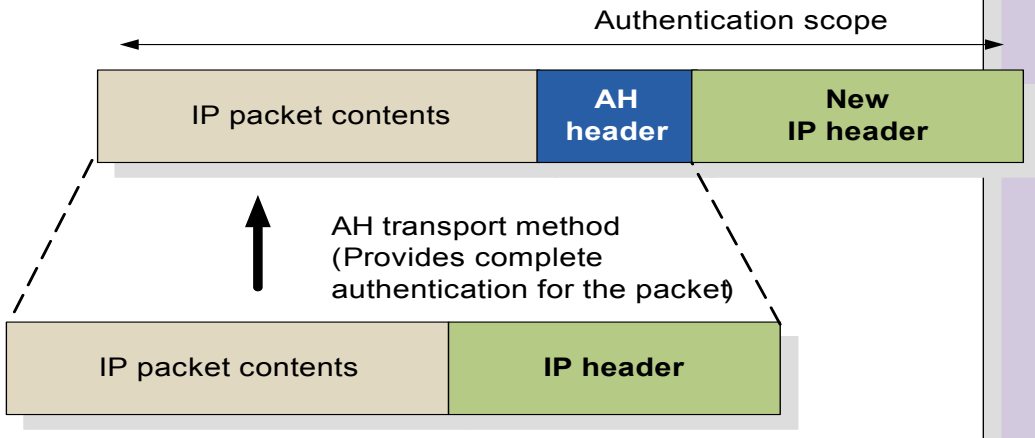
For IPSec (one of the most popular tunnelling methods):

- UDP Port 500 is the key exchange port. If it is blocked there can be no tunnel.
- TCP Port 50 for IPSec ESP (Encapsulated Security Protocol).
- TCP Port 51 for IPSec AH (Authentication Header)

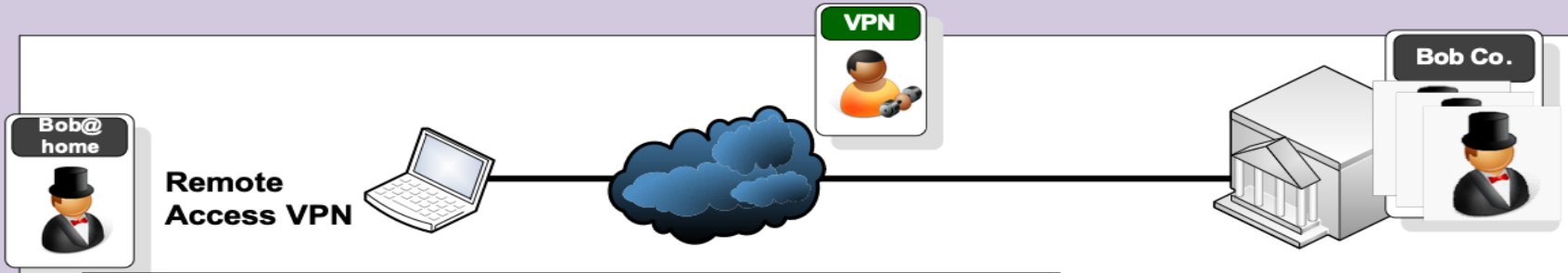
The IPSec protocol has:

- **ESP (Encapsulated Security Protocol)**. ESP takes the original data packet, and breaks off the IP header. The rest of the packet is encrypted, with the original header added at the start, along with a new ESP field at the start, and one at the end. It is important that the IP header is not encrypted as the data packet must still be read by routers as it travels over the Internet. Only the host at the other end of the IPSec tunnel can decrypt the contents of the IPSec data packet.
- **AH (Authentication Header)**. This encrypts the complete contents of the IP data packet, and adds a new packet header. ESP has the weakness that an intruder can replay previously sent data, whereas AH provides a mechanism of sequence numbers to reduce this problem.





1 ICMP Internet Control Message [RFC792]
6 TCP Transmission Control [RFC793]
8 EGP Exterior Gateway Protocol [RFC888]
9 IGP any private interior gateway [IANA]
47 GRE General Routing Encapsulation
(PPTP)
50 ESP Encap Security Payload [RFC2406]
51 AH Authentication Header [RFC2402]
55 MOBILE IP Mobility
88 EIGRP EIGRP [CISCO]
89 OSPFIGP OSPFIGP [RFC1583]
115 L2TP Layer Two Tunneling Protocol



Phase 1 (IKE – Internet Key Exchange)

UDP port 500 is used for IKE

Define the policies between the peers

IKE Policies

- Hashing algorithm (SHA/MD5)
- Encryption (DES/3DES)
- Diffie-Hellman agreements
- Authentication (pre-share, RSA nonces, RSA sig).

```
isakmp enable outside
isakmp key AB&FDD address 176.16.0.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 5 authen pre-share
isakmp policy 5 encrypt des
isakmp policy 5 hash sha
isakmp policy 5 group 1
isakmp policy 5 lifetime 86400
sysopt connection permitipsec
```

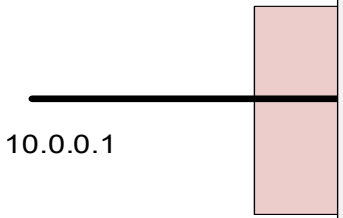
Phase 2

Defines the policies for transform sets, peer IP addresses/hostnames and lifetime settings.

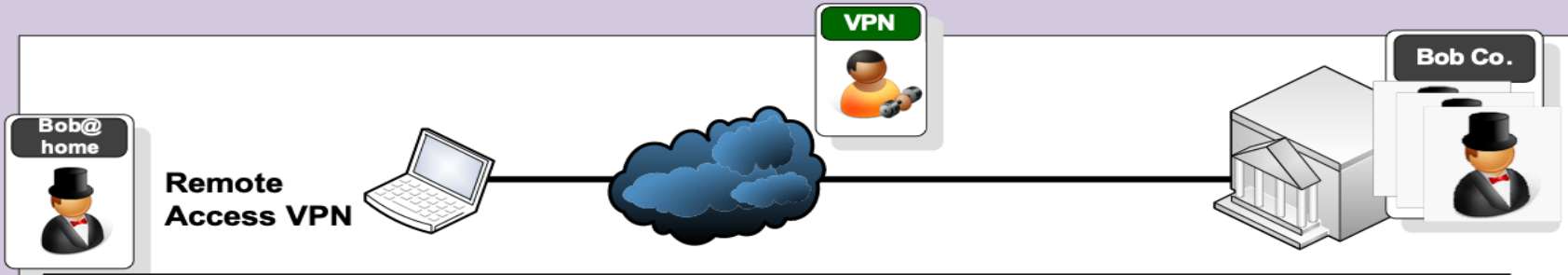
Crypto maps are exchanged

- AH, ESP (or both)
- Encryption (DES, 3DES)
- ESP (tunnel or transport)
- Authentication (SHA/MD5)
- SA lifetimes defined
- Define the traffic of interest

```
crypto ipsec transform-set MYIPSECFORMAT esp-des esp-sha-hmac
crypto map MYIPSEC 10 ipsec-isakmp
access-list 111 permit ip 10.0.0.0  255.255.255.0  176.16.0.0
255.255.255.0
crypto map MYIPSEC 10 match address 111
crypto map MYIPSEC 10 set peer 176.16.0.2
crypto map MYIPSEC 10 set transform-set MYIPSECFORMAT
crypto map MYIPSEC interface outside
```




```
No.     Time        Source                Destination           Protocol Info
81 5.237402    192.168.0.3           146.176.210.2         ISAKMP   Aggressive

Frame 81 (918 bytes on wire, 918 bytes captured)
Ethernet II, Src: IntelCor_34:02:f0 (00:15:20:34:62:f0), Dst: Netgear_b0:d6:8c
(00:18:4d:b0:d6:8c)
Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 146.176.210.2 (146.176.210.2)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
    Source port: isakmp (500)
    Destination port: isakmp (500)
    Length: 884
    Checksum: 0xd89d [correct]
Internet Security Association and Key Management Protocol
    Initiator cookie: 5ABABE2D49A2D42A
    Responder cookie: 0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Aggressive (4)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 860
    Security Association payload
        Next payload: Key Exchange (4)
        Payload length: 556
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
        Proposal payload # 1
            Next payload: NONE (0)
            Payload length: 544
            Proposal number: 1
            Protocol ID: ISAKMP (1)
            SPI Size: 0
            Proposal transforms: 14
            Transform payload # 1
                Next payload: Transform (3)
                Payload length: 40
                Transform number: 1
                Transform ID: KEY_IKE (1)
                Encryption-Algorithm (1): AES-CBC (7)
                Hash-Algorithm (2): SHA (2)
                Group-Description (4): Alternate 1024-bit MODP group (2)
                Authentication-Method (3): XAUTHInitPreShared (65001)
                Life-Type (11): Seconds (1)
                Life-Duration (12): Duration-Value (2147483)
                Key-Length (14): Key-Length (256)
```

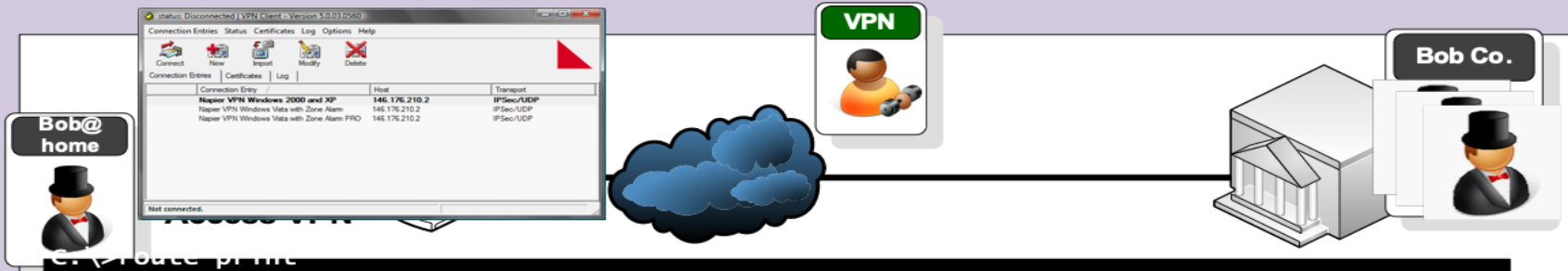



```
C:\>route print
===========================================================================
Interface List
 10 ...00 1d 09 3f 49 8d ......  Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ......  Intel(R) PRO/Wireless 3945ABG Network Connection

  1 ...........................  Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.0.1    192.168.0.3     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.0.0    255.255.255.0         On-link    192.168.0.3    281
      192.168.0.3  255.255.255.255         On-link    192.168.0.3    281
    192.168.0.255  255.255.255.255         On-link    192.168.0.3    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.0.3    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.0.3    281
===========================================================================
Persistent Routes:
  None
```

VPN

Network Security

Before connecting to the VPN

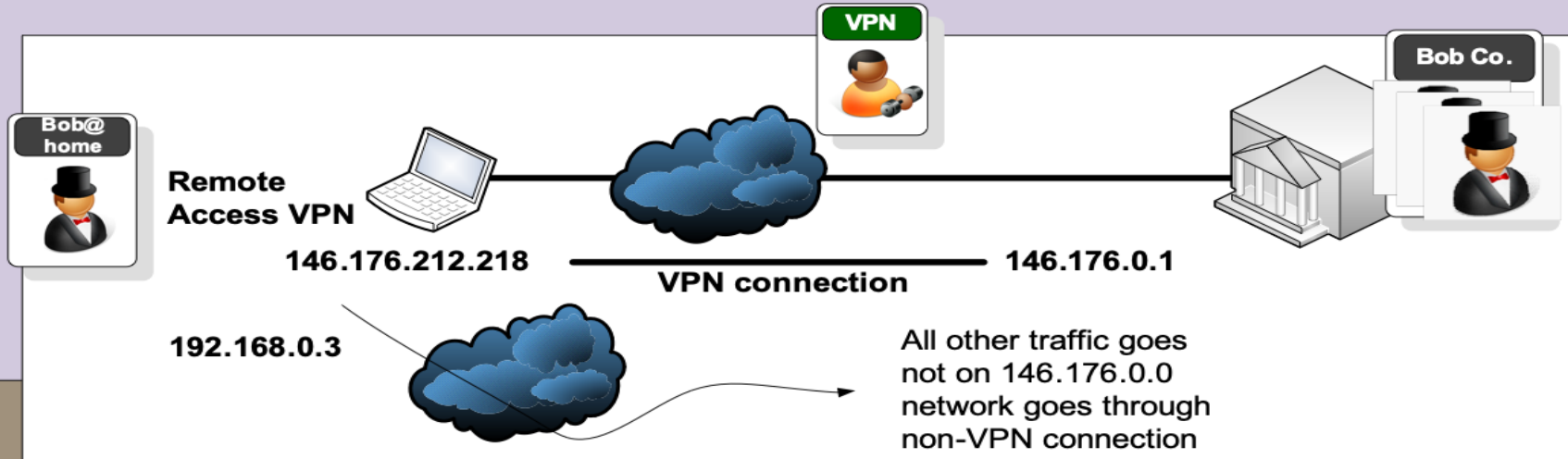



```
===========================================================================
Interface List
 21 ...00 05 9a 3c 78 00 ......Cisco Systems VPN Adapter
 10 ...00 1d 09 3f 49 8d ......Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ......Intel(R) PRO/Wireless 3945ABG Network Connectio
  1 ...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      192.168.0.3      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
      146.176.0.0      255.255.0.0         On-link   146.176.212.218     281
      146.176.1.0    255.255.255.0      146.176.0.1   146.176.212.218     100
      146.176.2.0    255.255.255.0      146.176.0.1   146.176.212.218     100
...
    146.176.210.2  255.255.255.255      192.168.0.1      192.168.0.3     100
    146.176.211.0    255.255.255.0      146.176.0.1   146.176.212.218     100
  146.176.212.218  255.255.255.255         On-link   146.176.212.218     281
...
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link      192.168.0.3      281
  255.255.255.255  255.255.255.255         On-link   146.176.212.218     281
===========================================================================
Persist
```

VPN

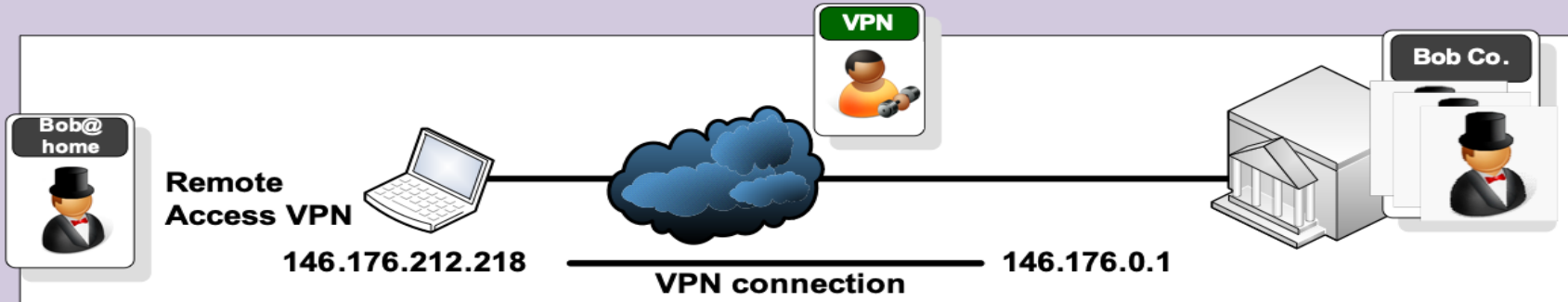
Network Security

After connecting to the VPN




```
===========================================================================
Interface List
 21 ...00 05 9a 3c 78 00 ......  Cisco Systems VPN Adapter
 10 ...00 1d 09 3f 49 8d ......  Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ......  Intel(R) PRO/Wireless 3945ABG Network Connectio

  1 ...........................  Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      192.168.0.3      25
        127.0.0.0        255.0.0.0         On-link        127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1     306
      146.176.0.0      255.255.0.0         On-link   146.176.212.218     281
      146.176.1.0    255.255.255.0      146.176.0.1   146.176.212.218     100
      146.176.2.0    255.255.255.0      146.176.0.1   146.176.212.218     100
...
===========================================================================
Persist
```

After connecting to the VPN




```
C:\>tracert www.napier.ac.uk

Tracing route to www.napier.ac.uk [146.176.222.174]
over a maximum of 30 hops:

  1     2 ms     2 ms     6 ms  192.168.0.1
  2    36 ms    38 ms    38 ms  cr0.escra.uk.easynet.net [87.87.249.224]
  3    31 ms    31 ms    30 ms  ip-87-87-146-129.easynet.co.uk [87.87.146.129]
  4    43 ms    43 ms    43 ms  be2.er10.thlon.ov.easynet.net [195.66.224.43]
  5    48 ms    45 ms    45 ms  linx-gw1.ja.net [195.66.224.15]
  6    45 ms    44 ms    45 ms  so-0-1-0.lond-sbr4.ja.net [146.97.35.129]
  7    49 ms    79 ms    49 ms  so-2-1-0.leed-sbr1.ja.net [146.97.33.29]
  8    58 ms    56 ms    56 ms  EastMAN-E1.site.ja.net [146.97.42.46]
  9    59 ms    57 ms    57 ms  vlan16.s-pop2.eastman.net.uk [194.81.56.66]
 10    57 ms    59 ms    58 ms  gi0-1.napier-pop.eastman.net.uk [194.81.56.46]
 11
```

Before VPN connection

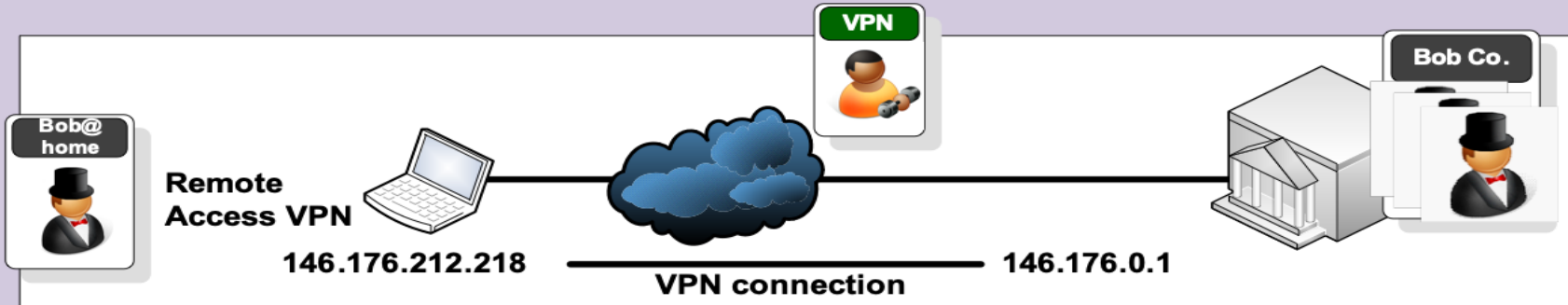
```
C:\>tracert www.napier.ac.uk

Tracing route to www.napier.ac.uk [146.176.222.174]
over a maximum of 30 hops:

  1    57 ms    58 ms    57 ms  146.176.210.2
  2    58 ms    56 ms    57 ms  www.napier.ac.uk [146.176.222.174]
  3    58 ms    59 ms    56 ms  www.napier.ac.uk [146.176.222.174]
```

After VPN connection

VPN

Network Security

Traceroute for VPN




```
C:\>tracert www.intel.com

Tracing route to a961.g.akamai.net [90.223.246.33]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.0.1
  2    35 ms    43 ms    36 ms  cr0.escra.uk.easynet.net [87.87.249.224]
  3    32 ms    31 ms    32 ms  ip-87-87-146-129.easynet.co.uk [87.87.146.129]
  4    46 ms    45 ms    45 ms  te7-0-0.sr0.enlcs.ov.easynet.net [89.200.132.109]
  5    46 ms    47 ms    47 ms  5adff621.bb.sky.com [90.223.246.33]
```

Before VPN connection

```
C:\>tracert www.intel.com

Tracing route to a961.g.akamai.net [90.223.246.33]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.0.1
  2    35 ms    43 ms    36 ms  cr0.escra.uk.easynet.net [87.87.249.224]
  3    32 ms    31 ms    32 ms  ip-87-87-146-129.easynet.co.uk [87.87.146.129]
  4    46 ms    45 ms    45 ms  te7-0-0.sr0.enlcs.ov.easynet.net [89.200.132.109]
  5    46 ms    47 ms    47 ms  5adff621.bb.sky.com [90.223.246.33]
```

After VPN connection

Traceroute for VPN

Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

http://asecuritysite.com/encryption
http://asecuritysite.com/unit06