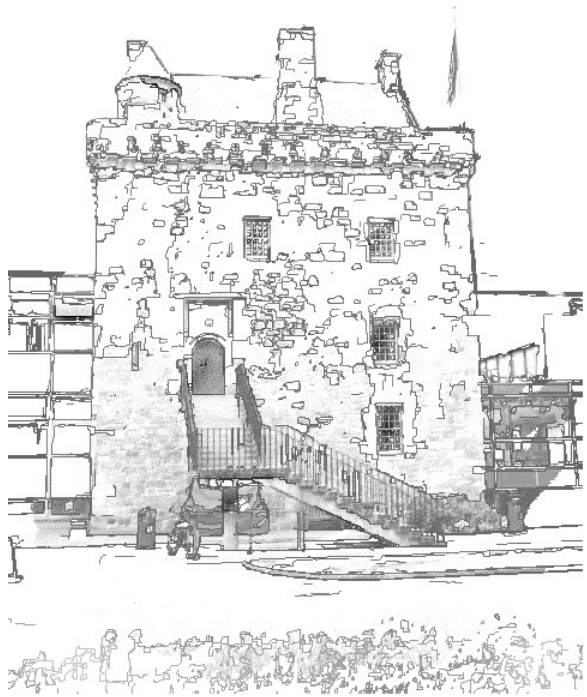
Symposium on Intelligence in Security and Forensic Computing



Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Centre for Mobile Computing and Security

Application Layer Covert Channels

Zbigniew Kwecka
Matric No. 03008457
BSc (HONS) Networked Computing

Supervised by:
Prof. William Buchanan

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

- HND Electronics – Telecommunication
- HND Electronics – Computer Technologies
- Senior Debug Technician (Electronics)
- Cisco Certified Networking Professional
- BSc(HONS) Networked Computing - 4th year

CCNP CISCO CERTIFIED®

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Centre for Mobile Computing and Security

Application Layer Covert Channels

Internet allows heterogeneous systems from around the World to communicate.

Its protocol stack was designed to be as universal as possible.

This allowed for rapid Internet application development.

Trade off: SECURITY

Aim: <u>To investigate Application Layer Data hiding, with special focus on the detection of covert communication.</u>

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

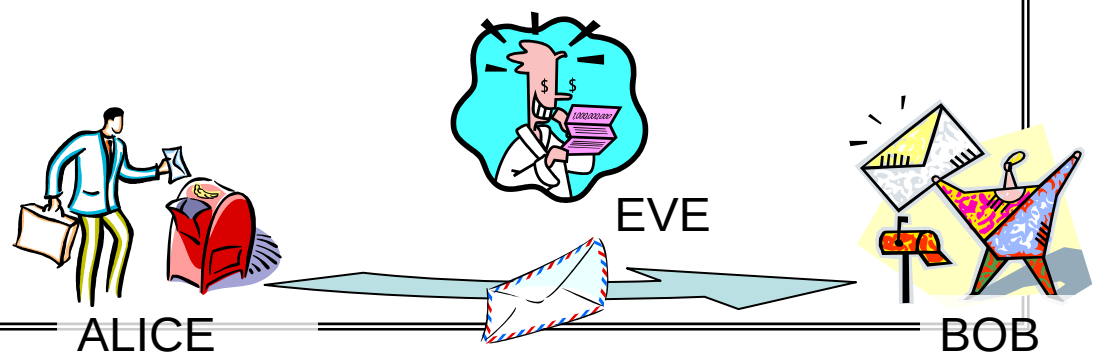
Covert Channel:

"Any communication channel that can be exploited … to transfer information in a manner that violates the systems' security policy" (Rogers, 2004, pp. 3).

"Anything that can be changed by one and seen by another can be used to send data" (Kaminsky)

Classification:

- Storage and Timing
- Noisy and Noiseless
- Aggregated and not-aggregated



Centre for Mobile Computing and Security

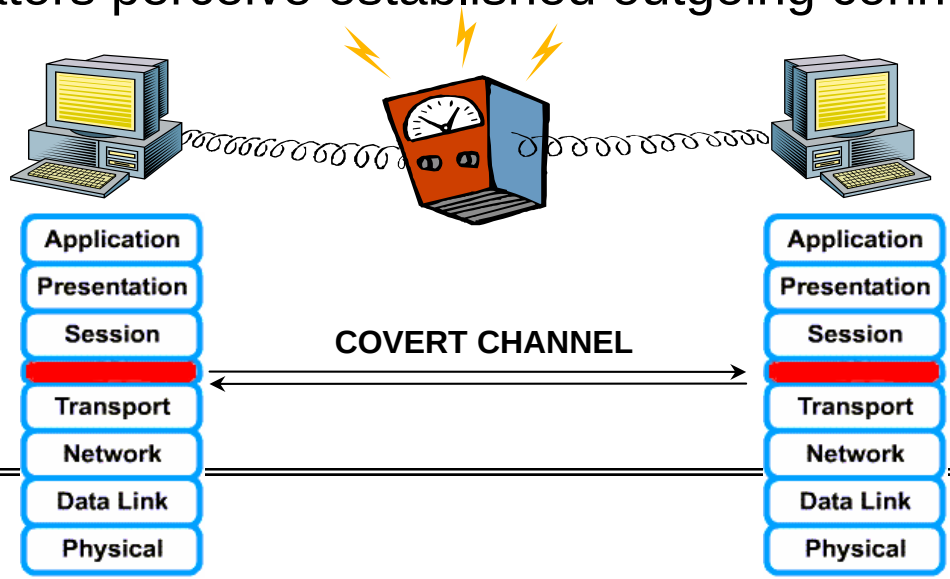
INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

Application Layer:

- Data hiding in lower layers of TCP/IP has been under investigation for a number of years now
- Ways of securing the networks from low level access exist
- Data payload scanners implemented in the security software usually filter only the genuine communication channels
- Administrators perceive established outgoing connections as harmless



Application Layer Covert Channels

Application Layer Envelope

TCP/IP

- Application
- Transport
- Internet
- Network

OSI

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Centre for Mobile Computing and Security

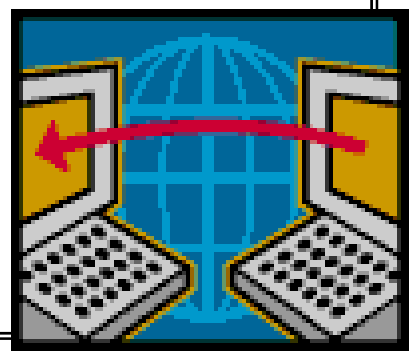
Application Layer Covert Channels

Most vulnerable protocols:

HTTP:
- World Wide Web traffic
- Various auto-updates and feedback software
- Tunnels for other protocols (Firepass, HTTunel, Corkscrew, etc)

DNS:
- Domain name translation
- DNS Spoofing
- Tunnels: NSTX, Ozyman, VoiceOverDNS
- Covert channels used by botnets and malware

SMTP:
- Mail exchange protocol
- Similar to both HTTP and DNS in operation
- Slower and subject to logging



Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Methods and techniques will apply to SMTP and DNS as well

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Request / Response Line

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Request Method

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Request Path

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Request Version

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Message Header

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Header Name

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

HTTP:

- Fast
- Relatively easy to investigate, implement and test
- Very similar to SMTP and DNS

How does it work:

- Request-Response architecture
- Client initiates the connection

HTTP Envelope:

```
GET /home.html HTTP/1.1
Host: www.bbc.com
```

Header Value

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

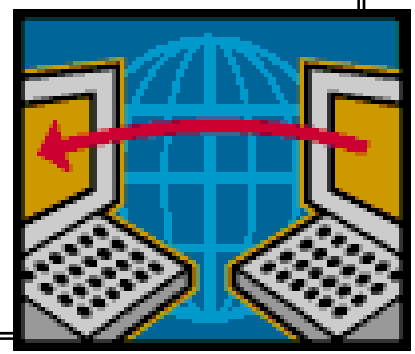
Application Layer Covert Channels

Ways to implement covert channels:

- Reordering
- Case Changing
- Optional Headers/Values/Flags
- New Header
- Linear spacing characters
- Modifying server object

Detection:

- Protocol-based
- Signature-based
- Behaviour-based



Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

Ways to implement covert channels:

- Reordering, Example

1st Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

2nd Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Connection: Keep-Alive
Host: www.bbc.com
```

Application Layer Covert Channels

Ways to implement covert channels:

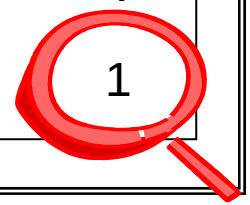
- Reordering, Example

1st Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

2nd Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Connection: Keep-Alive
Host: www.bbc.com
```



Application Layer Covert Channels

Ways to implement covert channels:

- Case Changing, Example

Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
ConnECtIon: Keep-Alive
```

Application Layer Covert Channels

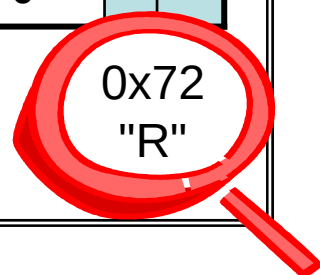
Ways to implement covert channels:

- Case Changing, Example

Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
ConnECtIon: Keep-Alive
```

Letter	C	o	n	n	E	C	t	I	o	n
Hex	0x43	0x6F	0x6E	0x6E	0x45	0x43	0x74	0x49		
Mask	0xDF	0xDF	0xDF	0xDF	0xDF	0xDF	0xDF	0xDF		
Result	0	1	1	1	0	0	1	0		



Application Layer Covert Channels

Ways to implement covert channels:

- Optional Headers/Values/Flags, Example

1st Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

2nd Request

```
GET / HTTP/1.1
Accept: text/xml, */*;q=0.5
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

Application Layer Covert Channels

Ways to implement covert channels:

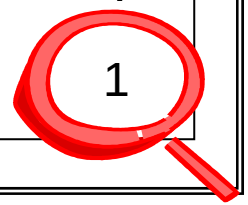
- Optional Headers/Values/Flags, Example

1st Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```

2nd Request

```
GET / HTTP/1.1
Accept: text/xml, */*;q=0.5
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
```



Application Layer Covert Channels

Ways to implement covert channels:

- New Header, Example

Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
Covert-Channel: My Covert Channel
```

Application Layer Covert Channels

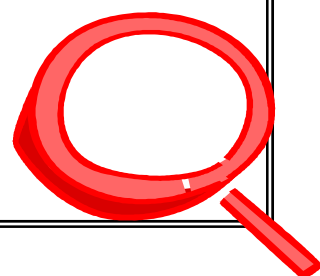
Ways to implement covert channels:

- New Header, Example

Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.bbc.com
Connection: Keep-Alive
Covert-Channel: My Covert Channel
```

If a server doesn't recognise a header is MUST be ignored.
Transparent Proxies must forward unknown headers.



Application Layer Covert Channels

Ways to implement covert channels:

- Linear Spacing Characters, Example

Request

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host: www.bbc.com
Connection: Keep-Alive
```

Application Layer Covert Channels

Ways to implement covert channels:

- Linear Spacing Characters, Example

Request

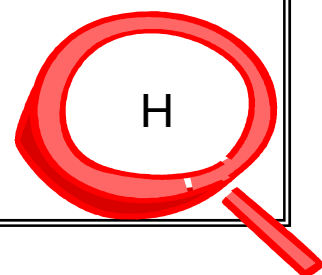
```
GET[SP]/[SP]HTTP/1.1[CRLF]
Accept:[SP]*/*[HT][SP][SP][HT][SP][SP][SP][CRLF]
Accept-Language:[SP]en-gb[CRLF]
Accept-Encoding:[SP]gzip,[SP]deflate[CRLF]
User-Agent:[SP]Mozilla/4.0[CRLF]
Host:[SP]www.bbc.com[CRLF]
Connection:[SP]Keep-Alive[CRLF]
```

[SP] – SPACE - **0**

[HT] – TAB - **1**

[CRLF] – CR + LF

01001000 = "H"



Centre for Mobile Computing and Security

Application Layer Covert Channels

Ways to implement covert channels:

- Modifying Server Object, Example

GMT 00:00	
GMT 00:30	`GET /news.rss HTTP/1.1`
GMT 01:00	`GET /news.rss HTTP/1.1`
GMT 01:30	
GMT 02:00	`GET /news.rss HTTP/1.1`
GMT 02:30	
GMT 03:00	`GET /news.rss HTTP/1.1`
GMT 03:30	

Application Layer Covert Channels

Ways to implement covert channels:

- Modifying Server Object, Example

GMT 00:00	
GMT 00:30	`GET /news.rss HTTP/1.1`
GMT 01:00	`GET /news.rss HTTP/1.1`
GMT 01:30	
GMT 02:00	`GET /news`
GMT 02:30	
GMT 03:00	`GET /news`
GMT 03:30	

Centre for Mobile Computing and Security

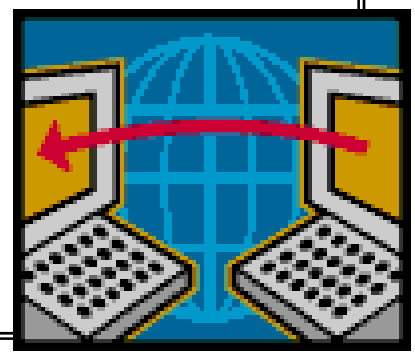
Application Layer Covert Channels

Ways to implement covert channels:

- Reordering
- Case Changing
- Optional Headers/Values/Flags
- New Header
- Linear spacing characters
- Modifying server object

Detection:

- Protocol-based
- Signature-based
- Behaviour-based



Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

Detection:

Protocol-based

- Checks for compliance to the protocol's specification
- Fast = low cost
- Will flag few basic covert channel implementations

```
HTTP/1.1 200 OK
Date: Thu, 30 Mar 2006 19:46:22 GMT
Server: Apache/2.0.54 (Unix)
Last-Modified: Mon, 19 Feb 2001 09:41:36 GMT
Transfer-Coding: chunked
Content-Length: 233
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=300
Connection: Keep-Alive
Content-Type: text/html
```

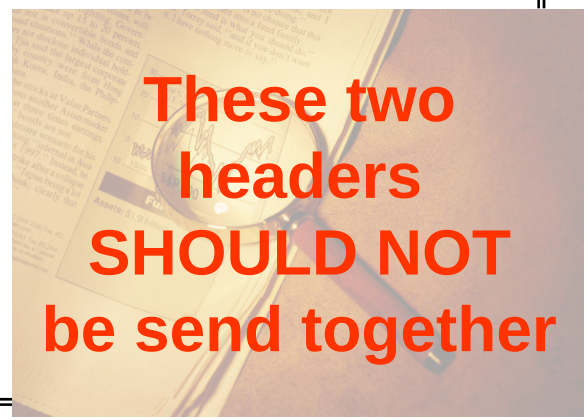
Application Layer Covert Channels

Detection:

Protocol-based

- Checks for compliance to the protocol's specification
- Fast = low cost
- Will flag few basic covert channel implementations

```
HTTP/1.1 200 OK
Date: Thu, 30 Mar 2006 19:46:22 GMT
Server: Apache/2.0.54 (Unix)
Last-Modified: Mon, 19 Feb 2001 09:41:36 GMT
Transfer-Coding: chunked
Content-Length: 233
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=300
Connection: Keep-Alive
Content-Type: text/html
```



Application Layer Covert Channels

Detection:

Signature-based

- Compares messages to signatures of known covert channels
- Checks against database of protocol's known implementations
- Medium speed = moderate cost
- Flags most tunnelling tools and high-bandwidth covert channels

```
HTTP/1.1 200 OK
Date: Thu, 30 Mar 2006 19:46:22 GMT
Server: Apache/2.0.54 (Unix)
lAst-modified: Mon, 19 Feb 2001 09:41:36 GMT
ETag: "e9-bb533400"
Accept-Ranges: bytes
Content-Length: 233
Keep-Alive: timeout=5, max=300
Connection: Keep-Alive
Content-Type: text/html
```

Application Layer Covert Channels

Detection:

Signature-based

- Compares messages to signatures of known covert channels
- Checks against database of protocol's known implementations
- Medium speed = moderate cost
- Flags most tunnelling tools and high-bandwidth covert channels

```
HTTP/1.1 200 OK
Date: Thu, 30 Mar 2006 19:46:22 GMT
Server: Apache/2.0.54 (Unix)
lAst-modified: Mon, 19 Feb 2001 09:41:36 GMT
ETag: "e9-bb533400"
Accept-Ranges: bytes
Content-Length: 233
Keep-Alive: timeout=5, max=300
Connection: Keep-Alive
Content-Type: text/html
```

Apache always uses "title case" to generate message headers

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

Signatures:

-Browsers

Opera:

Internet Explorer:

Firefox:

Netscape:

```
Host: www.bbc.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; rv:1.7.3) Gecko/20040913 Firefox/0.10.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

-Automated Software

Symantec Autoupdate:

Instant massaging application:

```
User-Agent: GG
Host: adserver.gadu-gadu.pl
Cache-Control: no-cache
```

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Application Layer Covert Channels

Internet Explorer:

```
Accept: */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
Host: www.bbc.com
Connection: Keep-Alive
```

Firefox and Netscape:

```
Host: www.bbc.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1;
Accept: text/xml,application/xml,application/xhtml+xml,
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Connection: keep-alive
```

Opera:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
Accept: text/html, application/xml;q=0.9, image/gif, image
Accept-Language: en
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Connection: Keep-Alive
```

Application Layer Covert Channels

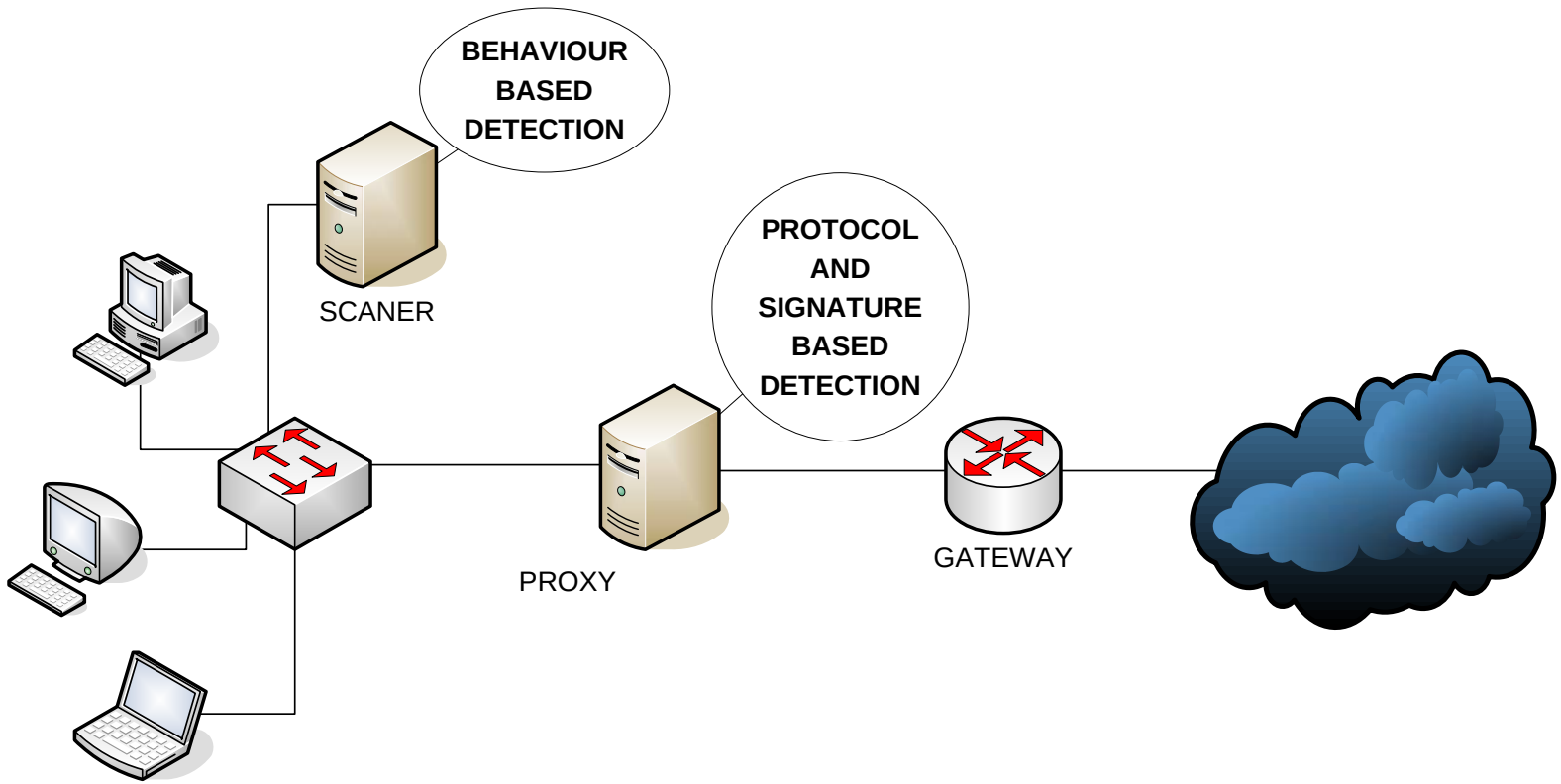
Detection:

Behaviour-based

- Users profiling
- Applications profiling
- Traffic profiling
- Requires large number of resources = Expensive
- If used in line may slow down the traffic
- Very efficient, but still not 100% correct

Application Layer Covert Channels

Detection:

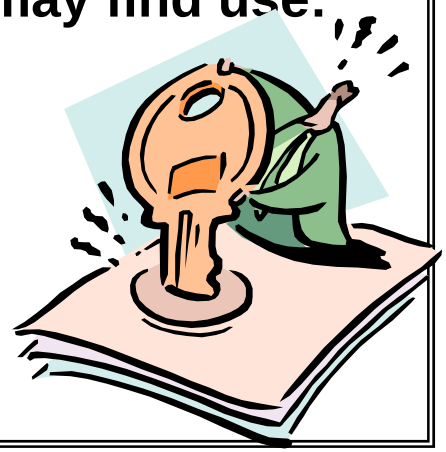


Application Layer Covert Channels

Our plans:
- Development of Secure Browser
- Research signatures of various HTTP implementations
- Recognise outdated parts of those implementations

Areas directly related to the research:
- Information leakage prevention
- Digital surveillance of criminal suspects

Areas where results and techniques described may find use:
- Stopping Distributed Denial of Services
- Anti-Spam Software
- Inline mail filtering for malicious signatures



Centre for Mobile Computing and Security

Application Layer Covert Channels

Zbigniew Kwecka

Matric No. 03008457

BSc (HONS) Networked Computing

e-mail: 03008457@napier.ac.uk
z.kwecka@gmail.com

Centre for Mobile Computing and Security

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH