Advanced Security and Network Forensics

Contact:

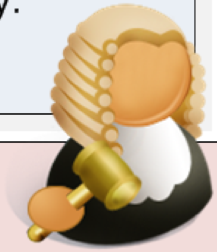
- Prof Bill Buchanan, C.63/ Rich McFarlane.
- MSN Messenger (w_j_buchanan@napier.ac.uk) or Skype (billatnapier).
- http://buchananweb.co.uk

Aim:

The aim of the module is to develop a deep understanding of advanced areas related to security, digital forensics and next-generation Web-based systems, that will allow graduates to act professionally in the design, analysis, implementation, and reporting of enhanced software systems, security strategies, and in forensic computing investigations.

Part 1:

- Security Threats, Security Models, Security Evaluation, and Mitigation Strategies. This involves an in-depth analysis of a range of current threats.
- Secure Architectures/Frameworks.
- Network, Cloud, e-Discovery and Mobile Forensics.
- Data hiding. Data hiding methods, Covert Channel Analysis, Stenography.



Part 2:

- Cloud/grid computing. Principles, distributed architectures, and layered approaches. Data grid and Semantic Web. Cloud/grid applications.
- Service-oriented architectures (SOAs). Interfacing to SOAs, middleware infrastructures, and discovering services.
- Web-service/Remoting infrastructures and Service Platforms. Example Clouds (Amazon EC2, Google, and so on), Web security (Focus on Web-based infrastructures, XAML and WS-*, SAML), Next Generation Web-based Systems.
- Web Security, Authentication infrastructures. Principles, Kerberos, enhanced and scalable authentication infrastructures.
- Virtualization methodologies. Software-/Hardware-as-a-Service (SaaS/HaaS), Fault tolerance and reliability, Distributed data storage/Clustering. High-performance computing.
- Professional Certification.

Content

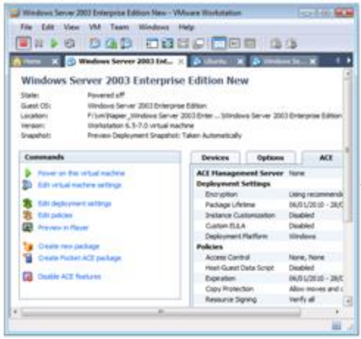
Overview

Module Content

Schedule

Overview

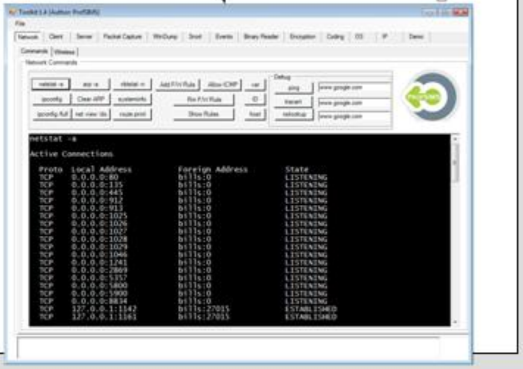
Date	Academic	Assessment	Lab/Tutorial
19/01/11	1: Introduction		Lab 1: Windows Services/ Toolkit 1 (Cmds)
26/01/11	2: Threats		Lab 2: Linux Services/ Toolkit 2 (WinDump)
02/02/11	3: Network Forensics		Lab 3: Vulnerability Analysis/ Toolkit 3 (Snort/Nmap)
09/02/11	4: Data Hiding		Lab 4: Network Forensics/ Toolkit 4 (Packet Capture)
16/02/11	Revision		Lab 5: Data Hiding/ Toolkit 5 (Analysis)
23/02/11		**MCQ Test 1**	Lab 6: Secure Connections/ Toolkit 6 (Data Hiding)
02/03/11	5: Web Infrastructures		Lab 7: SAML/ Toolkit 7 (URL cache)
09/03/11	6: Cloud/grid computing		Lab 8: Using AWS (Web, Database, Telnet and FTP)
16/03/11	7: Integrated Forensic Investigations		Lab 9: Using AWS (LAMP)
23/03/11	Professional Certification (CEH or CISSP)		Lab 10: Integrated Forensics
30/03/11	Professional Certification (CEH or CISSP)		
06/04/11		**MCQ Test 2/ C/W hand-in**	
13/04/11			
21/04/11			


Windows Server 2003 Enterprise Edition New - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
Home
Windows Server 2003 Ent...
Ubuntu
Windows Se...
Commands
Power on this virtual machine
Edit virtual machine settings
Edit deployment settings
Edit policies
Preview in Player
Create new package
Create Pocket ACE package
Disable ACE features
Devices
Options
ACE

Windows Server 2003 Enterprise Edition New

State: Powered off
Guest OS: Windows Server 2003 Enterprise Edition
Location: F:\vm\Napier_Windows Server 2003 Enter ... \Windows Server 2003 Enterprise Edition
Version: Workstation 6.5-7.0 virtual machine
Snapshot: Preview Deployment Snapshot: Taken Automatically

ACE Management Server	None
Deployment Settings	
Encryption	Using recommende
Package Lifetime	06/01/2010 - 28/C
Instance Customization	Disabled
Custom EULA	Disabled
Deployment Platform	Windows
Policies	
Access Control	None, None
Host-Guest Data Script	Disabled
Expiration	06/01/2010 - 28/C
Copy Protection	Allow moves and c
Resource Signing	Verify all

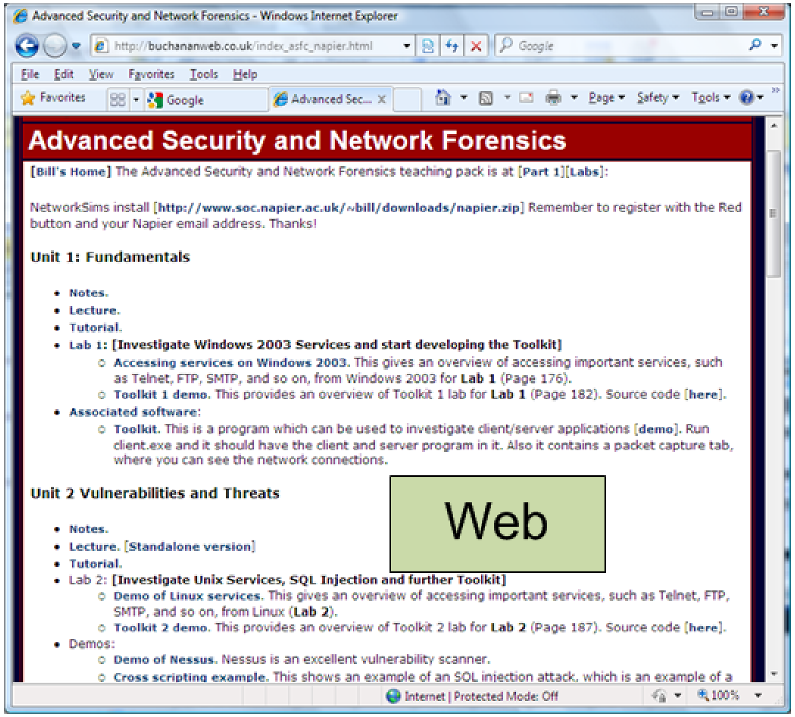


```
netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             bills:0                LISTENING
  TCP    0.0.0.0:135            bills:0                LISTENING
  TCP    0.0.0.0:445            bills:0                LISTENING
  TCP    0.0.0.0:912            bills:0                LISTENING
  TCP    0.0.0.0:913            bills:0                LISTENING
  TCP    0.0.0.0:1025           bills:0                LISTENING
  TCP    0.0.0.0:1026           bills:0                LISTENING
  TCP    0.0.0.0:1027           bills:0                LISTENING
  TCP    0.0.0.0:1028           bills:0                LISTENING
  TCP    0.0.0.0:1029           bills:0                LISTENING
  TCP    0.0.0.0:1046           bills:0                LISTENING
  TCP    0.0.0.0:1241           bills:0                LISTENING
  TCP    0.0.0.0:2869           bills:0                LISTENING
  TCP    0.0.0.0:5357           bills:0                LISTENING
  TCP    0.0.0.0:5800           bills:0                LISTENING
  TCP    0.0.0.0:5900           bills:0                LISTENING
  TCP    0.0.0.0:8834           bills:0                LISTENING
  TCP    127.0.0.1:1142         bills:27015            ESTABLISHED
  TCP    127.0.0.1:1161         bills:27015            ESTABLISHED
```

Schedule


Advanced Security and Network Forensics - Windows Internet Explorer
http://buchananweb.co.uk/index_asfc_napier.html
Google
File Edit View Favorites Tools Help
Favorites
Google
Advanced Sec...
Page Safety Tools
Internet | Protected Mode: Off
100%

Advanced Security and Network Forensics

[Bill's Home] The Advanced Security and Network Forensics teaching pack is at [Part 1][Labs]:

NetworkSims install [http://www.soc.napier.ac.uk/~bill/downloads/napier.zip] Remember to register with the Red button and your Napier email address. Thanks!

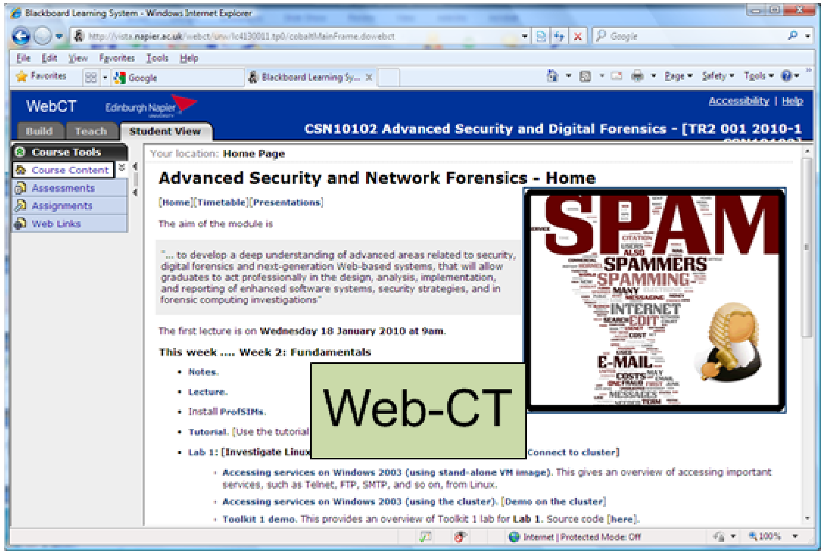
Unit 1: Fundamentals

- Notes.
- Lecture.
- Tutorial.
- Lab 1: [Investigate Windows 2003 Services and start developing the Toolkit]
  - Accessing services on Windows 2003. This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Windows 2003 for Lab 1 (Page 176).
  - Toolkit 1 demo. This provides an overview of Toolkit 1 lab for Lab 1 (Page 182). Source code [here].
- Associated software:
  - Toolkit. This is a program which can be used to investigate client/server applications [demo]. Run client.exe and it should have the client and server program in it. Also it contains a packet capture tab, where you can see the network connections.

Unit 2 Vulnerabilities and Threats

- Notes.
- Lecture. [Standalone version]
- Tutorial.
- Lab 2: [Investigate Unix Services, SQL Injection and further Toolkit]
  - Demo of Linux services. This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Linux (Lab 2).
  - Toolkit 2 demo. This provides an overview of Toolkit 2 lab for Lab 2 (Page 187). Source code [here].
- Demos:
  - Demo of Nessus. Nessus is an excellent vulnerability scanner.
  - Cross scripting example. This shows an example of an SQL injection attack, which is an example of a

Web


Blackboard Learning System - Windows Internet Explorer
http://vista.napier.ac.uk/webct/urw/lc4130011.tp0/cobaltMainFrame.dowebct
Google
File Edit View Favorites Tools Help
Favorites
Google
Blackboard Learning Sy...
Page Safety Tools
WebCT
Edinburgh Napier University
Accessibility | Help
Build
Teach
Student View
Course Tools
Course Content
Assessments
Assignments
Web Links
SPAM
SPAMMERS
SPAMMING
MANY
INTERNET
EDIT
E-MAIL
COSTS
MESSAGES
Internet | Protected Mode: Off
100%

CSN10102 Advanced Security and Digital Forensics - [TR2 001 2010-1

Your location: **Home Page**

Advanced Security and Network Forensics - Home

[Home][Timetable][Presentations]

The aim of the module is

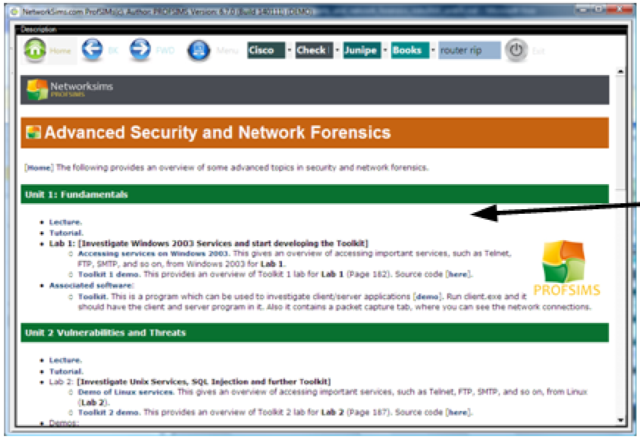
> "... to develop a deep understanding of advanced areas related to security, digital forensics and next-generation Web-based systems, that will allow graduates to act professionally in the design, analysis, implementation, and reporting of enhanced software systems, security strategies, and in forensic computing investigations"

The first lecture is on **Wednesday 18 January 2010 at 9am.**

This week .... Week 2: Fundamentals

- Notes.
- Lecture.
- Install ProfSIMs.
- Tutorial. [Use the tutorial
- Lab 1: [Investigate Linux Connect to cluster]
  - Accessing services on Windows 2003 (using stand-alone VM image). This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Linux.
  - Accessing services on Windows 2003 (using the cluster). [Demo on the cluster]
  - Toolkit 1 demo. This provides an overview of Toolkit 1 lab for **Lab 1**. Source code [here].

Web-CT



Advanced Security and Network Forensics

[Home] The following provides an overview of some advanced topics in security and network forensics.

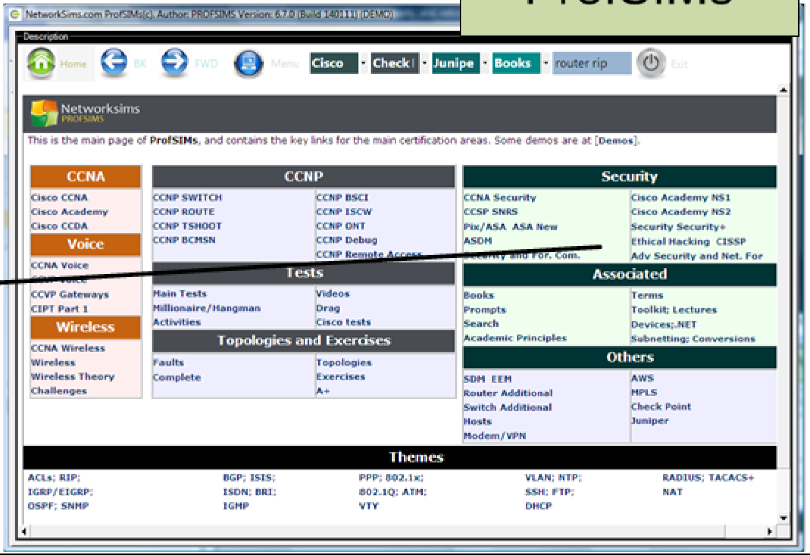
Unit 1: Fundamentals

- Lecture.
- Tutorial.
- Lab 1: [Investigate Windows 2003 Services and start developing the Toolkit]
  - Accessing services on Windows 2003. This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Windows 2003 for **Lab 1**.
  - Toolkit 1 demo. This provides an overview of Toolkit 1 lab for **Lab 1** (Page 182). Source code [here].
- Associated software:
  - Toolkit. This is a program which can be used to investigate client/server applications [demo]. Run client.exe and it should have the client and server program in it. Also it contains a packet capture tab, where you can see the network connections.

Unit 2 Vulnerabilities and Threats

- Lecture.
- Tutorial.
- Lab 2: [Investigate Unix Services, SQL Injection and further Toolkit]
  - Demo of Linux services. This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Linux (**Lab 2**).
  - Toolkit 2 demo. This provides an overview of Toolkit 2 lab for **Lab 2** (Page 187). Source code [here].
- Demos:

ProfSIMs


NetworkSims.com ProfSIMs(c). Author: PROFSIMS Version: 6.7.0 (Build 140111) (DEMO)
Description
Home
BK
FWD
Menu
Cisco
Check
Junipe
Books
router rip
Exit
Networksims
PROFSIMS

This is the main page of **ProfSIMs**, and contains the key links for the main certification areas. Some demos are at [Demos].

CCNA
Cisco CCNA Cisco Academy Cisco CCDA
Voice
CCNA Voice [illegible] CCVP Gateways CIPT Part 1
Wireless
CCNA Wireless Wireless Wireless Theory Challenges

CCNP	
CCNP SWITCH CCNP ROUTE CCNP TSHOOT CCNP BCMSN	CCNP BSCI CCNP ISCW CCNP ONT CCNP Debug CCNP Remote Access
Tests	
Main Tests Millionaire/Hangman Activities	Videos Drag Cisco tests
Topologies and Exercises	
Faults Complete	Topologies Exercises A+

Security	
CCNA Security CCSP SNRS Pix/ASA ASA New ASDM Security and For. Com.	Cisco Academy NS1 Cisco Academy NS2 Security Security+ Ethical Hacking CISSP Adv Security and Net. For
Associated	
Books Prompts Search Academic Principles	Terms Toolkit; Lectures Devices;.NET Subnetting; Conversions
Others	
SDM EEM Router Additional Switch Additional Hosts Modem/VPN	AWS MPLS Check Point Juniper

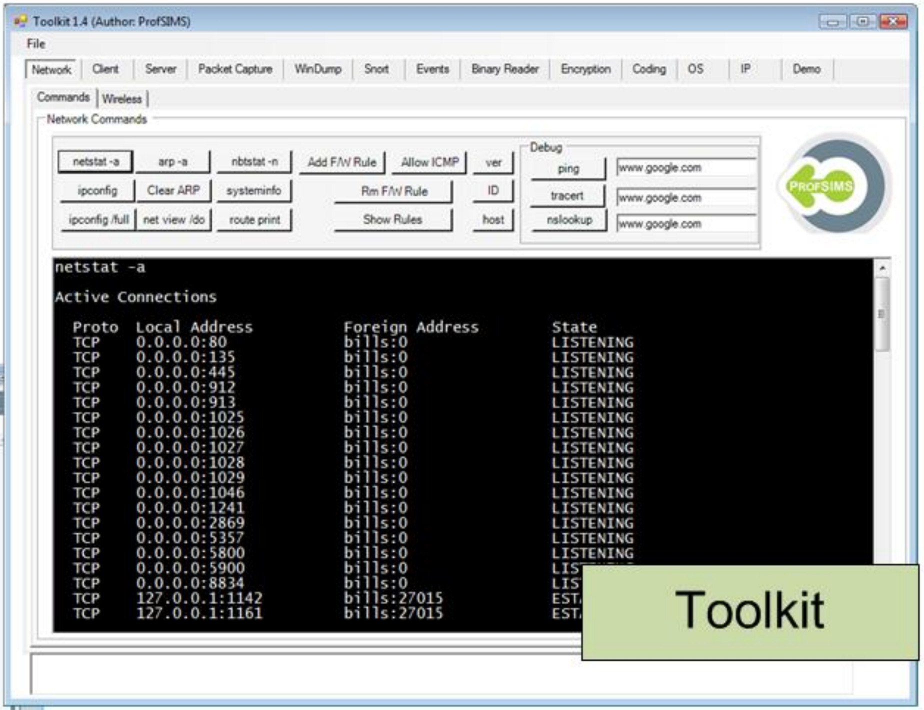
Themes				
ACLs; RIP;	BGP; ISIS;	PPP; 802.1x;	VLAN; NTP;	RADIUS; TACACS+
IGRP/EIGRP;	ISDN; BRI;	802.1Q; ATM;	SSH; FTP;	NAT
OSPF; SNMP	IGMP	VTY	DHCP	

Material

Overview

Material

Microsoft Visual Studio 2008

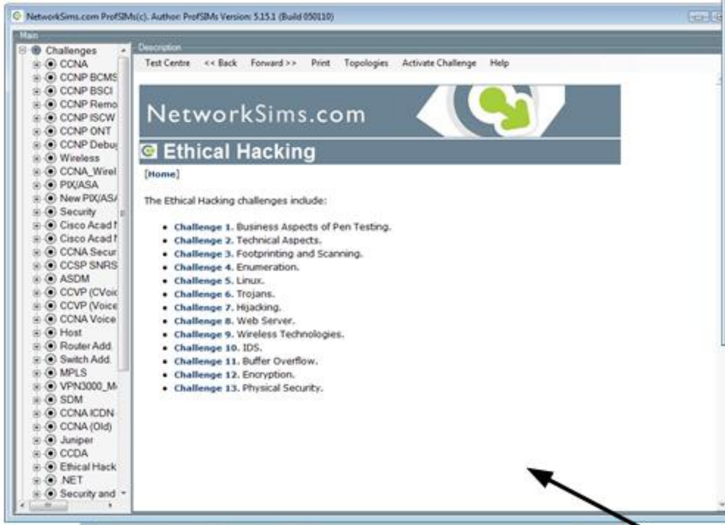


```
netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             bills:0                LISTENING
  TCP    0.0.0.0:135            bills:0                LISTENING
  TCP    0.0.0.0:445            bills:0                LISTENING
  TCP    0.0.0.0:912            bills:0                LISTENING
  TCP    0.0.0.0:913            bills:0                LISTENING
  TCP    0.0.0.0:1025           bills:0                LISTENING
  TCP    0.0.0.0:1026           bills:0                LISTENING
  TCP    0.0.0.0:1027           bills:0                LISTENING
  TCP    0.0.0.0:1028           bills:0                LISTENING
  TCP    0.0.0.0:1029           bills:0                LISTENING
  TCP    0.0.0.0:1046           bills:0                LISTENING
  TCP    0.0.0.0:1241           bills:0                LISTENING
  TCP    0.0.0.0:2869           bills:0                LISTENING
  TCP    0.0.0.0:5357           bills:0                LISTENING
  TCP    0.0.0.0:5800           bills:0                LISTENING
  TCP    0.0.0.0:5900           bills:0                LIS
  TCP    0.0.0.0:8834           bills:0                LIS
  TCP    127.0.0.1:1142         bills:27015            EST
  TCP    127.0.0.1:1161         bills:27015            EST
```

Toolkit

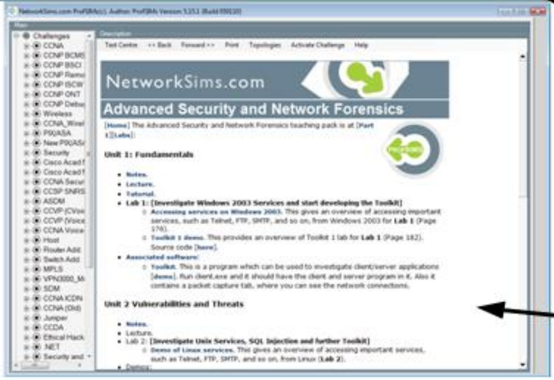


Ethical Hacking

[Home]

The Ethical Hacking challenges include:

- **Challenge 1.** Business Aspects of Pen Testing.
- **Challenge 2.** Technical Aspects.
- **Challenge 3.** Footprinting and Scanning.
- **Challenge 4.** Enumeration.
- **Challenge 5.** Linux.
- **Challenge 6.** Trojans.
- **Challenge 7.** Hijacking.
- **Challenge 8.** Web Server.
- **Challenge 9.** Wireless Technologies.
- **Challenge 10.** IDS.
- **Challenge 11.** Buffer Overflow.
- **Challenge 12.** Encryption.
- **Challenge 13.** Physical Security.



Advanced Security and Network Forensics

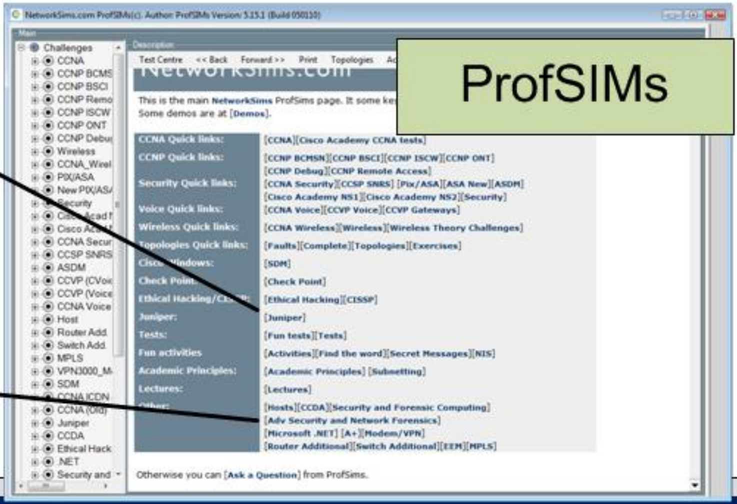
[Home] The Advanced Security and Network Forensics teaching pack is at [Part 1][Labs].

Unit 1: Fundamentals

- Notes.
- Lecture.
- Tutorial.
- Lab 1: **[Investigate Windows 2003 Services and start developing the Toolkit]**
  - **Accessing services on Windows 2003.** This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Windows 2003 for **Lab 1** (Page 176).
  - **Toolkit 1 demo.** This provides an overview of Toolkit 1 lab for **Lab 1** (Page 182). Source code [here].
- **Associated software:**
  - **Toolkit.** This is a program which can be used to investigate client/server applications [demo]. Run client.exe and it should have the client and server program in it. Also it contains a packet capture tab, where you can see the network connections.

Unit 2 Vulnerabilities and Threats

- Notes.
- Lecture.
- Lab 2: **[Investigate Unix Services, SQL Injection and further Toolkit]**
  - **Demo of Linux services.** This gives an overview of accessing important services, such as Telnet, FTP, SMTP, and so on, from Linux (**Lab 2**).
- Demos:



This is the main **NetworkSims** ProfSims page. It some ke
Some demos are at [**Demos**].

CCNA Quick links:	[CCNA][Cisco Academy CCNA tests]
CCNP Quick links:	[CCNP BCMSN][CCNP BSCI][CCNP ISCW][CCNP ONT] [CCNP Debug][CCNP Remote Access]
Security Quick links:	[CCNA Security][CCSP SNRS] [Pix/ASA][ASA New][ASDM] [Cisco Academy NS1][Cisco Academy NS2][Security]
Voice Quick links:	[CCNA Voice][CCVP Voice][CCVP Gateways]
Wireless Quick links:	[CCNA Wireless][Wireless][Wireless Theory Challenges]
Topologies Quick links:	[Faults][Complete][Topologies][Exercises]
Cisco Windows:	[SDM]
Check Point:	[Check Point]
Ethical Hacking/CISSP:	[Ethical Hacking][CISSP]
Juniper:	[Juniper]
Tests:	[Fun tests][Tests]
Fun activities	[Activities][Find the word][Secret Messages][NIS]
Academic Principles:	[Academic Principles] [Subnetting]
Lectures:	[Lectures]
Other:	[Hosts][CCDA][Security and Forensic Computing] [Adv Security and Network Forensics] [Microsoft .NET] [A+][Modem/VPN] [Router Additional][Switch Additional][EEM][MPLS]

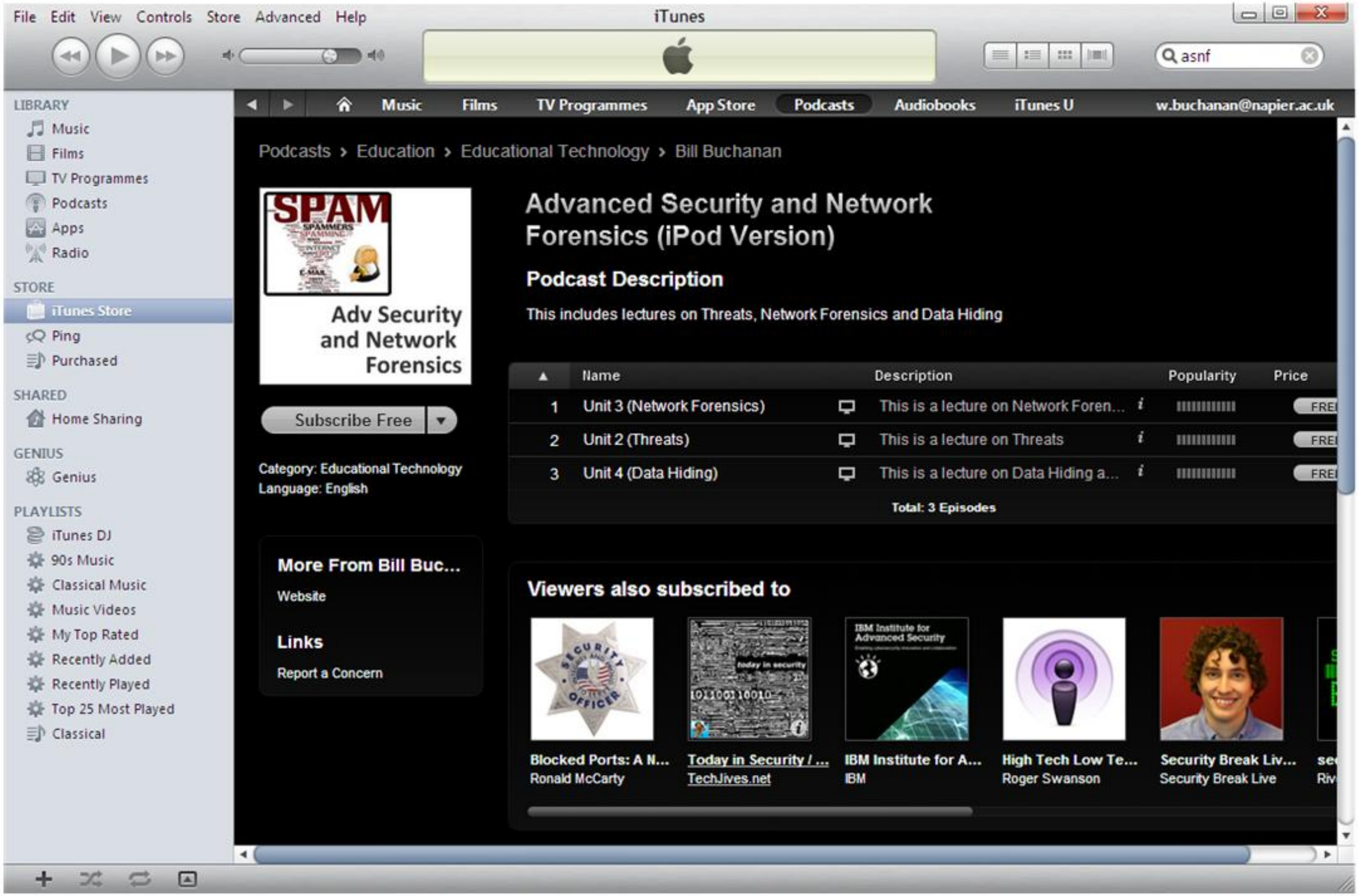
Otherwise you can [**Ask a Question**] from ProfSims.

ProfSIMs

Material

Overview

Material



Podcasts › Education › Educational Technology › Bill Buchanan

Advanced Security and Network Forensics (iPod Version)

Podcast Description

This includes lectures on Threats, Network Forensics and Data Hiding

▲	Name		Description		Popularity	Price
1	Unit 3 (Network Forensics)	🖵	This is a lecture on Network Foren...	i	IIIIIIIIIII	FRE
2	Unit 2 (Threats)	🖵	This is a lecture on Threats	i	IIIIIIIIIII	FRE
3	Unit 4 (Data Hiding)	🖵	This is a lecture on Data Hiding a...	i	IIIIIIIIIII	FRE

Total: 3 Episodes

Category: Educational Technology
Language: English

More From Bill Buc...

Website

Links

Report a Concern

Viewers also subscribed to

Blocked Ports: A N...
Ronald McCarty

Today in Security / ...
TechJives.net

IBM Institute for A...
IBM

High Tech Low Te...
Roger Swanson

Security Break Liv...
Security Break Live

se
Riv

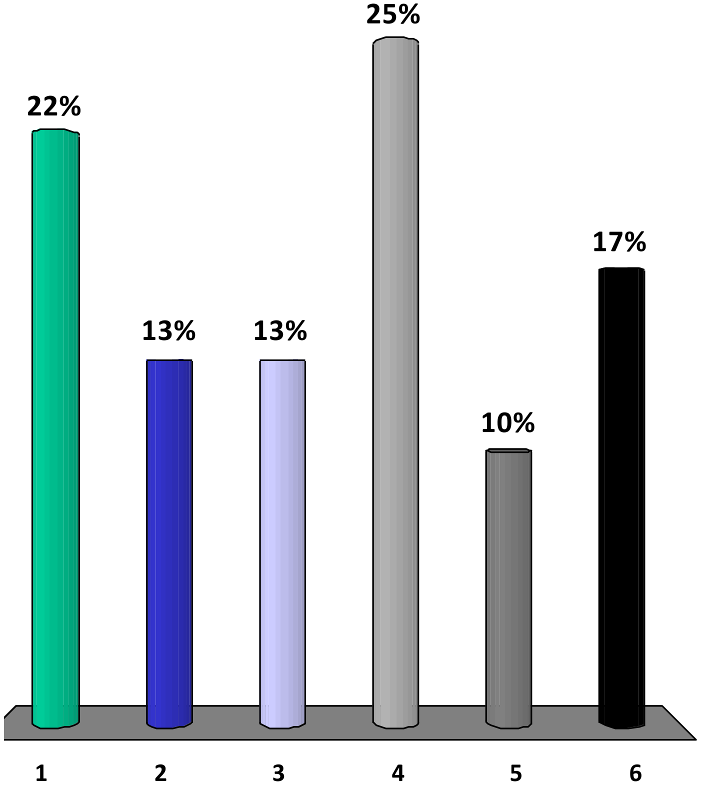
Content

Overview

Module Content

Which package should you download to be able to access the tests:

1. Packet Tracer
2. [✓ Networksims.com ProfSIMs]
3. WebCT Analyser
4. Security+ Net
5. Google Reader
6. iTunes Tester



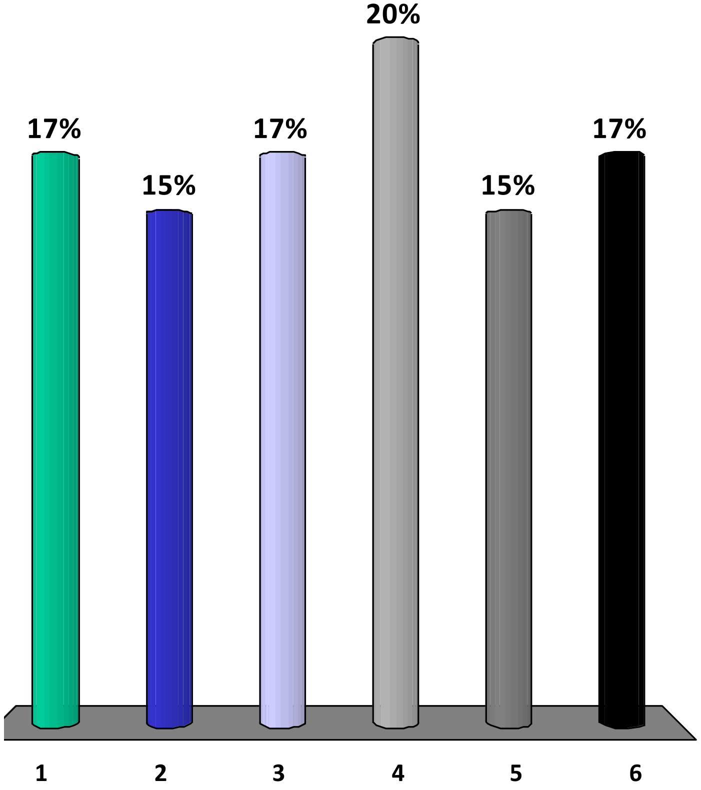
INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

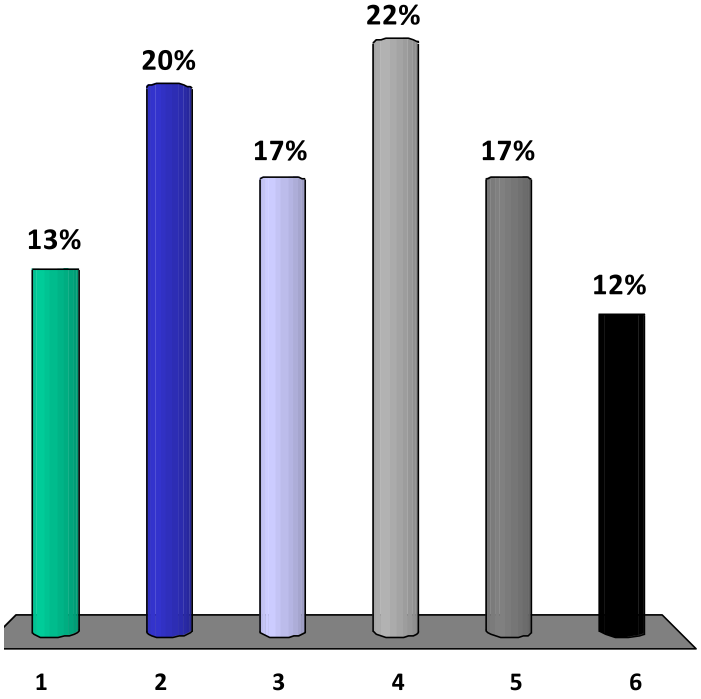
To downloads the iTunes version of the lectures, which is the search term:

1. AdvSecurity
2. Napier
3. [✓ ASFN]
4. SoC
5. AdvancedNapier
6. NetForensics



Which is not a subject taught on the module:

1. Cloud Computing
2. [✓ Compliance/Auditing]
3. Web Infrastructures
4. Threat Analysis
5. Network Forensics
6. Data Hiding



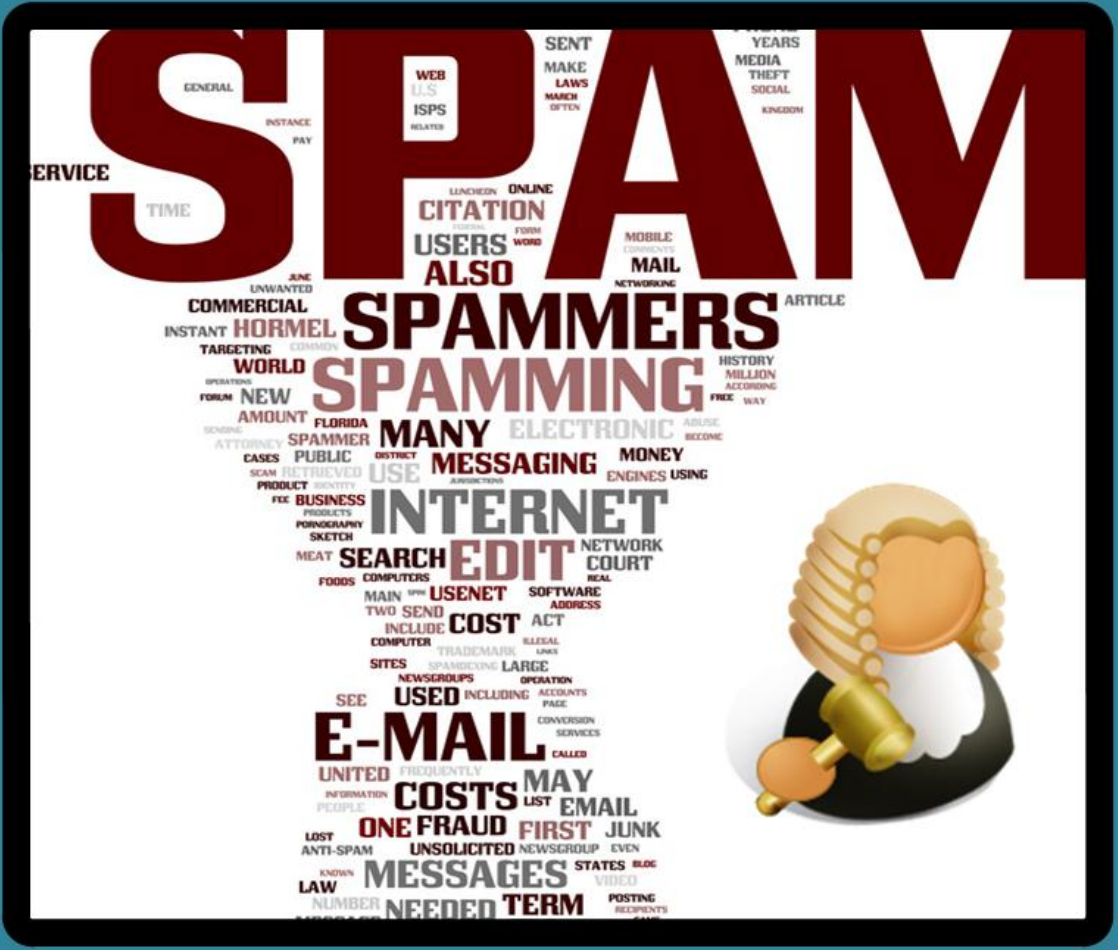
Participant Scores

3	Participant 25
2	Participant F3D61
2	Participant 2
2	Participant 4
2	Participant 16

Introduction

- Provide an outline of risk, and the terminology used.
- Provide an outline to a range of threats.
- Understand the usage of client/server connections.
- Outline the usage of services on Windows and Linux, and provide an introduction to service-oriented infrastructures.
- Provide a practical background in Windows and Linux for services, logging and auditing.

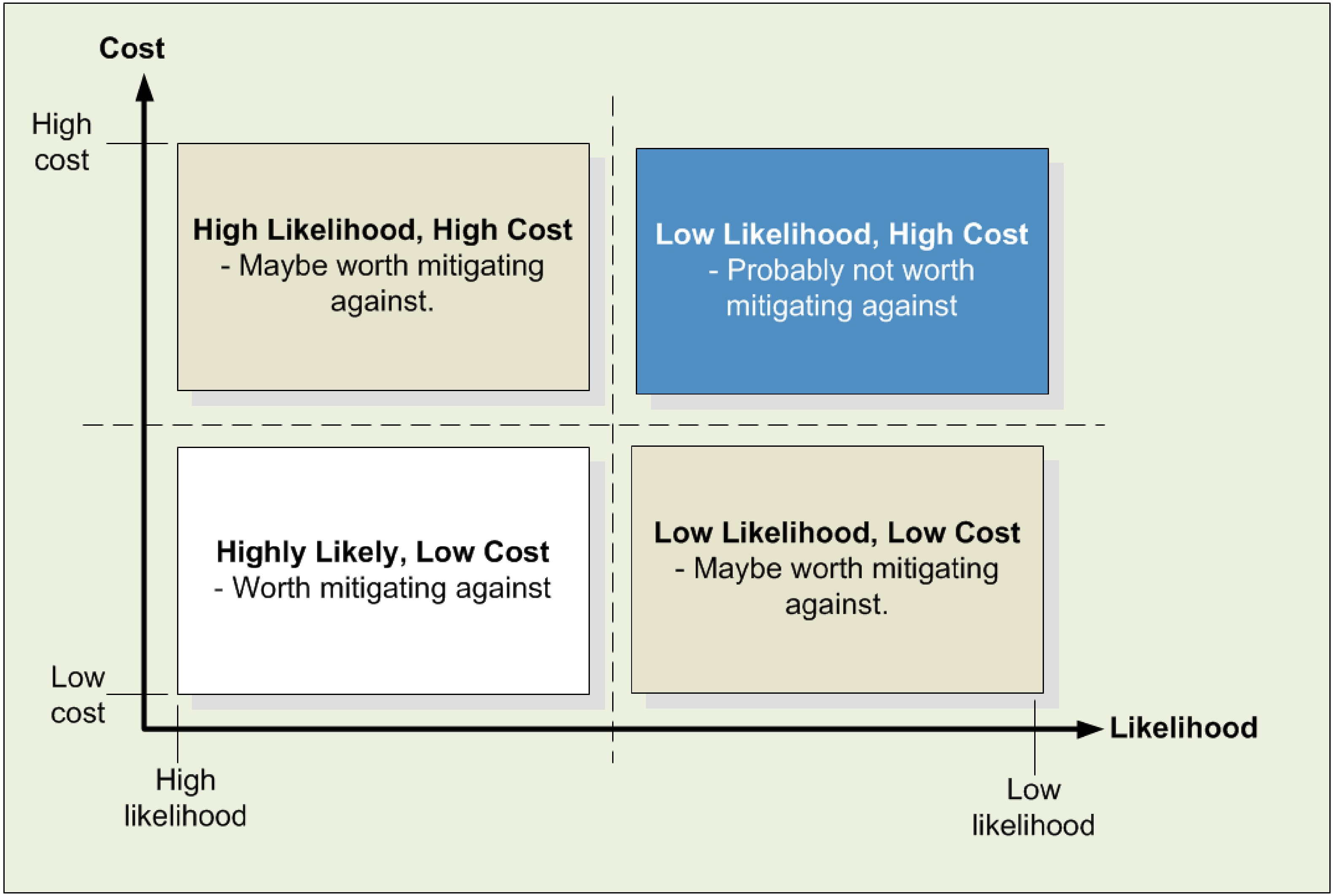
Introduction



Risk Analysis

Author: Prof Bill Buchanan

Risk analysis (Cost/likelihood)



High Likelihood, High Cost - Maybe worth mitigating against.

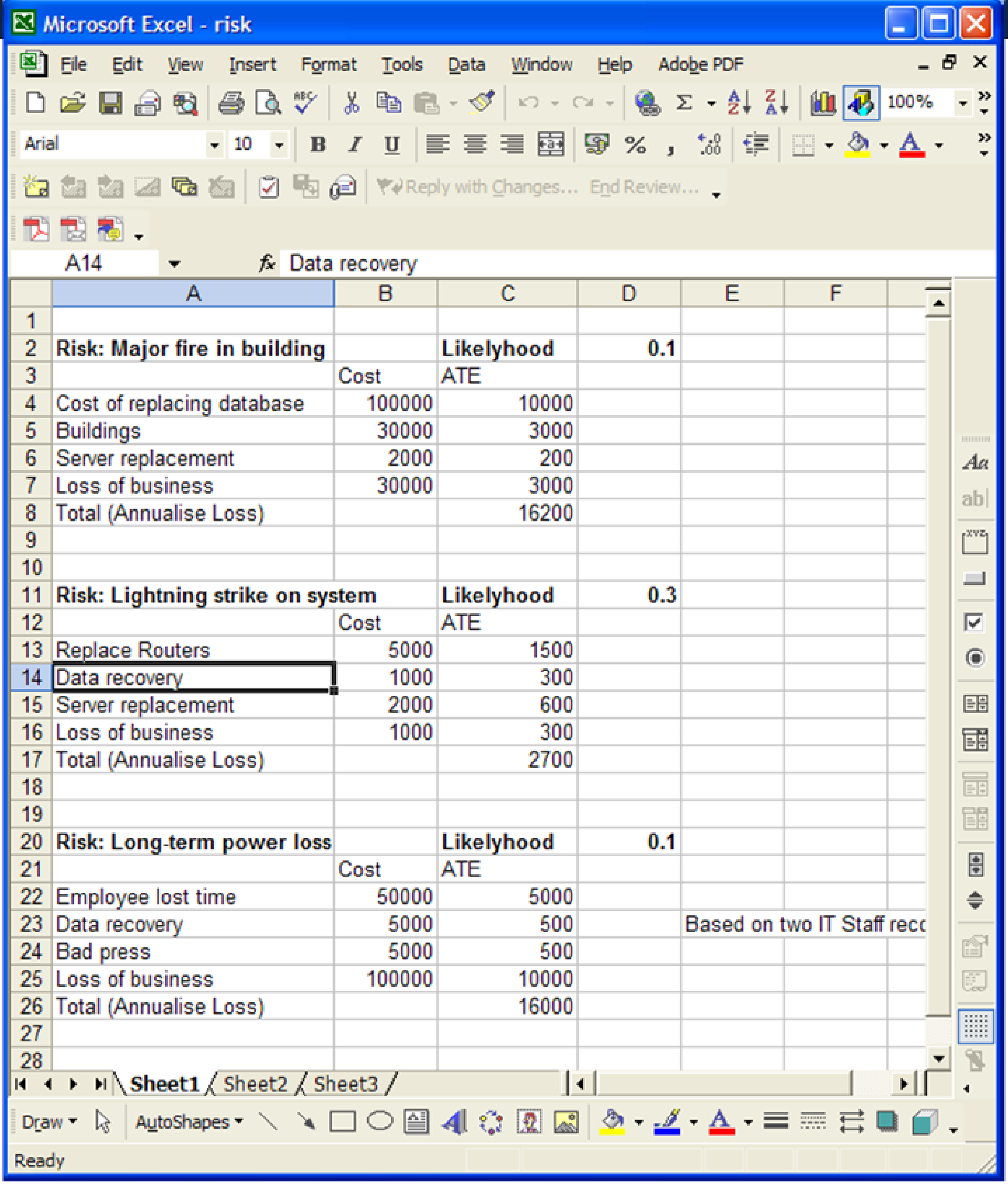
Low Likelihood, High Cost - Probably not worth mitigating against

Highly Likely, Low Cost - Worth mitigating against

Low Likelihood, Low Cost - Maybe worth mitigating against.

Author: Prof Bill Buchanan

Annual Loss Expectancy (ALE)


Microsoft Excel - risk
File Edit View Insert Format Tools Data Window Help Adobe PDF
Arial 10
100%
Reply with Changes... End Review...
Sheet1 Sheet2 Sheet3
Draw AutoShapes
Ready

A14 fx Data recovery

	A	B	C	D	E	F
1						
2	**Risk: Major fire in building**		**Likelyhood**	**0.1**		
3		Cost	ATE			
4	Cost of replacing database	100000	10000			
5	Buildings	30000	3000			
6	Server replacement	2000	200			
7	Loss of business	30000	3000			
8	Total (Annualise Loss)		16200			
9						
10						
11	**Risk: Lightning strike on system**		**Likelyhood**	**0.3**		
12		Cost	ATE			
13	Replace Routers	5000	1500			
14	Data recovery	1000	300			
15	Server replacement	2000	600			
16	Loss of business	1000	300			
17	Total (Annualise Loss)		2700			
18						
19						
20	**Risk: Long-term power loss**		**Likelyhood**	**0.1**		
21		Cost	ATE			
22	Employee lost time	50000	5000			
23	Data recovery	5000	500		Based on two IT Staff reco	
24	Bad press	5000	500			
25	Loss of business	100000	10000			
26	Total (Annualise Loss)		16000			
27						
28						

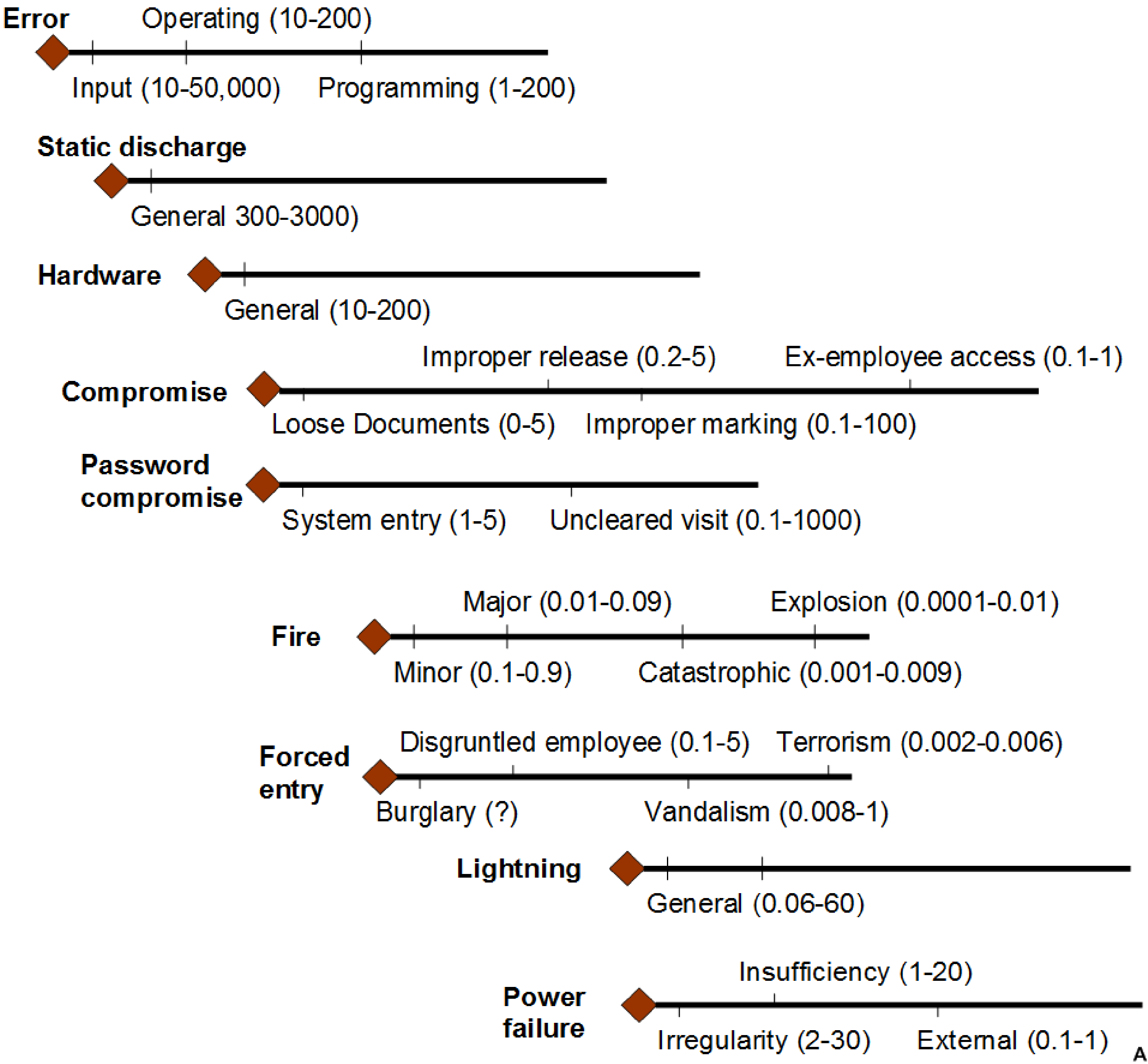
ALE = *T* x *V*

ALE is the Annual Lost Expectancy
T is the likelihood of a threat
V is the value of the particular asset.

Eg. If the likelihood of a denial-of-service on a WWW-based database is once every three years, and the loss to sales is £100K, then the ALE will be:

ALE = £100K x 1/3 = £33K per annum

Author: Prof Bill Buchanan



Error

Operating (10-200)

Input (10-50,000) Programming (1-200)

Static discharge

General 300-3000)

Hardware

General (10-200)

Compromise

Improper release (0.2-5) Ex-employee access (0.1-1)

Loose Documents (0-5) Improper marking (0.1-100)

Password compromise

System entry (1-5) Uncleared visit (0.1-1000)

Fire

Major (0.01-0.09) Explosion (0.0001-0.01)

Minor (0.1-0.9) Catastrophic (0.001-0.009)

Forced entry

Disgruntled employee (0.1-5) Terrorism (0.002-0.006)

Burglary (?) Vandalism (0.008-1)

Lightning

General (0.06-60)

Power failure

Insufficiency (1-20)

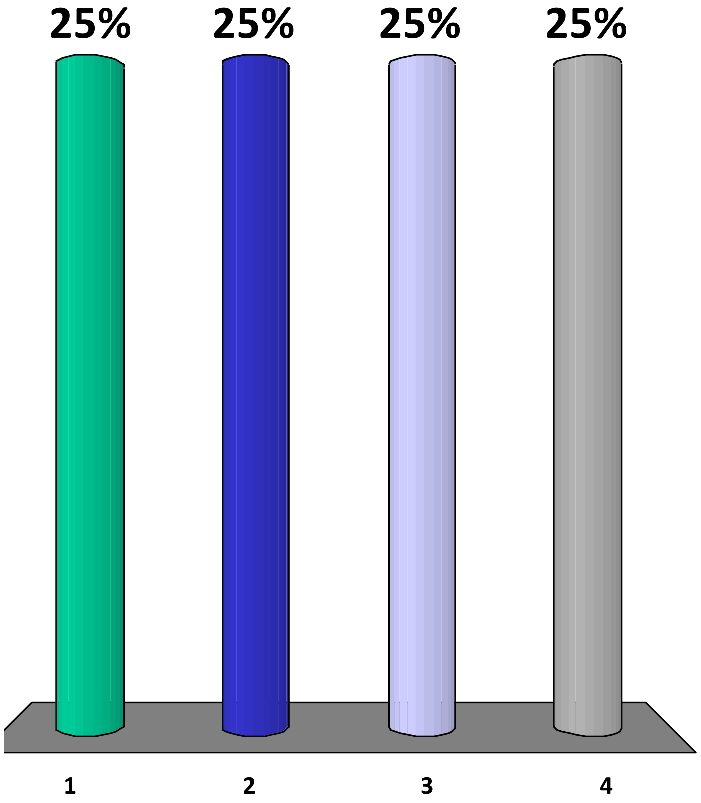
Irregularity (2-30) External (0.1-1)

Author: Prof Bill Buchanan

Probability of event

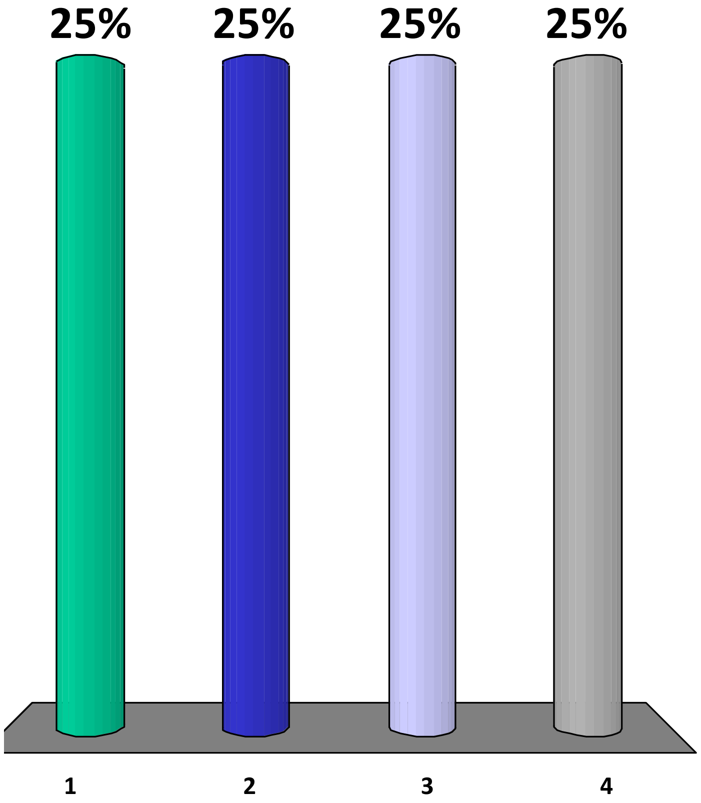
Which is a man-made/political threat :

1. Disgruntled employees
2. Outages
3. Earthquakes
4. Storms



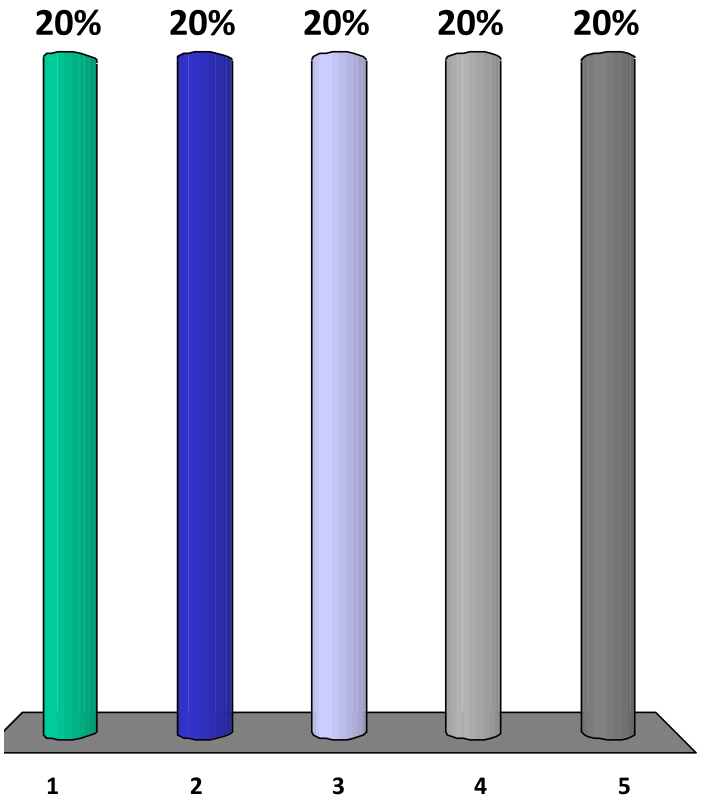
Which is a technical threat :

1. Riots
2. Equipment outages
3. Earthquakes
4. Storms



Which is a prolonged power loss:

1. Spike
2. Brownout
3. Sag
4. Fault
5. Blackout



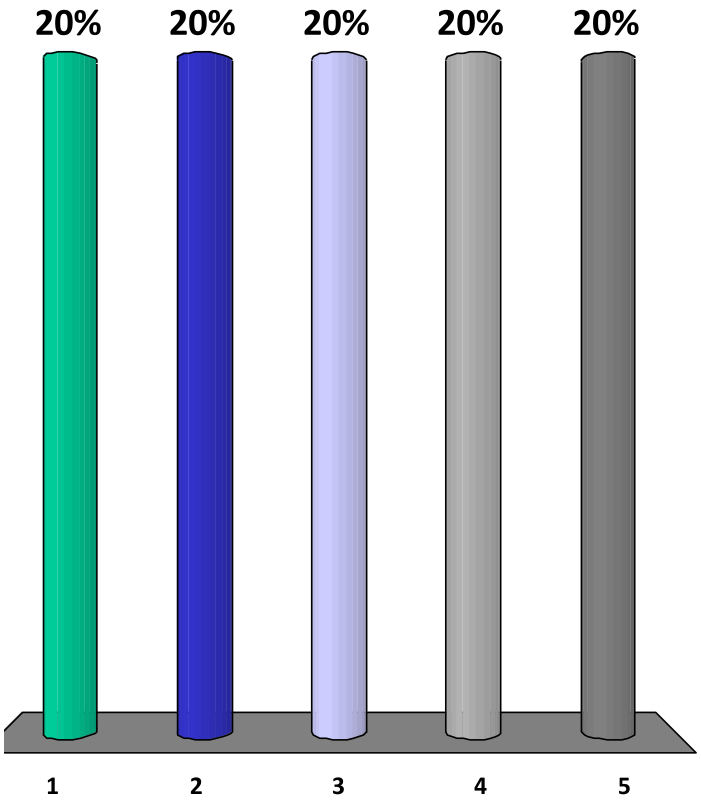
INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

Which is the term used for momentary high voltage:

1. Spike
2. Brownout
3. Sag
4. Fault
5. Blackout



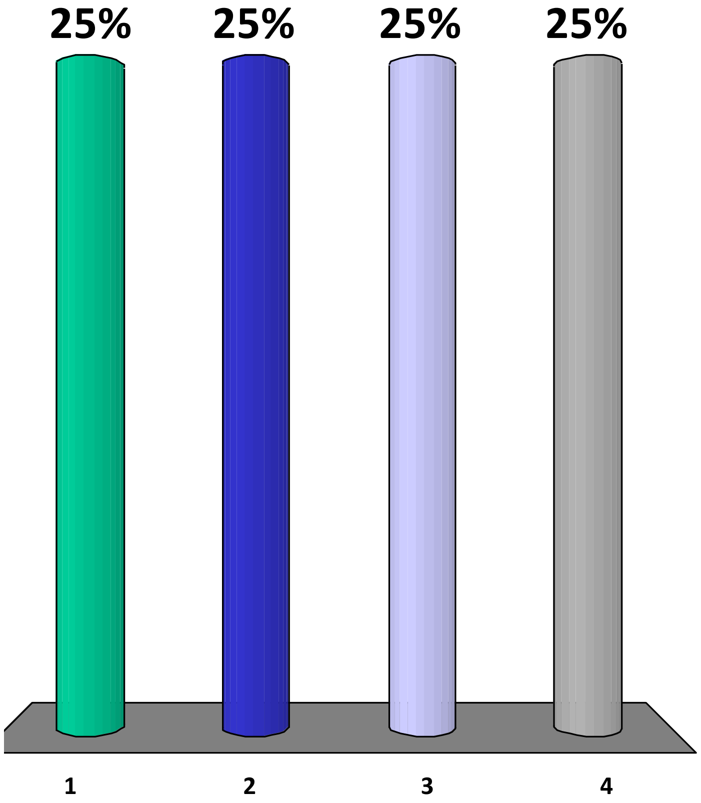
INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

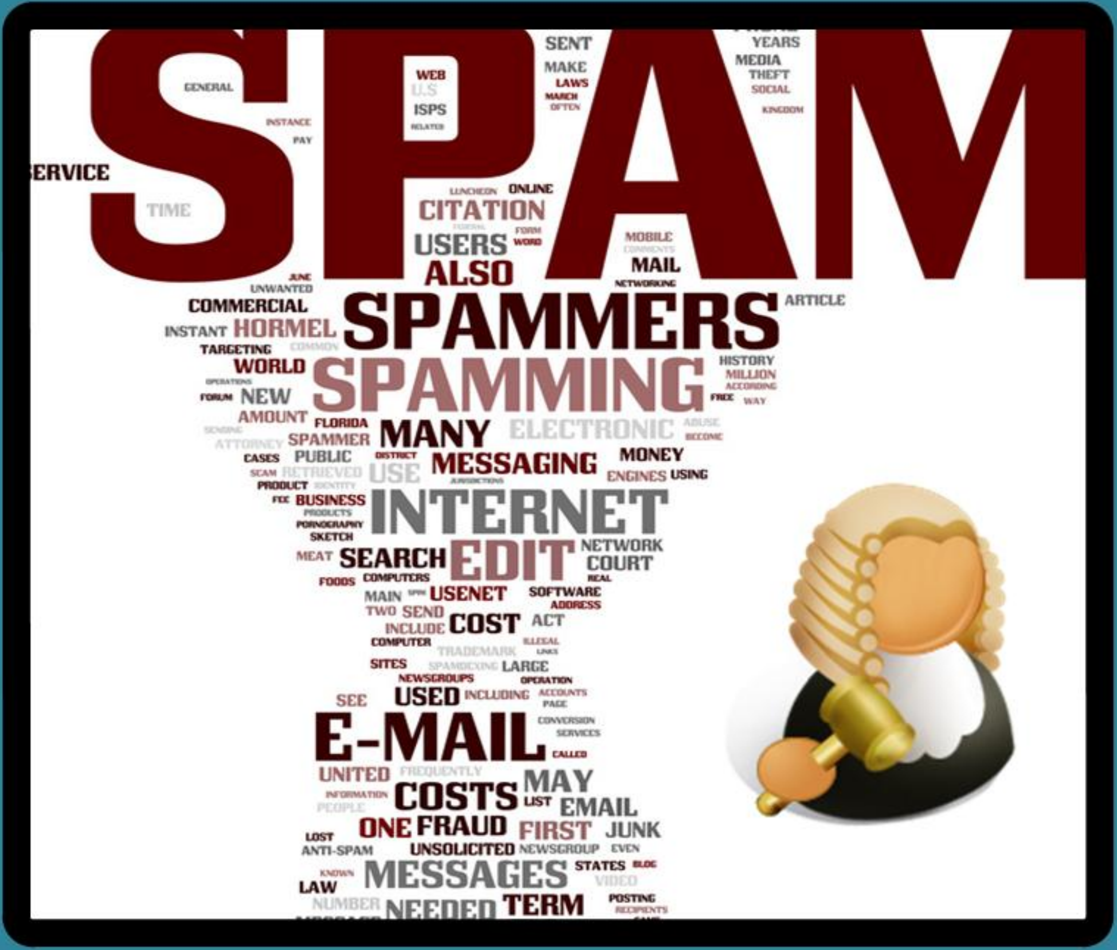
Author: Bill Buchanan

In a multi-story building, where is likely to be the best place to locate the data centre:

1. In the basement
2. On the top floor
3. On the middle floor
4. On the outside of the building



Introduction



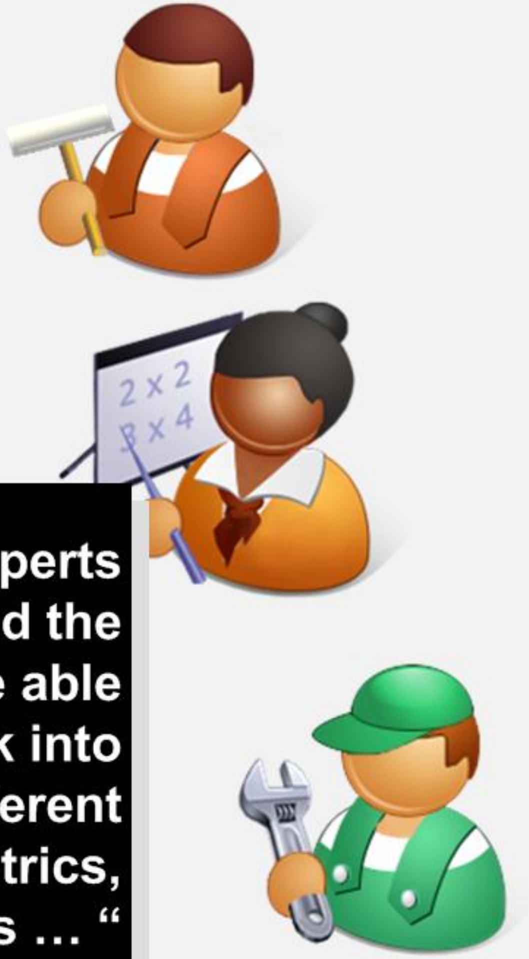
Risk Management

Author: Prof Bill Buchanan

Risk Management
Introduction

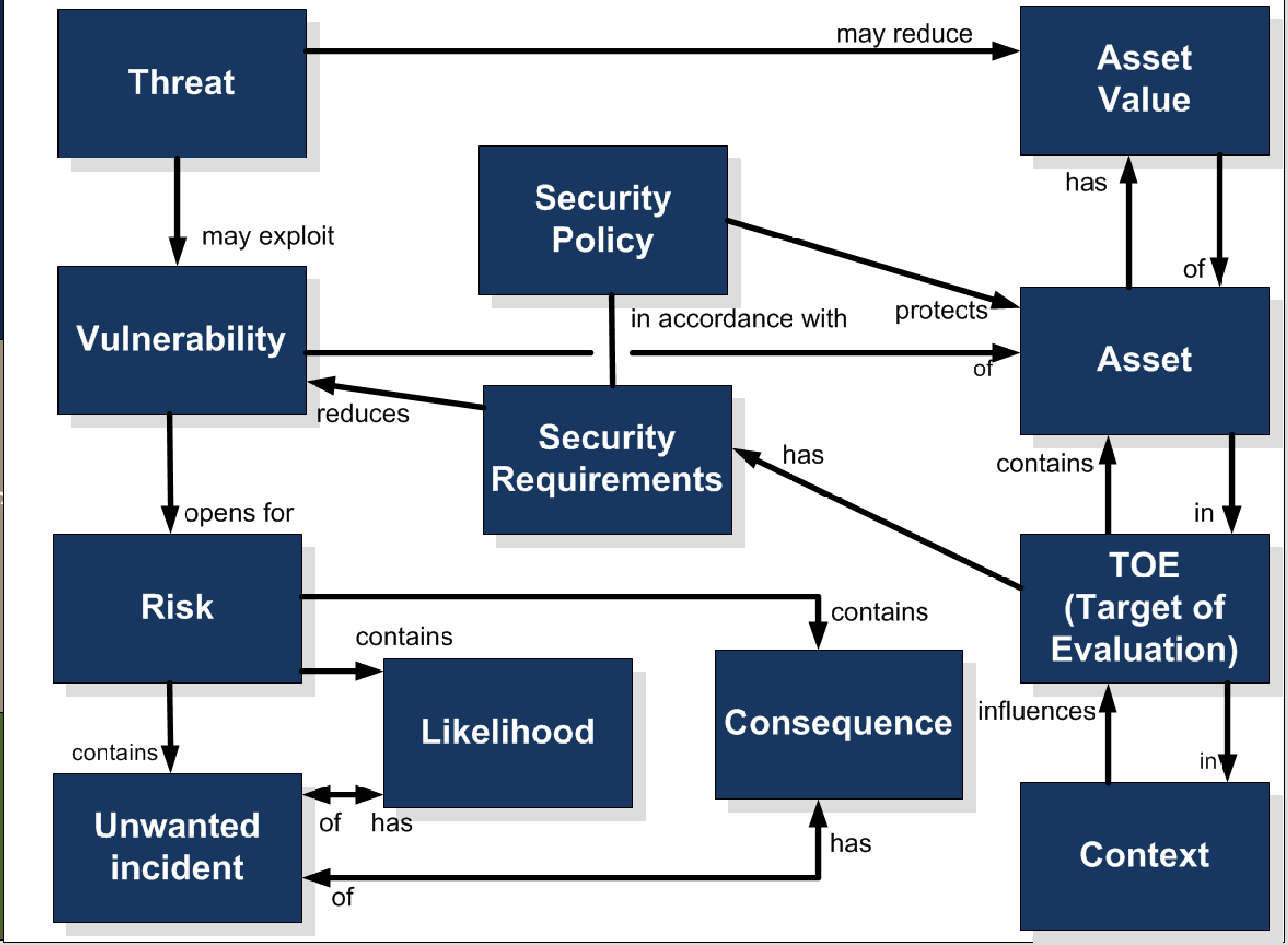
Business context

Technical context

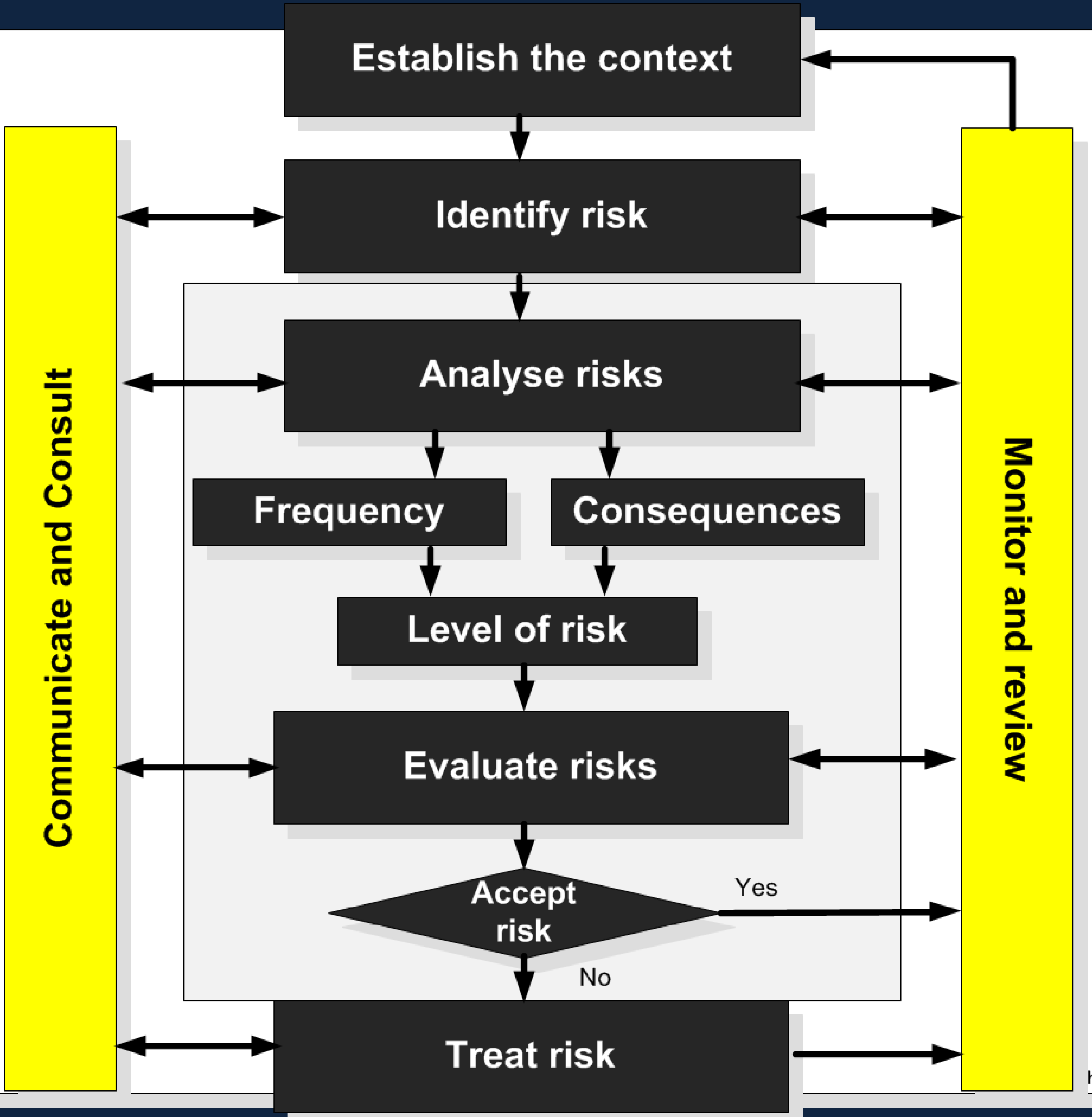


> "Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context … different vocabularies, definitions, metrics, processes and standards … "
> Woloch (2006)

CORAS ontology

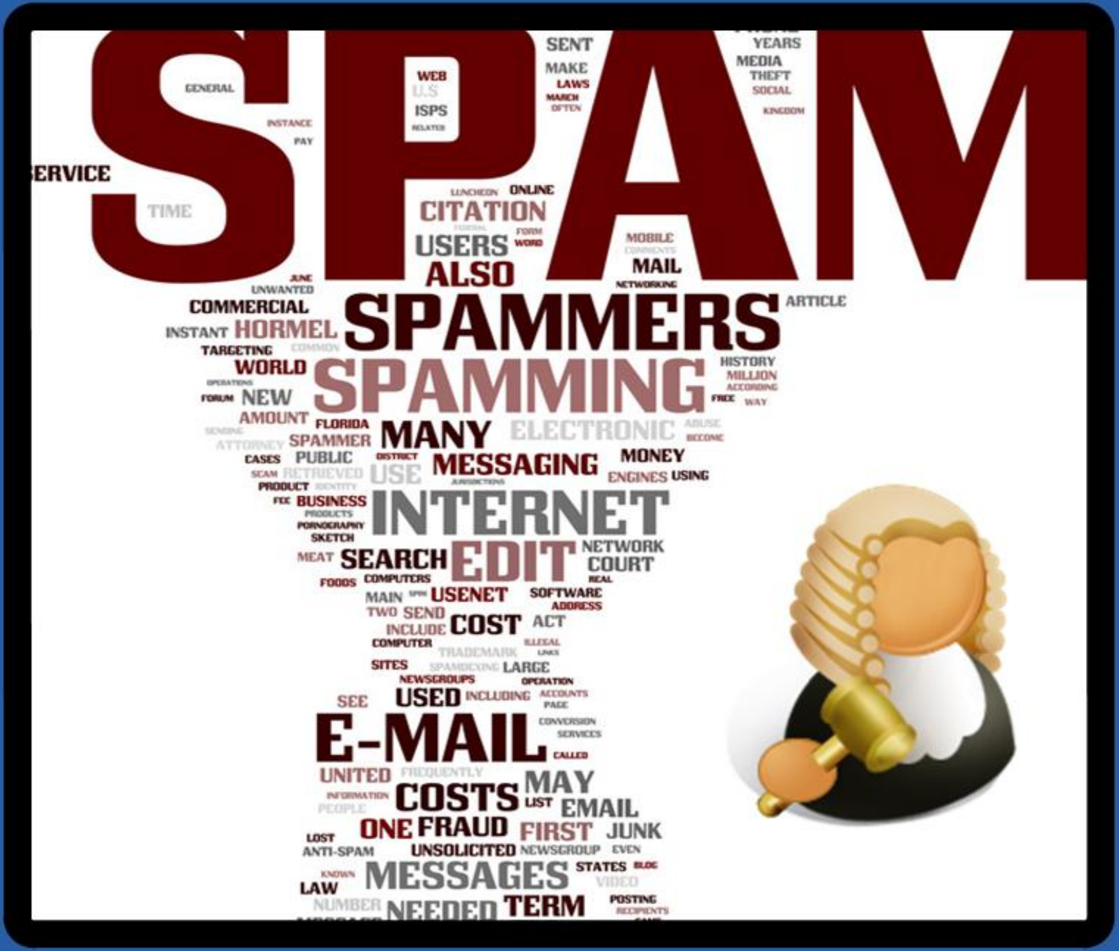


CORAS ontology



CORAS risk management

Introduction



Security Taxonomy

Author: Prof Bill Buchanan

A Threat:

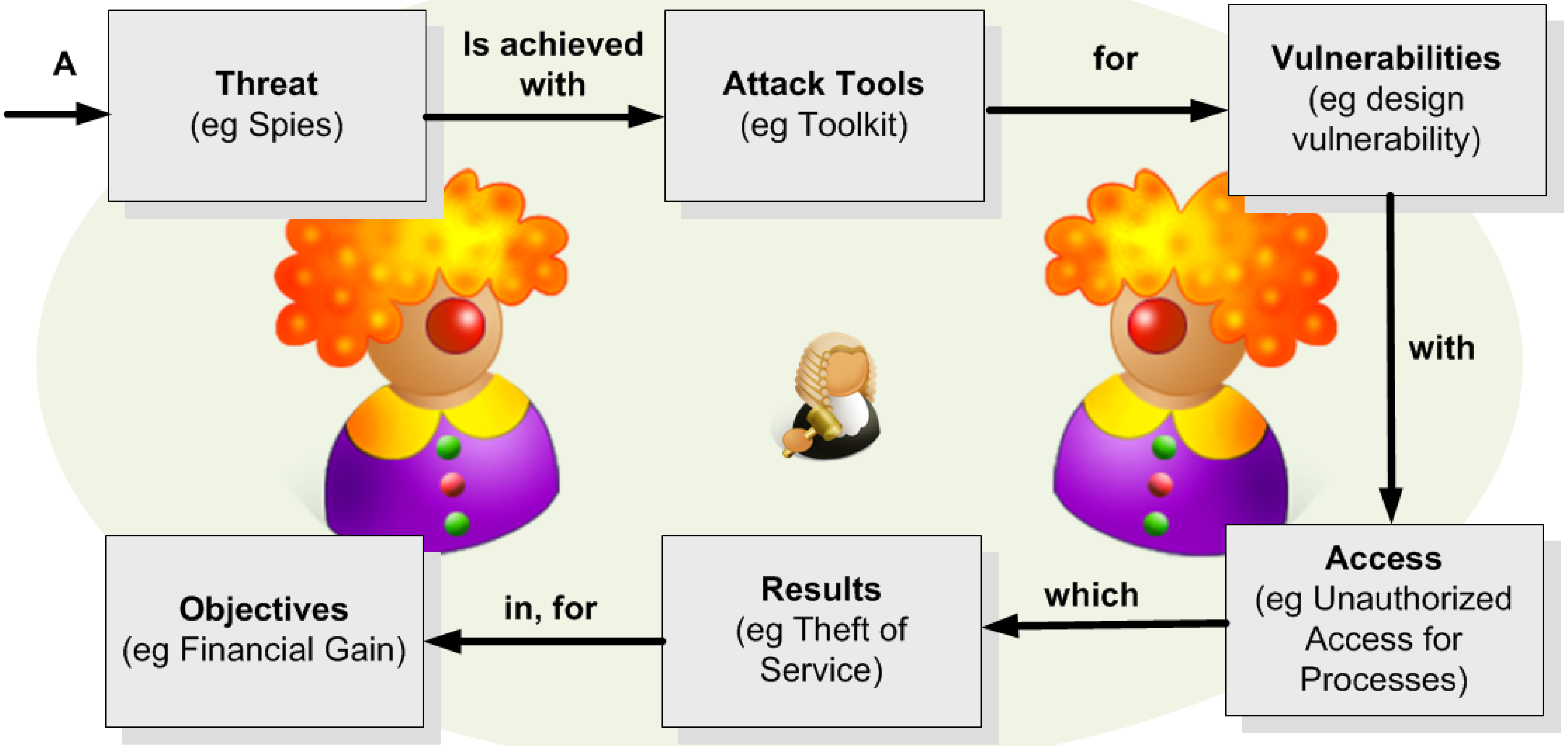
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:

- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:

- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.



A → **Threat** (eg Spies) → **Is achieved with** → **Attack Tools** (eg Toolkit) → **for** → **Vulnerabilities** (eg design vulnerability) → **with** → **Access** (eg Unauthorized Access for Processes) → **which** → **Results** (eg Theft of Service) → **in, for** → **Objectives** (eg Financial Gain)

for Objectives:

- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

which Results in:

- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:

- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

Security Incident taxonomy

Introduction

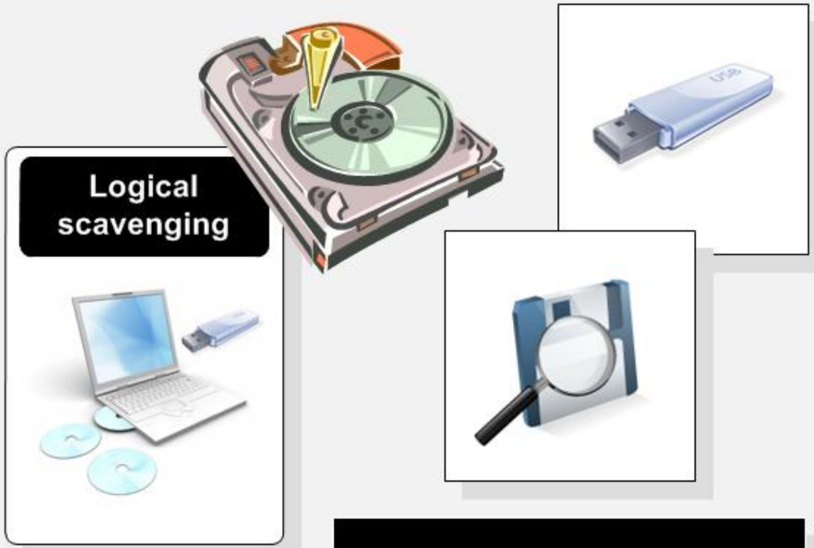
Threats

Author: Prof Bill Buchanan

Threats: Visual spying/misrepresentation

Eavesdropping

Eavesdropping. This involves intercepting communications.

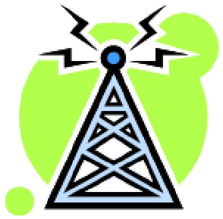

Logical scavenging

Logical scavenging. This involves scavenging through discarded media.

Author: Prof Bill Buchanan

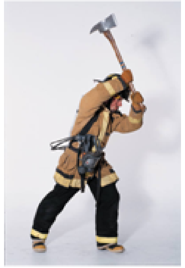
Threats: Interference/Physical attacks

Interference



Interference. This involves the actual interference of communications, such as jamming communications, or modifying it in some way.

Physical attacks

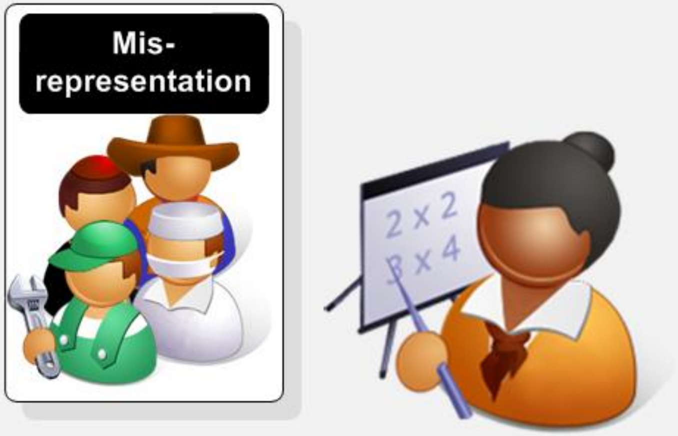


Physical removal

Physical attacks. This involves an actual physical attack on the hardware. **Physical removal**. This involves the actual physical removal of hardware.

Author: Prof Bill Buchanan

Visual spying. This actual physical viewing a user's activities, such as their keystrokes or mouse clicks.



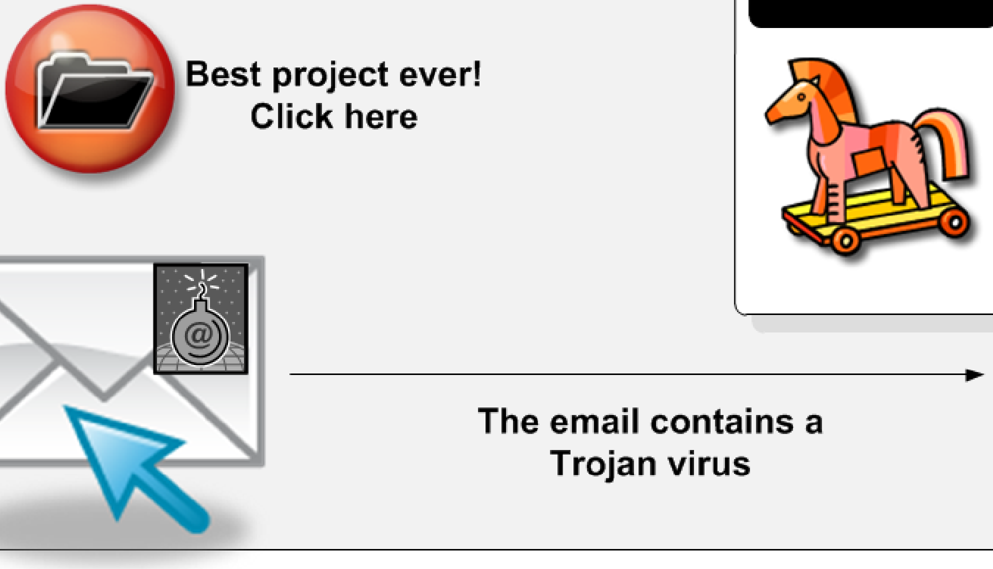
Misrepresentation. This involves the actual deception of users and system operators.

Author: Prof Bill Buchanan

Threats: Visual spying/misrepresentation

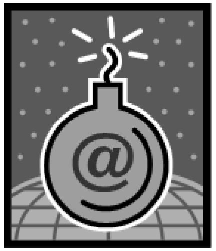
Trojan horses. This involves users running programs which look valid, but install an illicit program which will typically do damage to the host.

Logic bombs. This involves the installation of a program which will trigger some time in the future based on time or an event.



Trojan horse

Logic bombs



Threats

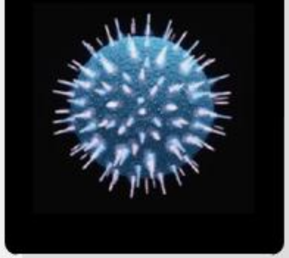
Introduction

Author: Prof Bill Buchanan

Threats:Trojan/logical bomb

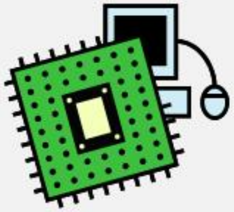
Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.

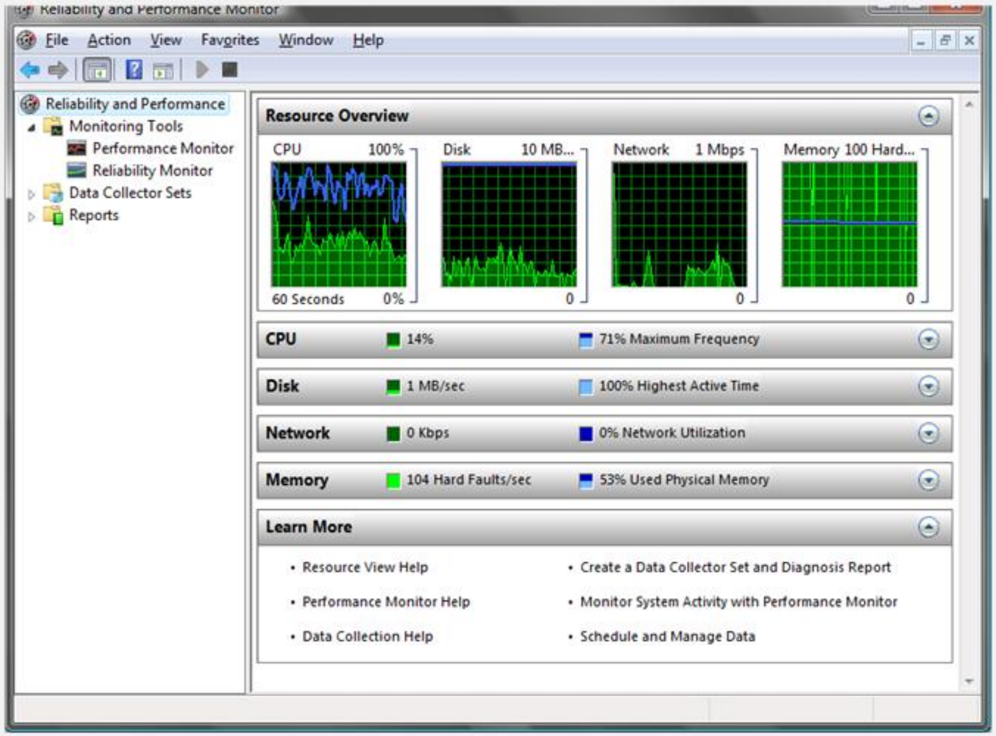
Viruses



Viruses. This involves attaching program which self replicate themselves.

Worms





Resource Overview

CPU	🟩 14%	🟦 71% Maximum Frequency
Disk	🟩 1 MB/sec	🟦 100% Highest Active Time
Network	🟩 0 Kbps	🟦 0% Network Utilization
Memory	🟩 104 Hard Faults/sec	🟦 53% Used Physical Memory

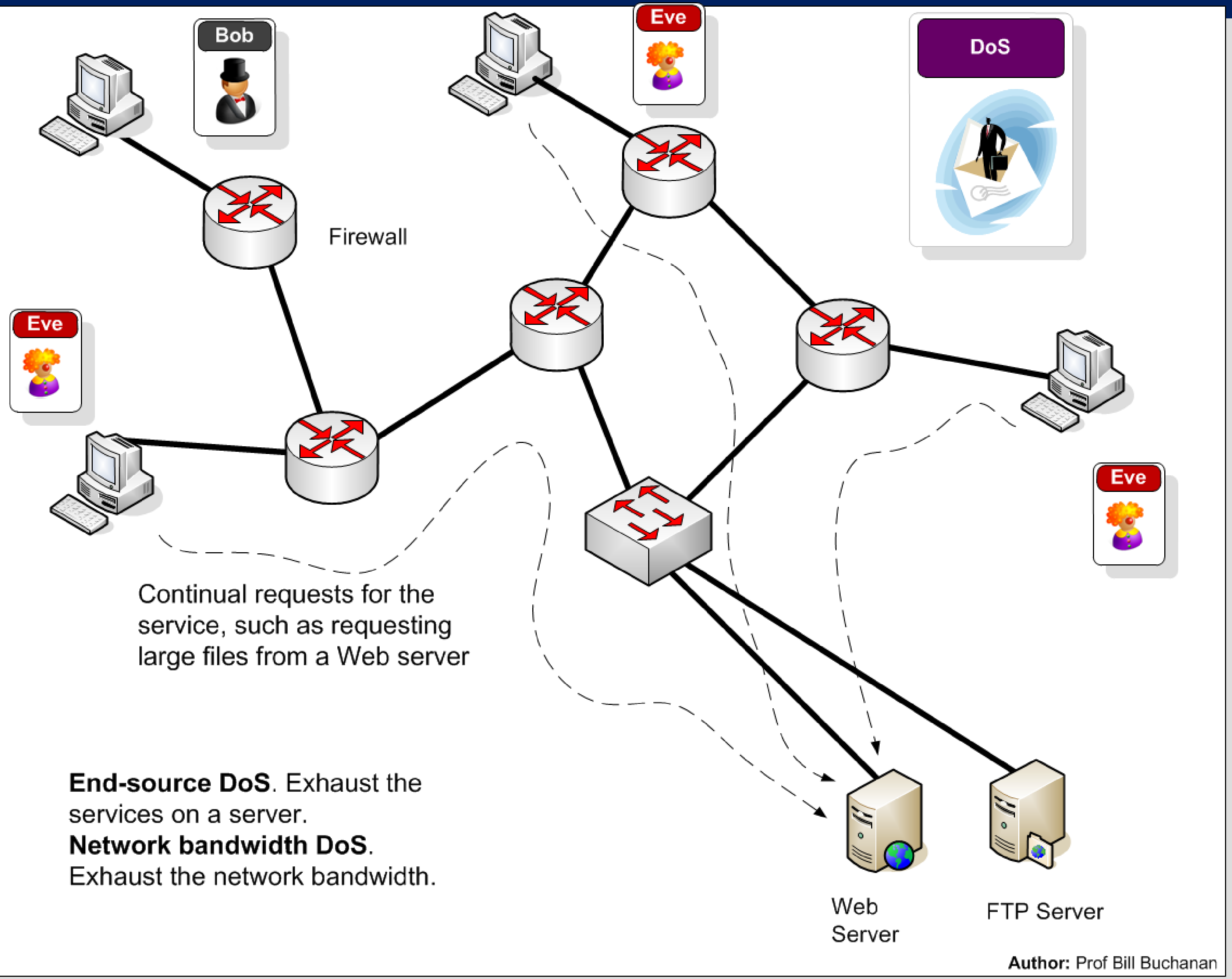
Learn More

- Resource View Help
- Performance Monitor Help
- Data Collection Help
- Create a Data Collector Set and Diagnosis Report
- Monitor System Activity with Performance Monitor
- Schedule and Manage Data

Threats

Introduction

Threats: Worms/viruses



Continual requests for the service, such as requesting large files from a Web server

End-source DoS. Exhaust the services on a server.
Network bandwidth DoS.
Exhaust the network bandwidth.

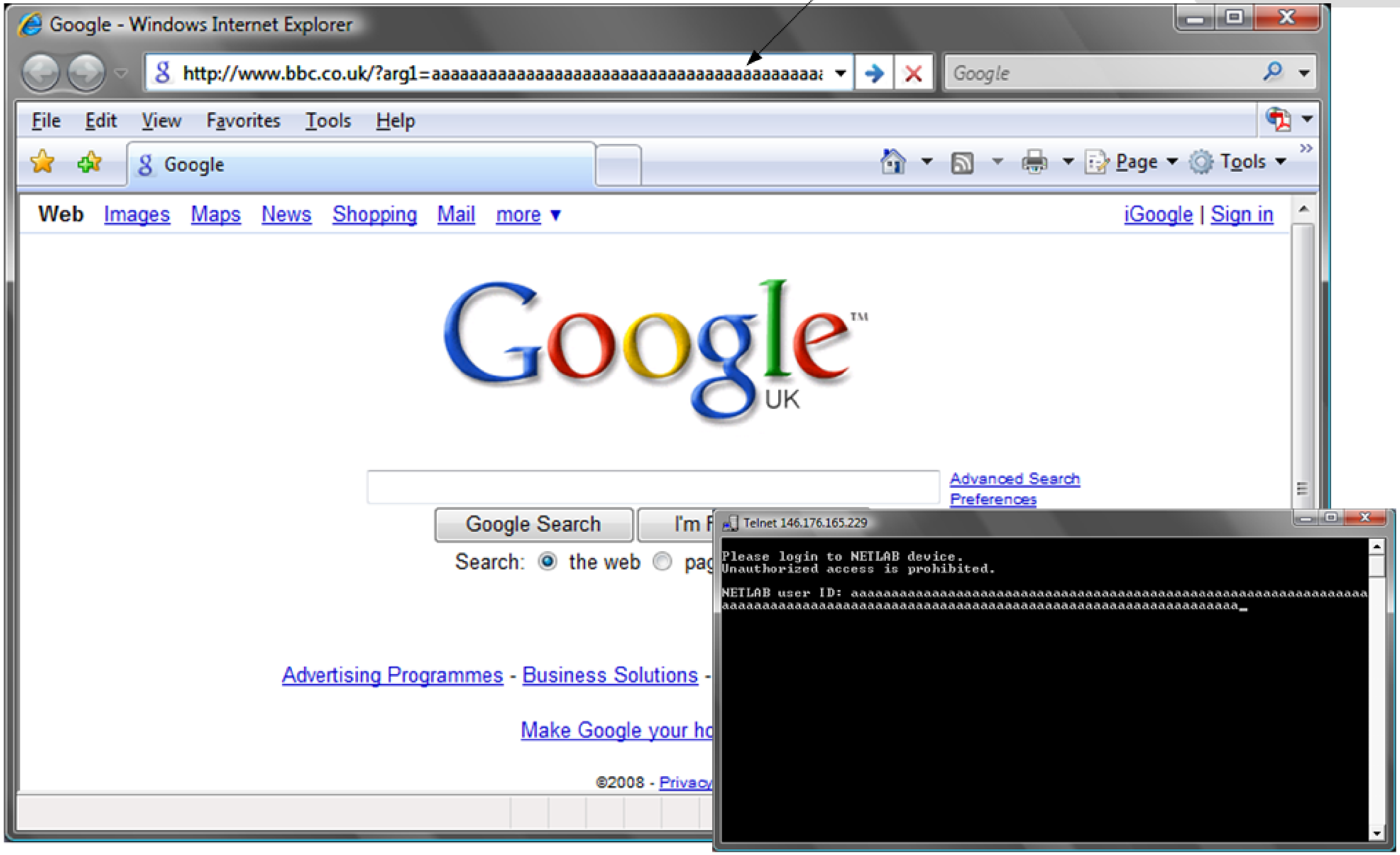
Author: Prof Bill Buchanan

Threats: DoS/DDoS

Active attack

Active attack. This entering incorrect data with the intention to do damage to the system.

Possible buffer overflow attack where the intruder tries to put incorrect information into the page


Google - Windows Internet Explorer
http://www.bbc.co.uk/?arg1=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Google
File Edit View Favorites Tools Help
Google
Page Tools
Web Images Maps News Shopping Mail more ▾
iGoogle | Sign in
Google UK
Advanced Search
Preferences
Google Search
I'm F
Search: ● the web ○ pag
Advertising Programmes - Business Solutions -
Make Google your ho
©2008 - Privacy
Telnet 146.176.165.229

```
Please login to NETLAB device.
Unauthorized access is prohibited.

NETLAB user ID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa_
```

Threats

Introduction

Author: Prof Bill Buchanan

Threats: Inference

Inference

Inference. This involves exploiting database weaknesses using inferences.

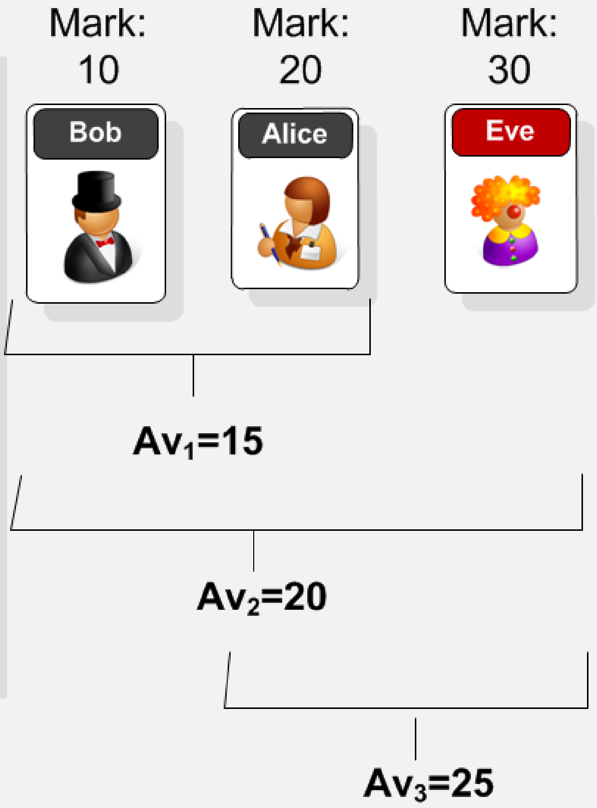
For example … the marks for any student is not allowed, but the average a number of students is allowed.

Query: Average(Bob,Alice) -> Av_1= (B+A)/2
Query: Average(Bob,Eve) -> Av_2= (B+E)/2
Query: Average(Alice,Eve) -> Av_3= (A+E)/2

Av_1-Av_2=(A-E)/2

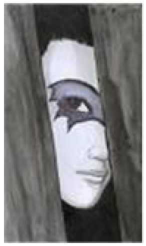
Av_1-Av_2+Av_3 = (A-E)/2+(A+E)/2=A

Alice's mark is Av_1-Av_2+Av_3



Alice's mark=Av_1-Av_2+Av_3=15-20+25=20

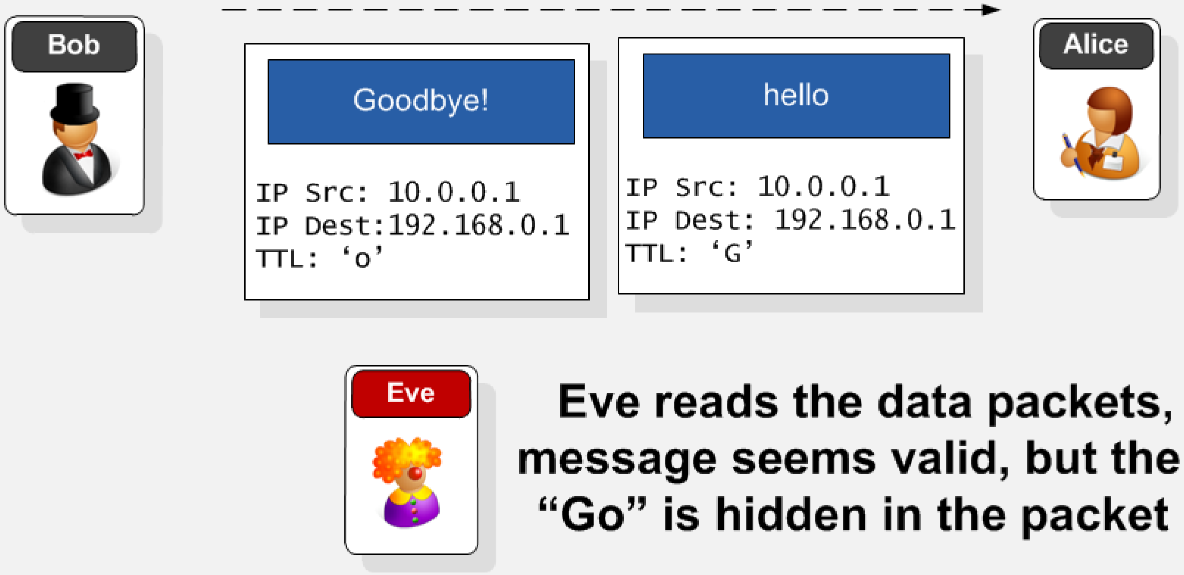
Covert channel



Covert channels. This involves hiding data in valid network traffic.

Timing channel. Transmit with relative timing of events.

Storage channel. Modify an object (such as adding to network packet headers).



```
IP Src: 10.0.0.1
IP Dest:192.168.0.1
TTL: 'o'
```

```
IP Src: 10.0.0.1
IP Dest: 192.168.0.1
TTL: 'G'
```

Eve reads the data packets, and the message seems valid, but the message "Go" is hidden in the packet headers.

Author: Prof Bill Buchanan

Threats: Covert channels

Spoofing. This involves the spoofing of devices.

Spoofing

Hello… I'm Bob!
Hello… I'm Bob!

Bob

Eve

Hello… I'm Bob!
Hello… I'm Bob!

Im-personation

Impersonation. This involves the impersonation of a user/device.

Author: Prof Bill Buchanan

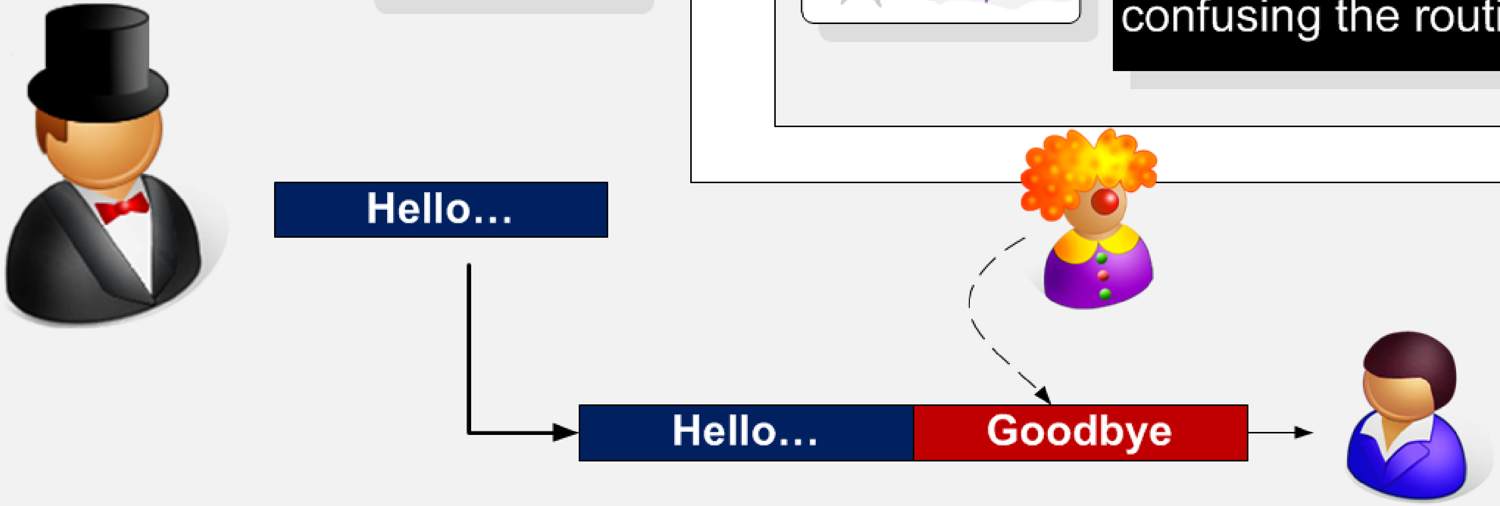
Threats: Spoofing/impersonation

Piggy back attacks. This involves adding data onto valid data packets.

Piggy back

Network weaving

Network weaving. This involves confusing the system onto the whereabouts of a device, or confusing the routing.



Hello…

Hello… Goodbye

A virus has piggybacked onto an email

Author: Prof Bill Buchanan

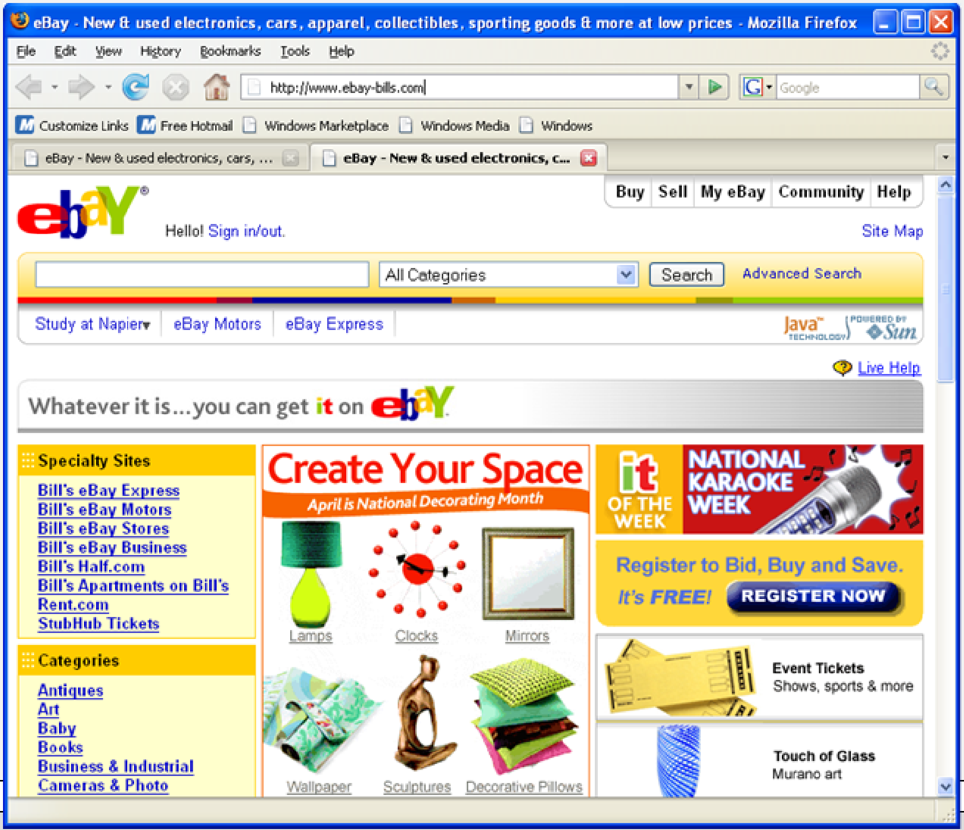
Threats: Piggy back/network weaving

Authorization attacks. This involves trying to gain access to a higher level of authorization than is valid for the user, such as with password attacks.

Trap-door

Trap door impersonation. This involves the creation of pages or login screens which look valid, but are used to gain information from a user, such as their bank details, or login password.

Authorization attack



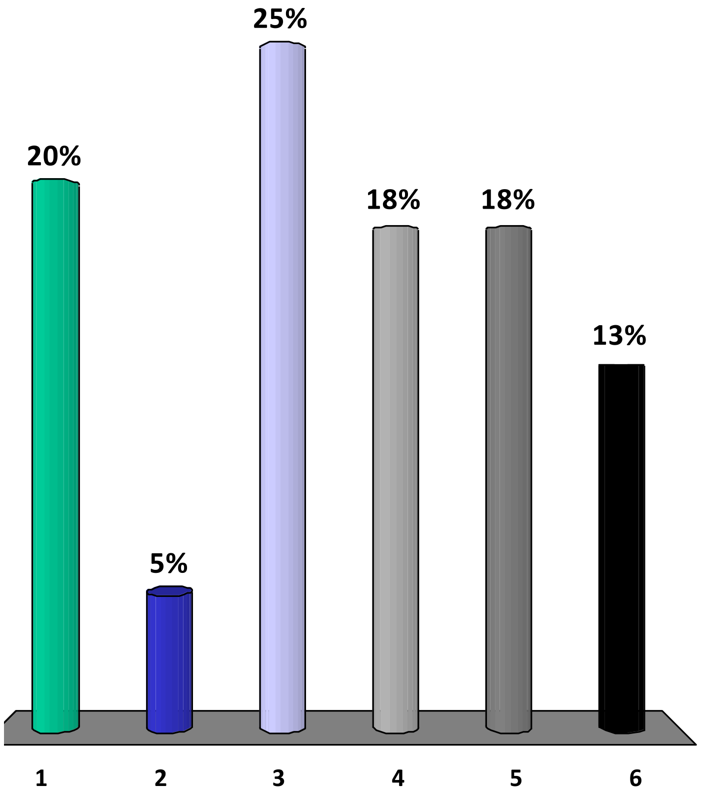
Threats

Introduction

Threats: Authorization attack/trap door

Which infects computer systems with the intentionally to copy themselves onto other systems

1. Viruses
2. Trojans
3. Logic bombs
4. Worms
5. Bots
6. Rootkits



Which pretends to be a useful application, but has malicious intent

1. Viruses
2. [✓ Trojans]
3. Logic bombs
4. Worms
5. Bots
6. Rootkits

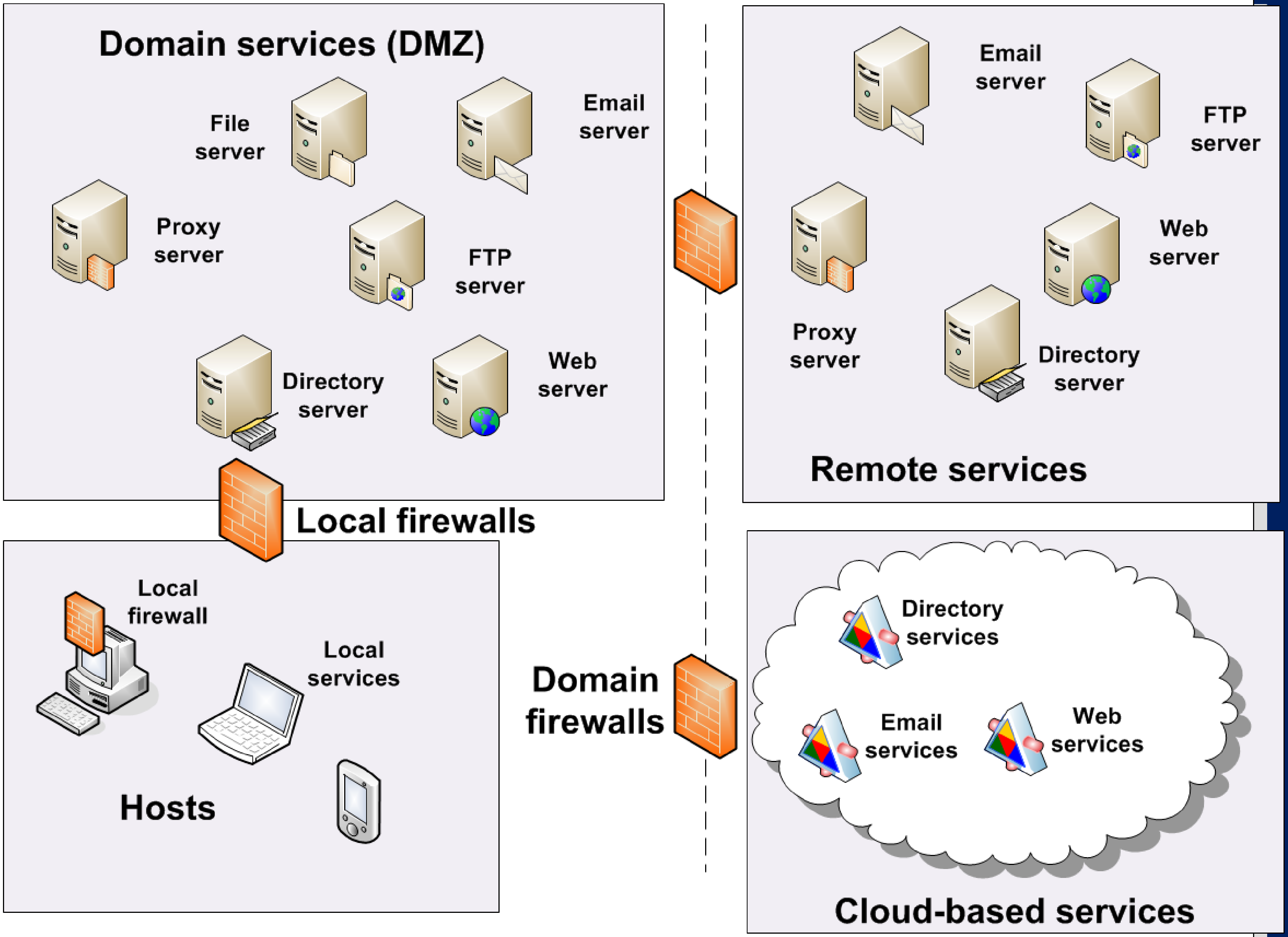
Participant Scores

3	Participant 2
3	Participant 4
3	Participant 25
2	Participant F3D61
2	Participant 14

Introduction

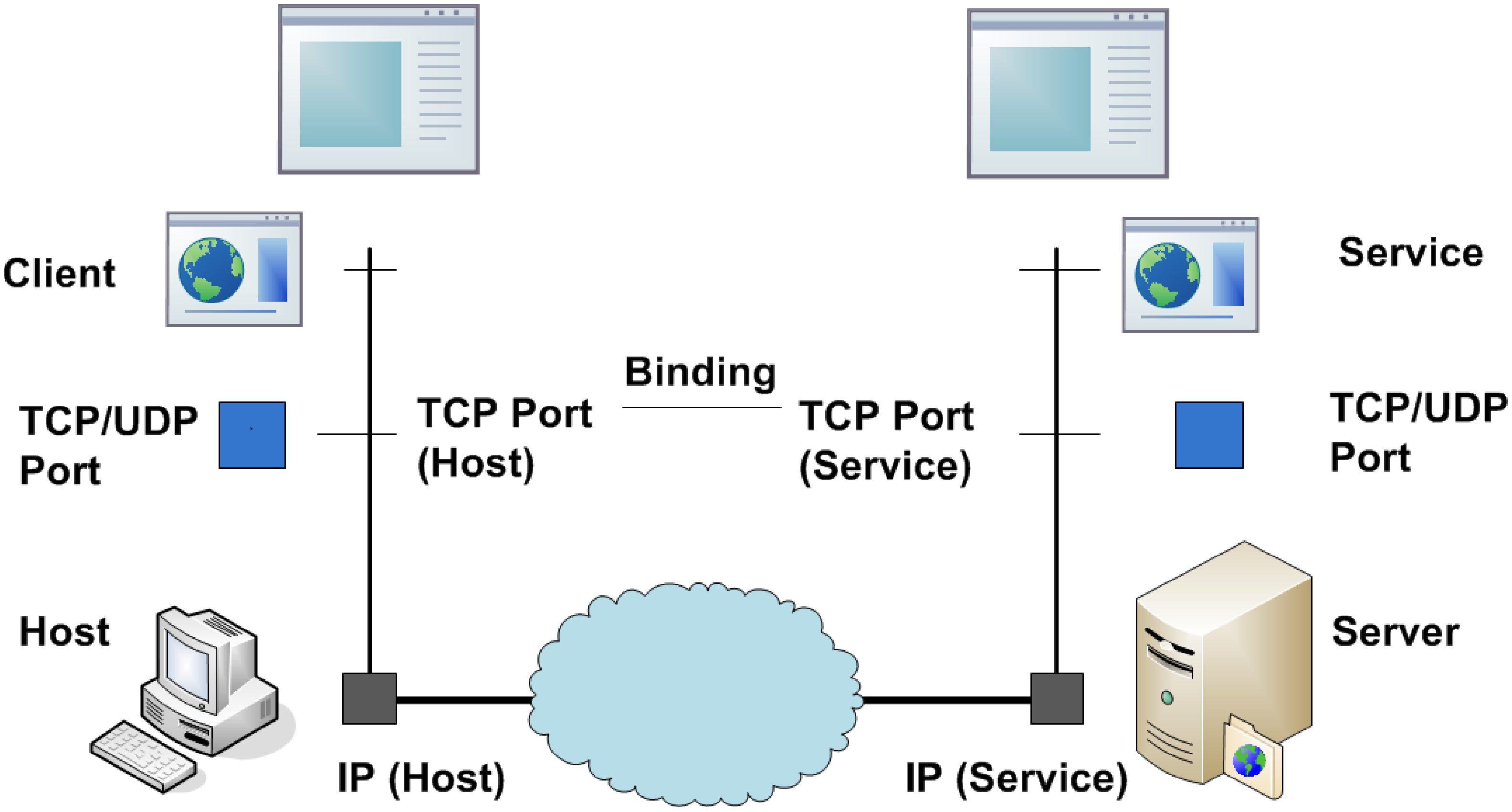
SoA

Author: Prof Bill Buchanan



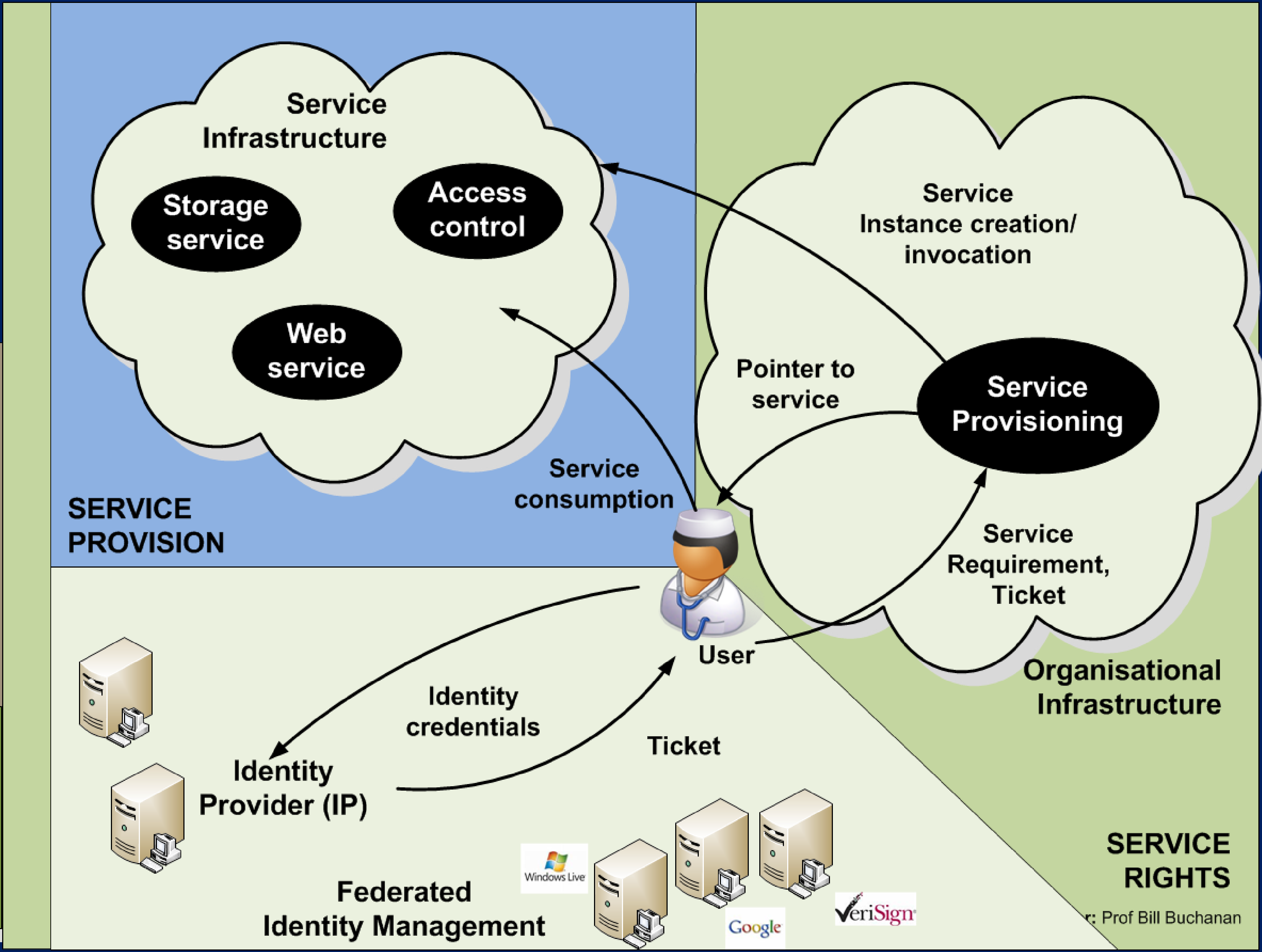
Author: Prof Bill Buchanan

Accessing services



Author: Prof Bill Buchanan

Port binding for services



Service Infrastructure

Storage service

Access control

Web service

SERVICE PROVISION

Service consumption

Service Instance creation/ invocation

Pointer to service

Service Provisioning

Service Requirement, Ticket

User

Organisational Infrastructure

Identity credentials

Ticket

Identity Provider (IP)

Federated Identity Management

SERVICE RIGHTS

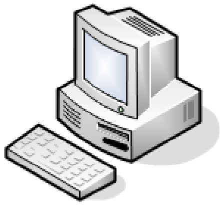
r: Prof Bill Buchanan

Next-generation Web infrastructure

Introduction

Cloud Computing

Author: Prof Bill Buchanan



Client

Software as a Service (SaaS)

- User interface.
- Machine interface

Platform as a Service (PaaS)

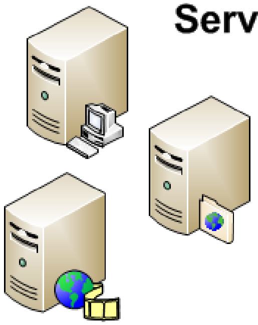
- Service Oriented Architecture (SOA)
- Sophisticated Web Services
- Developing
- Testing
- Deploying
- Hosting
- Service platform providers, e.g. Google GAE, Microsoft Windows Azure

Infrastructure as a Service (IaaS)

- Resource virtualisation
- Computing power
- Storage capacity
- Network bandwidth
- Usage-based payment scheme
- Cloud enablers, e.g. Amazon EC2 / S3

Hardware as a Service (HaaS)

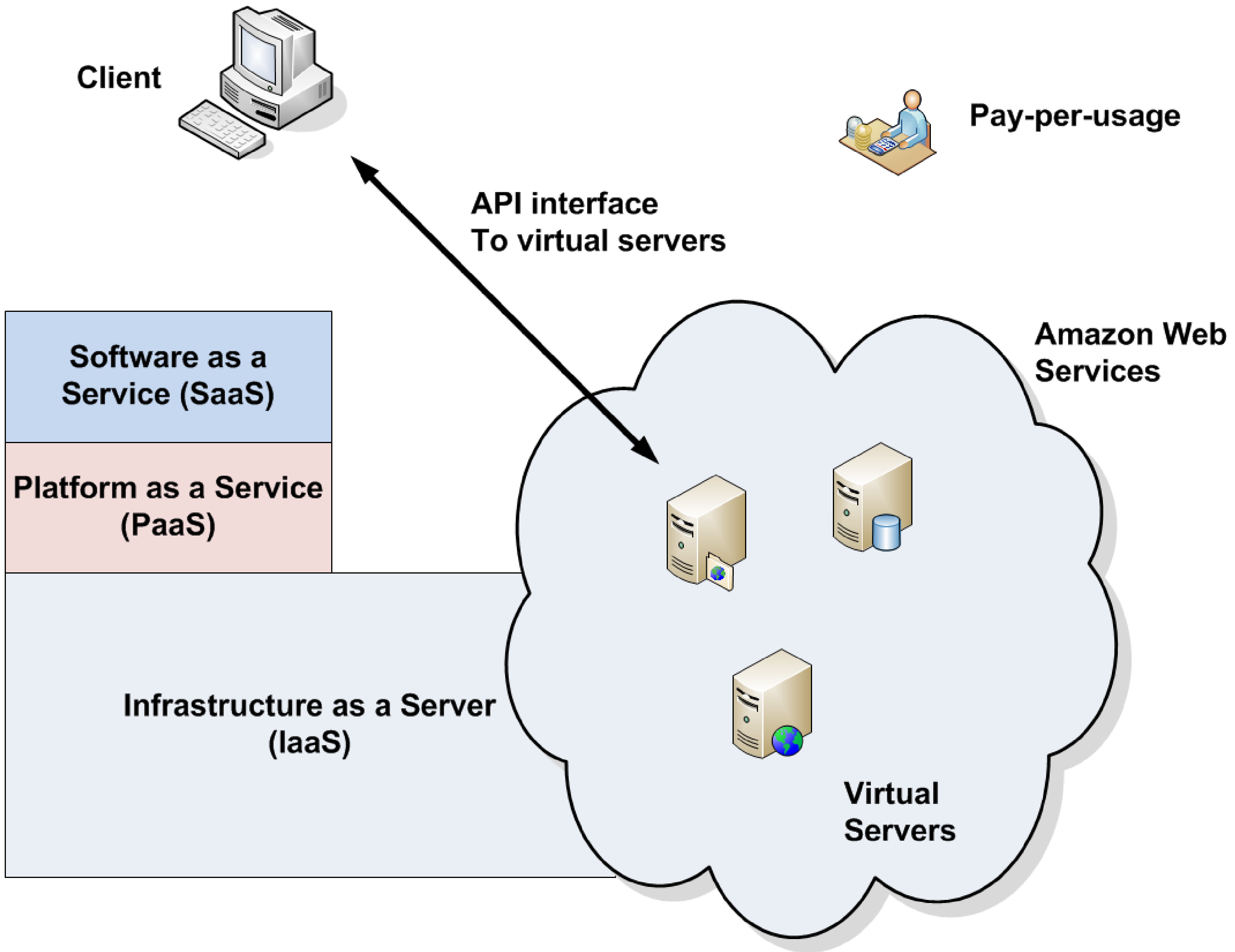
- Cluster & data centre providers
- Reduction of capital & operation investments
- Enhanced reliability – redundancy, replication & failover
- Enhanced scalability
- Enhanced load-balancing



Servers

Cloud/grid infrastructure

IaaS



Client

Pay-per-usage

API interface
To virtual servers

Software as a Service (SaaS)

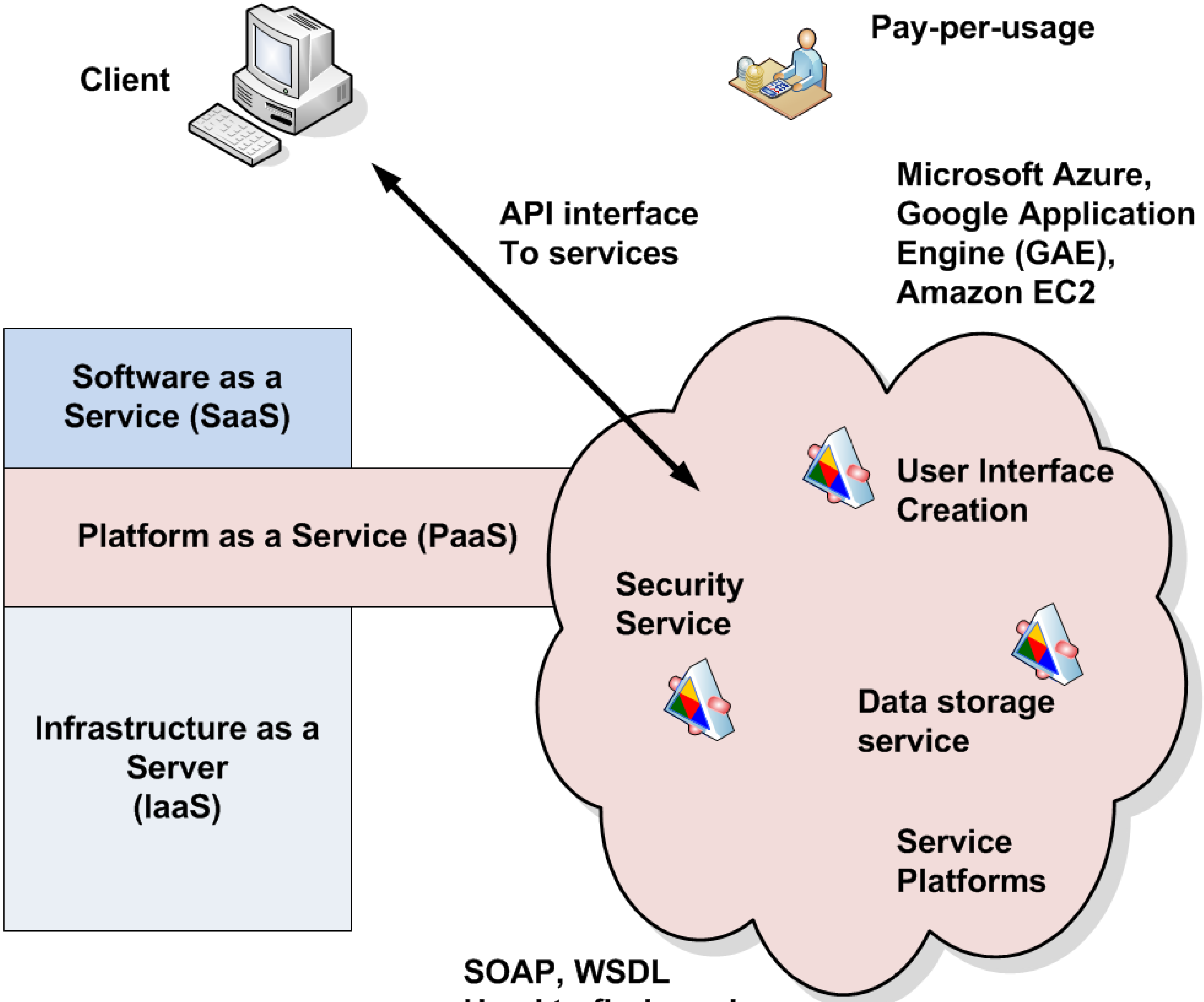
Platform as a Service (PaaS)

Infrastructure as a Server (IaaS)

Amazon Web Services

Virtual Servers

PaaS



Client

Pay-per-usage

API interface
To services

Microsoft Azure,
Google Application
Engine (GAE),
Amazon EC2

Software as a
Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a
Server
(IaaS)

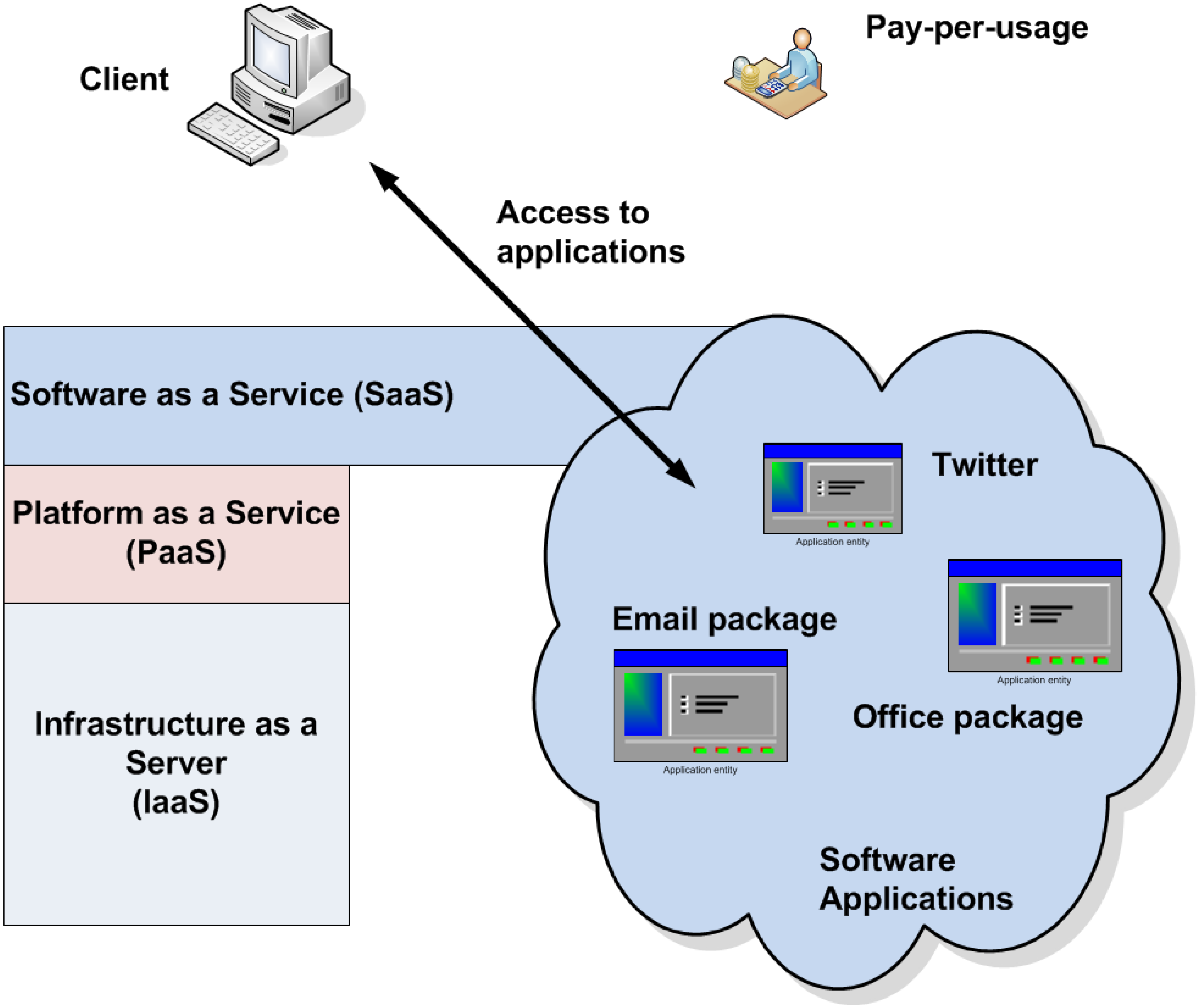
User Interface
Creation

Security
Service

Data storage
service

Service
Platforms

SOAP, WSDL
Used to find services



Client

Pay-per-usage

Access to applications

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Server (IaaS)

Twitter

Email package

Office package

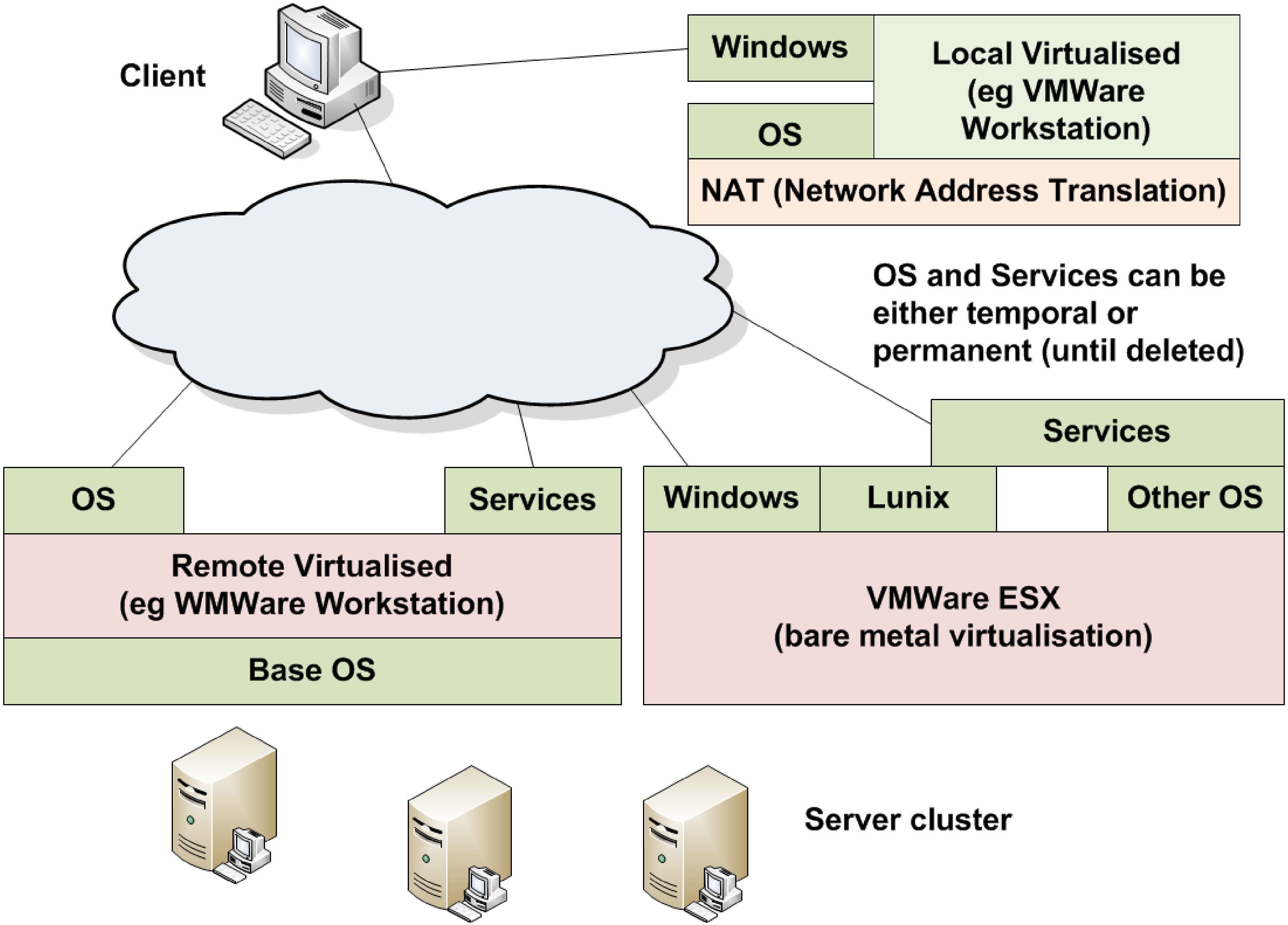
Software Applications

SaaS

Introduction

Virtualisation

Author: Prof Bill Buchanan



Client

Windows

OS

Local Virtualised (eg VMWare Workstation)

NAT (Network Address Translation)

OS and Services can be either temporal or permanent (until deleted)

OS

Services

Remote Virtualised (eg WMWare Workstation)

Base OS

Services

Windows

Lunix

Other OS

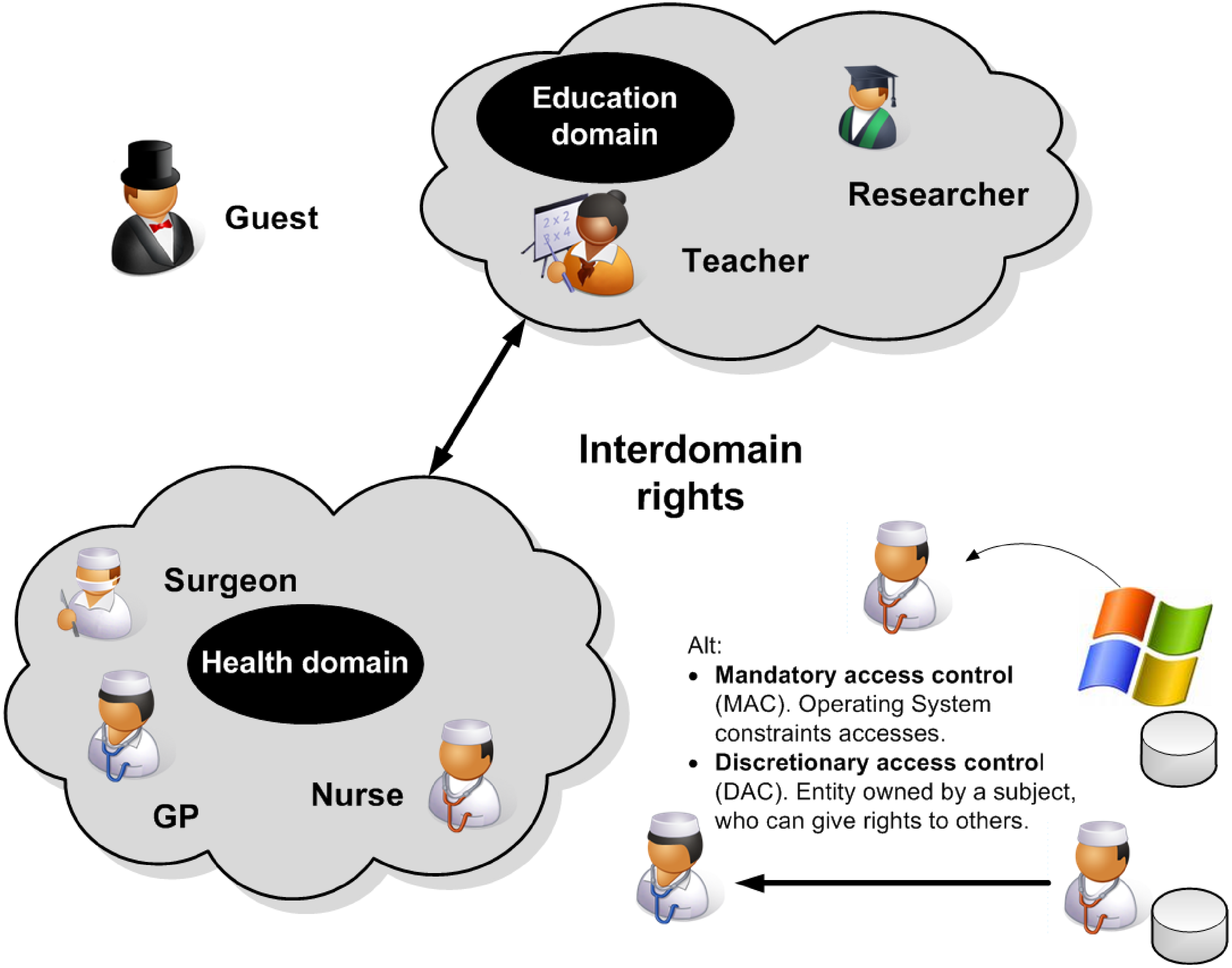
VMWare ESX (bare metal virtualisation)

Server cluster

Introduction

Role-based Security

Author: Prof Bill Buchanan



Alt:

- **Mandatory access control** (MAC). Operating System constraints accesses.
- **Discretionary access control** (DAC). Entity owned by a subject, who can give rights to others.

Introduction

- Provide an outline of risk, and the terminology used.
- Provide an outline to a range of threats.
- Understand the usage of client/server connections.
- Outline the usage of services on Windows and Linux, and provide an introduction to service-oriented infrastructures.
- Provide a practical background in Windows and Linux for services, logging and auditing.