Introduction

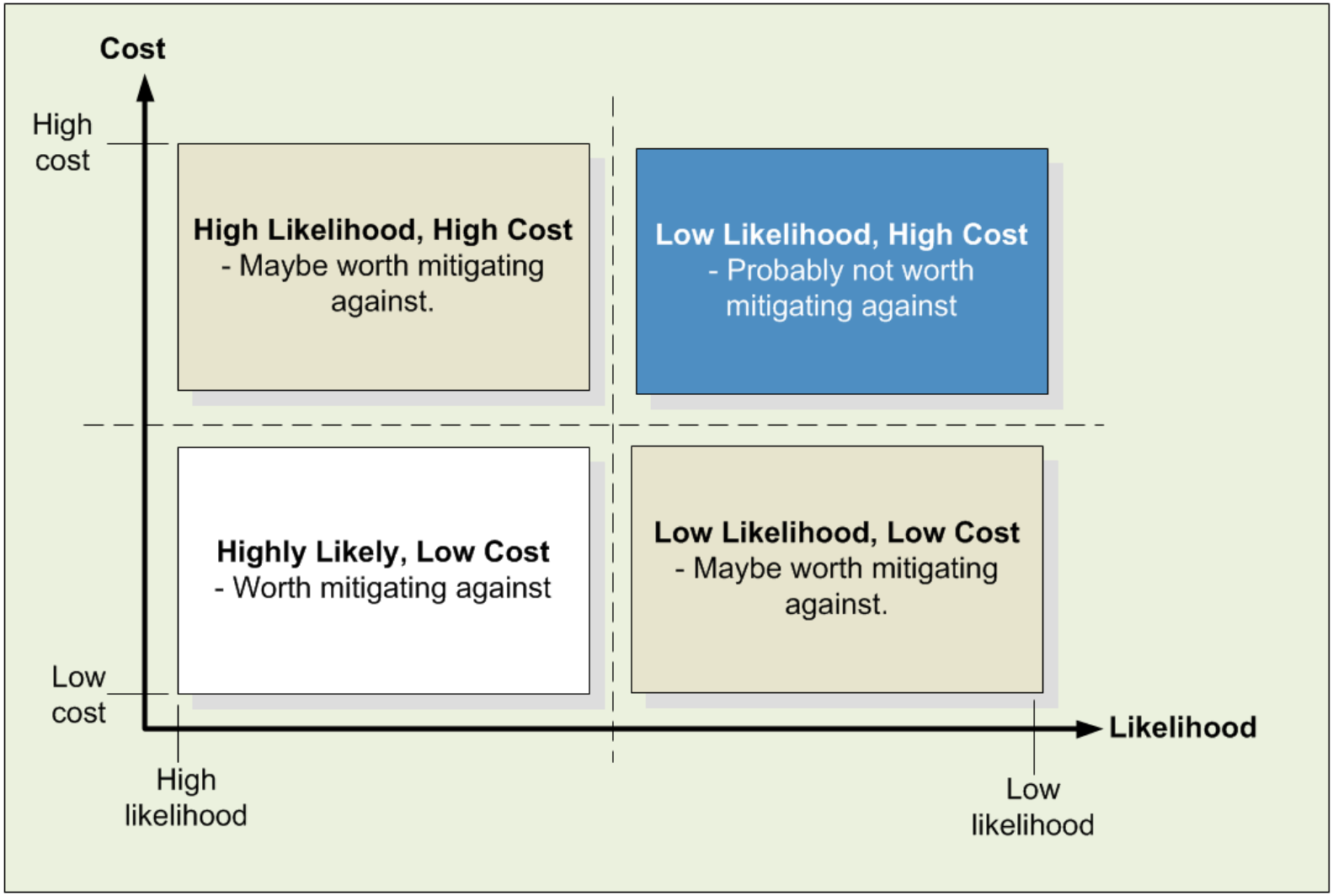
- Provide an outline of risk, and the terminology used.
- Provide an outline to a range of threats.
- Understand the usage of client/server connections.
- Outline the usage of services on Windows and Linux, and provide an introduction to service-oriented infrastructures.
- Provide a practical background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

Author: Prof Bill Buchanan

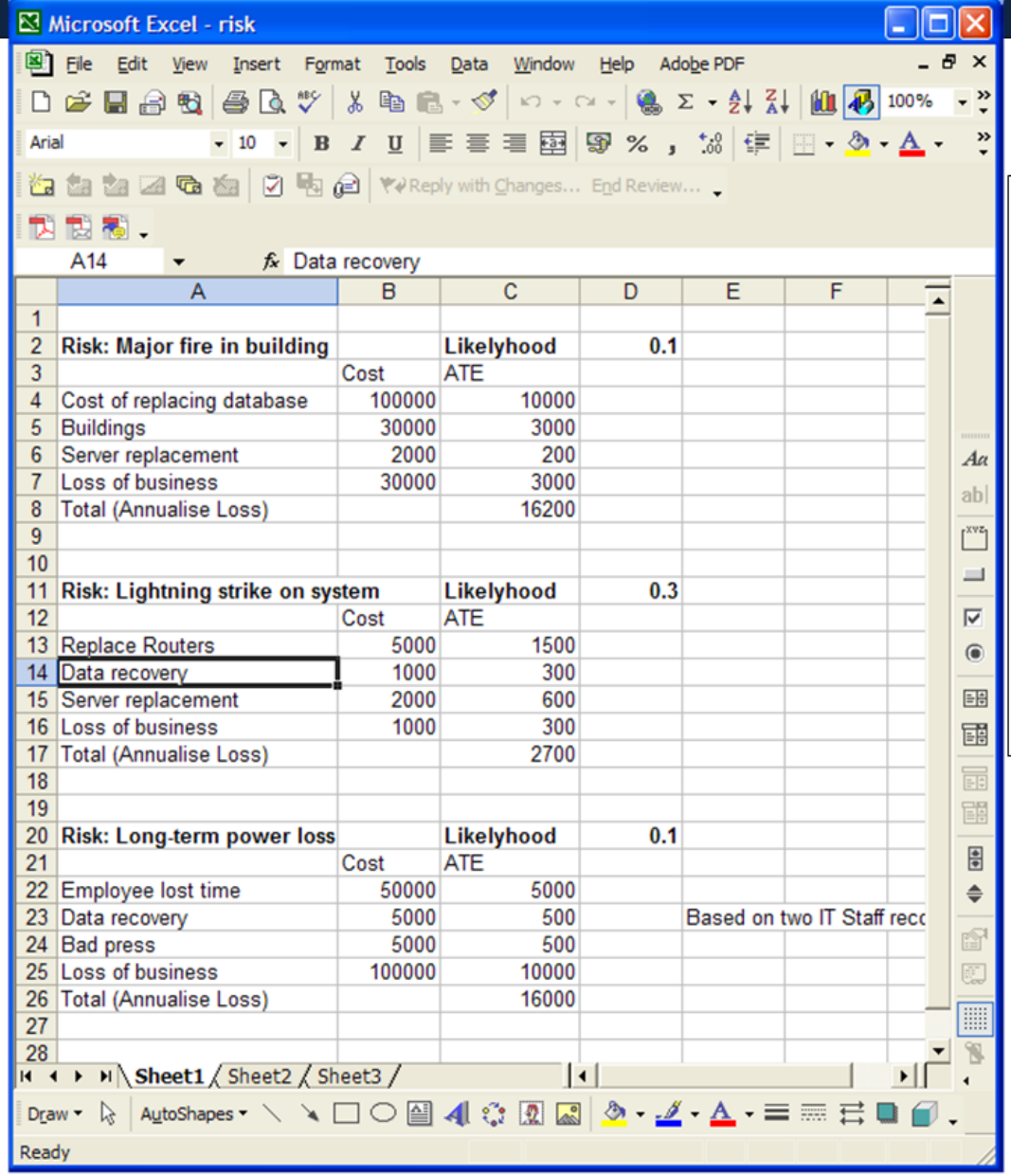
Introduction

Risk Analysis

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



	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 recc	
24	Bad press	5000	500			
25	Loss of business	100000	10000			
26	Total (Annualise Loss)		16000			
27						
28						

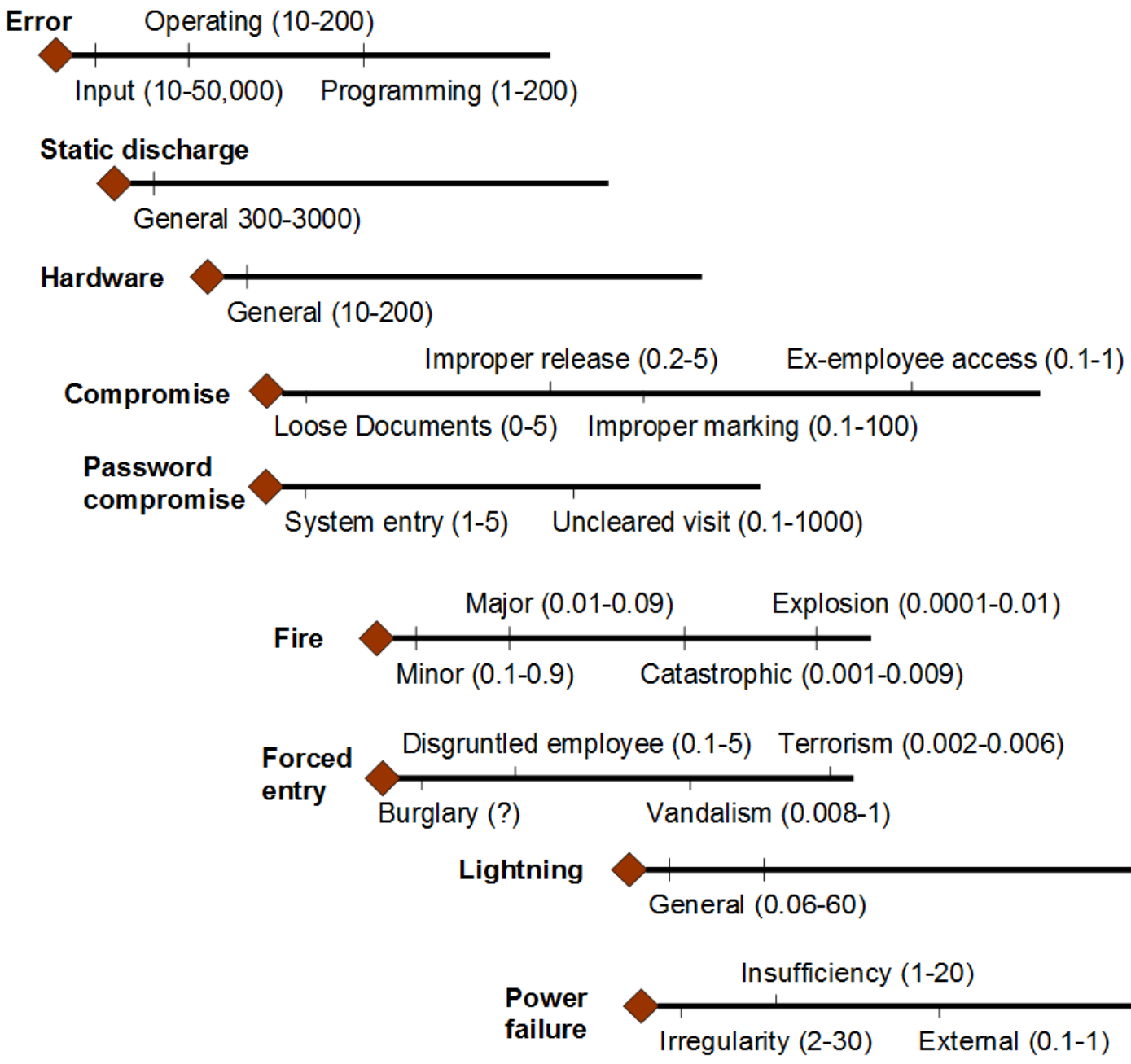
ALE = *T* x *V*

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



Author: Prof Bill Buchanan

Introduction

Risk Management

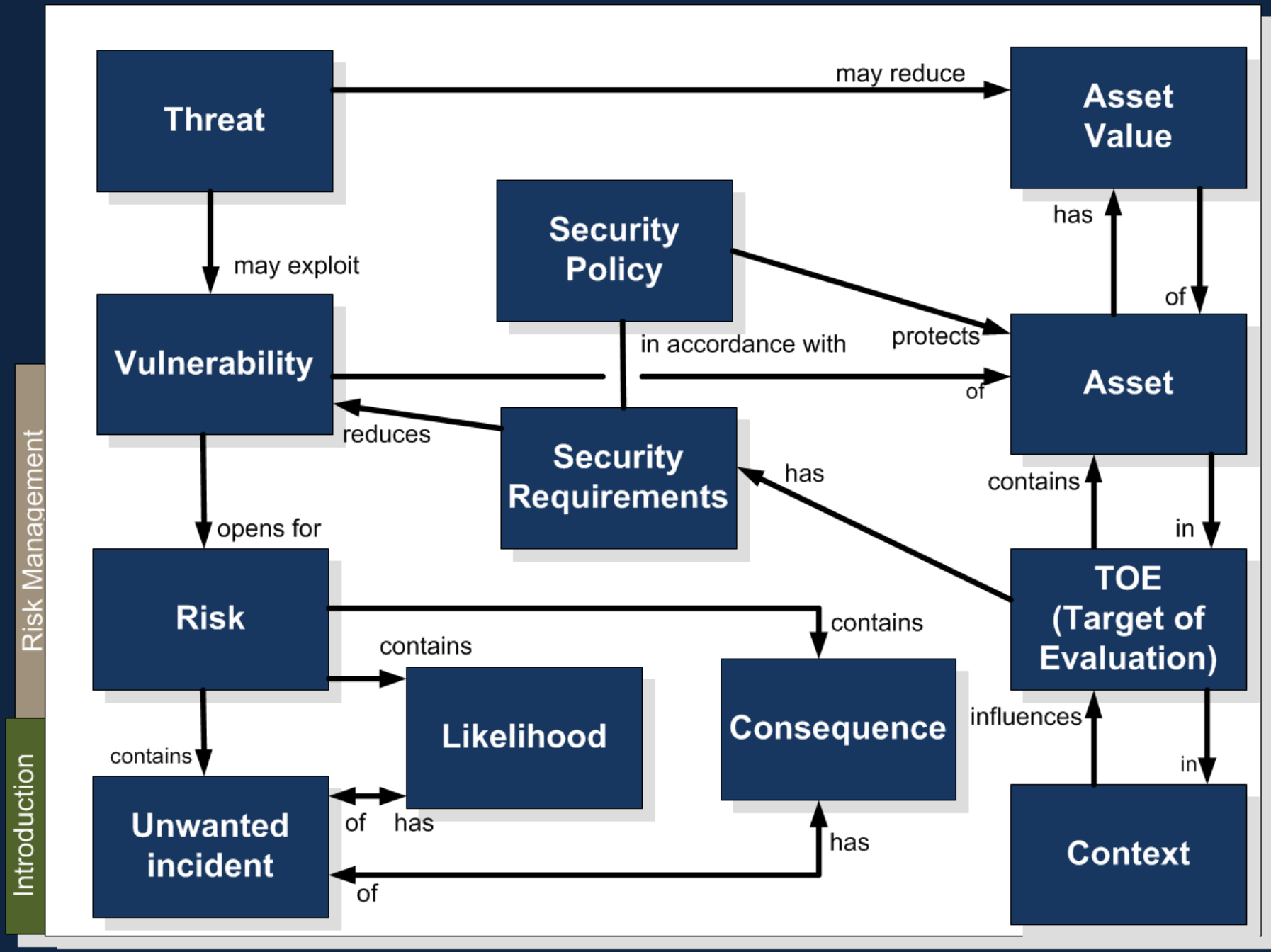
Author: Prof Bill Buchanan

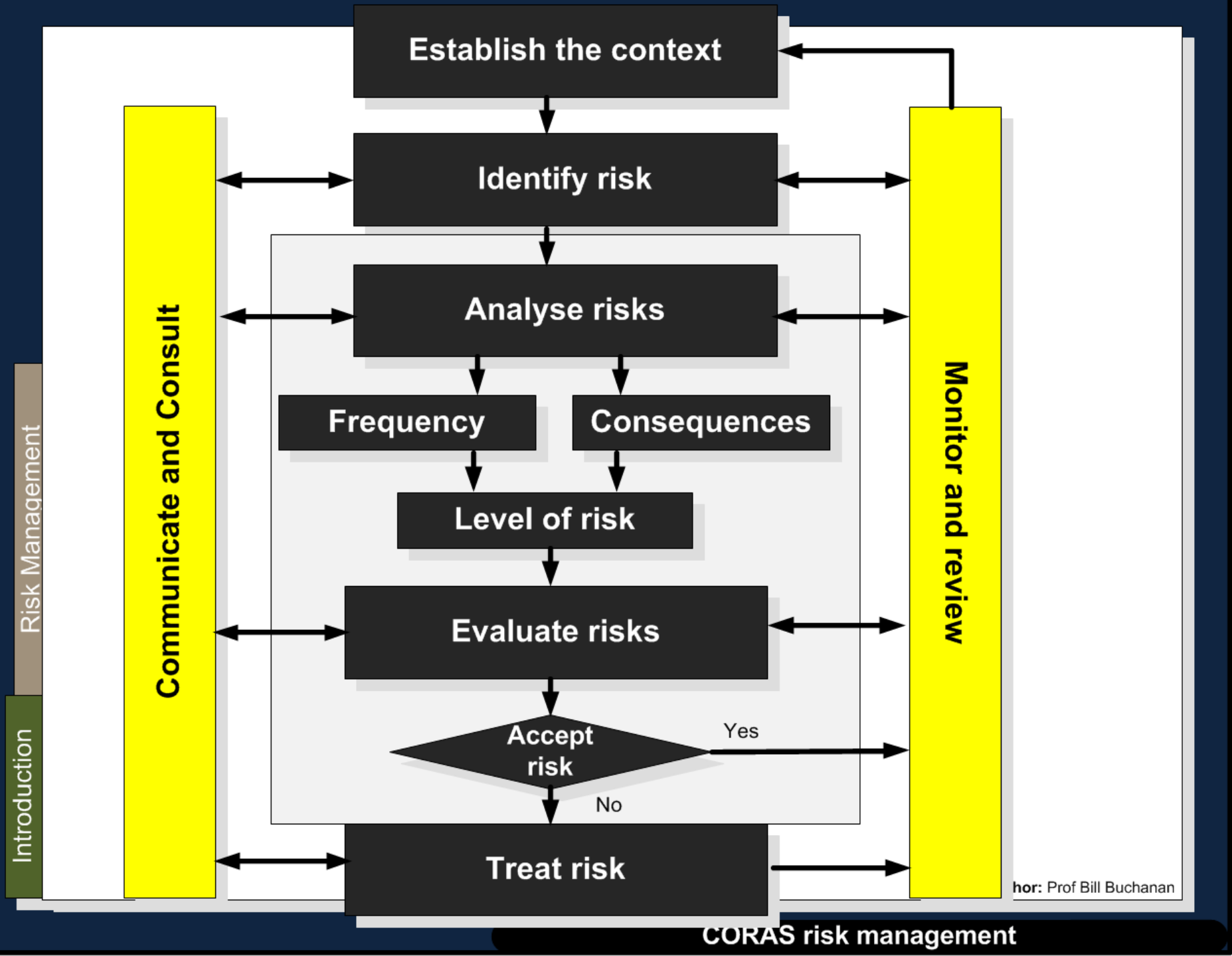
Business context

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)

Author: Prof Bill Buchanan


Threat
may reduce
Asset Value
Security Policy
has
may exploit
of
Vulnerability
in accordance with
protects
Asset
of
reduces
Security Requirements
has
contains
in
opens for
Risk
TOE (Target of Evaluation)
contains
contains
Likelihood
Consequence
influences
contains
in
Unwanted incident
of
has
has
Context
of
Risk Management
Introduction
CORAS ontology


Establish the context
Identify risk
Analyse risks
Frequency
Consequences
Level of risk
Evaluate risks
Accept risk
Yes
No
Treat risk
Communicate and Consult
Monitor and review
Risk Management
Introduction
hor: Prof Bill Buchanan
CORAS risk management

Introduction

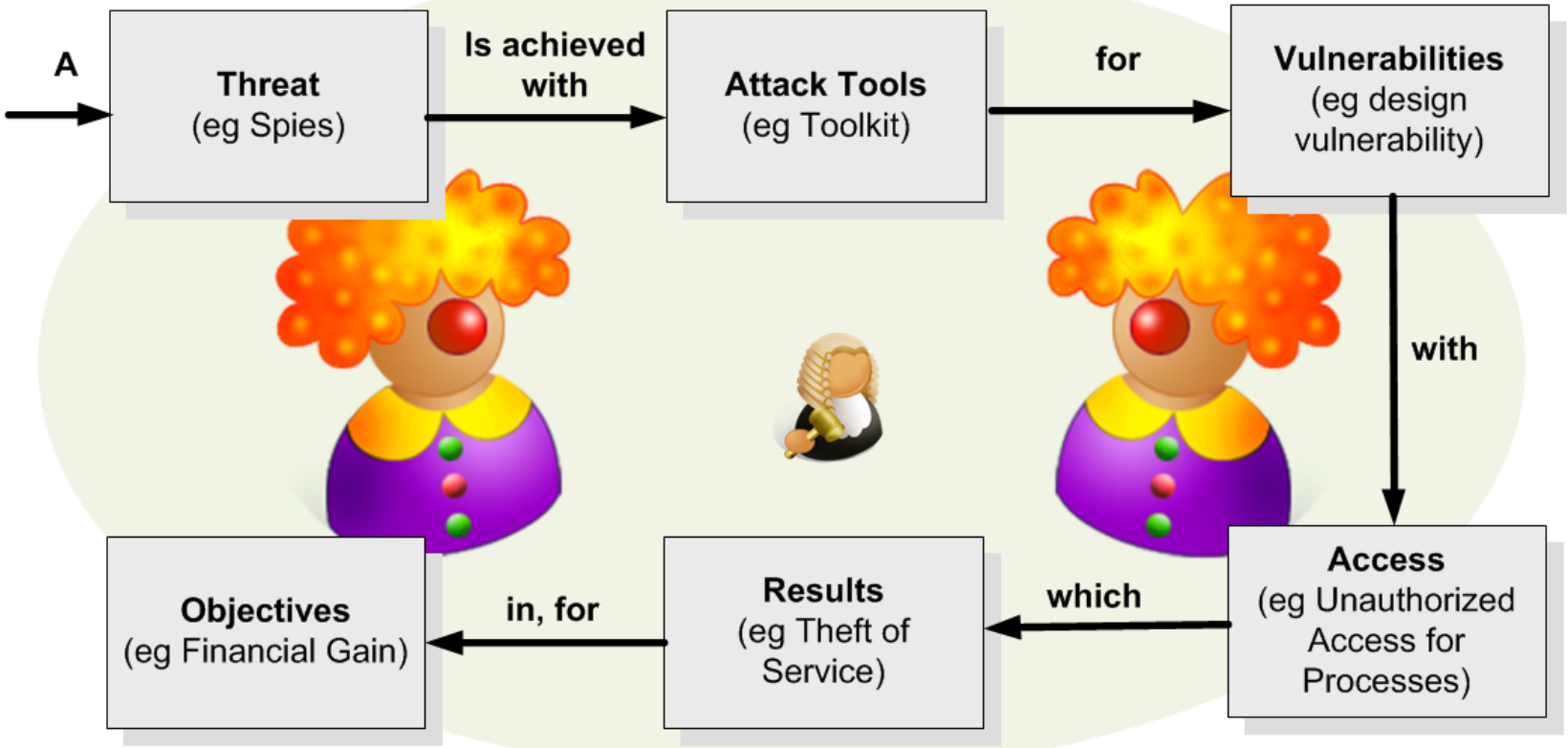
Security Taxonomy

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.



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

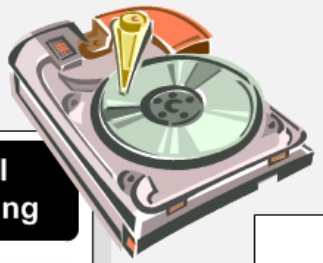
Introduction

Threats

Author: Prof Bill Buchanan

Eavesdropping

Eavesdropping. This involves intercepting communications.



Logical scavenging

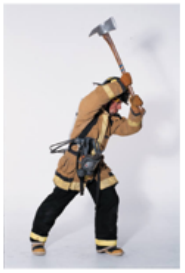
Logical scavenging. This involves scavenging through discarded media.

Author: Prof Bill Buchanan

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

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.

Best project ever!
Click here

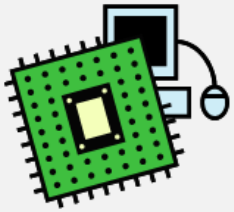
Trojan horse

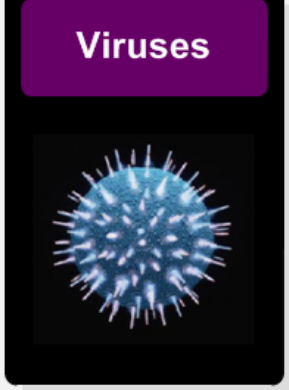
Logic bombs

The email contains a Trojan virus

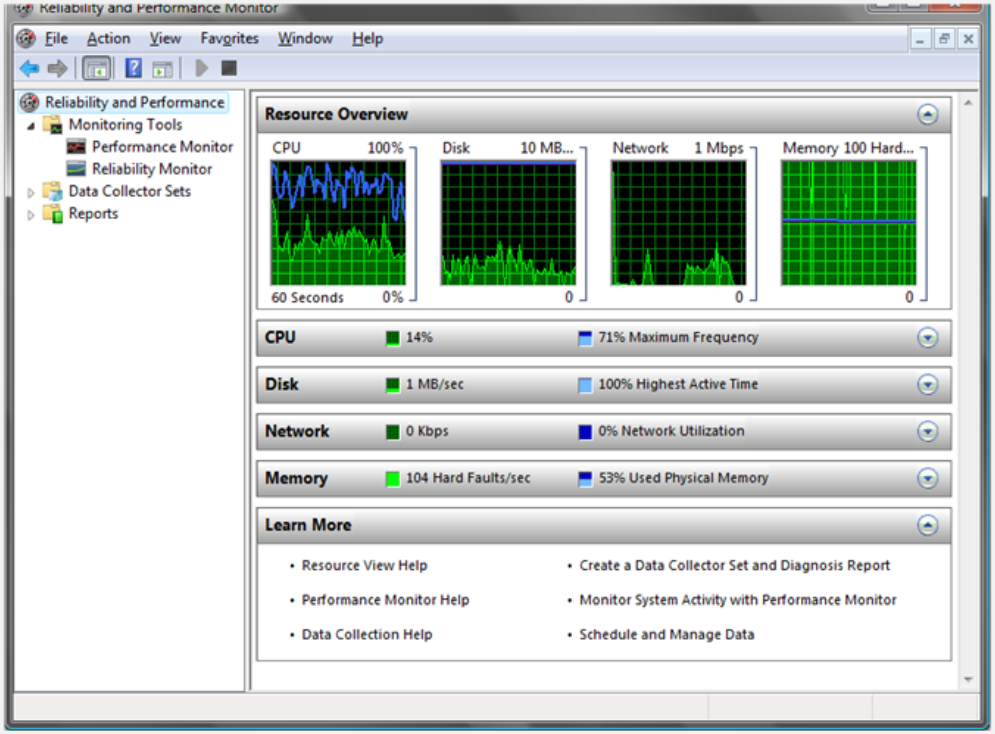
Author: Prof Bill Buchanan

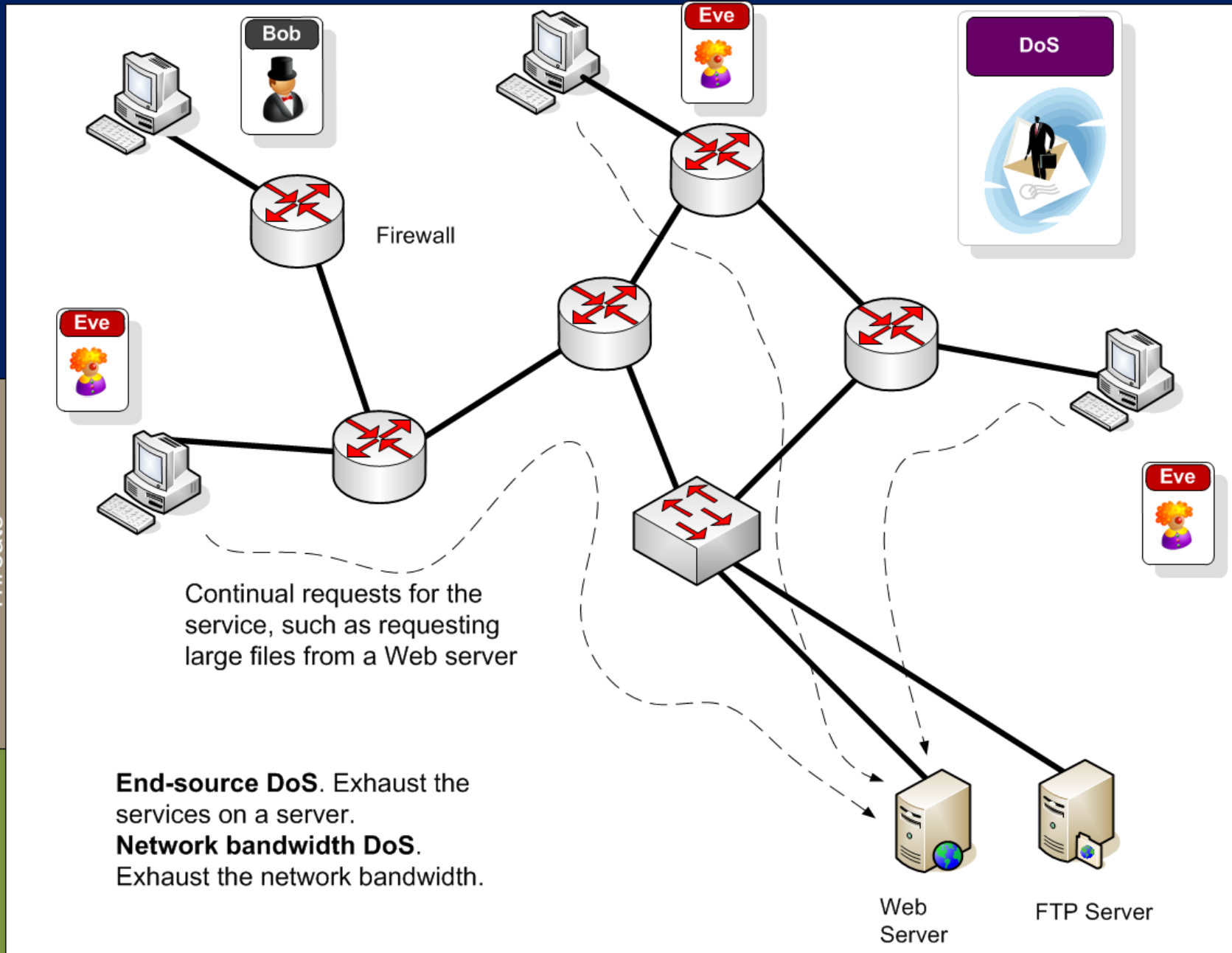
Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.





Viruses. This involves attaching program which self replicate themselves.



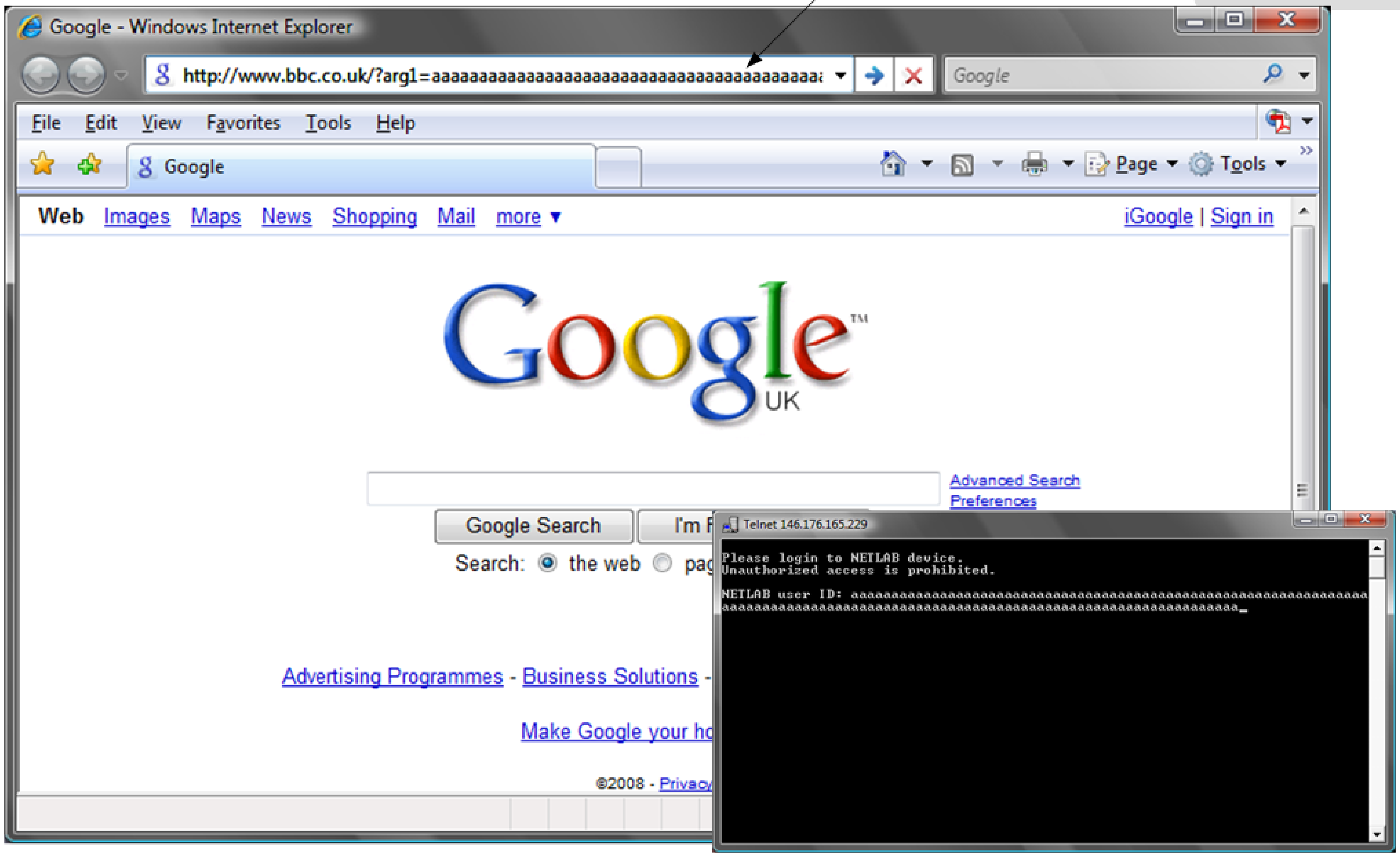


End-source DoS. Exhaust the services on a server.
Network bandwidth DoS. Exhaust the network bandwidth.

Author: Prof Bill Buchanan

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



Author: Prof Bill Buchanan

Inference

Inference. This involves exploiting database weaknesses using inferences.

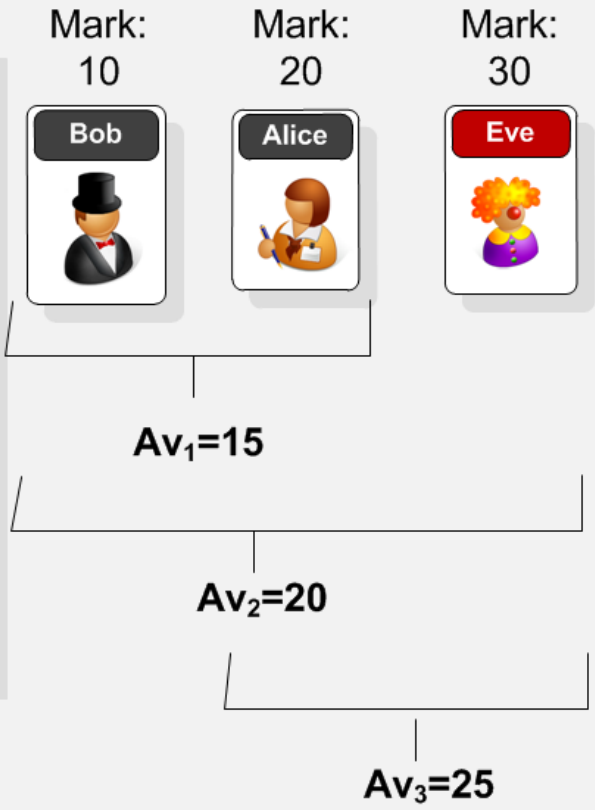
For example … the marks for any student is not allowed, but the average a number of students is allowed.

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



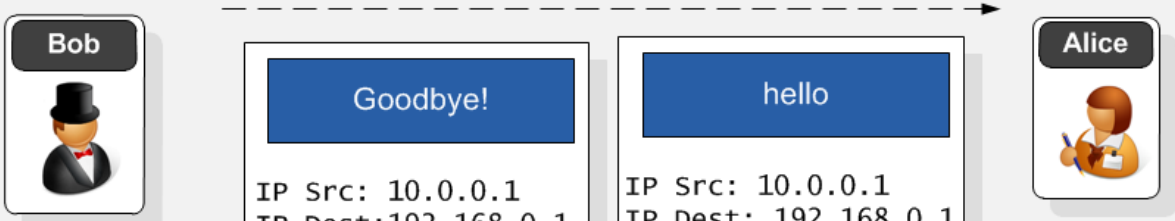
Alice's mark=Av_1-Av_2+Av_3=15-20+25=20

Author: Prof Bill Buchanan

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).



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

Author: Prof Bill Buchanan

Spoofing. This involves the spoofing of devices.

Spoofing

Bob

Hello… I'm Bob!

Hello… I'm Bob!

Eve

Hello… I'm Bob!

Hello… I'm Bob!

Im-personation

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

I'm a nuclear scientist

I'm a brain surgeon

Author: Prof Bill Buchanan

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

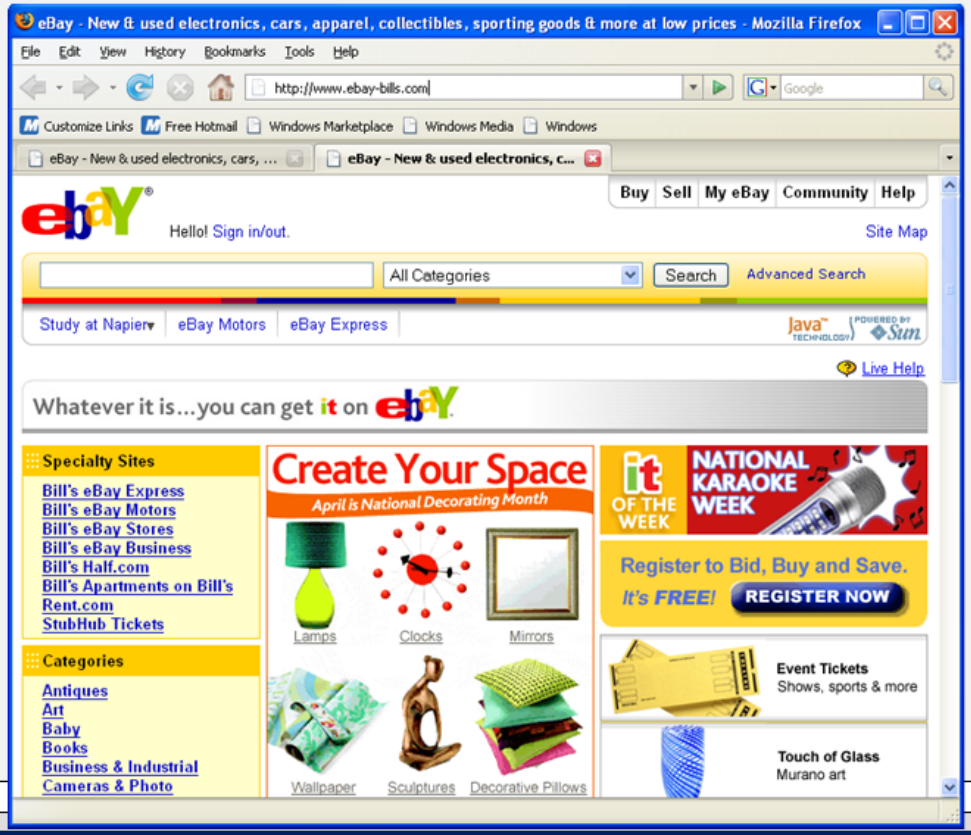
Author: Prof Bill Buchanan

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.

Authorization attack

Trap-door

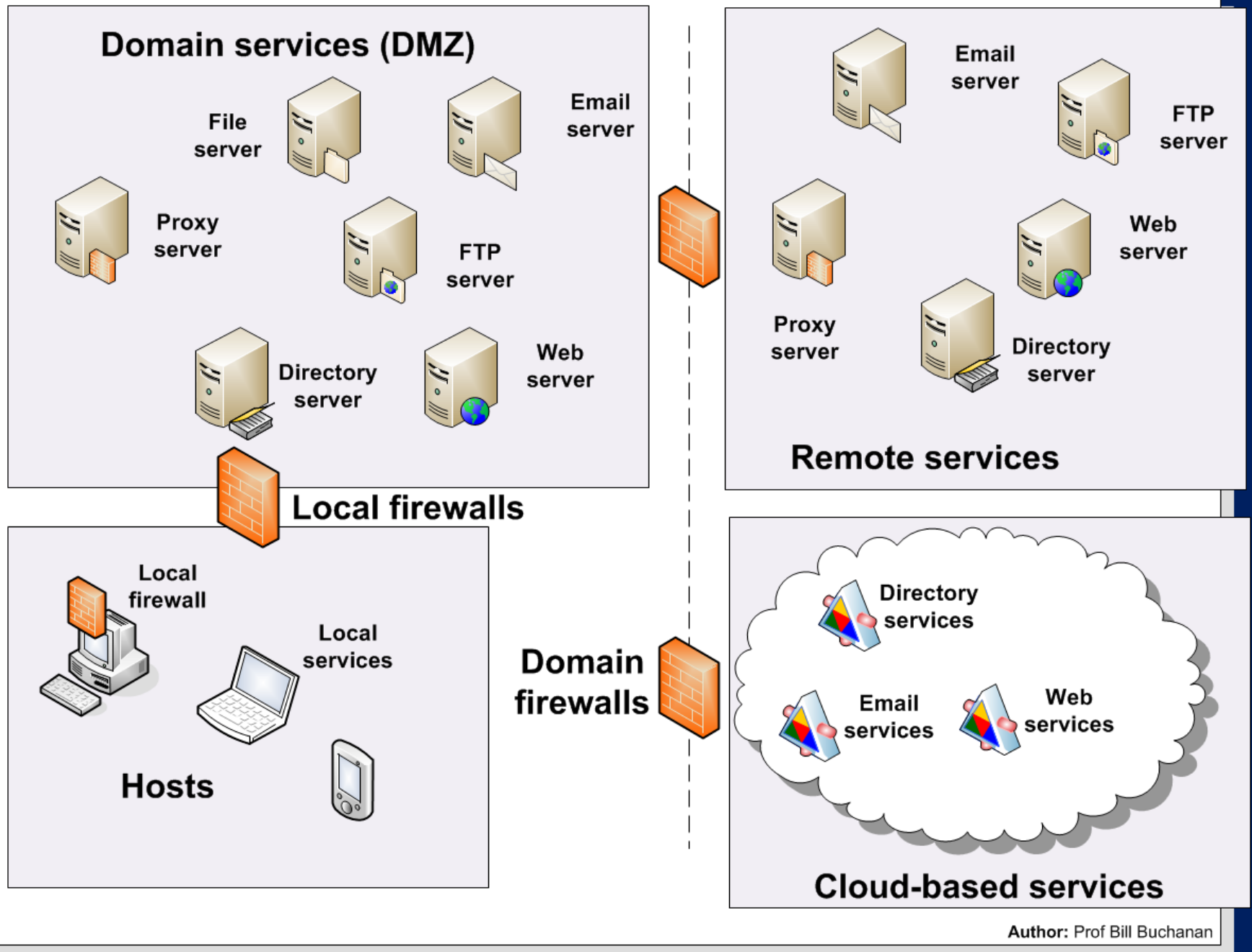
Trap door impersonation. This involves the creation of pages or login screens which look valid, but are used to gain information from a user, such as their bank details, or login password.



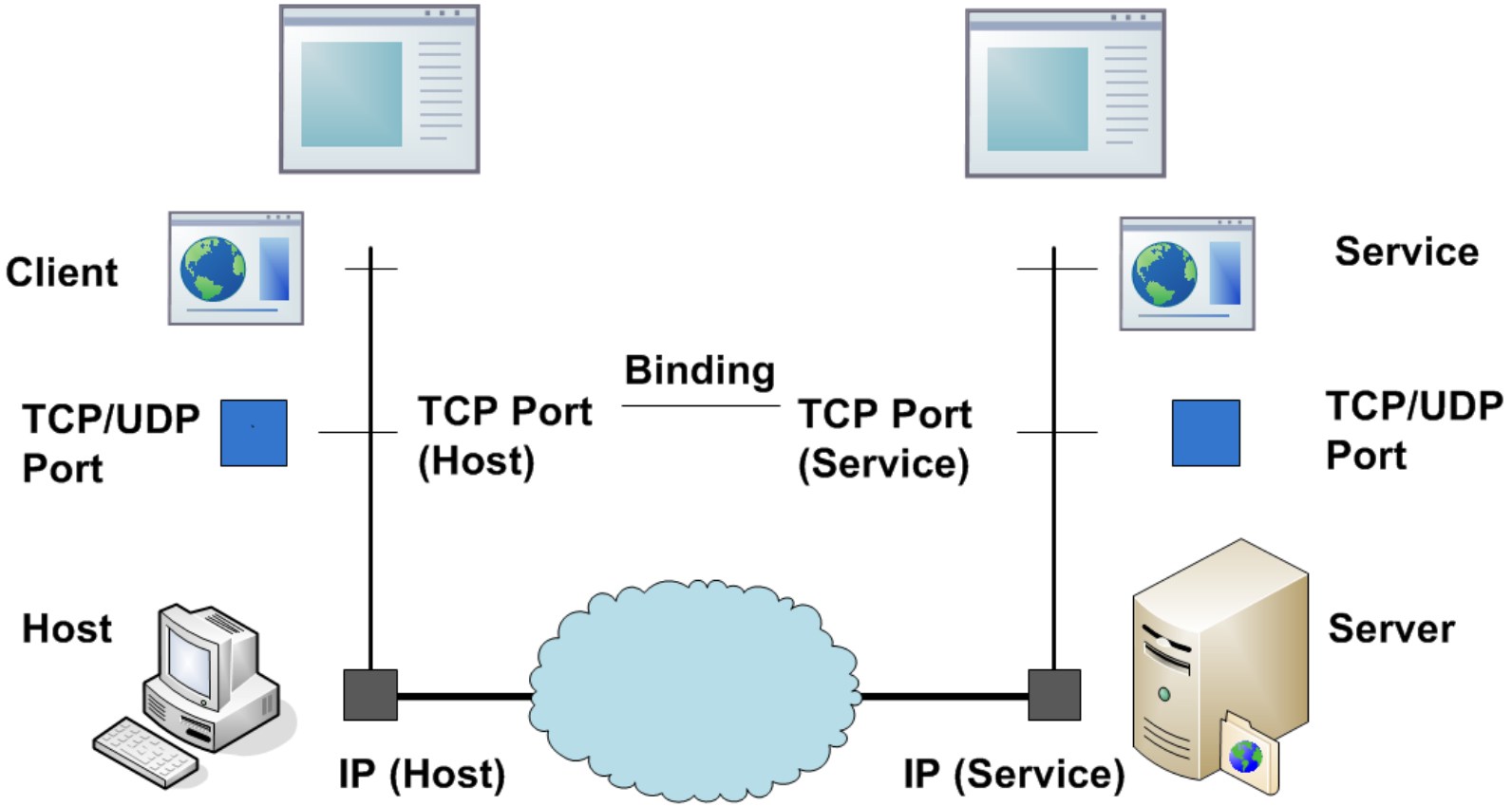
Introduction

SoA

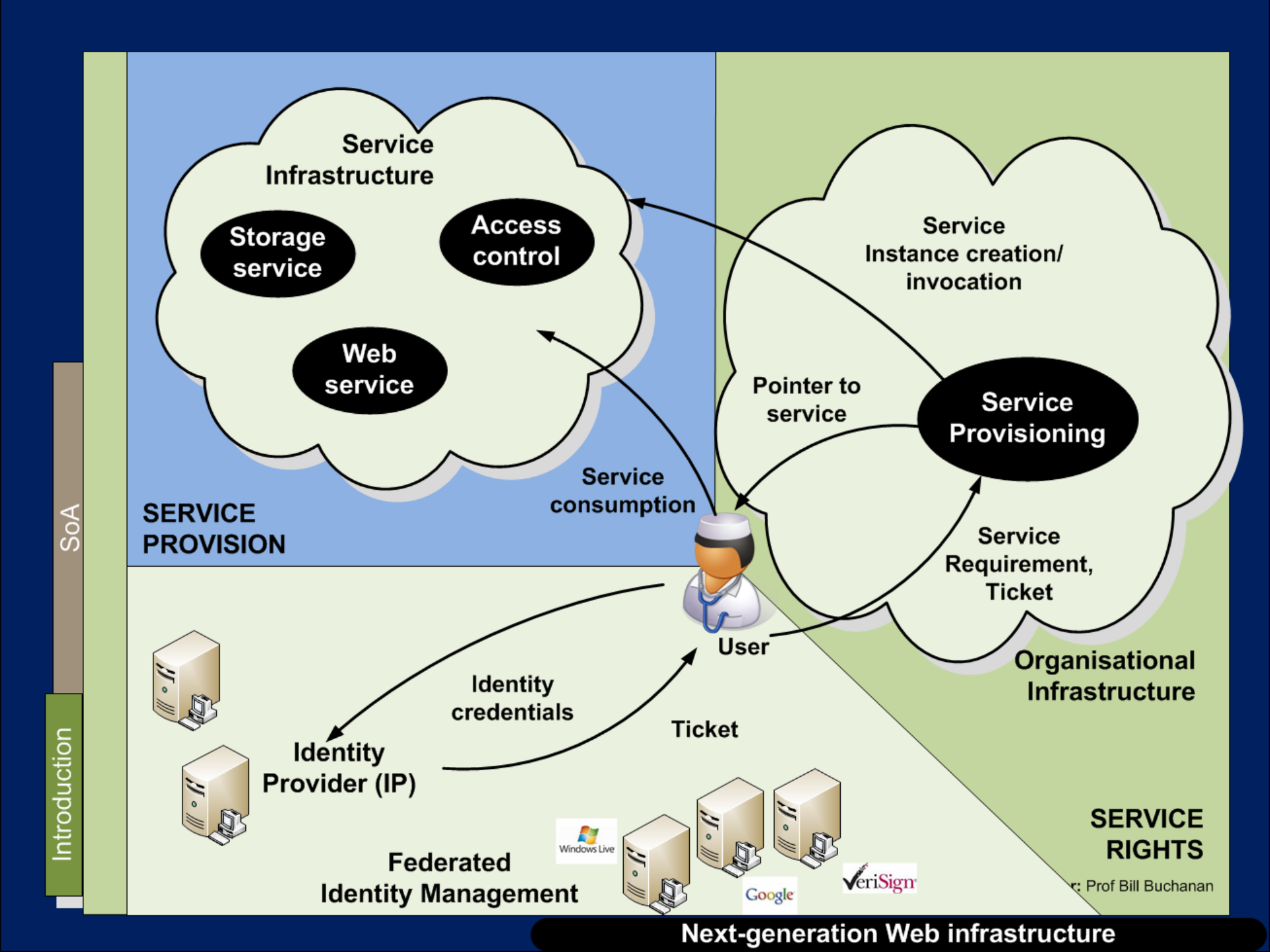
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



Author: Prof Bill Buchanan


Service Infrastructure
Storage service
Access control
Web service
SERVICE PROVISION
Service consumption
Service Instance creation/ invocation
Pointer to service
Service Provisioning
Service Requirement, Ticket
Organisational Infrastructure
User
Identity credentials
Ticket
Identity Provider (IP)
Federated Identity Management
SERVICE RIGHTS
Windows Live
Google
VeriSign
SoA
Introduction
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)

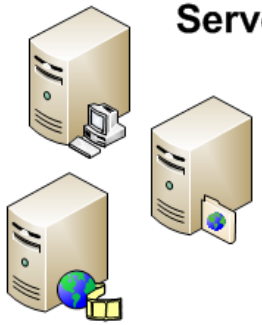
- Service Oriented Architecture (SOA)
- Sophisticated Web Services
- Developing
- Testing
- Deploying
- Hosting
- Service platform providers, e.g. Google GAE, Microsoft Windows Azure

Infrastructure as a Service (IaaS)

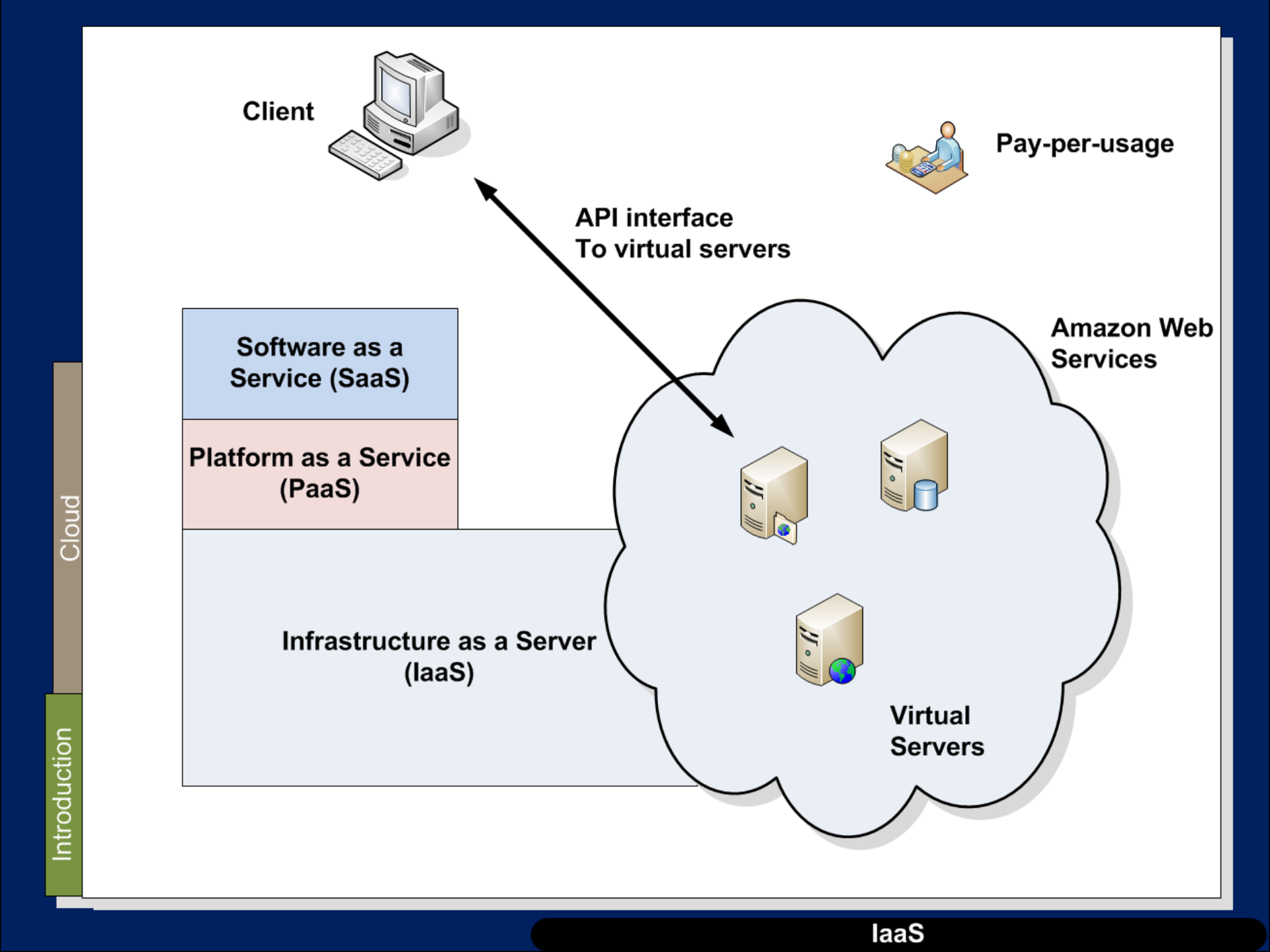
- Resource virtualisation
- Computing power
- Storage capacity
- Network bandwidth
- Usage-based payment scheme
- Cloud enablers, e.g. Amazon EC2 / S3

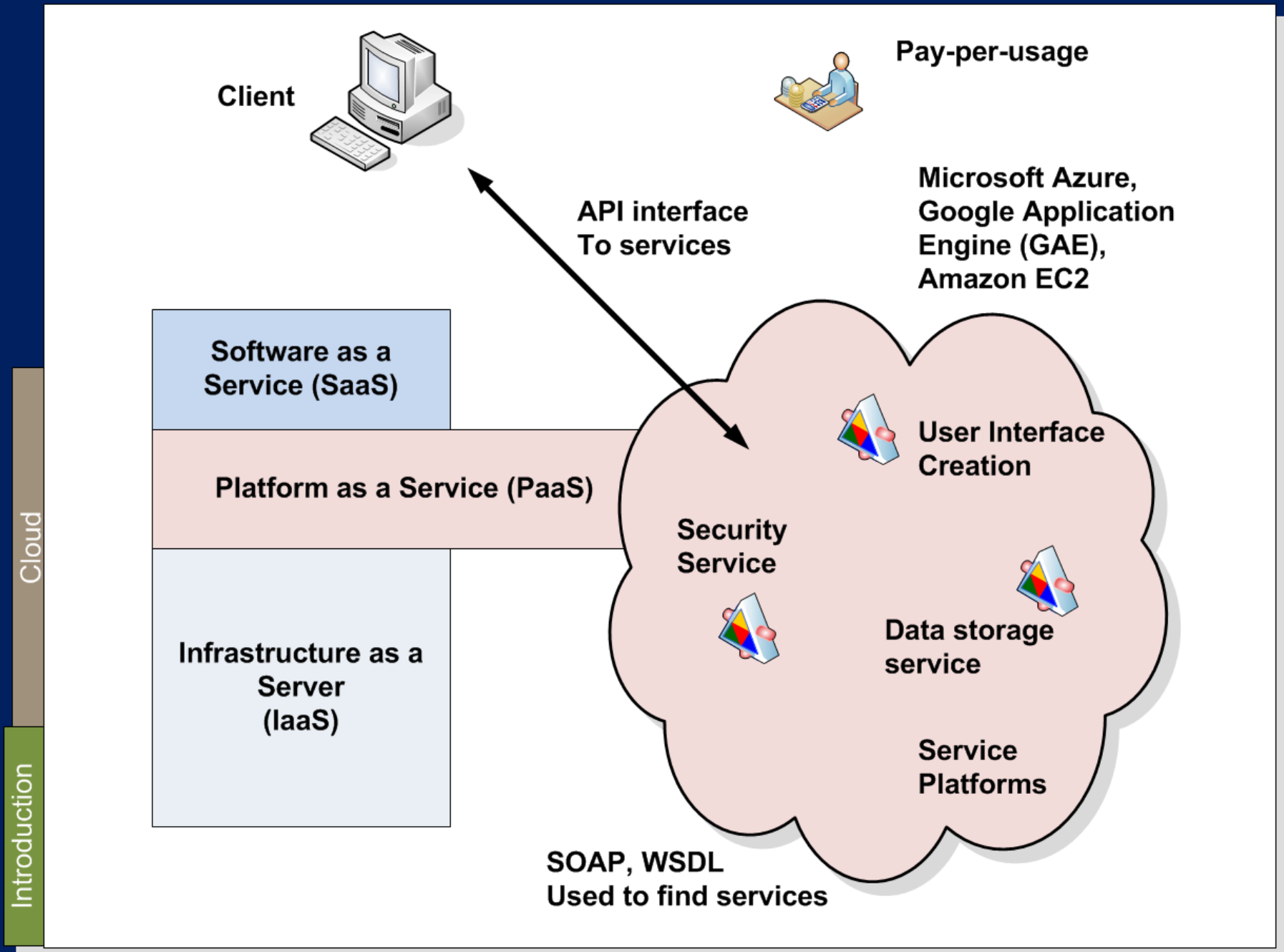
Hardware as a Service (HaaS)

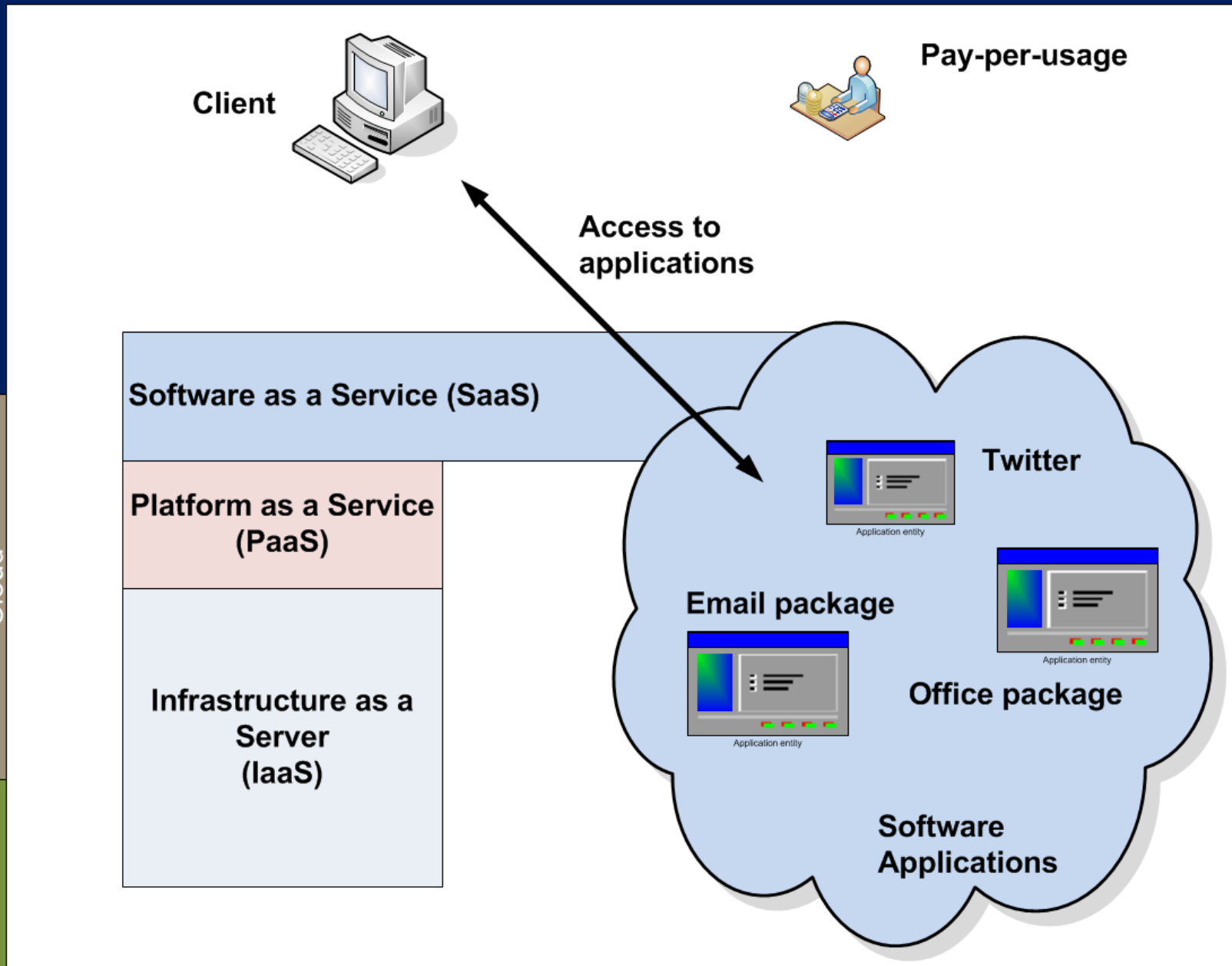
- Cluster & data centre providers
- Reduction of capital & operation investments
- Enhanced reliability – redundancy, replication & failover
- Enhanced scalability
- Enhanced load-balancing



Servers


Client
Pay-per-usage
API interface
To virtual servers
Amazon Web
Services
Software as a
Service (SaaS)
Platform as a Service
(PaaS)
Infrastructure as a Server
(IaaS)
Virtual
Servers
Cloud
Introduction
IaaS

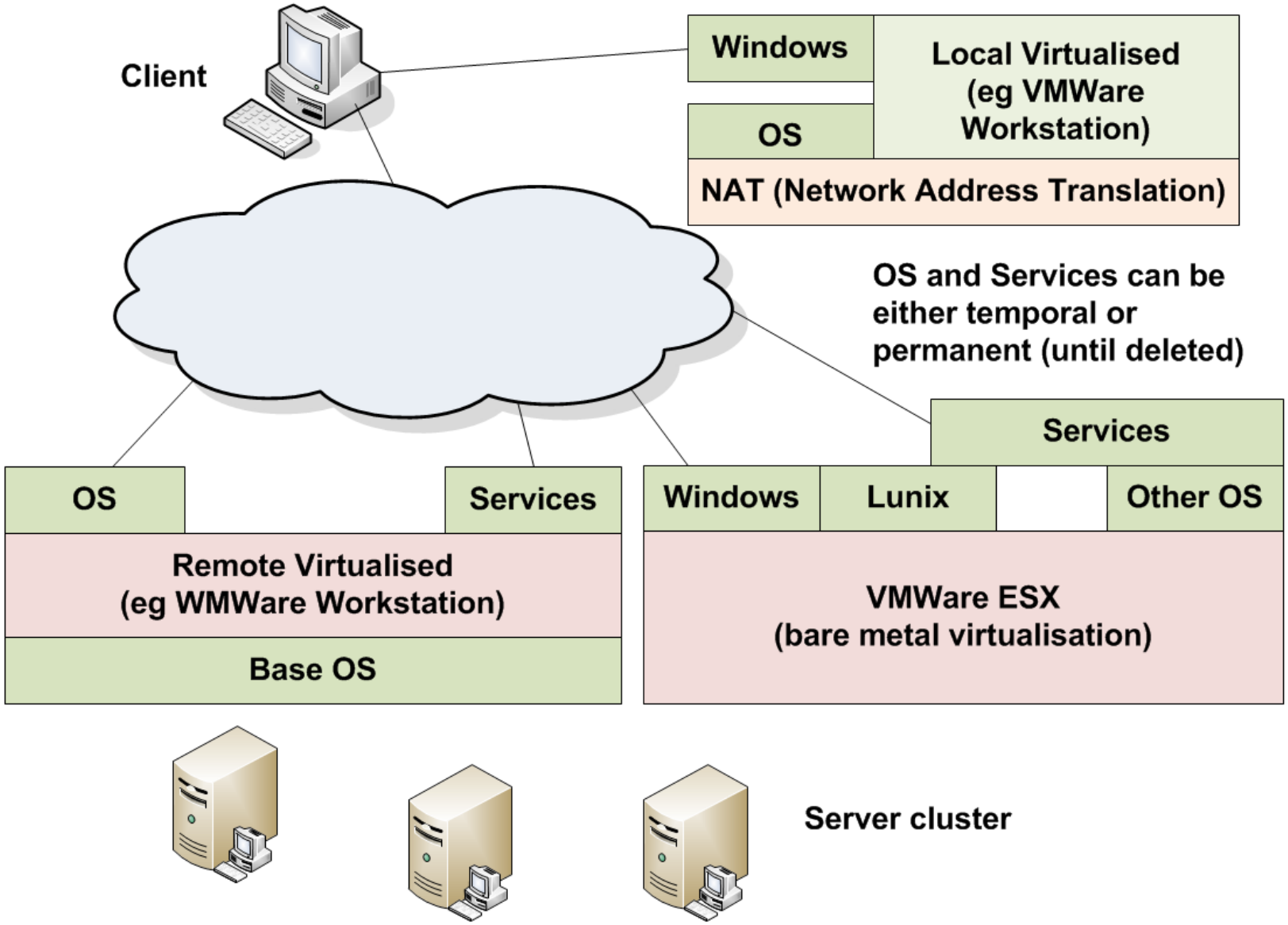

Client
Pay-per-usage
API interface
To services
Microsoft Azure,
Google Application
Engine (GAE),
Amazon EC2
Software as a
Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a
Server
(IaaS)
User Interface
Creation
Security
Service
Data storage
service
Service
Platforms
SOAP, WSDL
Used to find services
Cloud
Introduction
PaaS


Client
Pay-per-usage
Access to applications
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Server (IaaS)
Twitter
Application entity
Email package
Application entity
Application entity
Office package
Software Applications

Introduction

Virtualisation

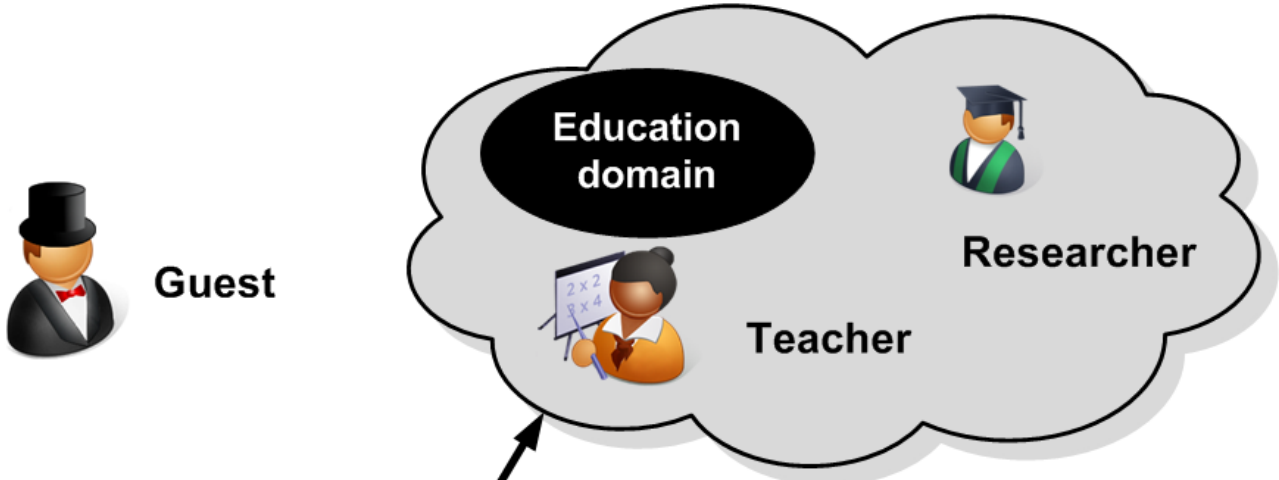
Author: Prof Bill Buchanan


Client
Windows
OS
Local Virtualised
(eg VMWare
Workstation)
NAT (Network Address Translation)
OS and Services can be
either temporal or
permanent (until deleted)
Services
OS
Services
Windows
Lunix
Other OS
Remote Virtualised
(eg WMWare Workstation)
Base OS
VMWare ESX
(bare metal virtualisation)
Server cluster

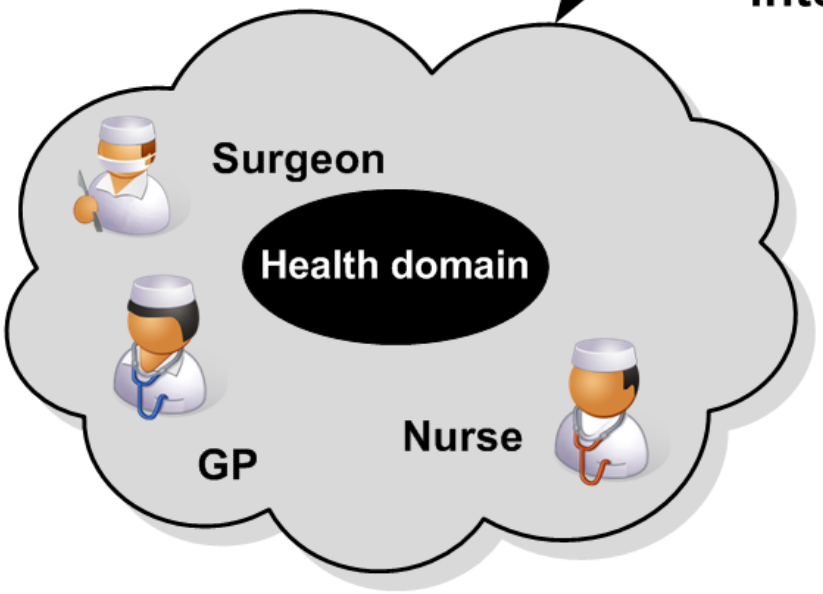
Introduction

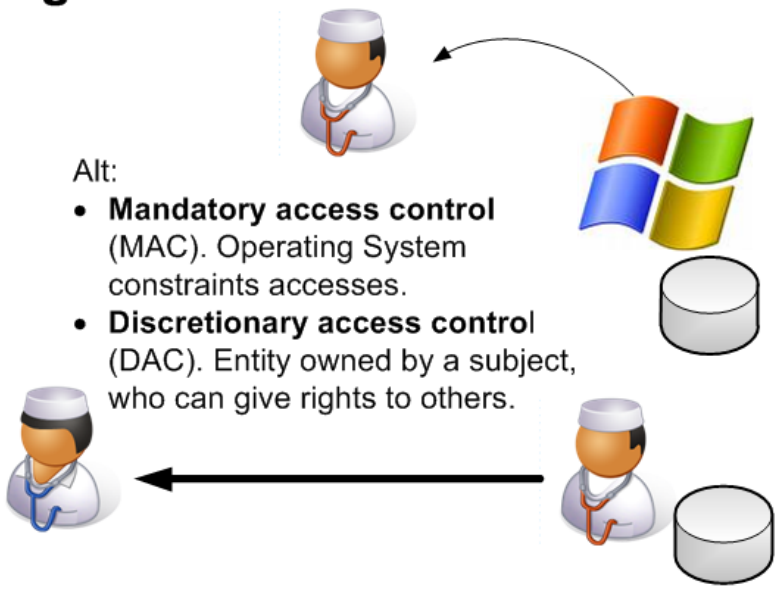
Role-based Security

Author: Prof Bill Buchanan



Interdomain rights





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.

Author: Prof Bill Buchanan