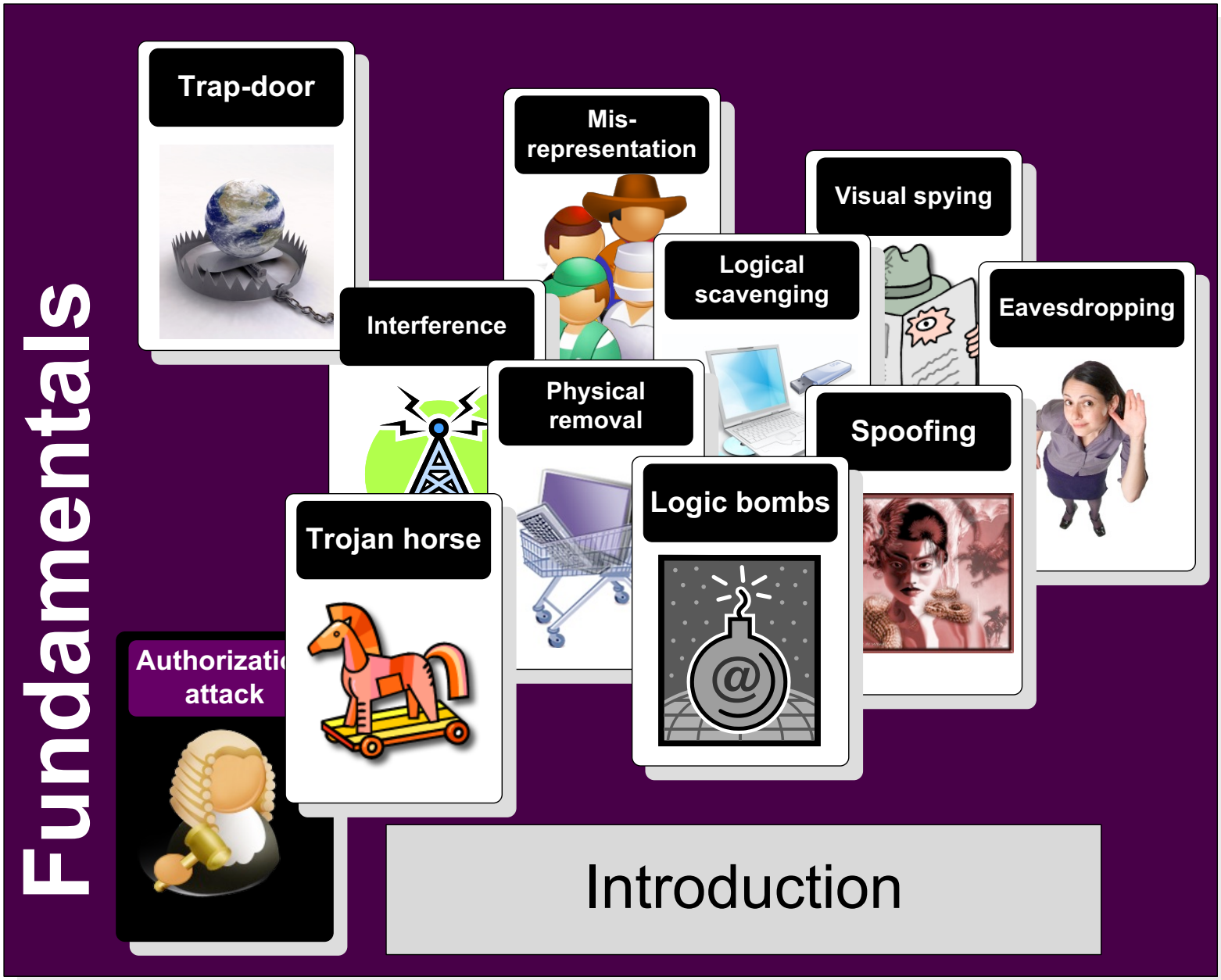
Fundamentals

Introduction
ISO 27002
Risk Analysis
Security Policy
Threats
Key Principles
Conclusions

Author: Prof Bill Buchanan

Fundamentals



Introduction

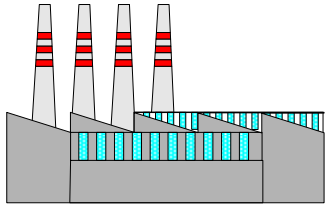
Author: Prof Bill Buchanan

Industrial Age

Postal system
Paper voting
Telephone
Physical shopping

Information Age

Email
E-voting
Voice-over-IP
E-shopping

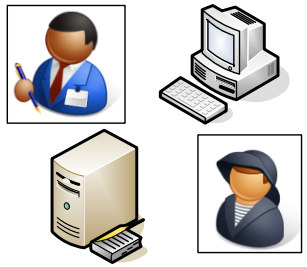


Fundamentals:
Security
Assurance
Authentication

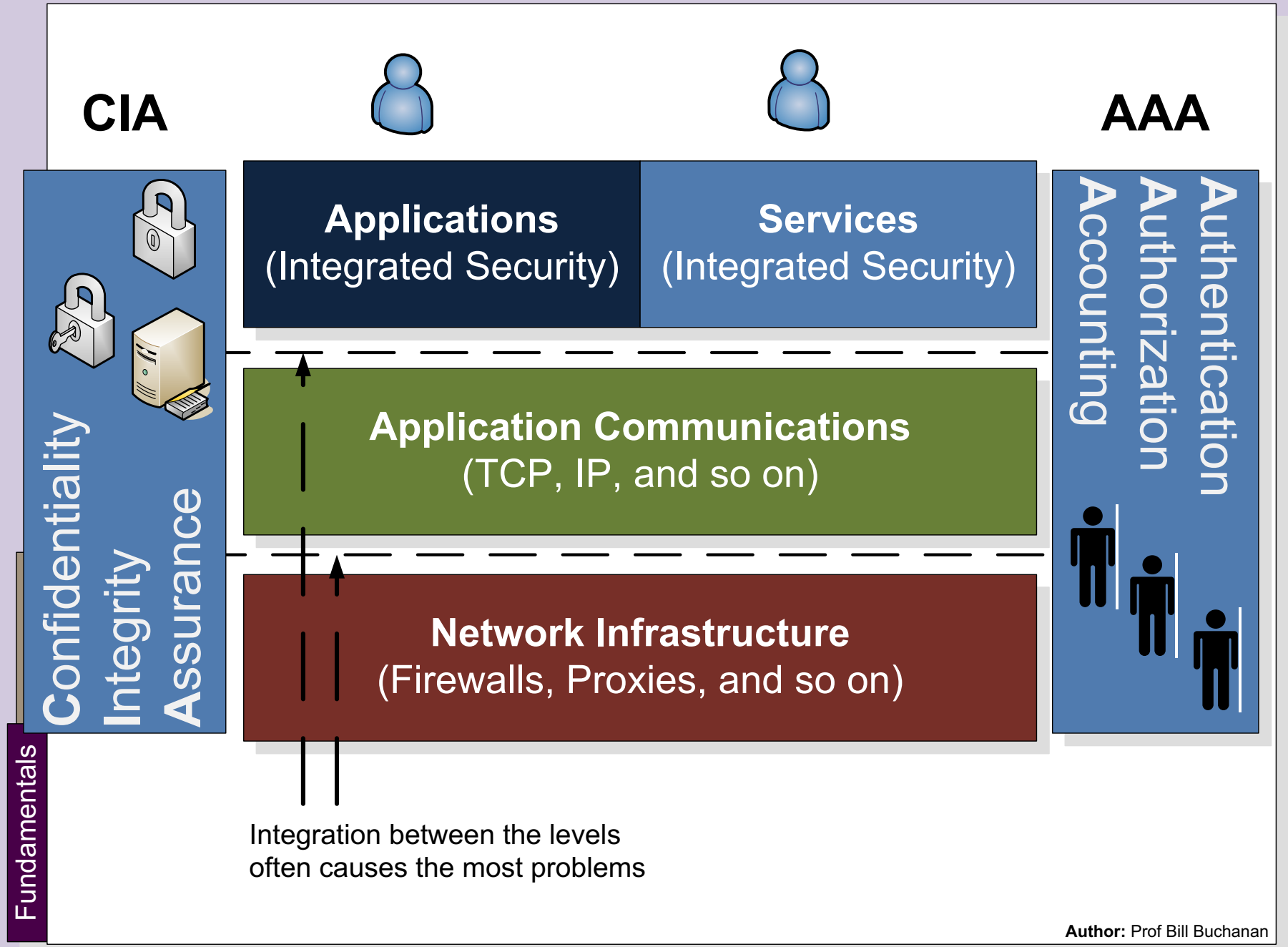
Authentication
(Device, User, Servers, Connections, etc)

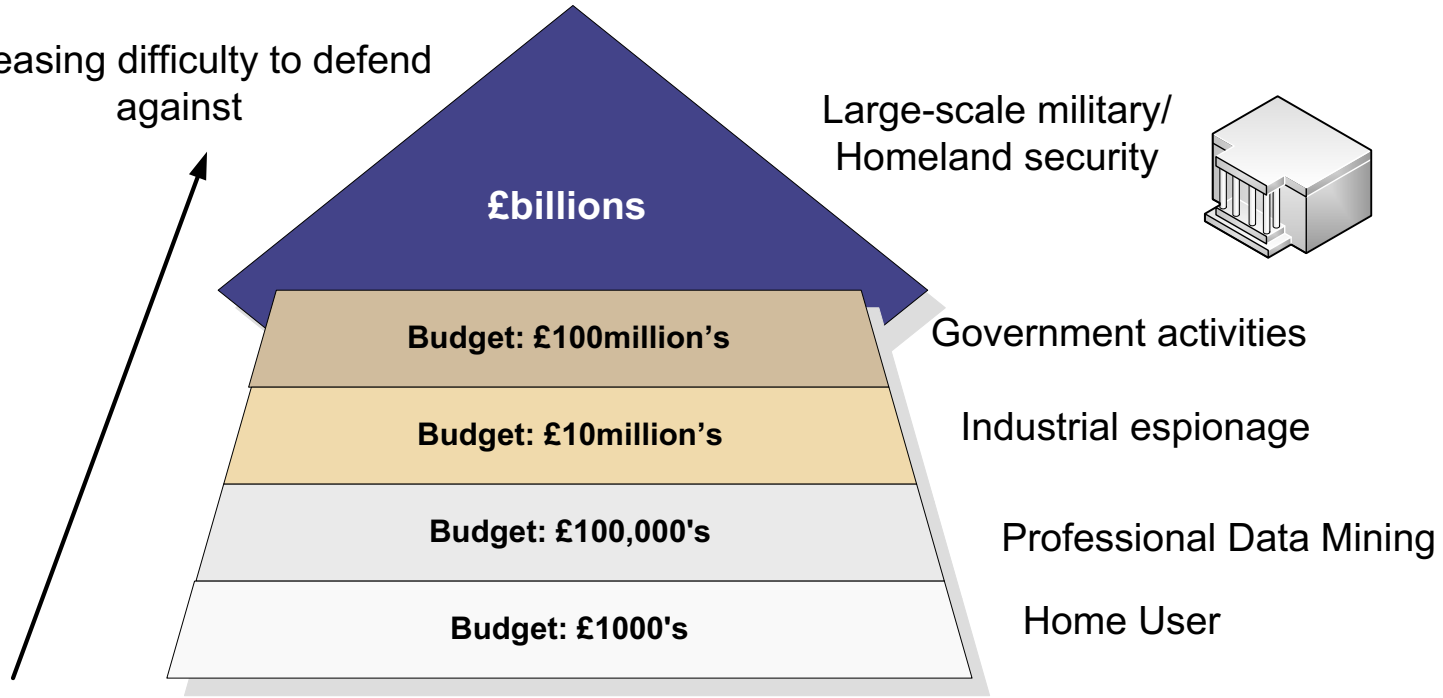
Confidentiality
(Encryption)

Assurance
(Integrity)

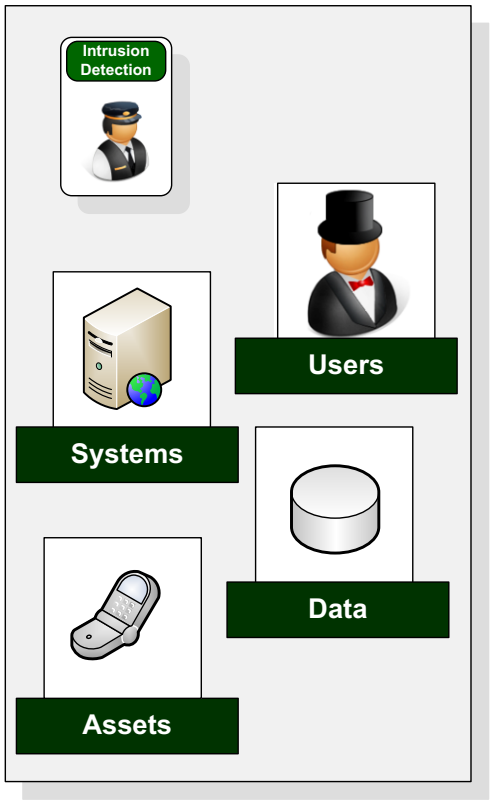


Author: Prof Bill Buchanan


CIA
AAA
Applications
(Integrated Security)
Services
(Integrated Security)
Application Communications
(TCP, IP, and so on)
Network Infrastructure
(Firewalls, Proxies, and so on)
Confidentiality
Integrity
Assurance
Authentication
Authorization
Accounting
Integration between the levels
often causes the most problems
Fundamentals
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



Corporate access

Email access

Web access

Network/ Organisational perimeter

Firewall/ gateway

Data stealing

External hack

DoS (Denial-of-sevice)

Personal abuse

Worms/viruses

Fraud

Terrorism/ extortion

Author: Prof Bill Buchanan

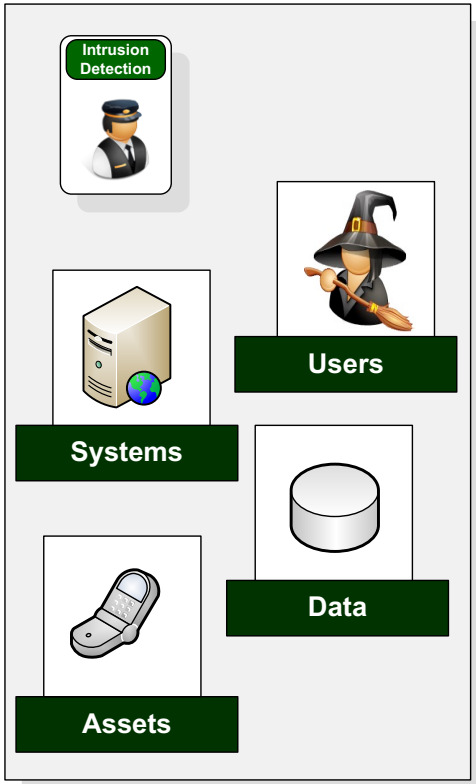
CSI (Computer Security Institute) found:

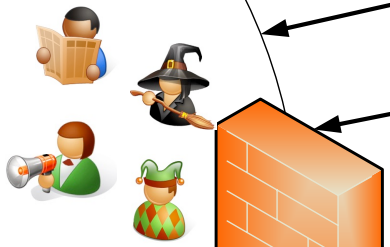
- 70% of organisation had breaches
- 60% of all breaches came from inside their own systems

Data stealing

External hack

Corporate access

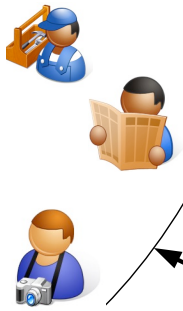




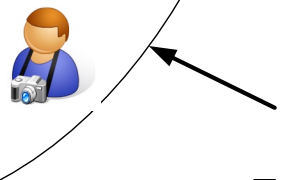
DoS (Denial-of-sevice)

Firewall/ Gateway (cannot deal with internal threats)

Personal abuse



Worms/viruses

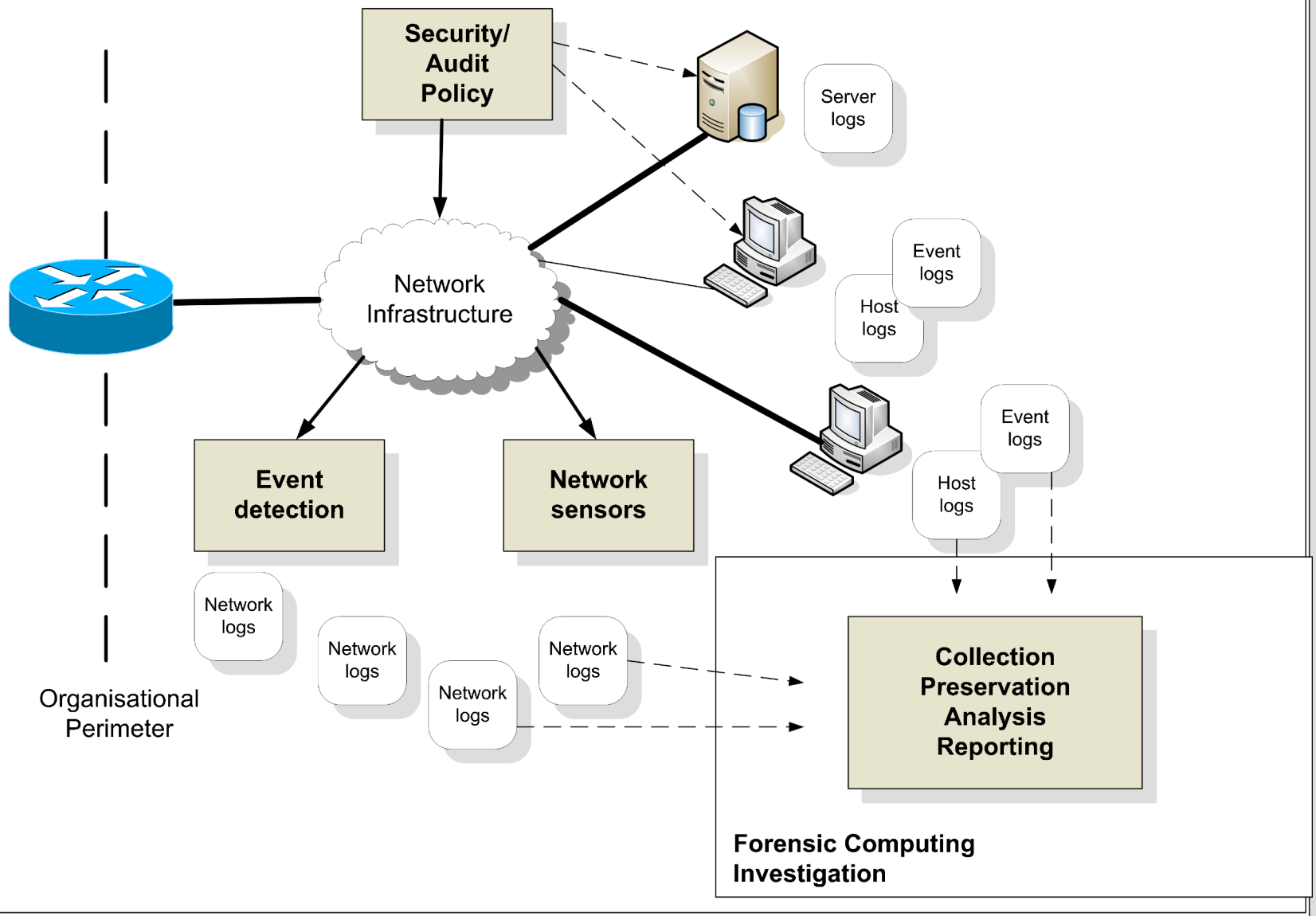


Terrorism/ extortion

Fraud

Network/ Organisational perimeter

Author: Prof Bill Buchanan

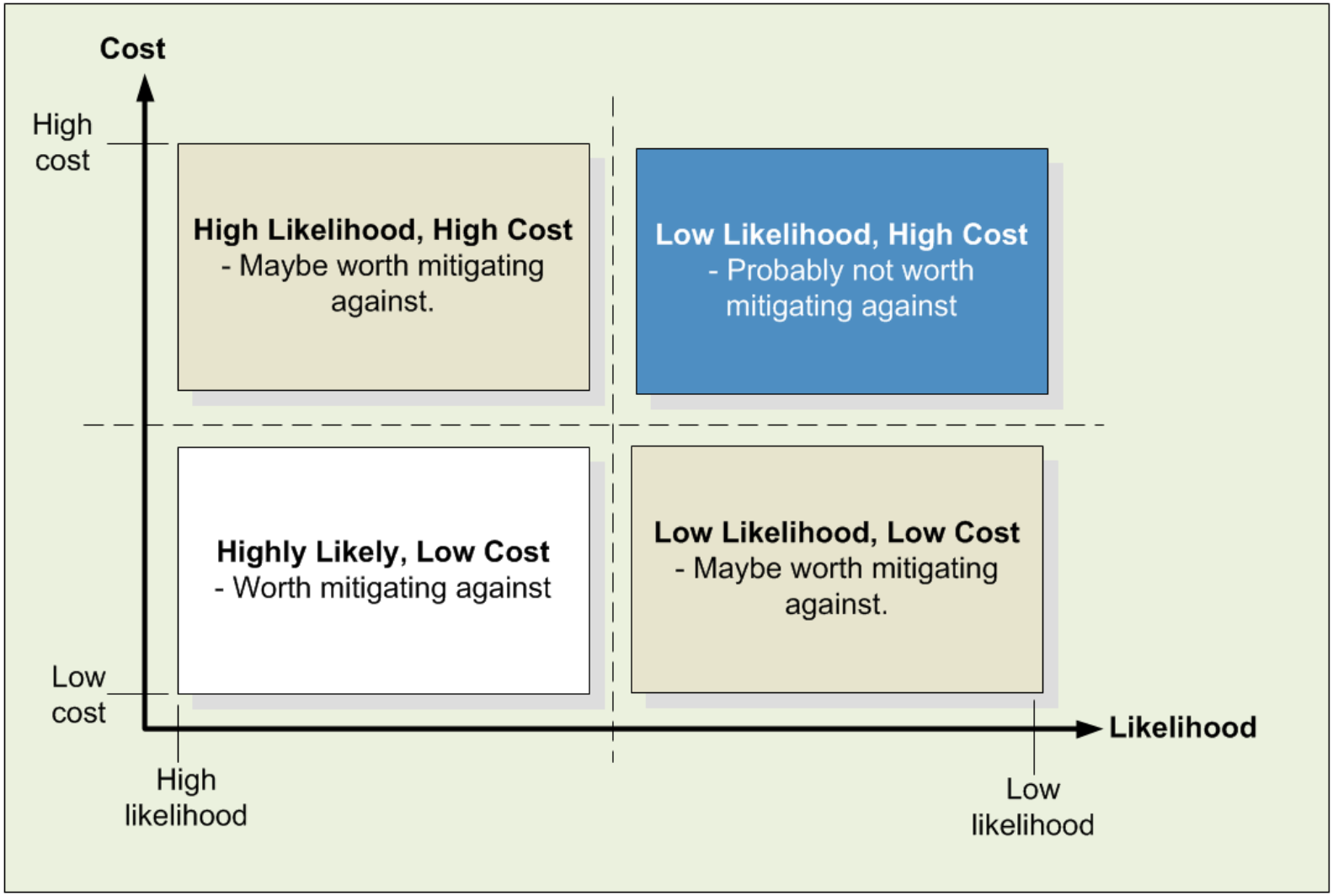


Author: Prof Bill Buchanan

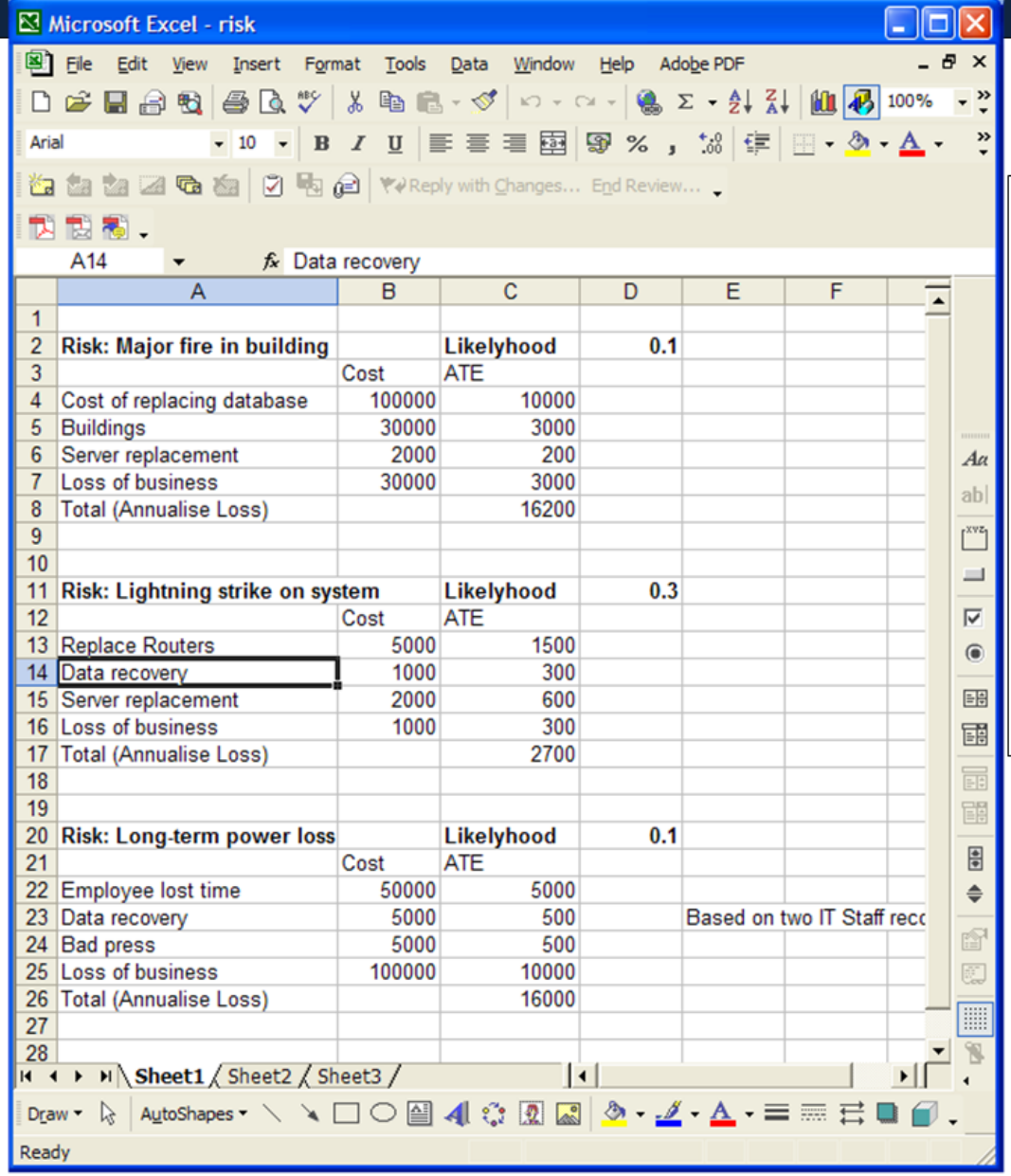
Introduction

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						

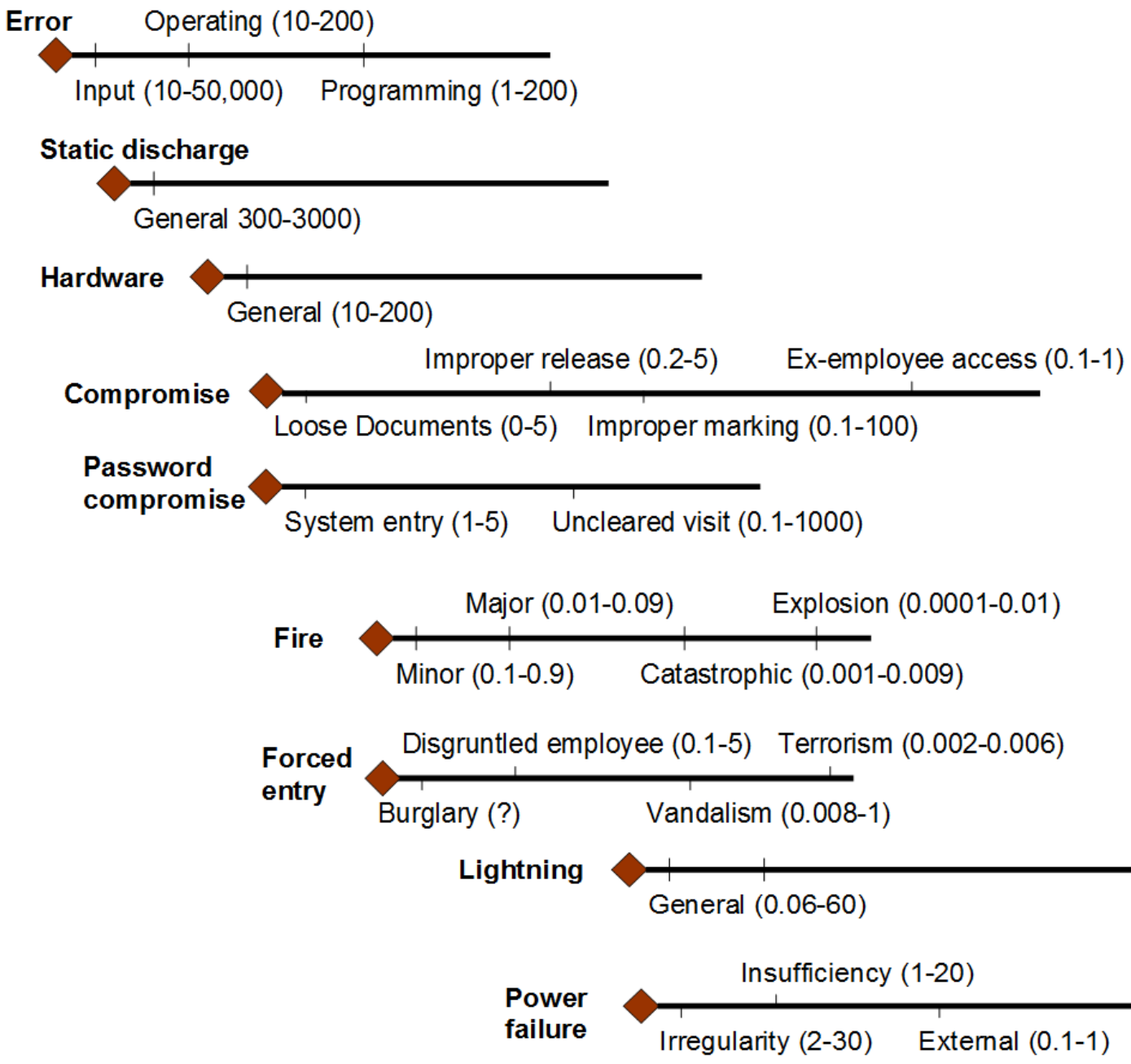
ALE = *T* x *V*

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

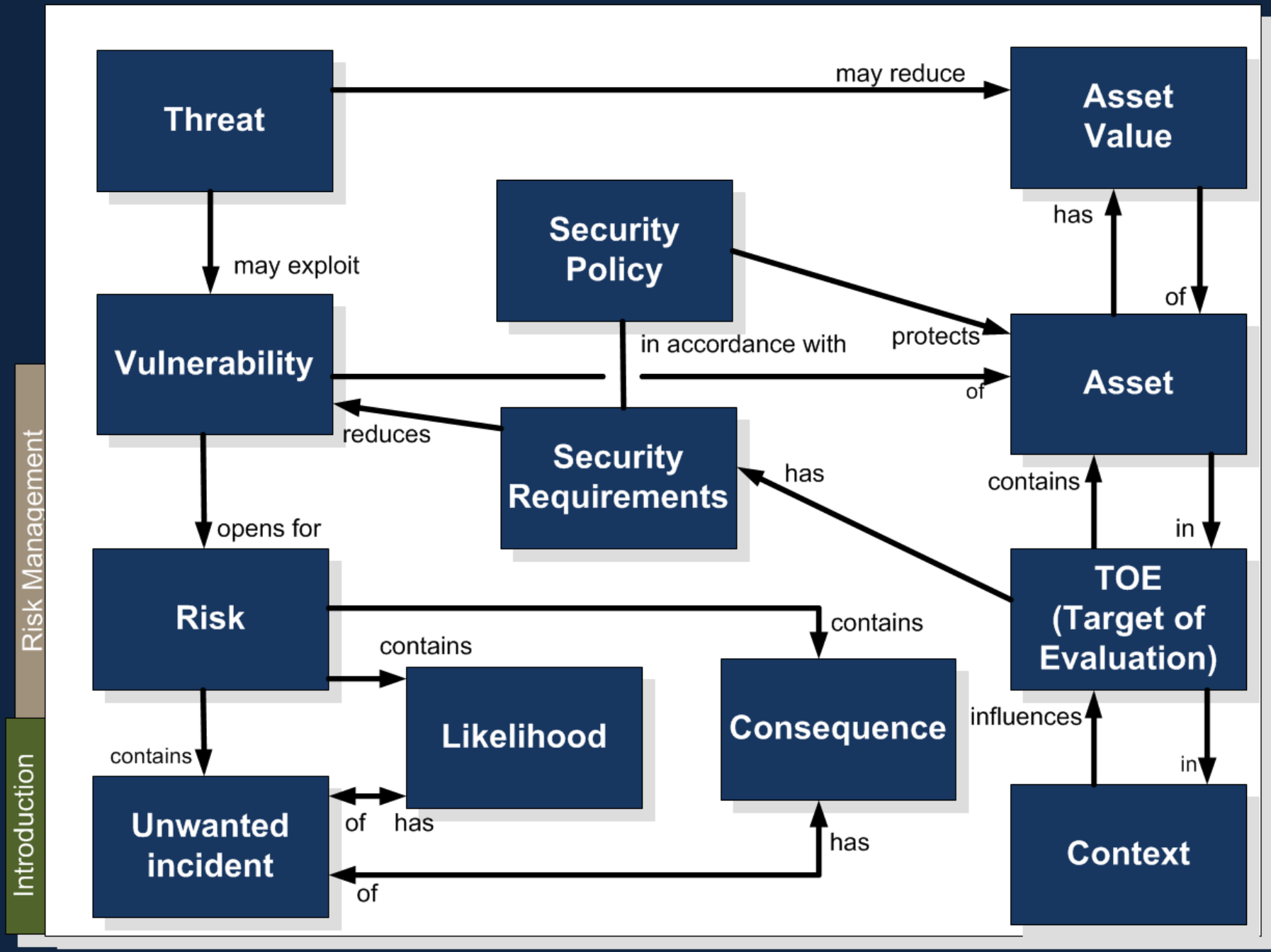
Author: Prof Bill Buchanan

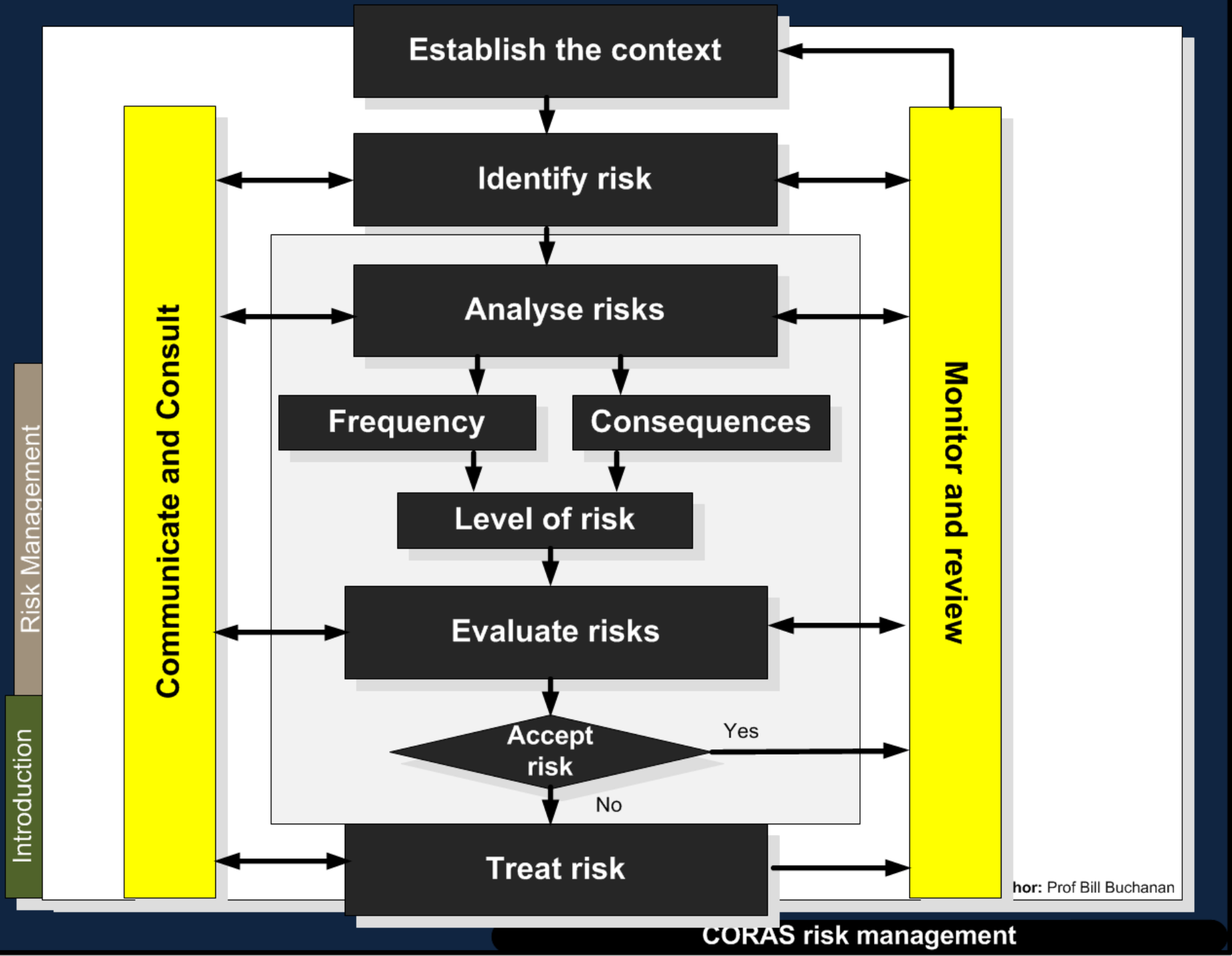
Business context

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

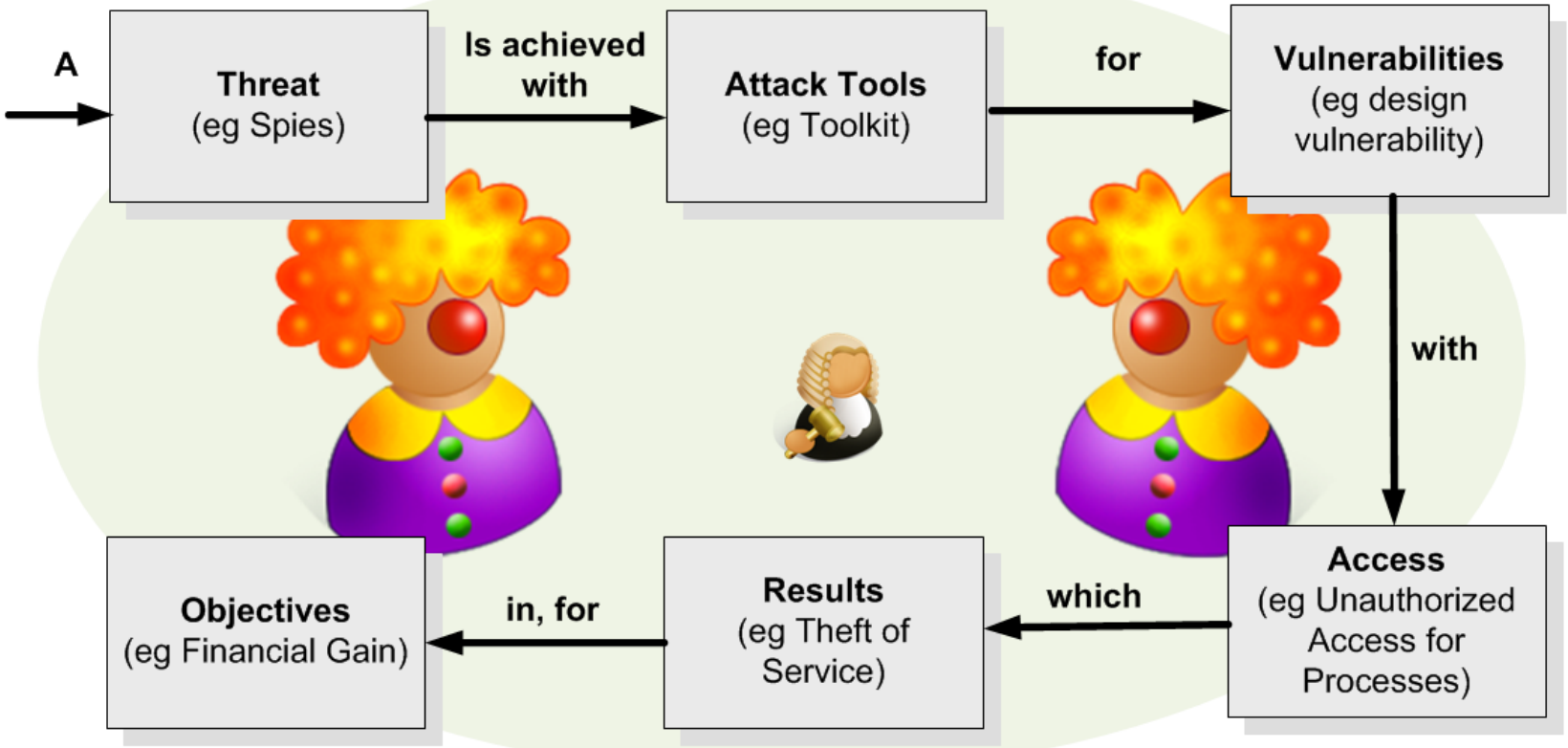
Security Taxonomy

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

Cyberterrorism. This can be attacks against critical national infrastructures, such as power plants, oil refineries, and so on,

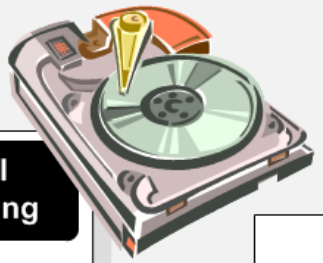
Natural Disasters

Natural Disasters. This includes storms, hurricanes, fire, floods, earthquakes, and natural events

Cyberterror

Eavesdropping

Eavesdropping. This involves intercepting communications.



Logical scavenging

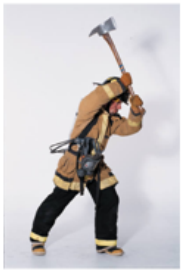
Logical scavenging. This involves scavenging through discarded media.

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

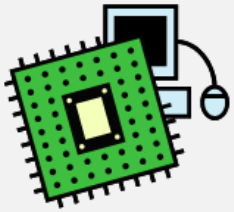
Trojan horse

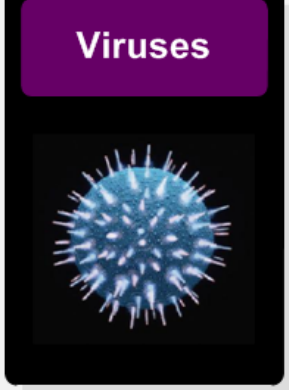
Logic bombs

The email contains a Trojan virus

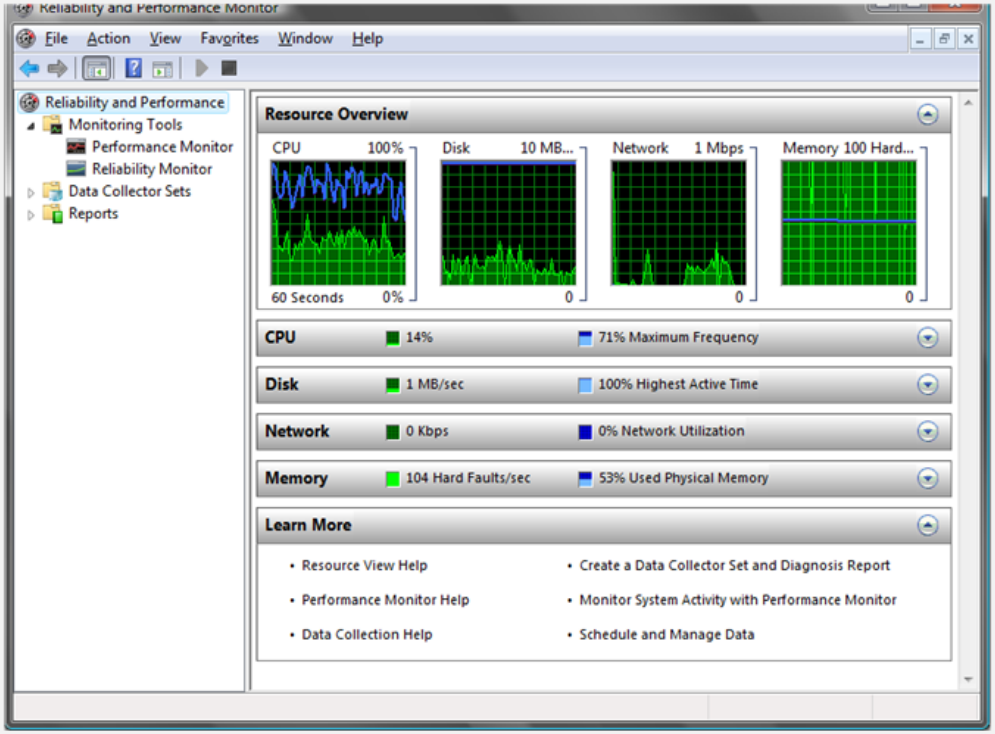
Author: Prof Bill Buchanan

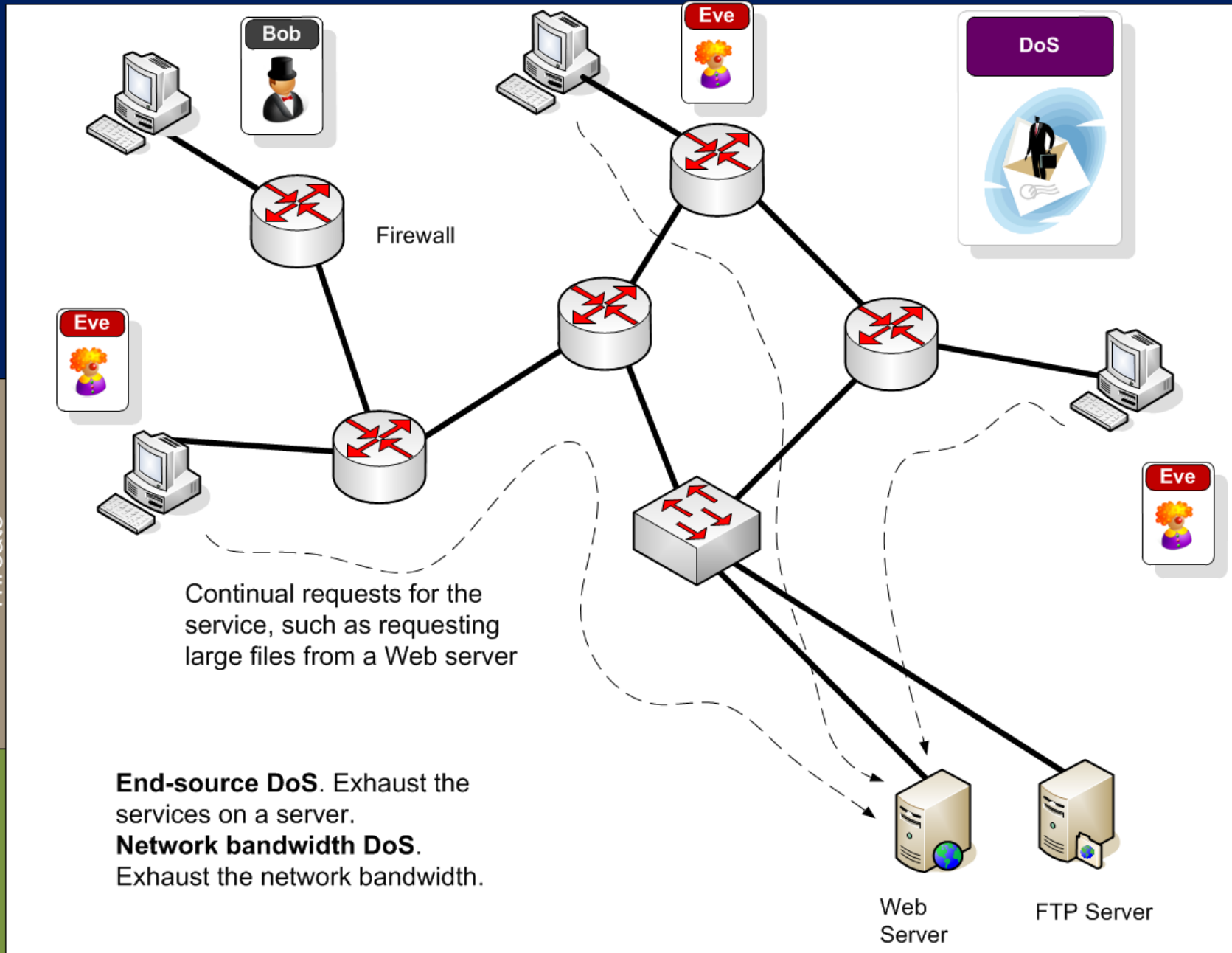
Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.





Viruses. This involves attaching program which self replicate themselves.





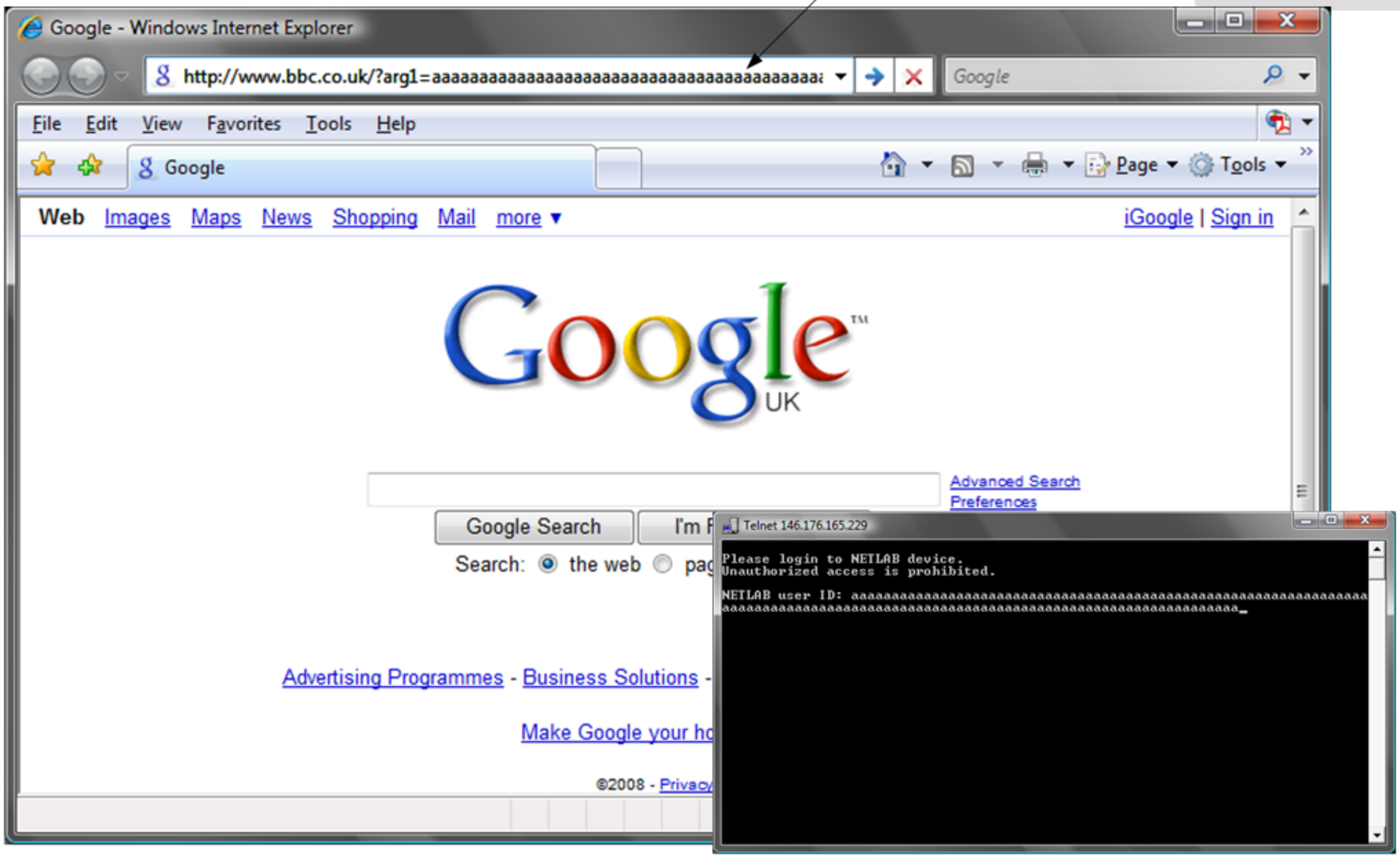
End-source DoS. Exhaust the services on a server.
Network bandwidth DoS. Exhaust the network bandwidth.

Author: Prof Bill Buchanan

Active attack

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



Threats

Introduction

Author: Prof Bill Buchanan

Inference

Inference. This involves exploiting database weaknesses using inferences.

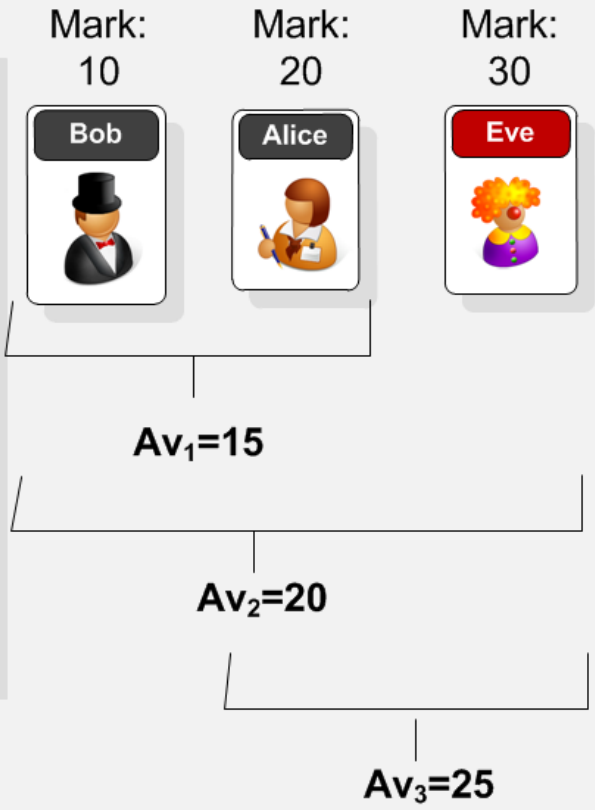
For example … the marks for any student is not allowed, but the average a number of students is allowed.

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



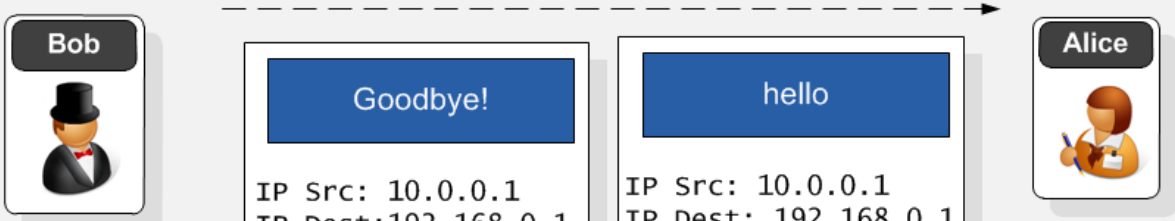
Alice's mark=Av_1-Av_2+Av_3=15-20+25=20

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

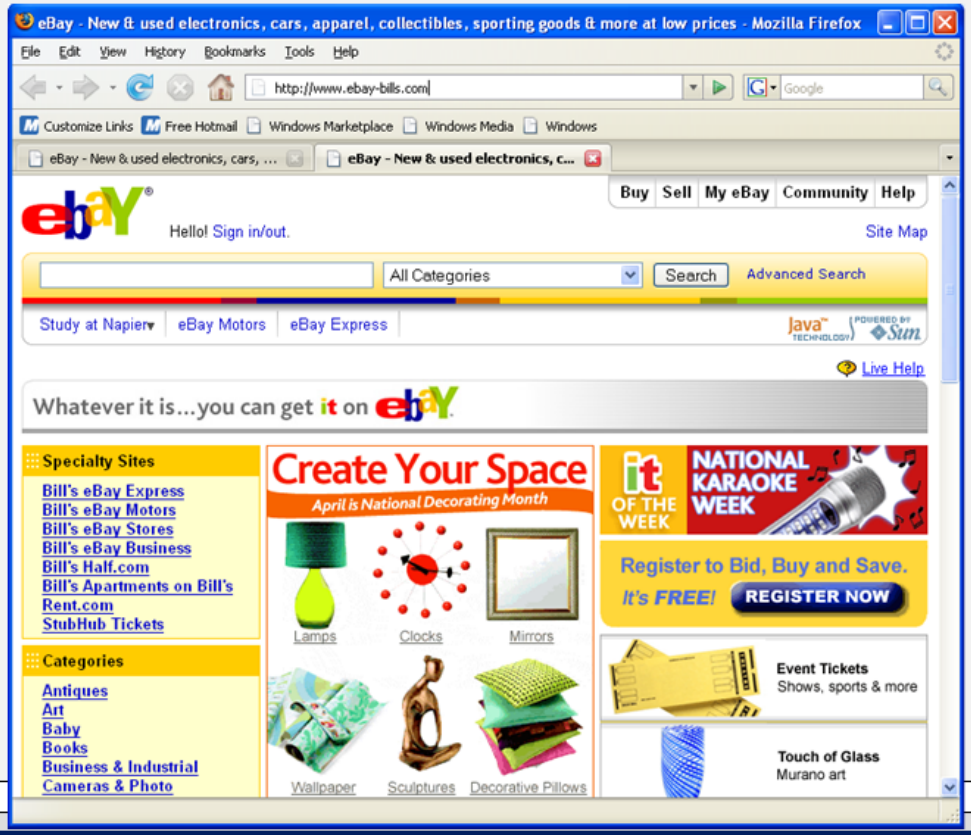
Author: Prof Bill Buchanan

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.

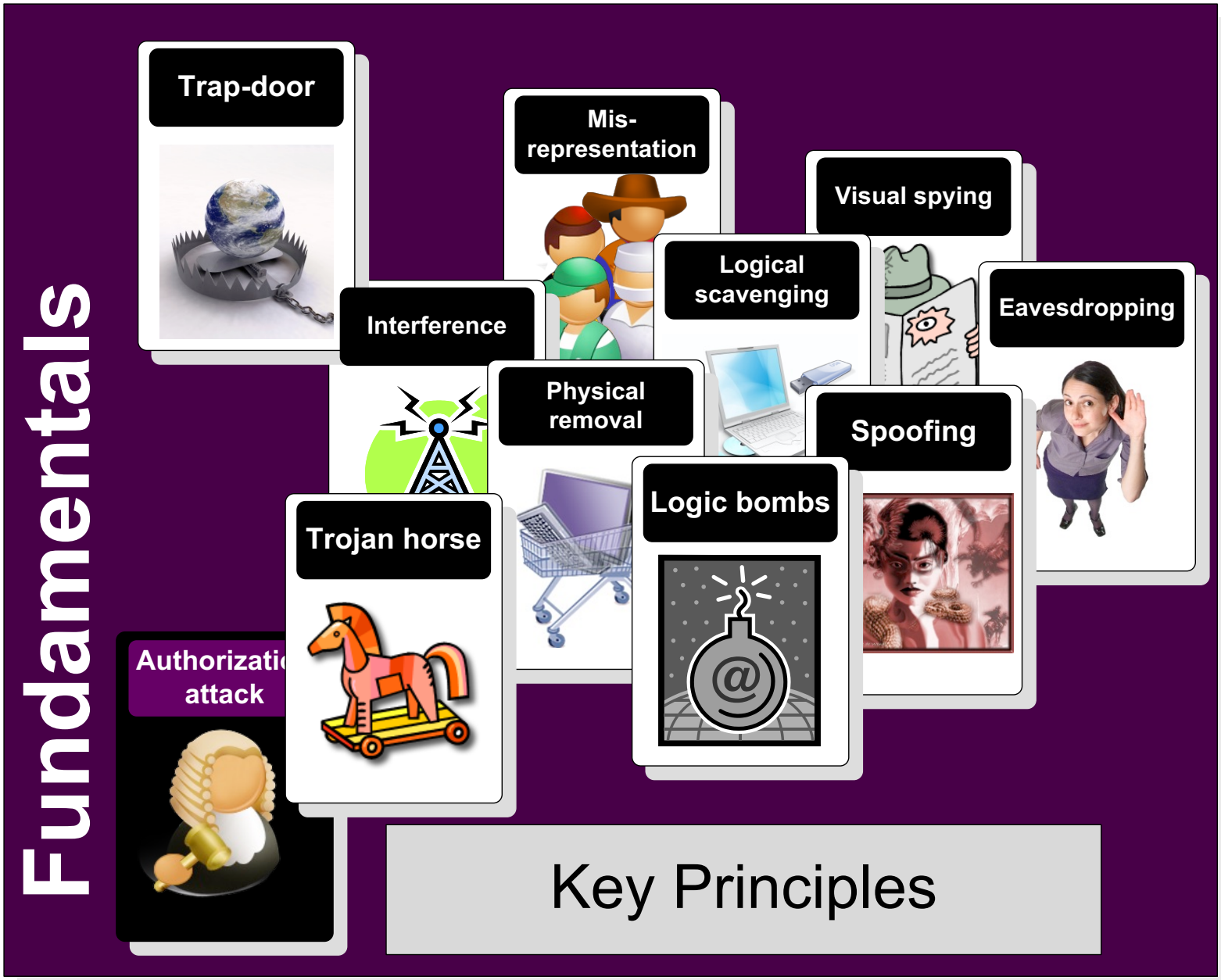
Authorization attack

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.

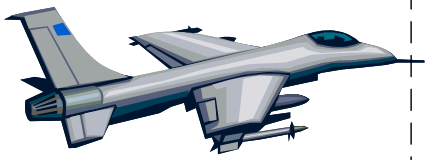


Fundamentals



Author: Prof Bill Buchanan

Enemy takes some time to breach each of the levels of defence

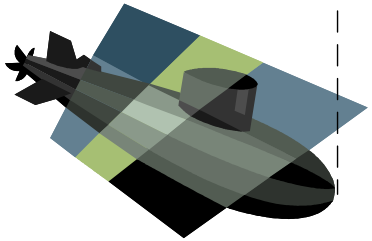


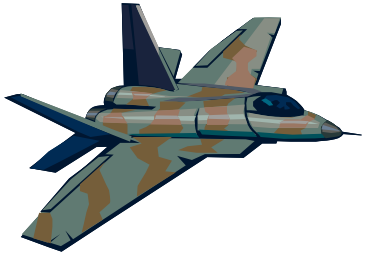
Defence

Defence

Defence

Defence





Forth-level defence

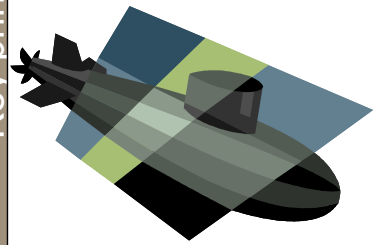
Third-level defence

Second-level defence

First-level defence

Author: Prof Bill Buchanan

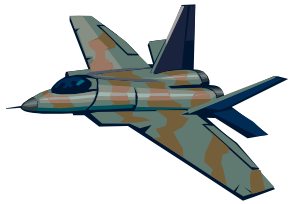



Trusted (our side)



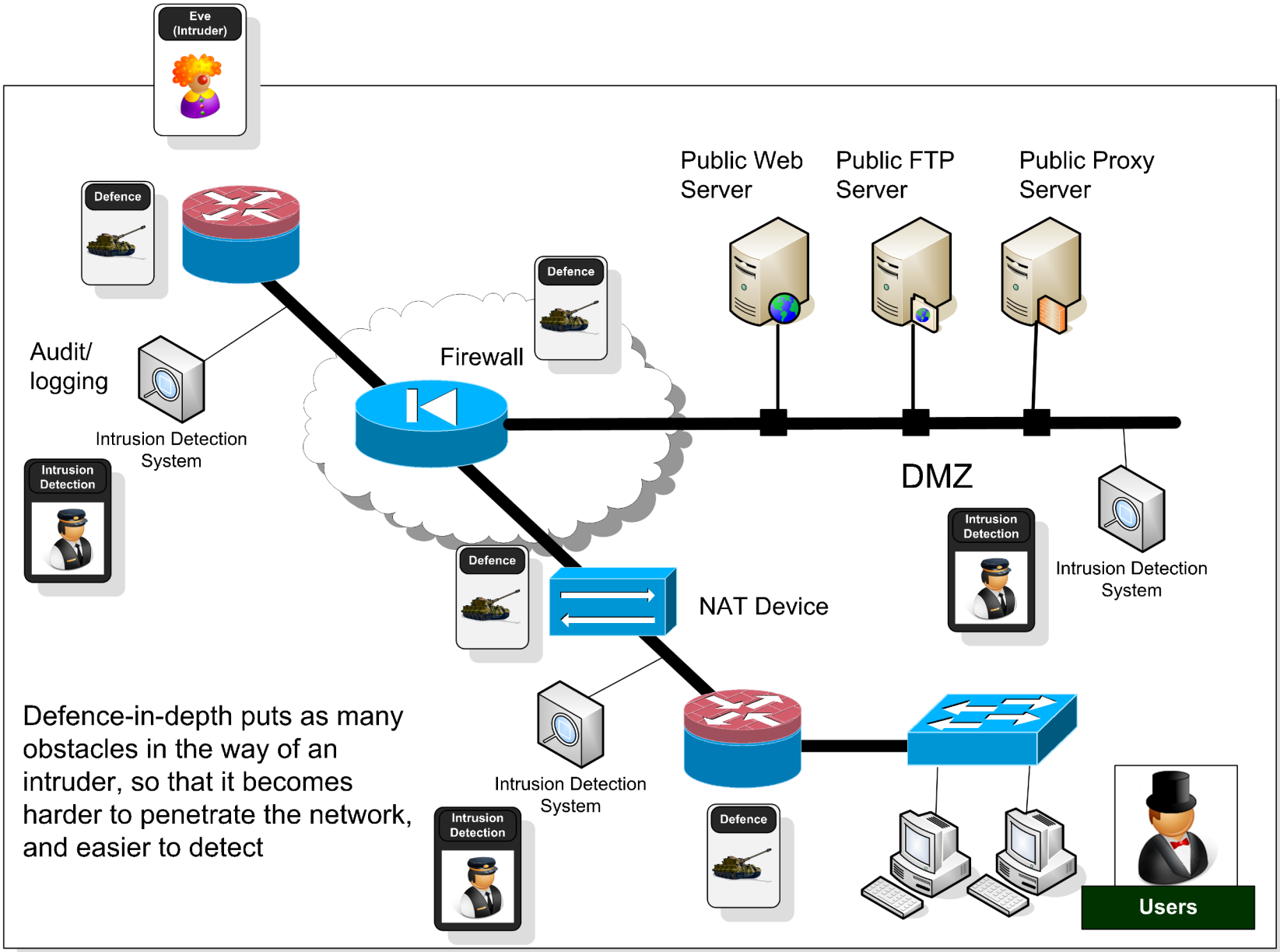

DMZ – an area where military actions are prohibited





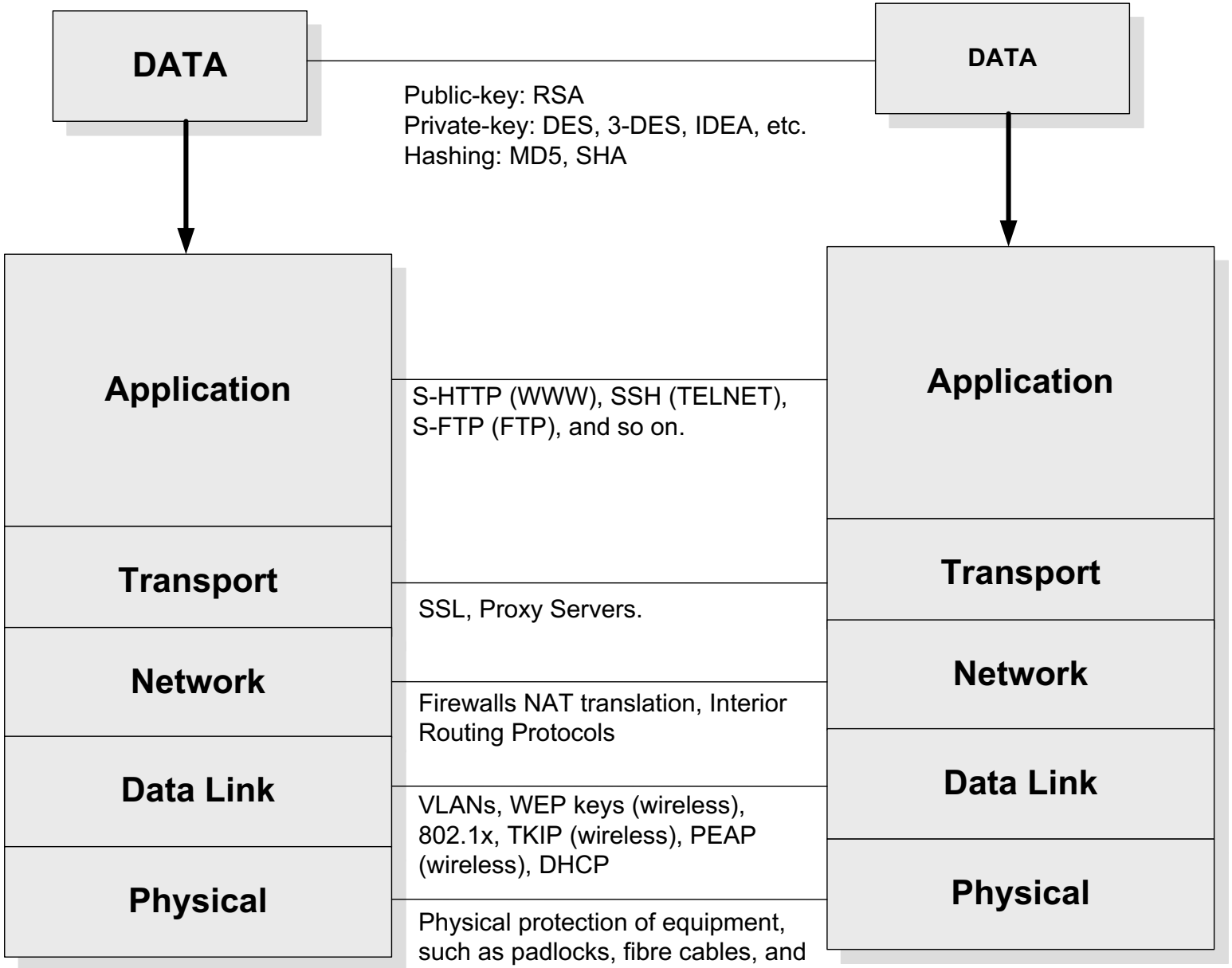
Untrusted (their side)

Author: Prof Bill Buchanan

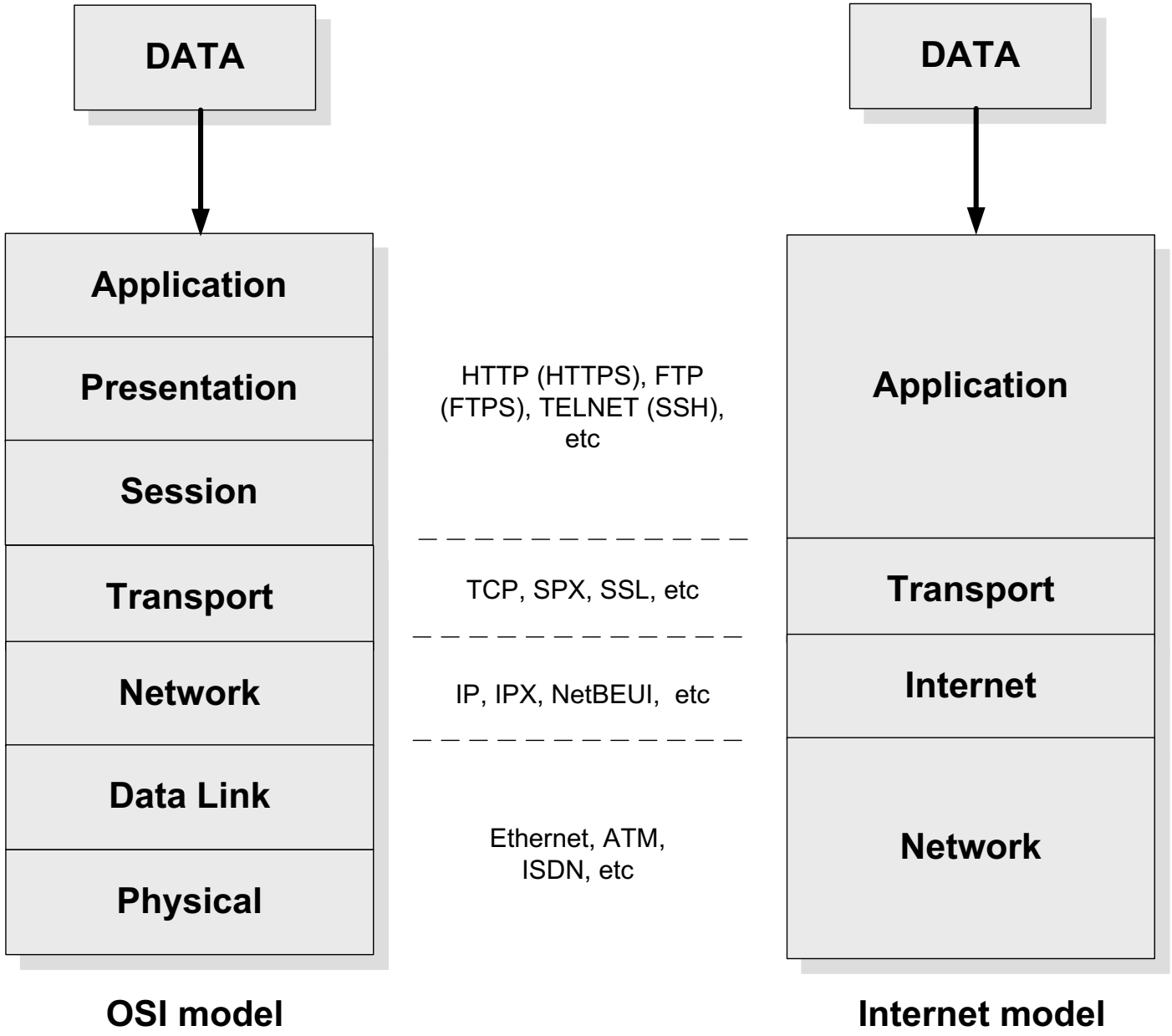


Defence-in-depth puts as many obstacles in the way of an intruder, so that it becomes harder to penetrate the network, and easier to detect

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



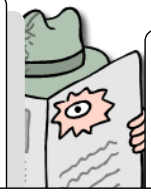
Author: Prof Bill Buchanan

Fundamentals

Trap-door

Mis-representation

Visual spying



Logical scavenging

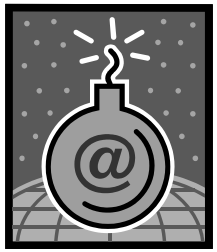
Eavesdropping

Interference

Physical removal

Spoofing

Logic bombs



Trojan horse

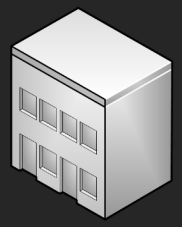
Authorizati attack

ISO 27002

Author: Prof Bill Buchanan

1. Business Continuity Planning

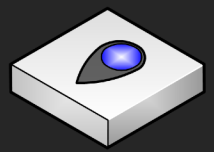
To counteract interruptions to business activities and to critical business processes.

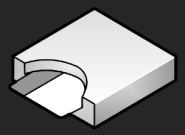


ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

2. Access Control

- Control access to information
- Prevent unauthorised access to information systems
- Ensure the protection of networked services
- Prevent unauthorized computer access
- Detect unauthorised activities.
- Ensure information security when using mobile computing and tele-networking facilities





3. System Acquisition, Development and Maintenance

- Ensure security is built into operational systems;
- Prevent loss, modification or misuse of user data in application systems;
- Protect the confidentiality, authenticity and integrity of information;
- Ensure IT projects and support activities are conducted in a secure manner;
- Maintain the security of application system software and data.

Fundam

Author: Prof Bill Buchanan

4. Physical and Environmental Security

- Prevent unauthorised access, damage and interference to business premises and information;
- Prevent loss, damage or compromise of assets and interruption to business activities;
- Prevent compromise or theft of information and information processing facilities.

ISO 27002.
Started life as "Information Security Code of Practice" from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

5. Compliance

- Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- Ensure compliance of systems with organizational security policies and standards
- Maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Human Resource Security

- To reduce risks of human error, theft, fraud or misuse of facilities;
- to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
- to minimise the damage from security incidents and malfunctions and learn from such incidents.

Author: Prof Bill Buchanan

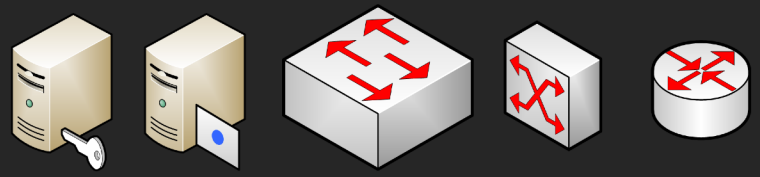
ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

7. Security Organisation

- Manage information security within the Company;
- Maintain the security of organizational information processing facilities and information assets accessed by third parties.
- Maintain the security of information when the responsibility for information processing has been outsourced to another organization.

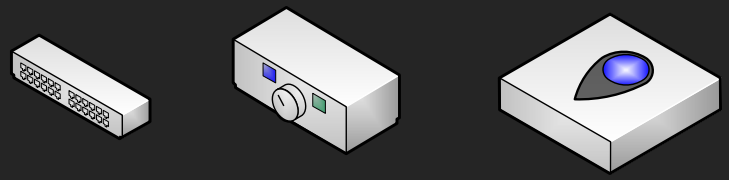
8. Computer and Network Management

- Ensure the correct and secure operation of information processing facilities;
- Minimise the risk of systems failures;
- Protect the integrity of software and information;
- Maintain the integrity and availability of information processing and communication;
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- Prevent damage to assets and interruptions to business activities;
- Prevent loss, modification or misuse of information exchanged between organizations.



9. Asset Classification and Control

Maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.



ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

11. Security Incident Management

Anticipating and responding appropriately to information security breaches

10. Security Policy

Provide management direction and support for information security.

12. Risk Analysis

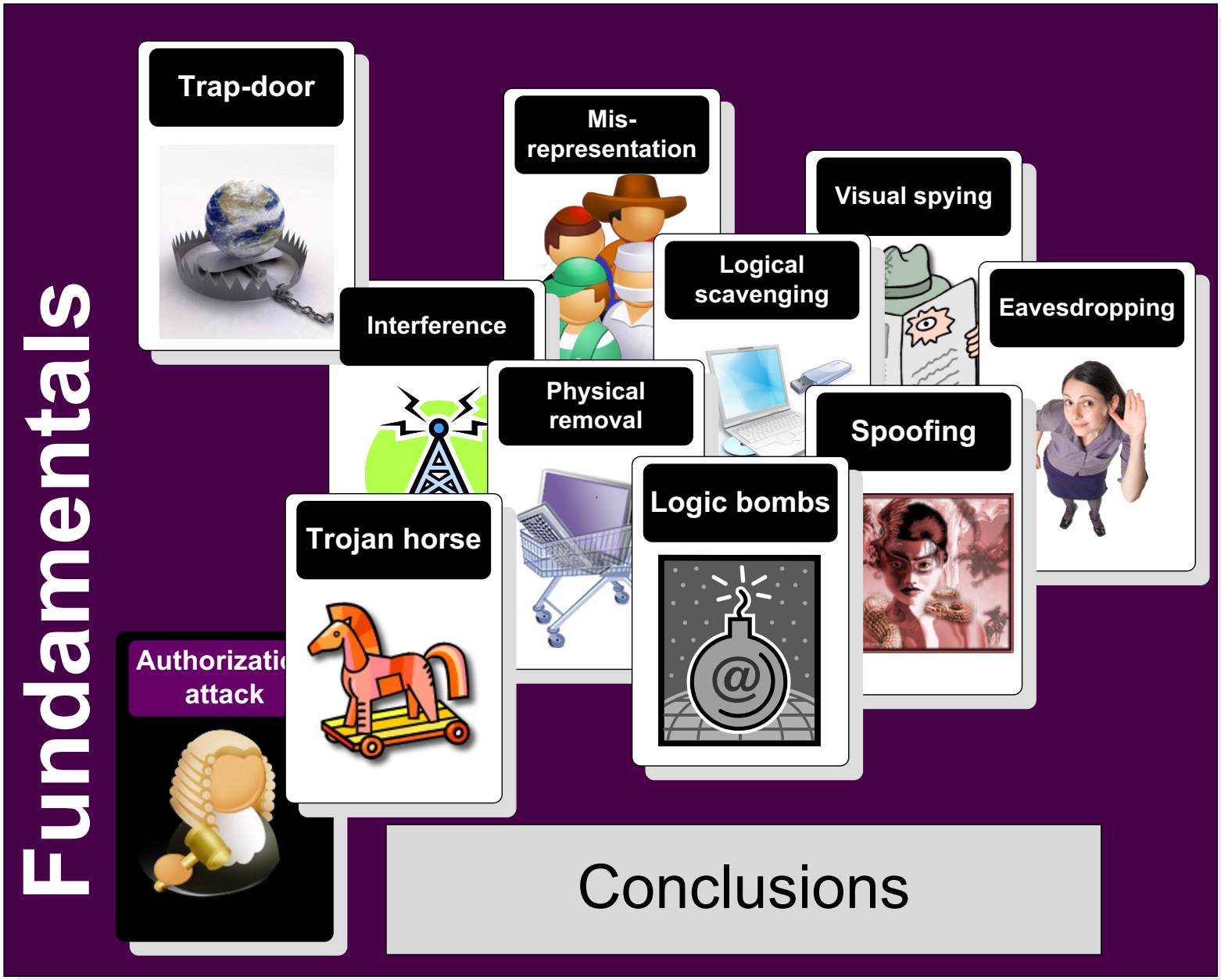
Understand risks involved

ISO 27002

Fundamentals

Author: Prof Bill Buchanan

Fundamentals



Author: Prof Bill Buchanan