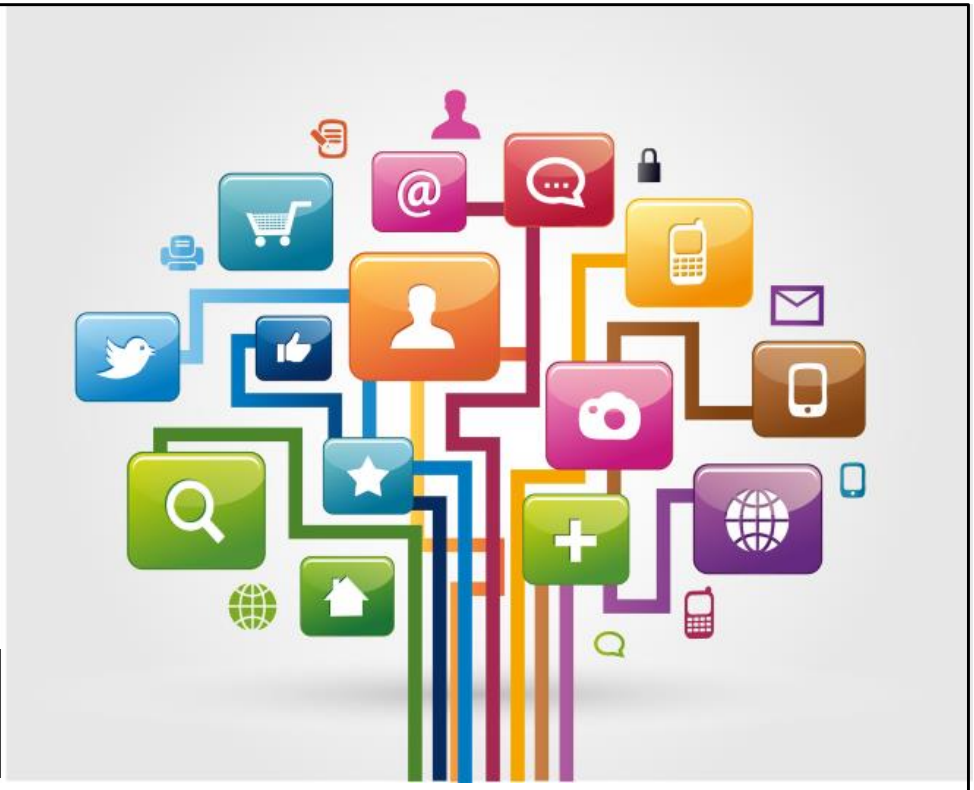
Edinburgh Napier UNIVERSITY

Computing Science: Now and The Future



Inc. Computer Security

Prof Bill Buchanan, Twitter: @billatnapier
Web: asecuritysite.com, brightredbooks.net

Edinburgh Napier UNIVERSITY

Xmas Cyber Lectures (3000 pupils – 4 cities) + IET Xmas this year

IT4U (Sensors, Cyber, Games, etc)
- 400 pupils/17 schools

Why Computing?

Bright Red Digital Zone (8,000 users)

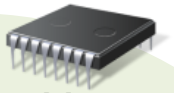
Engagement

- **Cyber Security**
- **Asecuritysite.com**
- **As Seen on TV**

Edinburgh Napier UNIVERSITY

Cloud is a disruptive technology … probably the most disruptive since the **transistor**

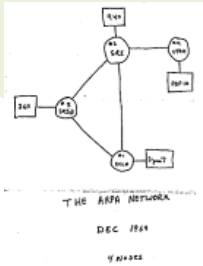
Transistor



Microchip

Microprocessor

The Cloud



The Internet

The Personal Computer

Edinburgh Napier UNIVERSITY

Large demand for IT graduates

We architecture, we design, we analyse, we build, and we test

Why Computing?

There's lots of different jobs

- Networking.
- Security.
- Software Development.
- Media Design
- Mobile Devices
- Web Development.

New areas every day ...

- Cloud Computing.
- Big Data.
- Mobile Devices.

Edinburgh Napier UNIVERSITY

Data increases every day:

- 12TB of Tweets.
- 90% of all data in the Cloud produced in the last two years.
- 2,500,000,000,000,000 bytes of data produced every data 2.5 Quintillion Bytes – 1 billion hard disks

It's part of every aspect of our lives...

Why Computing?

Everything Is dependent on the Internet

- Banking.
- Oil and Gas.
- E-Commerce.
- Transport.
- … virtually everthing

It's all going digital:

- Data.
- Voice.
- Video.
- Sensors.

Edinburgh Napier UNIVERSITY

Tech Companies

It's part of most companies ...

Why Computing?

Finance Industry

... and lots of others

Edinburgh Napier UNIVERSITY

School of Computing

Security and Digital Forensics

Meet the Cast ...

Meet the Cast ...

Intruder

Trusted third party

Meet the Cast ...

Jake Davis, Shetland Islands

Gary McKinnon

Lulzsec

Eve

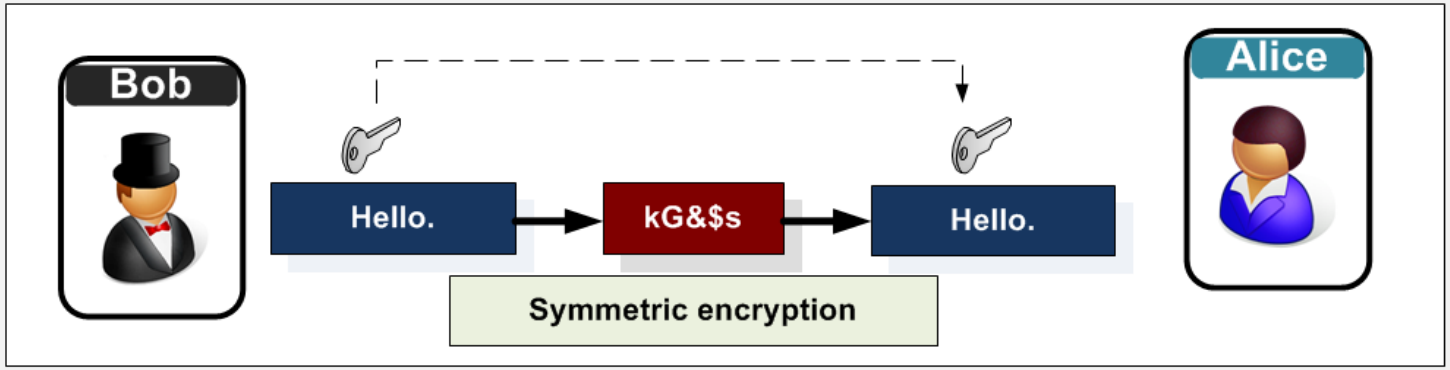
Intruder

Bob

Alice

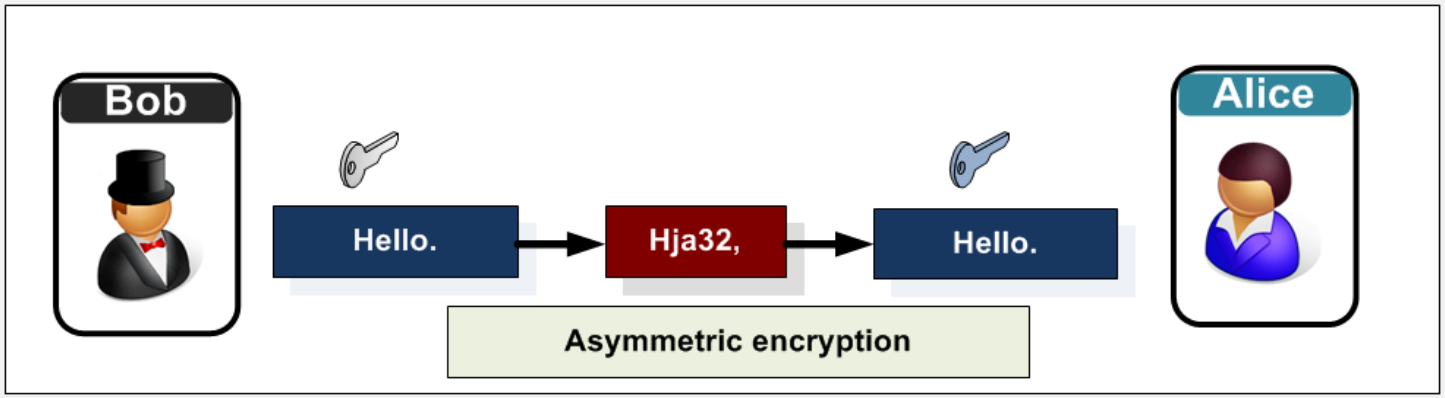
Trent

Trusted third party



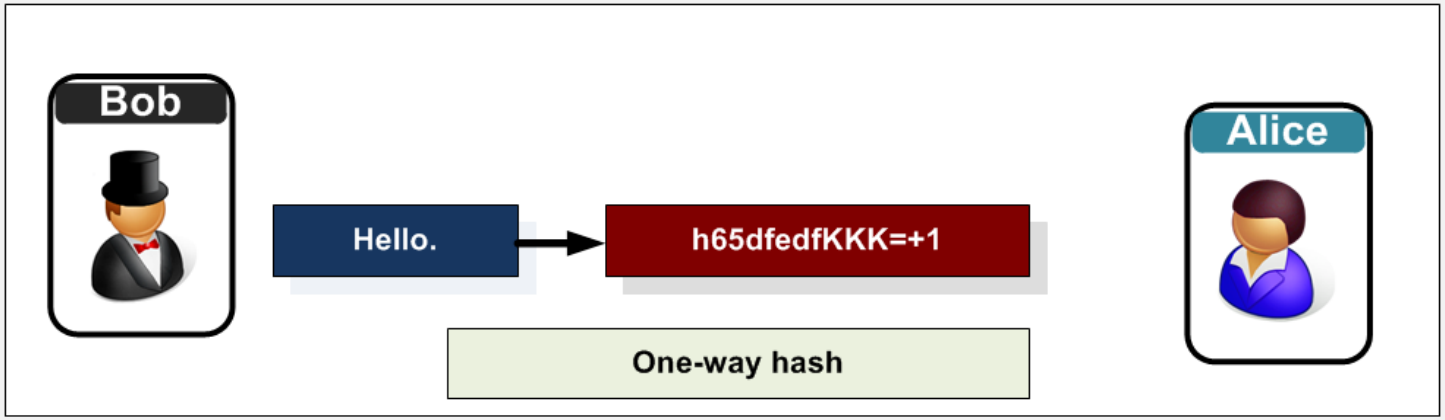
Private-key

Private-key: RC2, RC4, DES, 3DES, AES



Public-key

Public-key: RSA, DSA (factoring prime numbers) FIPS 186-2, ElGamal (Elliptic curve)



Hashing

Hashing: MD5, SHA-1

Strength: 80-bit DES -> 1024 RSA -> 160 bit Elliptic

Edinburgh Napier UNIVERSITY

Areas:

- Networks.
- Operating Systems.
- People/Motivations.
- Application Software.
- Encryption/Identity.
- Mobile Devices.
- Wireless ...

It's about understanding everything ...

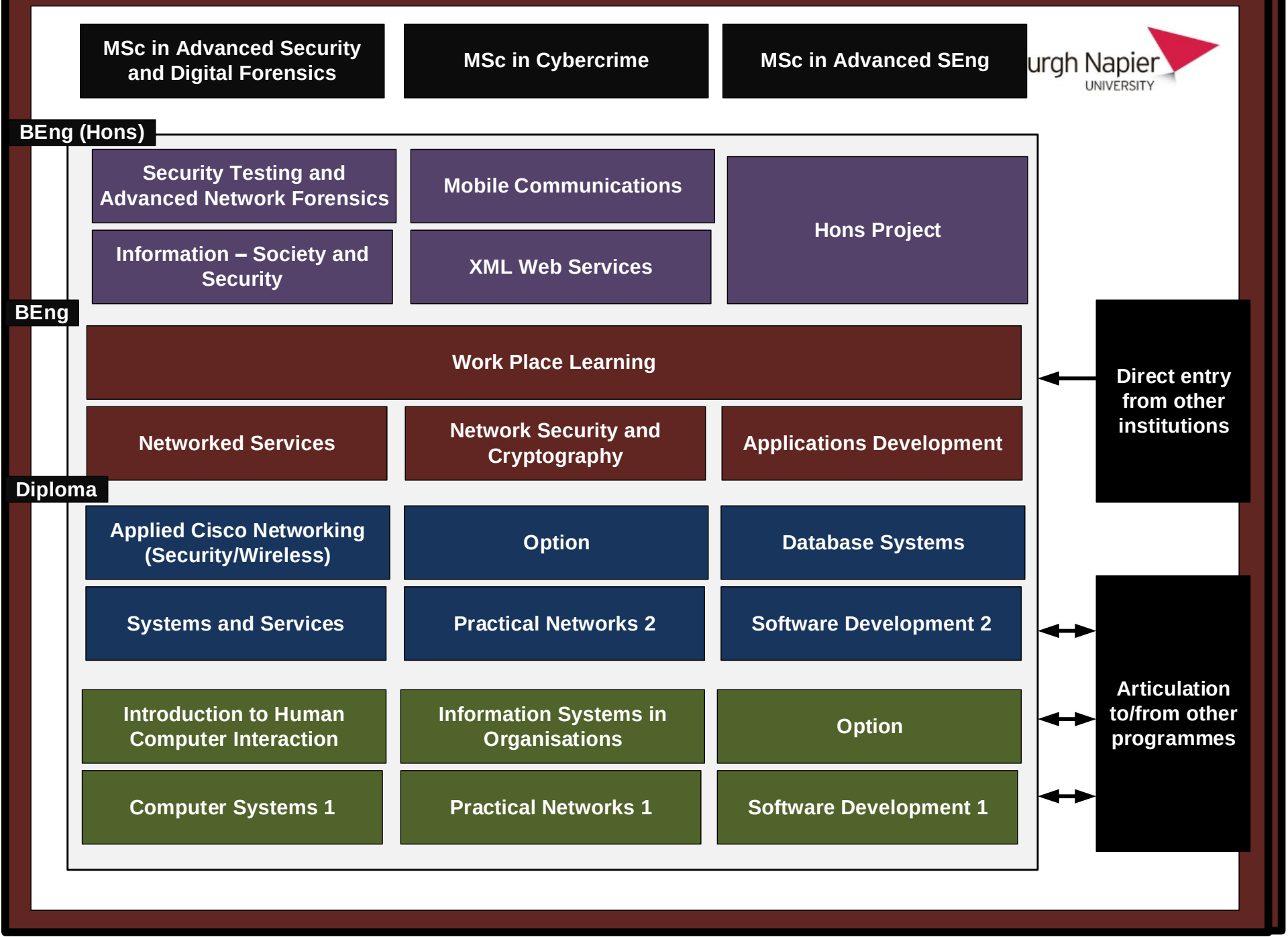
Computer Security and Digital Forensics

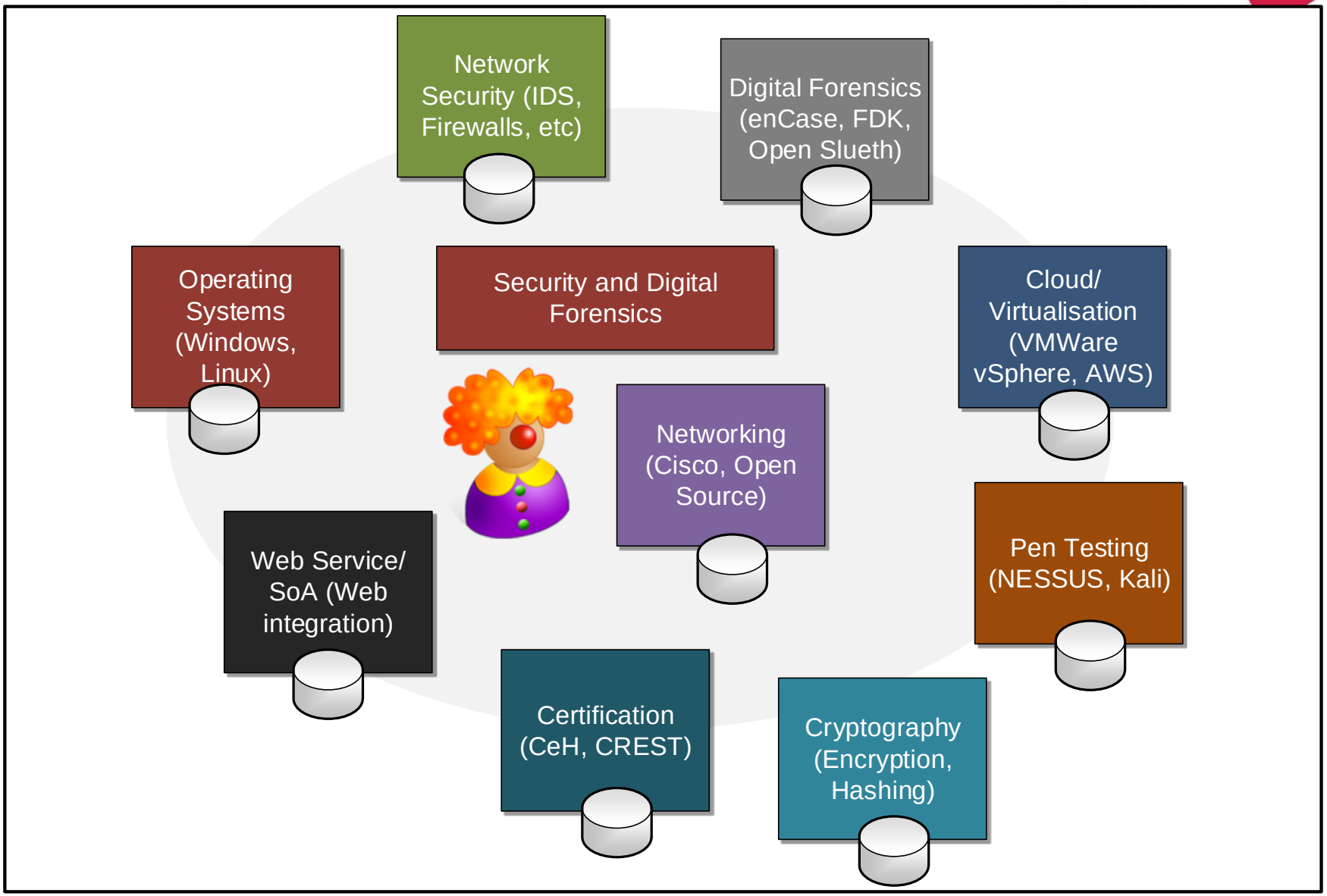
Every changing field

- New applications.
- New threats.
- Cloud and Mobility makes it an every great challenge.
- Lots of opportunities for different careers.

It's all going digital:

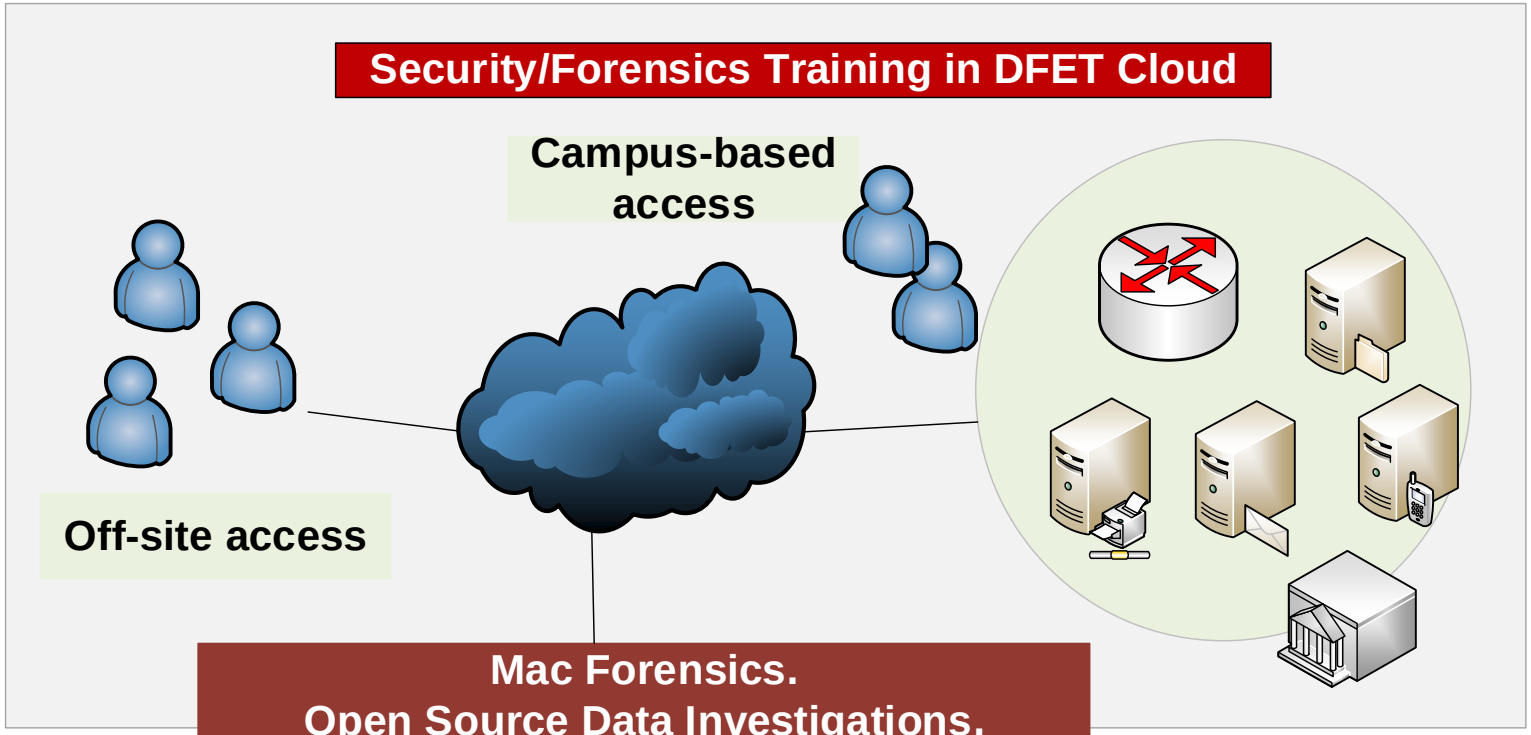
- Banking.
- On-line shopping.
- Media/News.
- Government.
- Health.


MSc in Advanced Security and Digital Forensics
MSc in Cybercrime
MSc in Advanced SEng
urgh Napier UNIVERSITY
BEng (Hons)
Security Testing and Advanced Network Forensics
Mobile Communications
Hons Project
Information – Society and Security
XML Web Services
BEng
Work Place Learning
Direct entry from other institutions
Networked Services
Network Security and Cryptography
Applications Development
Diploma
Applied Cisco Networking (Security/Wireless)
Option
Database Systems
Systems and Services
Practical Networks 2
Software Development 2
Introduction to Human Computer Interaction
Information Systems in Organisations
Option
Articulation to/from other programmes
Computer Systems 1
Practical Networks 1
Software Development 1


Network Security (IDS, Firewalls, etc)
Digital Forensics (enCase, FDK, Open Slueth)
Operating Systems (Windows, Linux)
Security and Digital Forensics
Cloud/ Virtualisation (VMWare vSphere, AWS)
Networking (Cisco, Open Source)
Pen Testing (NESSUS, Kali)
Web Service/ SoA (Web integration)
Certification (CeH, CREST)
Cryptography (Encryption, Hashing)

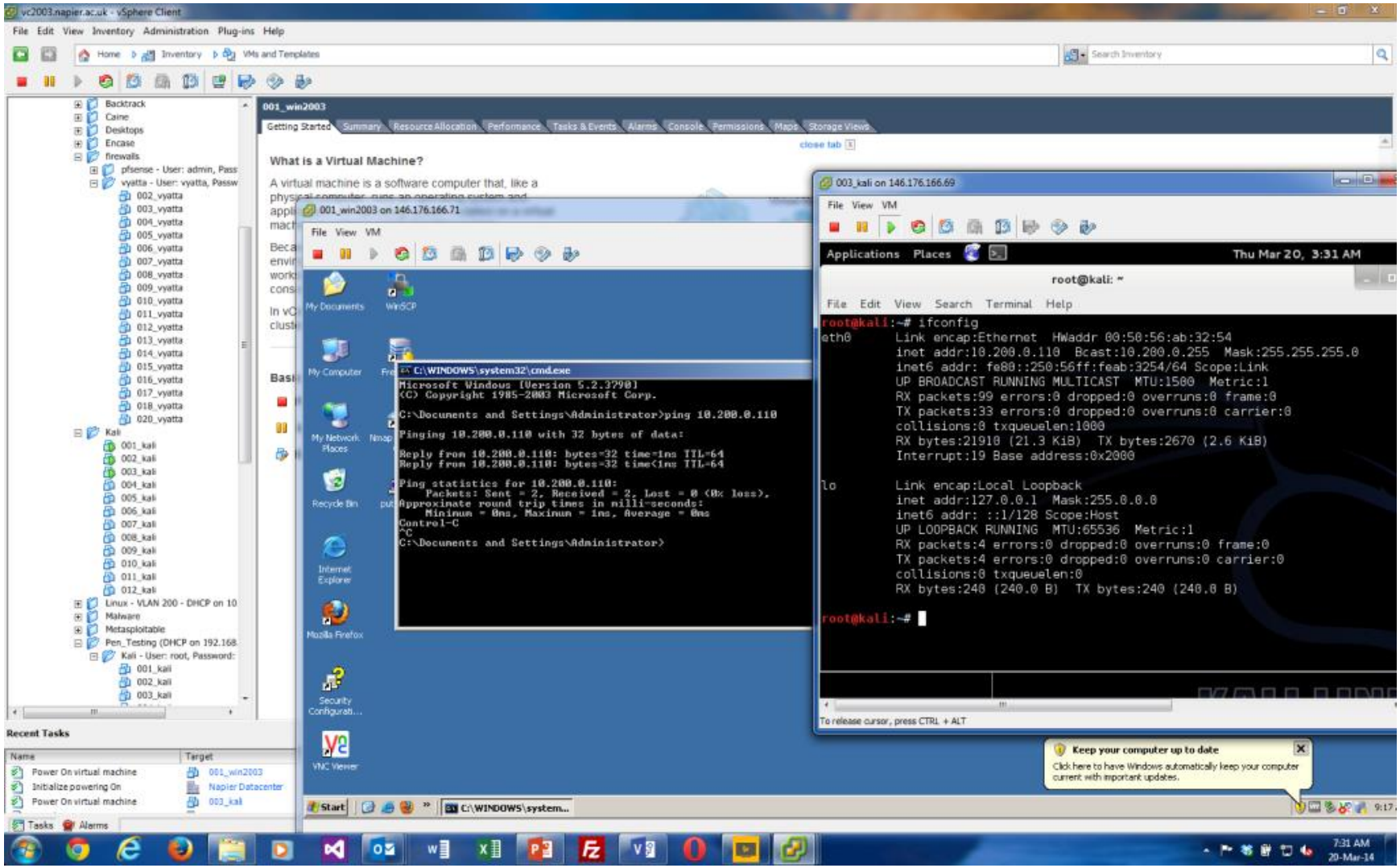
DFET

Edinburgh Napier UNIVERSITY



DFET Cloud

Edinburgh Napier UNIVERSITY



Edinburgh Napier UNIVERSITY

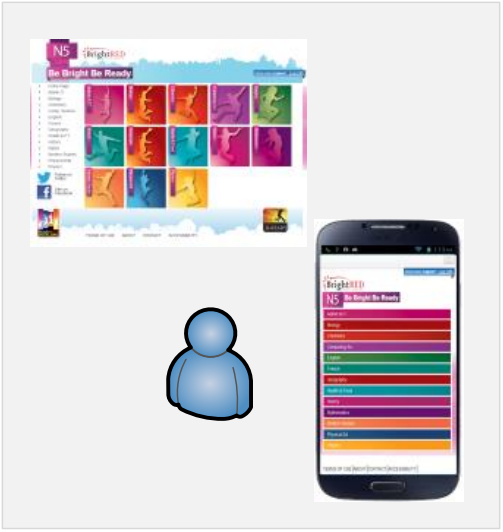
A Few Security Risks in Mobile Working

Mobile Working

Prof Bill Buchanan

Risk 1: Loss of Device

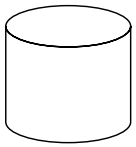
Edinburgh Napier UNIVERSITY



Web connections (Cloud+Corporate)

Email connections (Cloud+Corporate)

File connection (Cloud+Corportate)



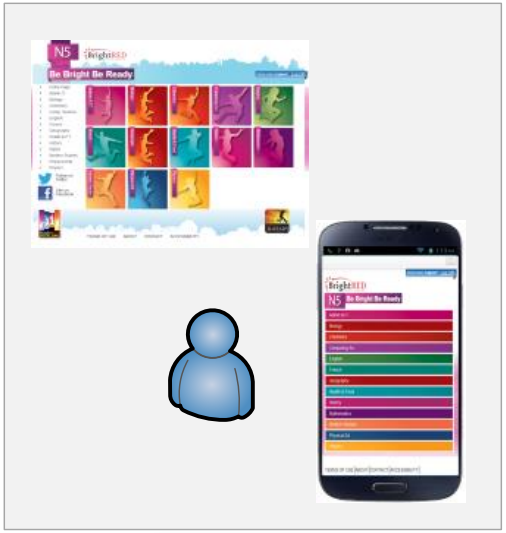
Location Records

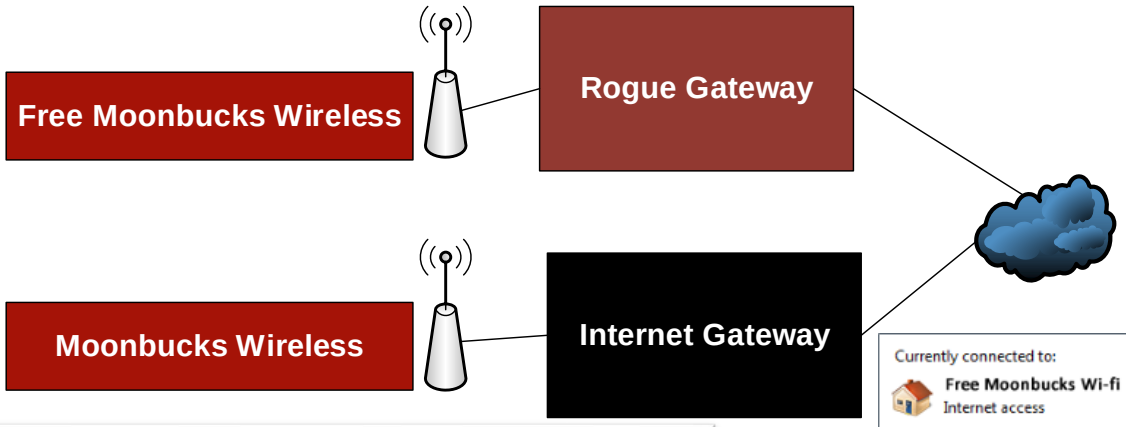
Phone Records

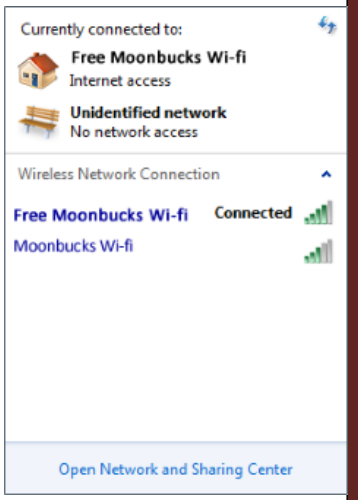
Break PIN → Root mobile phone → Extract Memory and Storage (USB) → Memory Analysis / Disk Storage Analysis

Risk 2: Rogue SSID/Gateway

Edinburgh Napier UNIVERSITY

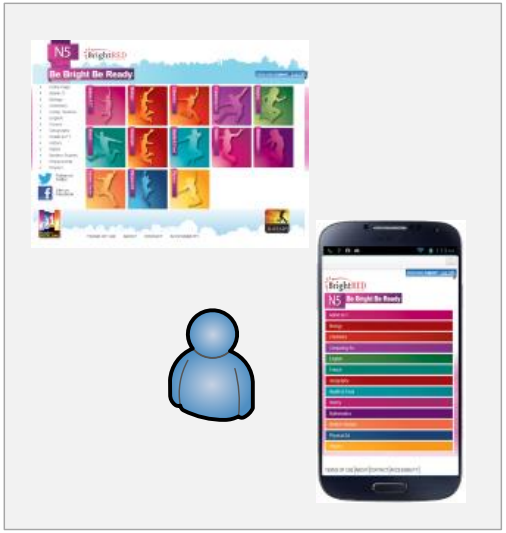


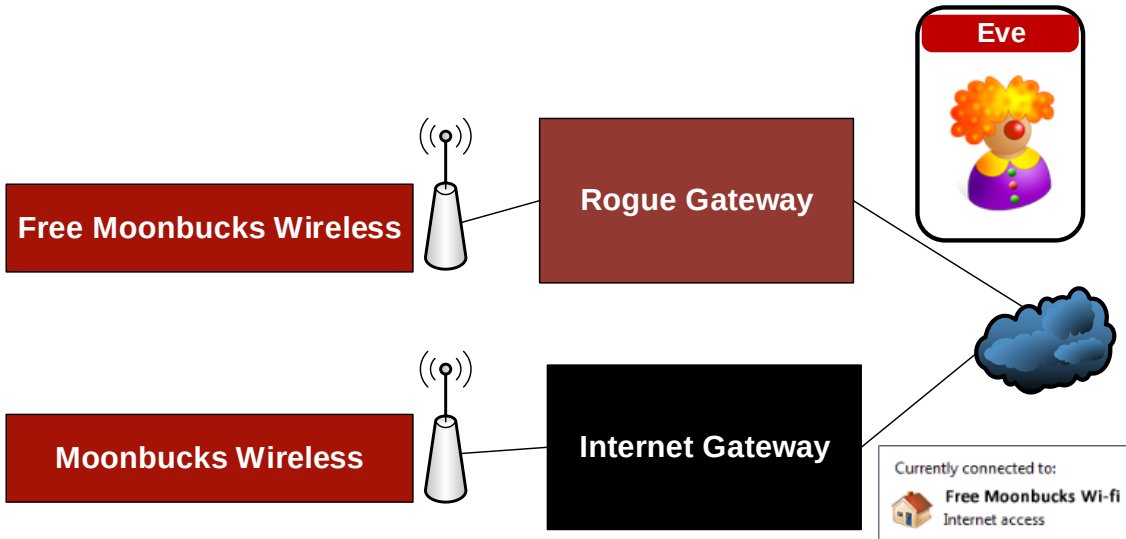


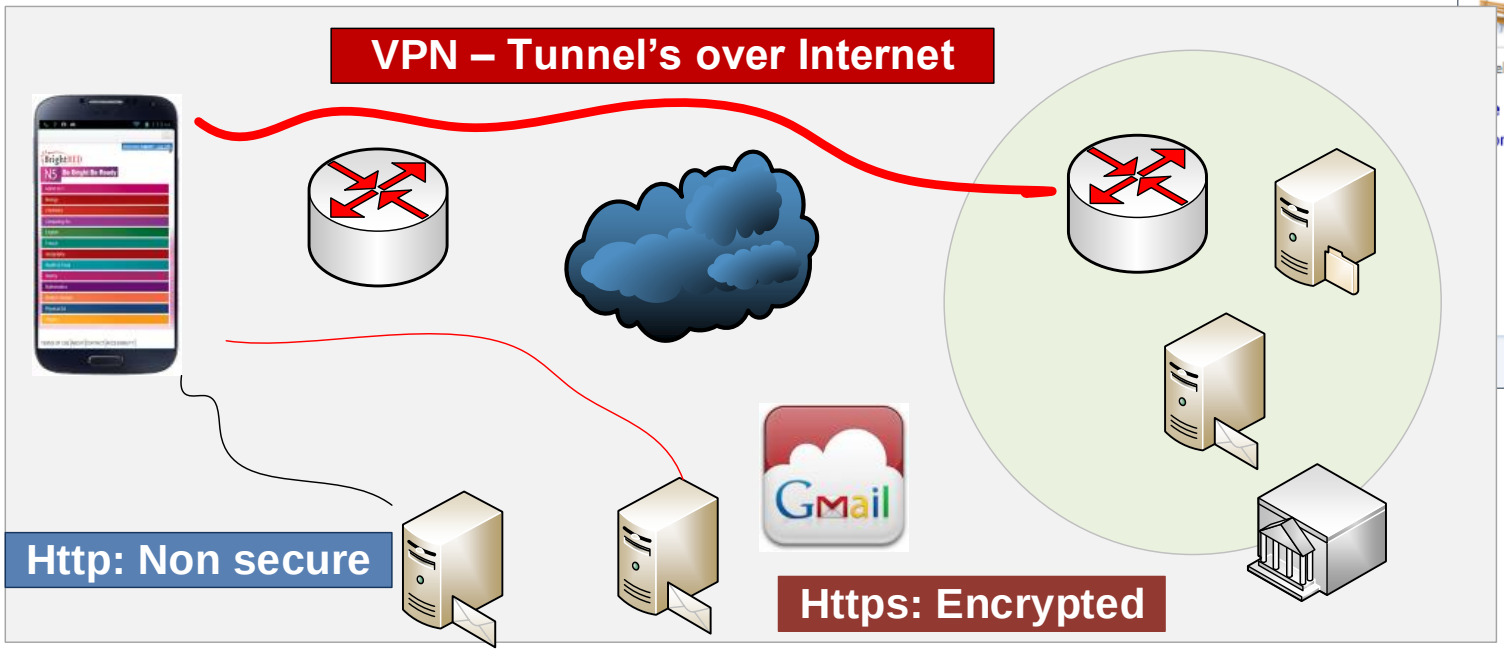


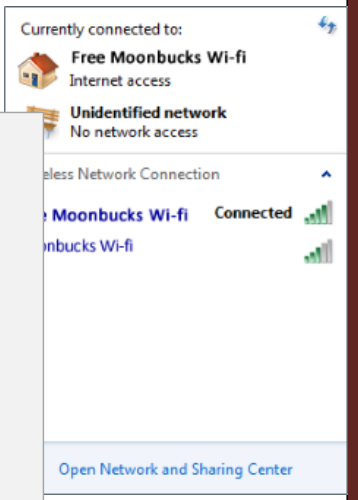
Risk 2: Rogue SSID/Gateway

Edinburgh Napier UNIVERSITY





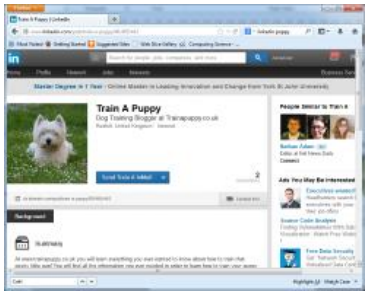




Risk 3: Lack of Separation

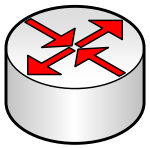
Edinburgh Napier UNIVERSITY

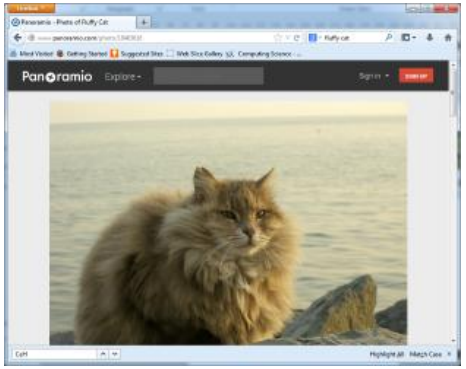
Business Life



Home Life

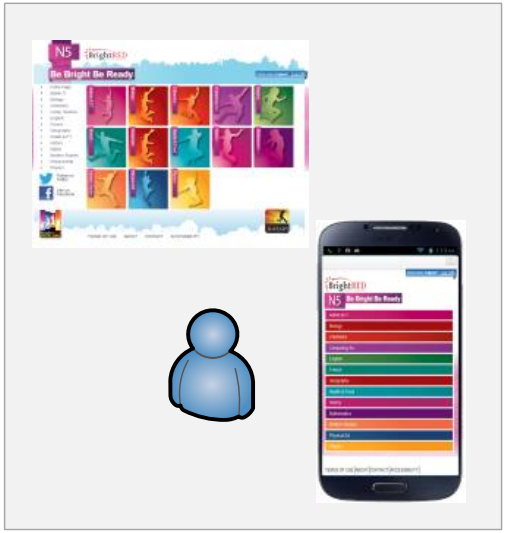
Corporate Firewall





Risk 4: One Password Fits All

Edinburgh Napier UNIVERSITY



Adobe

150 million accounts compromised

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

TJ-maxx Marshalls

47 million accounts

LinkedIn

6.5 million accounts (June 2013)

Windows Live

One account hack … leads to others

1 million accounts – in plain text. 77 million compromised

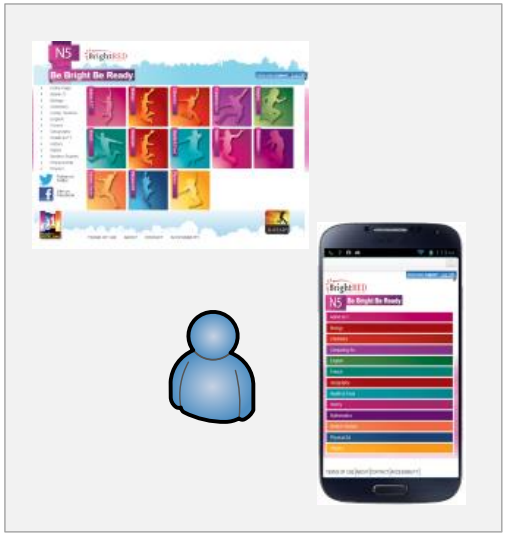
Dropbox compromised 2013

citigroup

200,000 client accounts

Risk 4: One Password Fits All

Edinburgh Napier UNIVERSITY

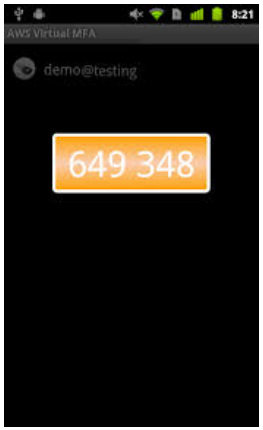


Adobe

150 million accounts compromised

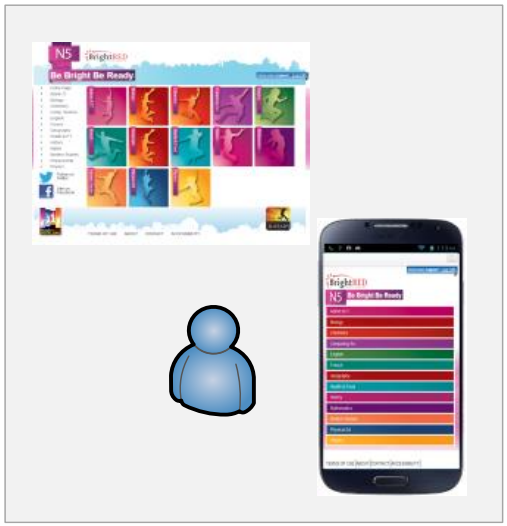
#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

Two-factor everything in the Cloud

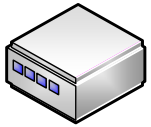


Risk 5: Device Poisoning

Edinburgh Napier UNIVERSITY



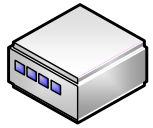
Who has this IP address (192.168.0.1)?



ARP Poisoning

Here is my MAC address (11:22:33:44:55:66)

Gateway (192.168.0.1)



Here is my MAC address (22:33:44:55:66)

DHCP Request ...

Here is your IP address, Gateway, and DNS IP

DNS Poisoning

1 0.000000 0.0.0.0 255.255.255.255 DHCP 314 DHCP Discover - Transaction ID 0x3d1d
Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

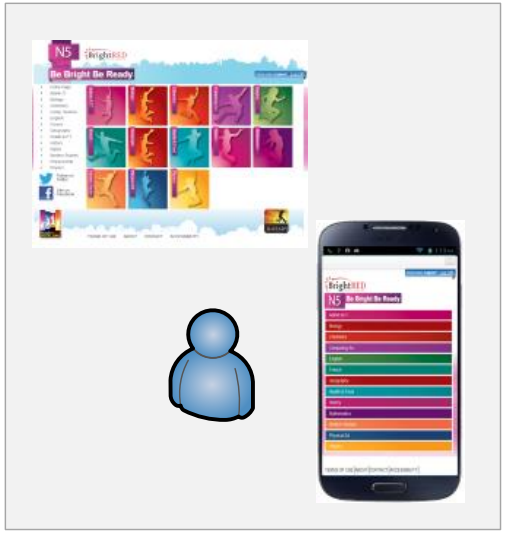
2 0.000295 192.168.0.1 192.168.0.10 DHCP 342 DHCP Offer - Transaction ID 0x3d1d
Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
Frame 3: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

4 0.070345 192.168.0.1 192.168.0.10 DHCP 342 DHCP ACK - Transaction ID 0x3d1e
Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

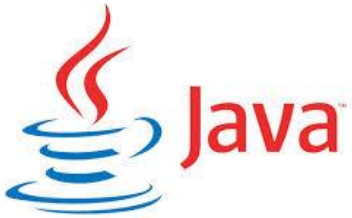
Risk 6: Unpatched Systems

Edinburgh Napier UNIVERSITY



CVE-2007-0071
Adobe Flash Player.
Integer overflow

Phoenix Exploit Kit



CVE-2013-5331
Adobe Flash Player.
Run code on machine.

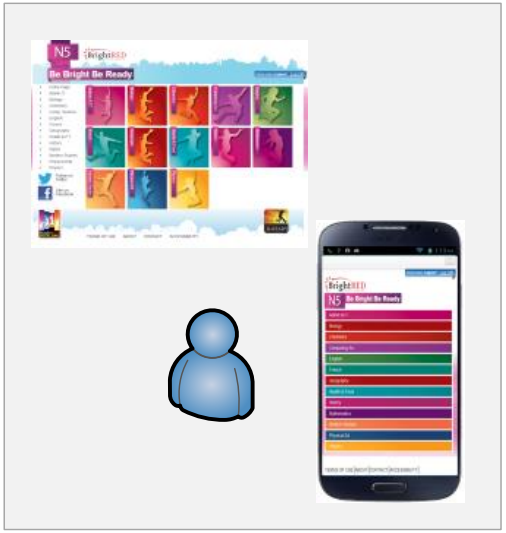
CVE-2013-1723
Java Exploit

CrimeBoss

http://asecuritysite.com/subjects/chapter14

Risk 7: Shoulder Surfing

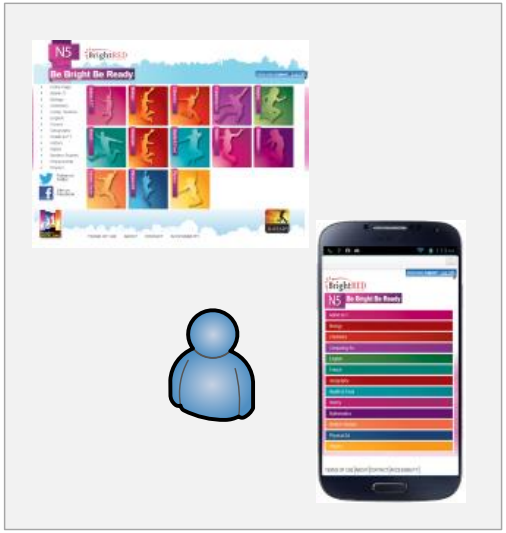
Edinburgh Napier UNIVERSITY



Passwords, customer details, emails, usernames, etc can all be shoulder surfed. Privacy filter is an inexpensive investment.

Risk 8: Storing Non-encrypted to the Cloud

Edinburgh Napier UNIVERSITY

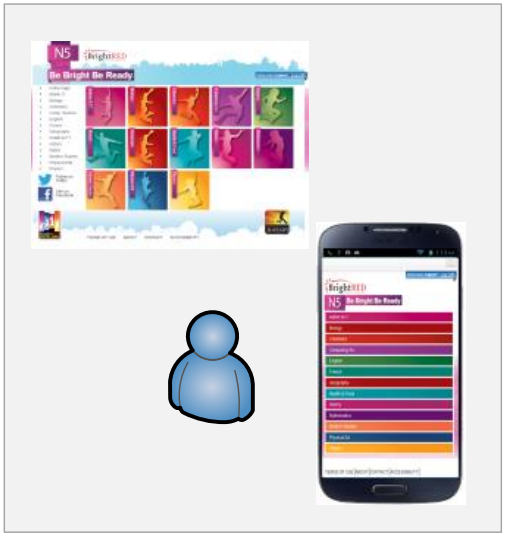


Encryption Layer

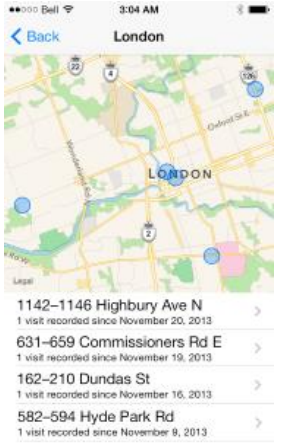
Non-UK/EU storage. Open to hack.

Risk 9: Digital Shadows

Edinburgh Napier UNIVERSITY



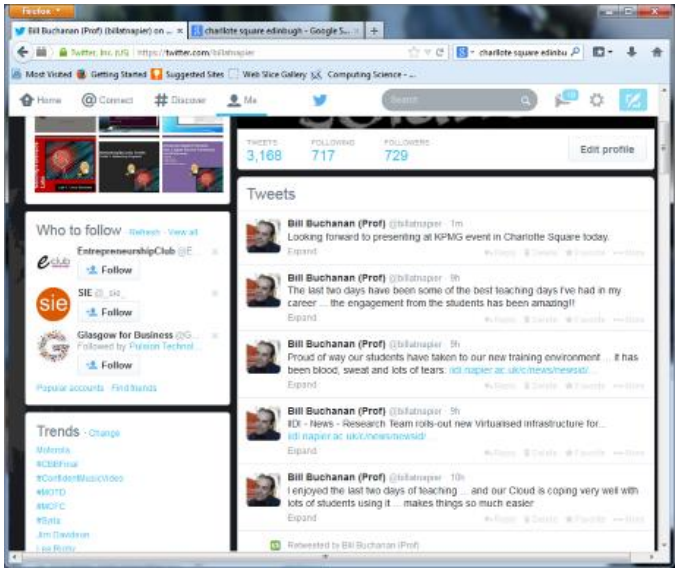
Photos



Device Records

Facebook

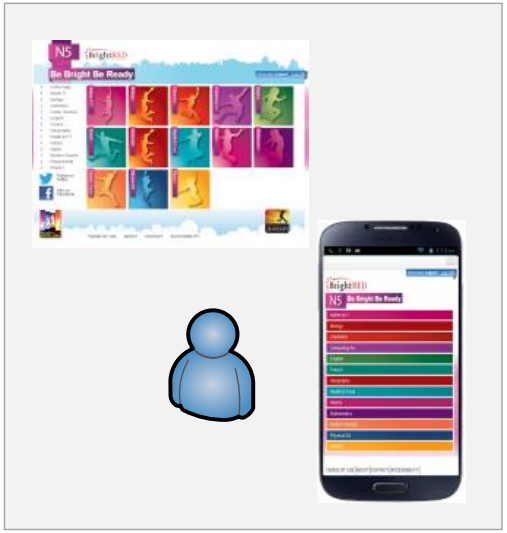
Forums

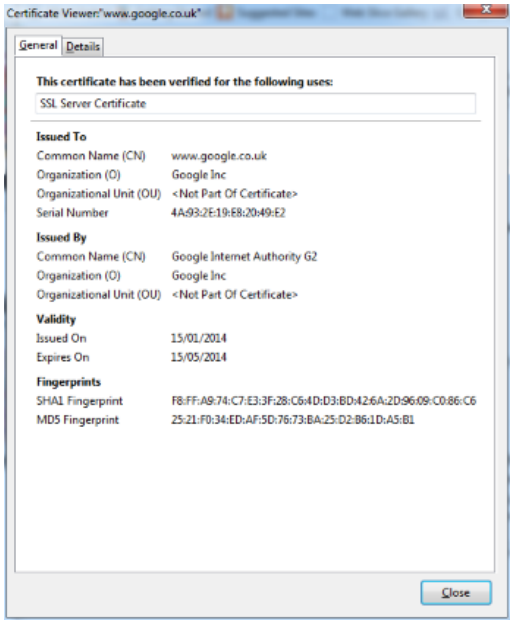


Twitter

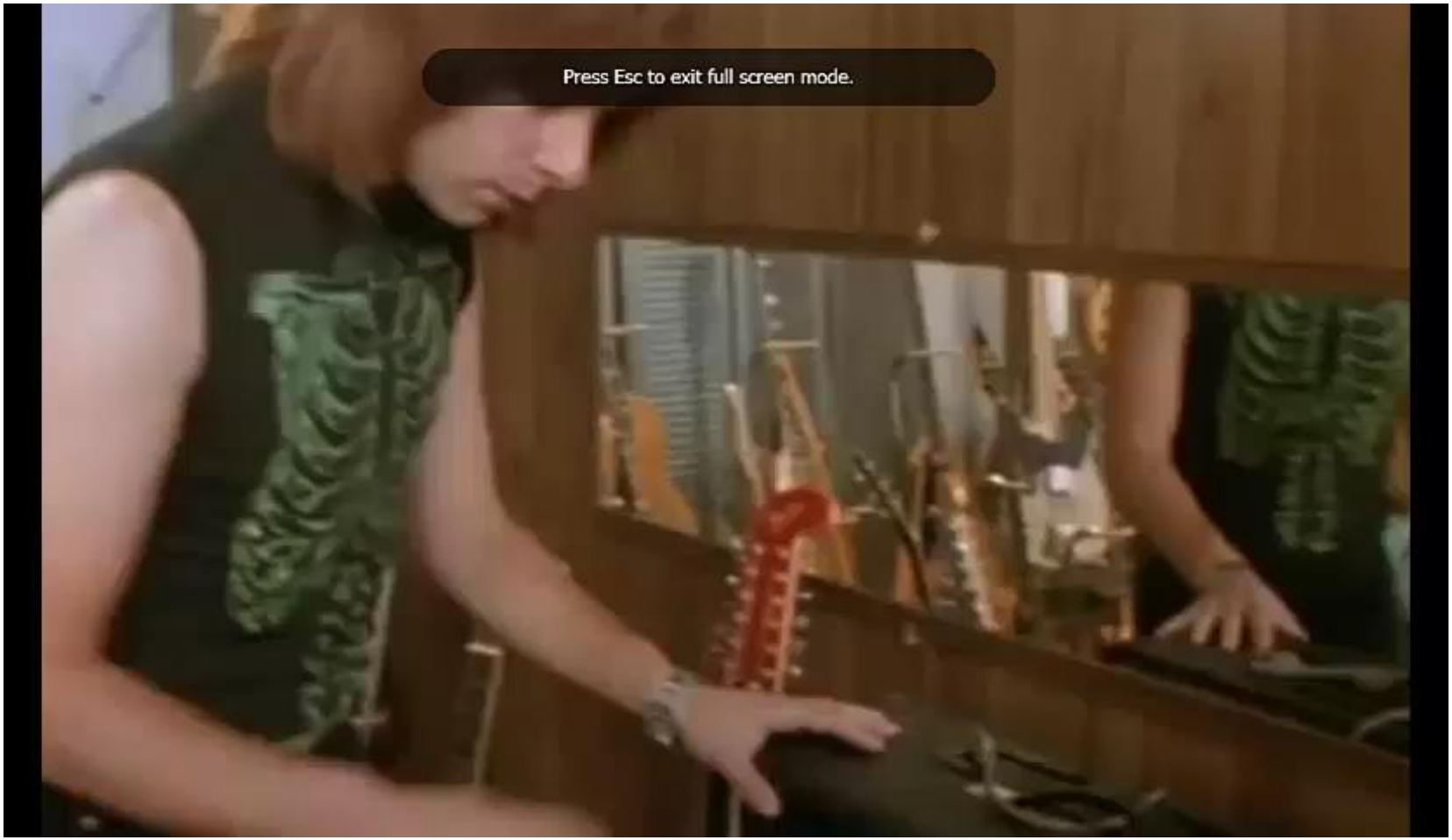
Risk 10: Trusting https and fake cert

Edinburgh Napier UNIVERSITY





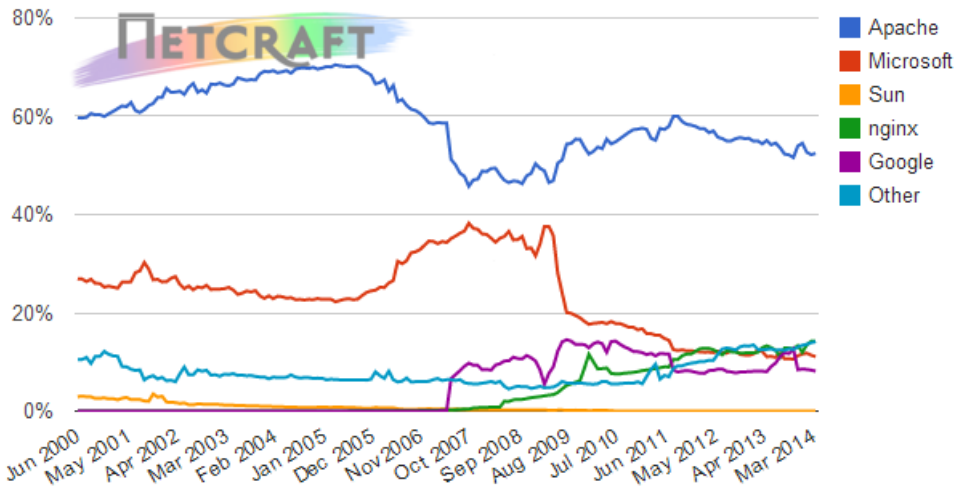
Eve-in-the-middle (Proxy/Fake Certificates)


Press Esc to exit full screen mode.

"On the scale of 1 to 10, this is an 11. Half a million sites are vulnerable, including my own."

Has anyone looked at all the low-margin non-upgradable embedded systems that use OpenSSL? An upgrade path that involves the trash, a visit to Best Buy, and a credit card isn't going to be fun for anyone.

… a 'catastrophic' revelation and suggested it could have been created deliberately to help snoop through firms' data.



I'm hearing that the CAs are completely clogged, trying to reissue so many new certificates. And I'm not sure we have anything close to the infrastructure necessary to revoke half a million certificates.

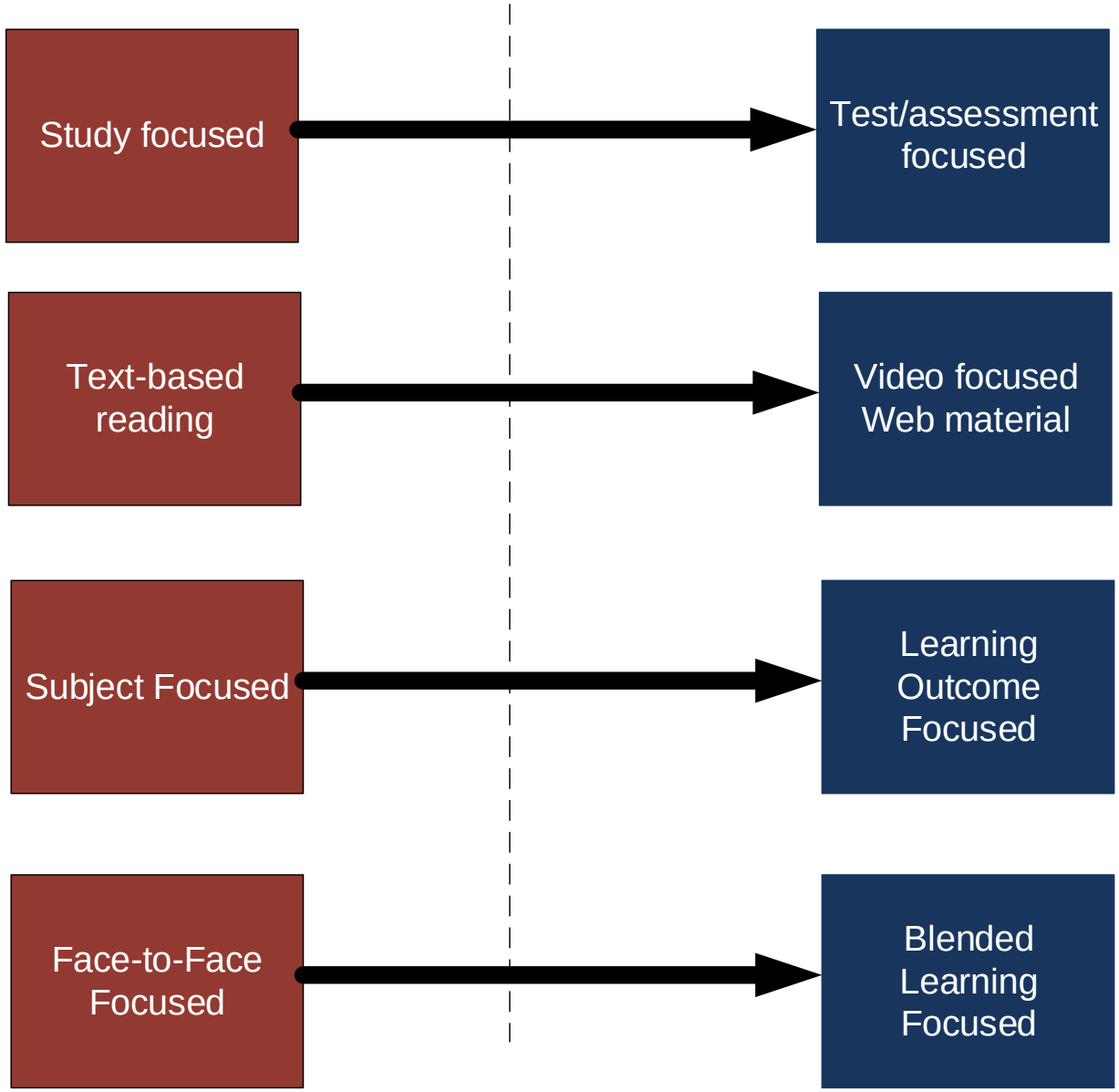
Author: Prof Bill Buchanan

N5 Integration

Motivation: Creating engaging and stimulating Web based material

- Blended Learning.
- Cloud Integration.
- Stimulating material.
- Evaluation of On-line Material.

Prof Bill Buchanan, School of Computing
Twitter: @billatnapier
Web: http://asecuritysite.com
http://brightredbooks.net

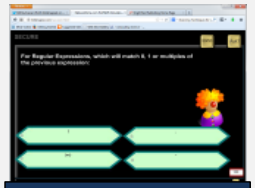

Edinburgh Napier
UNIVERSITY
Study focused
Test/assessment focused
Text-based reading
Video focused Web material
Subject Focused
Learning Outcome Focused
Face-to-Face Focused
Blended Learning Focused

BrightRED PUBLISHING

Edinburgh Napier UNIVERSITY

Twitter

On-line Lectures

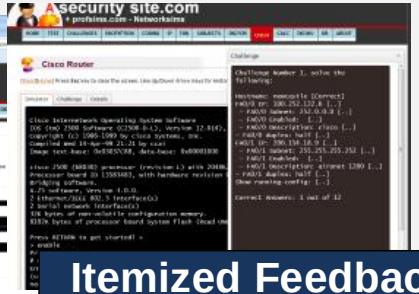


Fun Tests

Cloud Storage

On-line tests

Cloud-based teaching

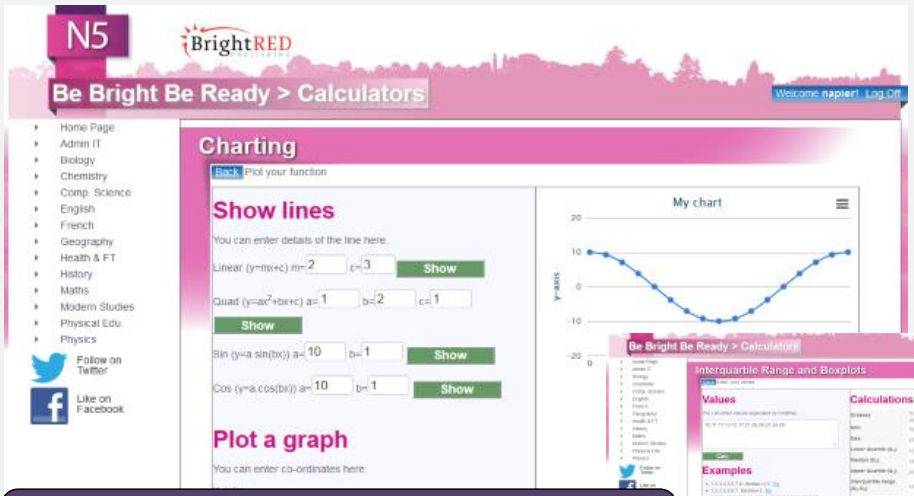


Itemized Feedback

Ever changing challenges

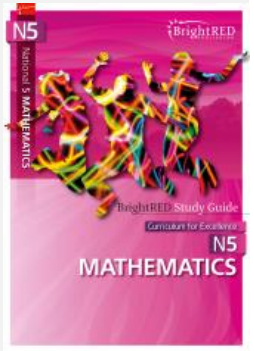
Responsive Designs

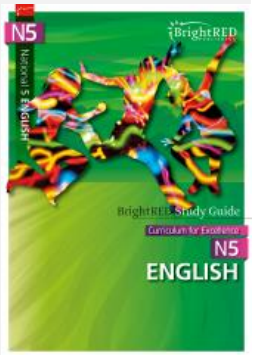
The Cloud can enhance teaching … but good teachers are the key!

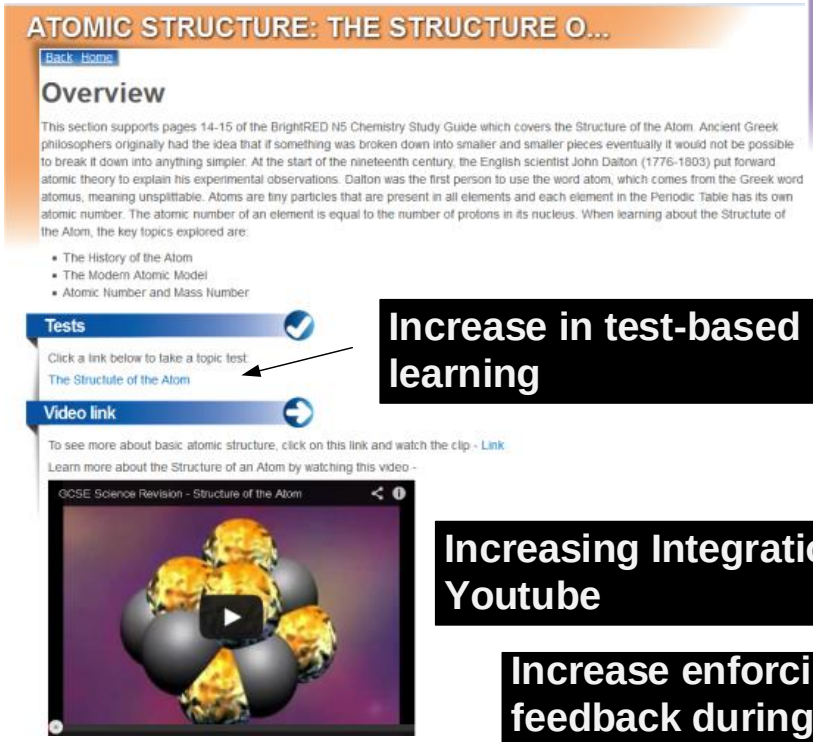


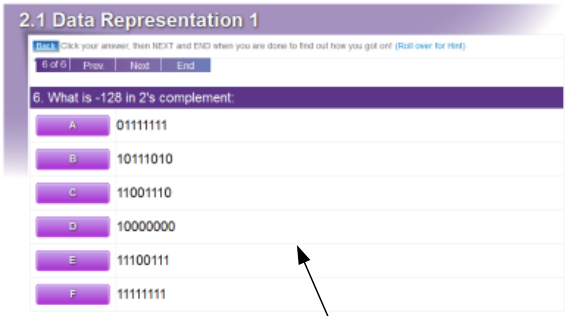
Focusing on supporting deep learning

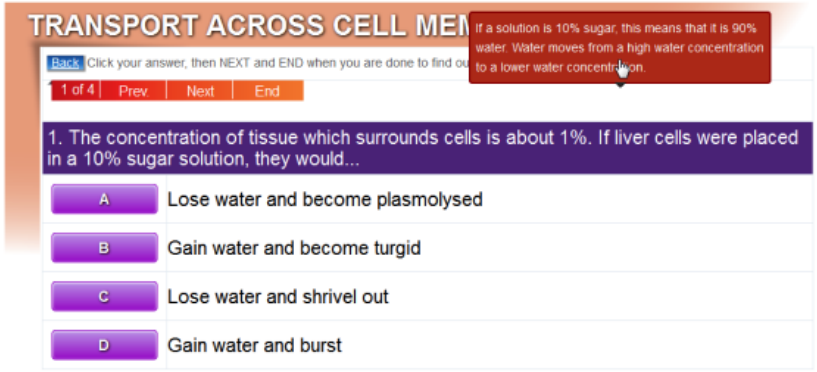
Allow for many ways of learning and delivery mechanisms

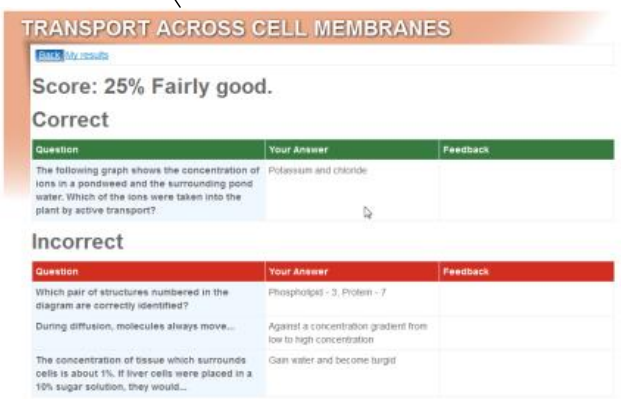










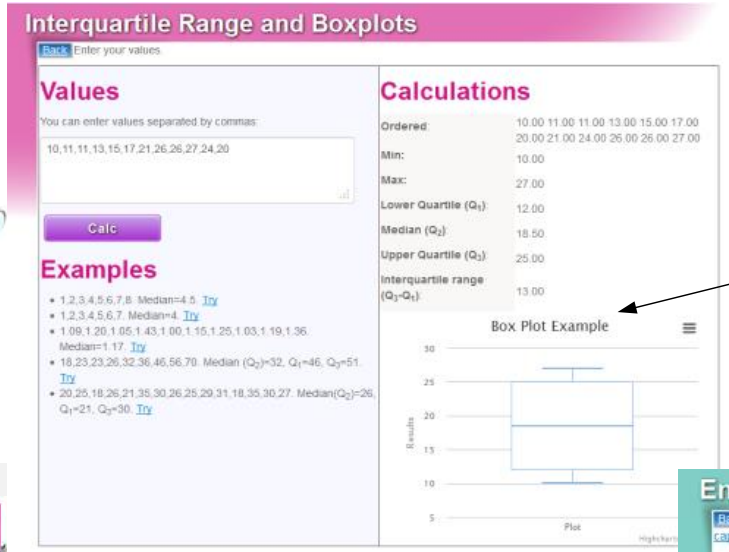


Increase in test-based learning

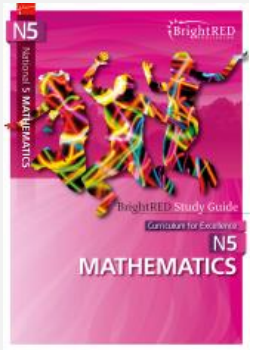
Ever-changing “infinite” tests

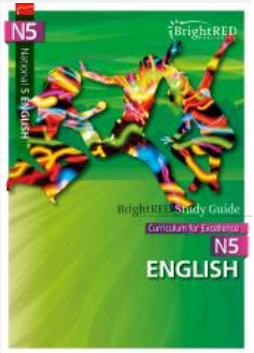
Increasing Integration with Youtube

Increase enforcing feedback during and after tests

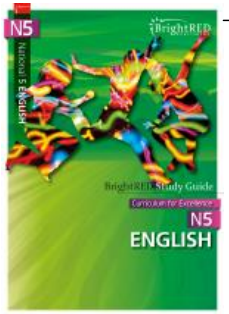


Supportive environments with solutions to problems





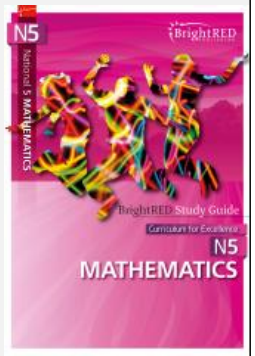
Integration of advanced Web services (eg Language translator)

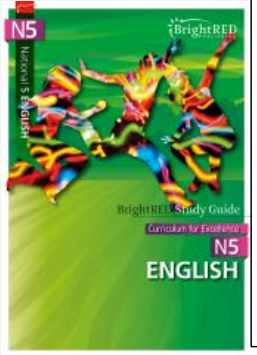


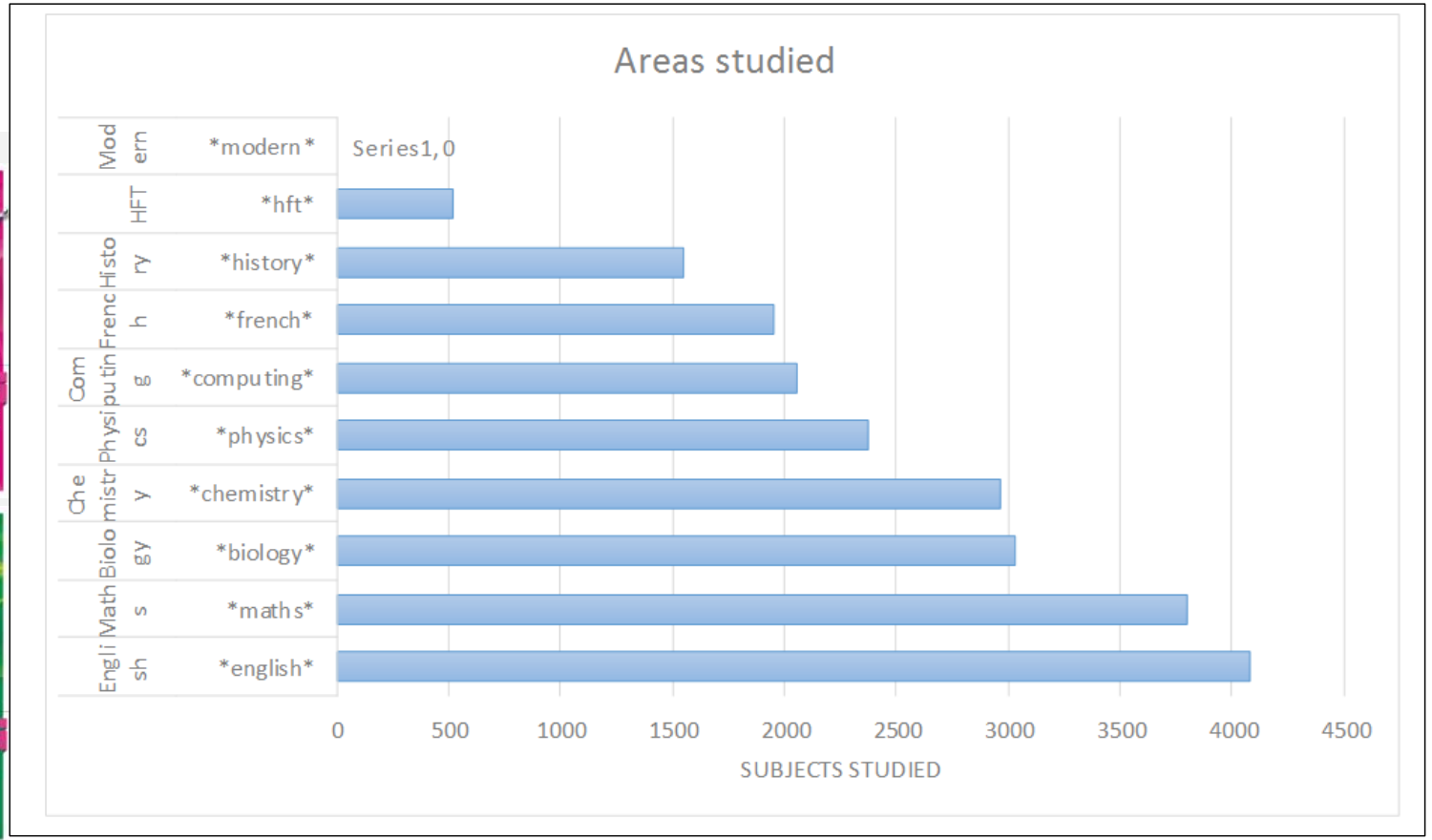
Automated conversion of books to Web site

Study Areas

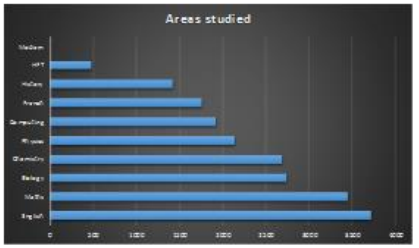
N5
BrightRED
Be Bright Be Ready

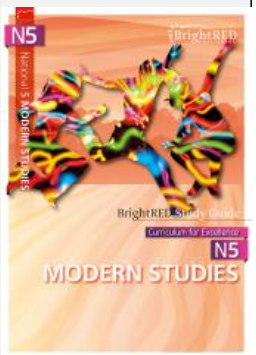

N5
BrightRED
MATHEMATICS

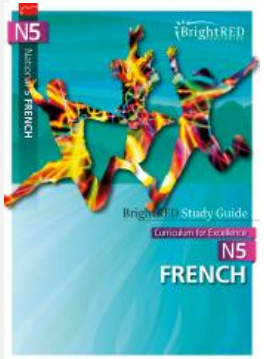

N5
BrightRED
ENGLISH

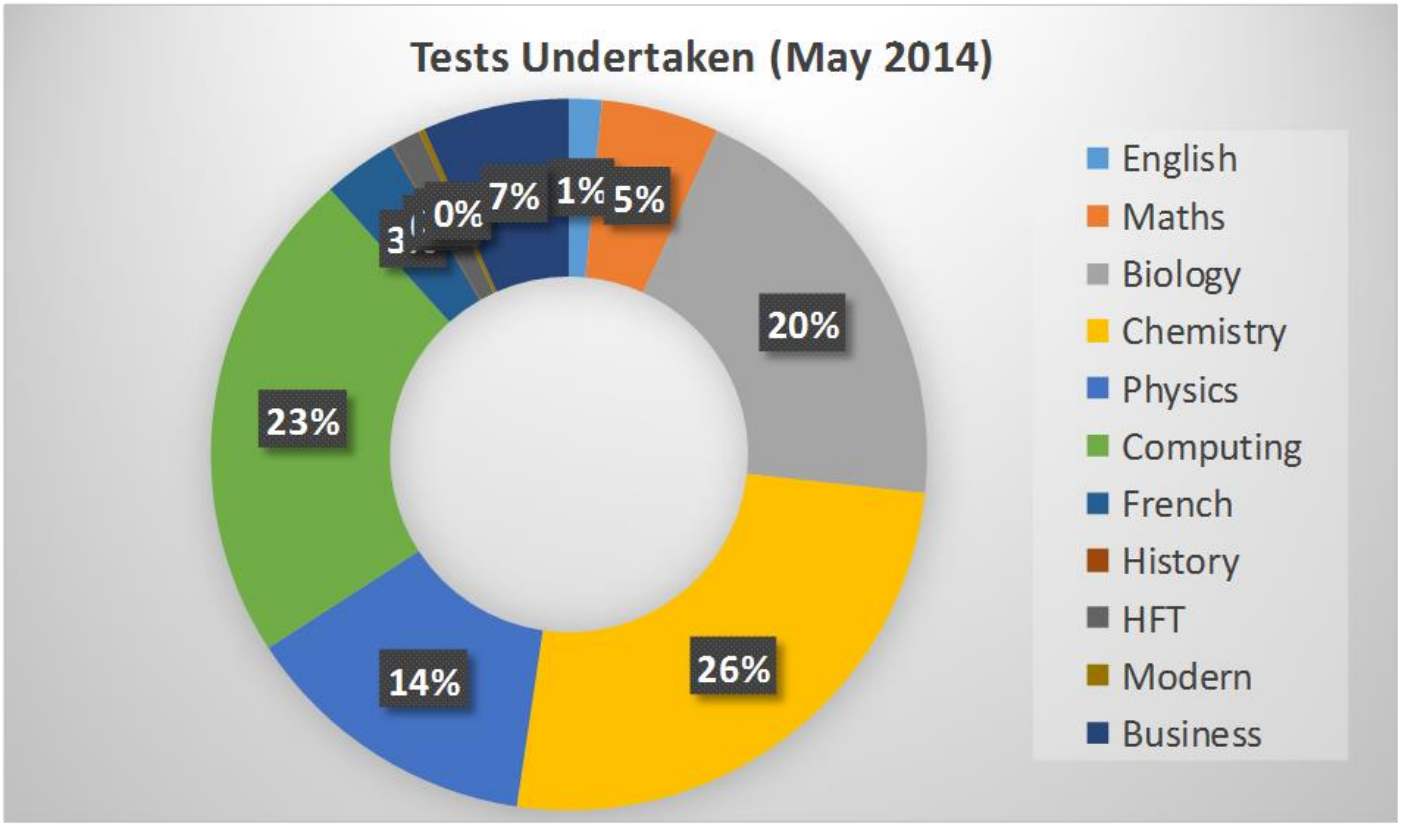

Areas studied
Modern
HFT
History
French
Computing
Physics
Chemistry
Biology
Maths
English
modern
hft
history
french
computing
physics
chemistry
biology
maths
english
Series1, 0
0
500
1000
1500
2000
2500
3000
3500
4000
4500
SUBJECTS STUDIED

Tests Undertaken (May 2014)

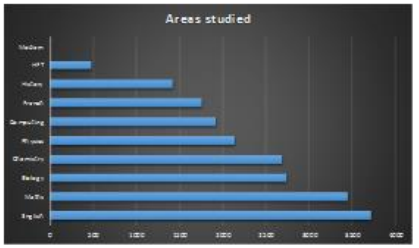


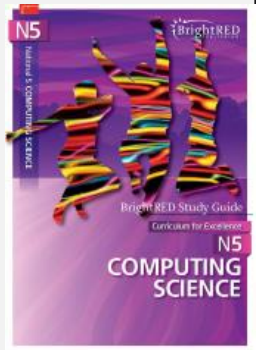


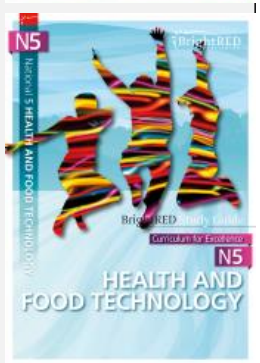


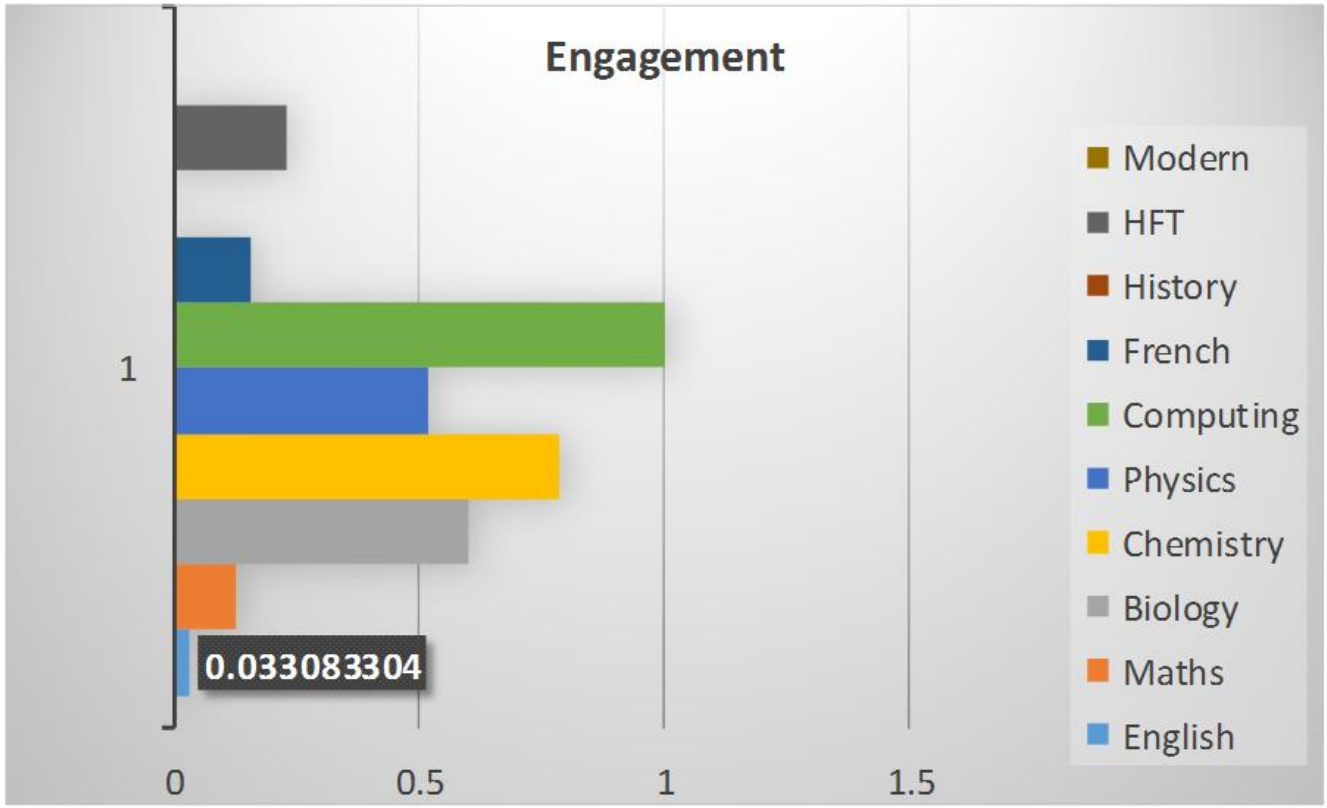


Engagement (May 2014)

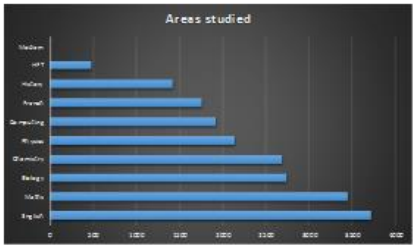


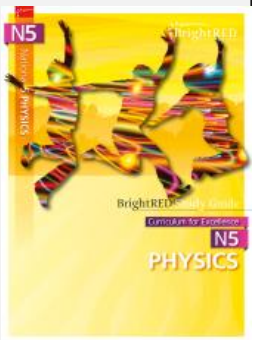


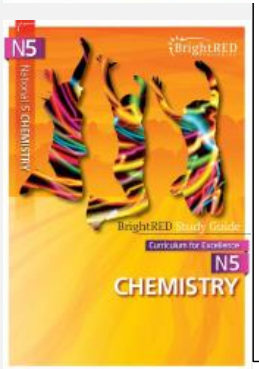


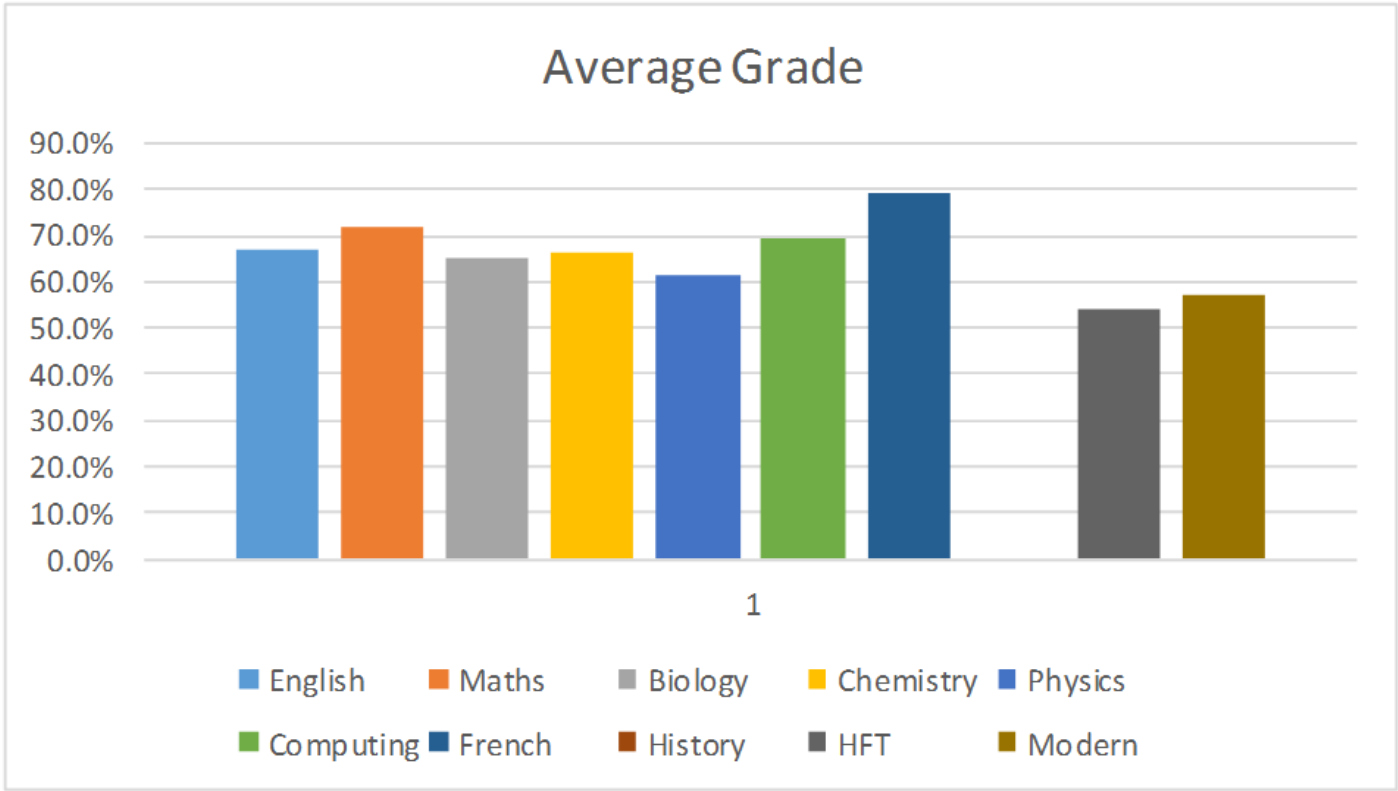


Average Grades

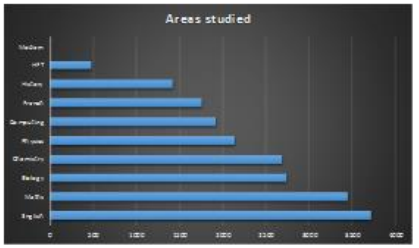


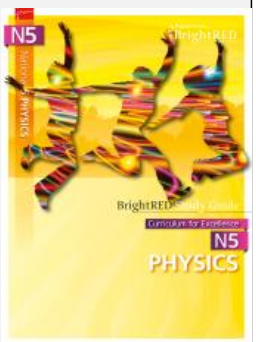


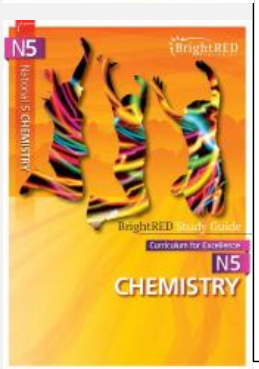


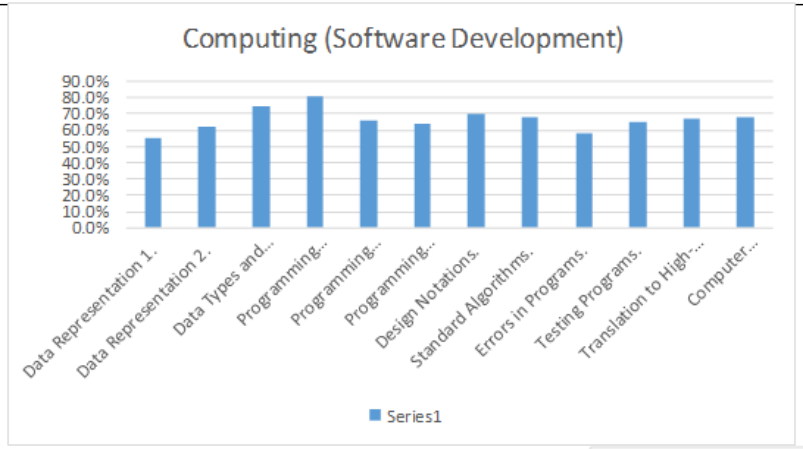


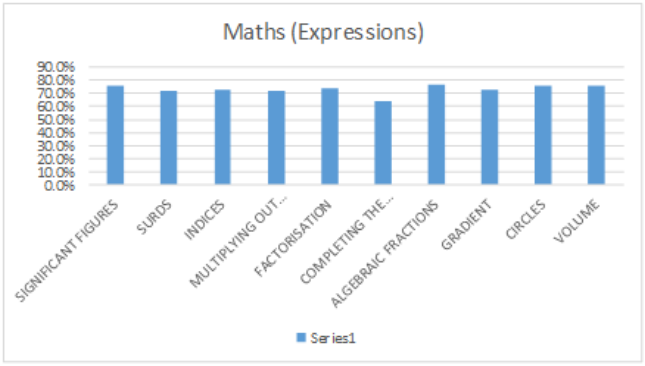
Scores for subjects

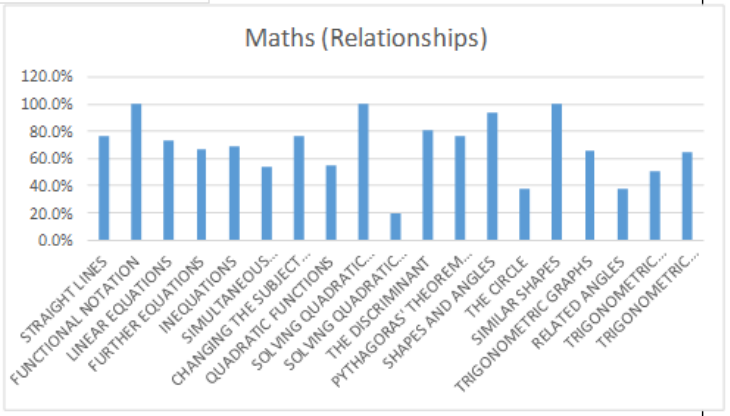




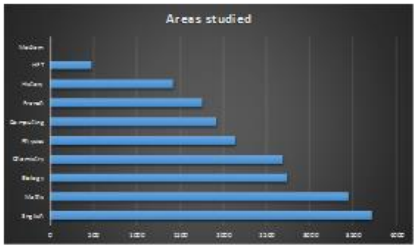


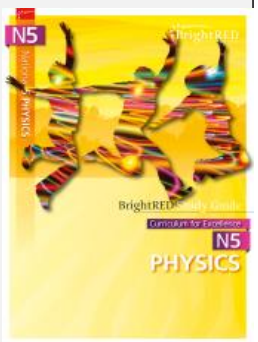


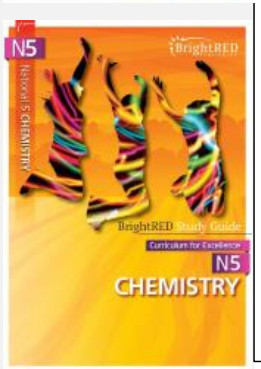


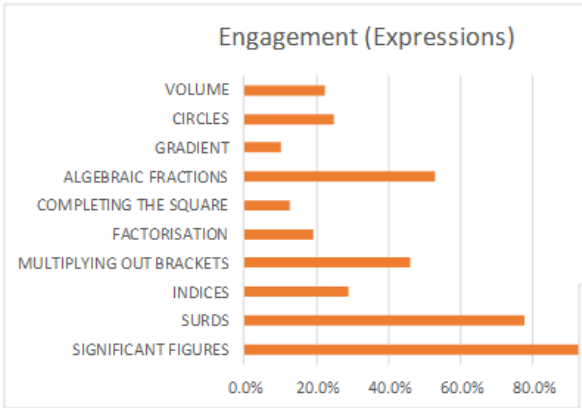


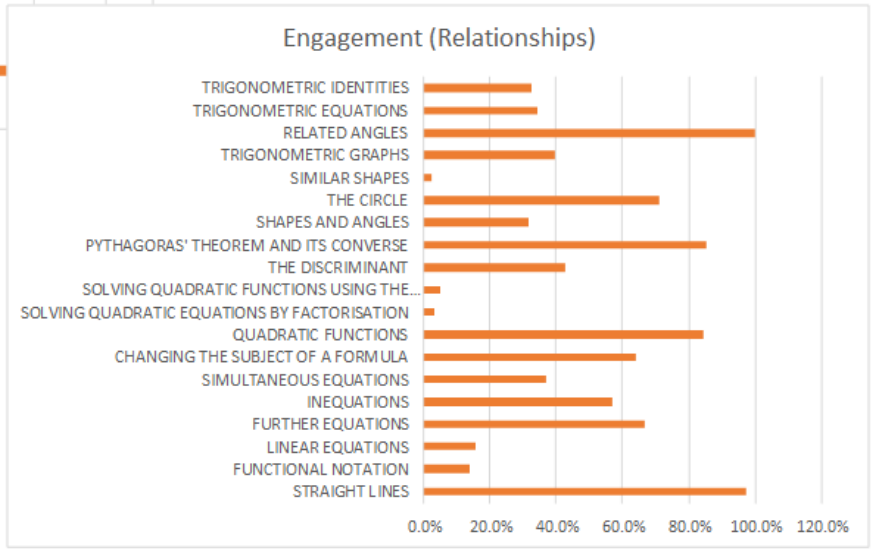
Engagement (Maths)



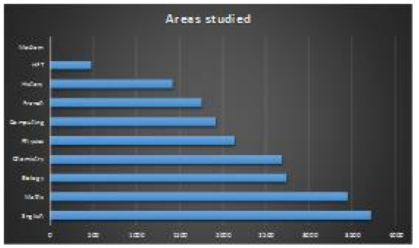


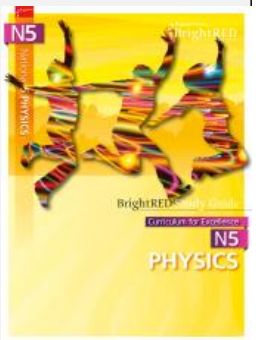


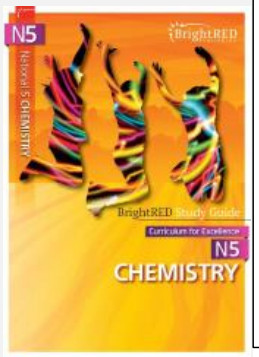




The most difficult question …







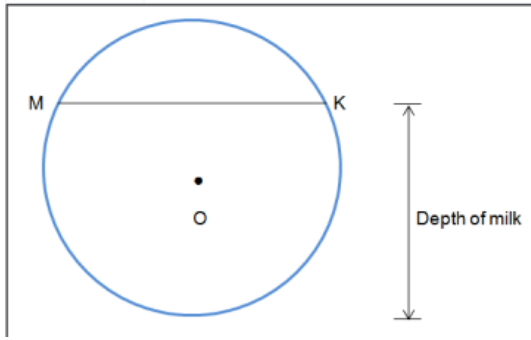
THE CIRCLE

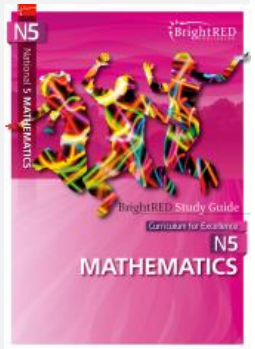
Back Click your answer, then NEXT and END when you are done to find out how you got on! Graphic

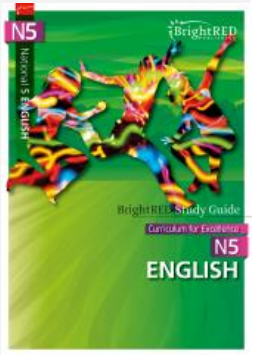
4 of 6 | Prev. | Next | End

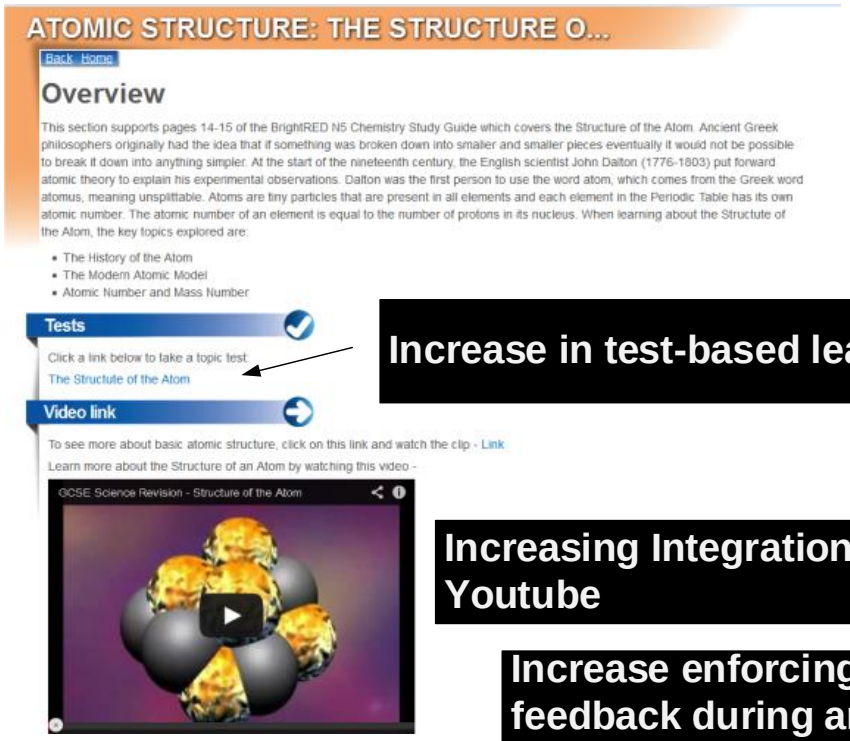
4. Milk is stored in a tank with a circular cross-section as shown below. The centre of the circle is O. MK is a chord of the circle. MK is 1.5 metres. The radius of the circle is 1.2 metres. Calculate the depth of the milk in the tank.

A	1.14 m
B	3.14 m
C	2.14 m
D	4.14 m





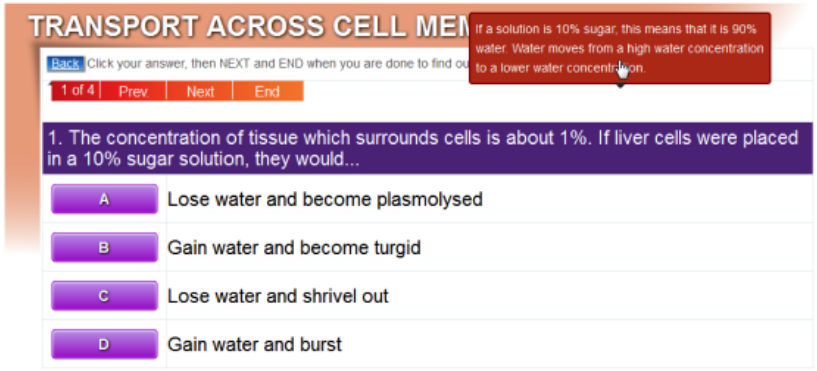


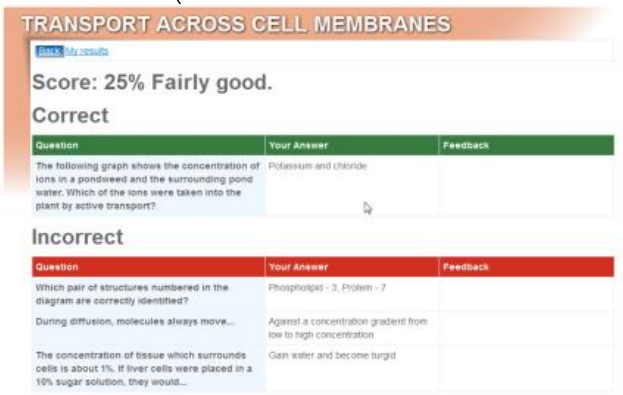


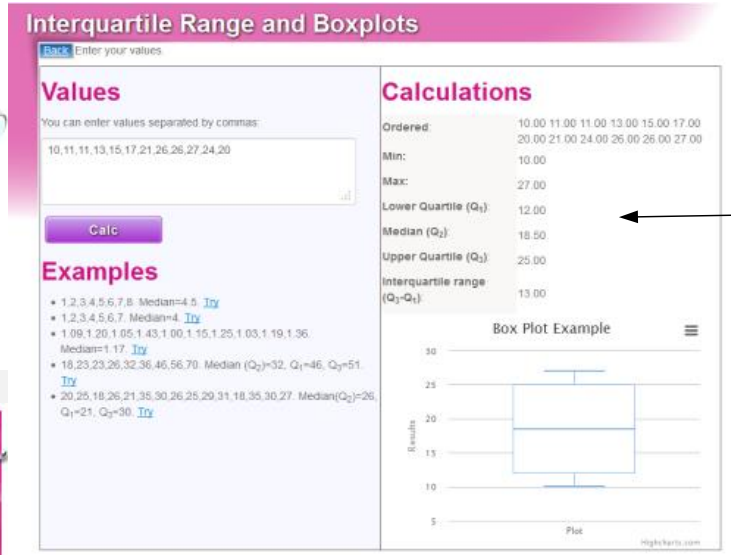
Increase in test-based learning

Increasing Integration with Youtube

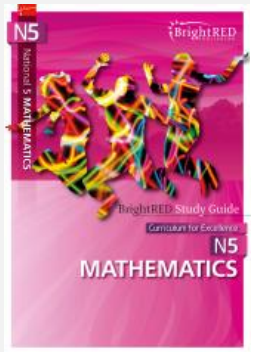
Increase enforcing feedback during and after tests

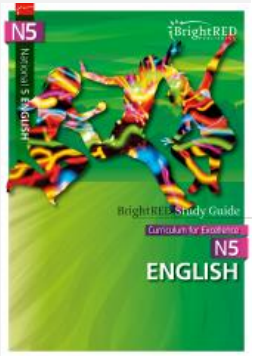




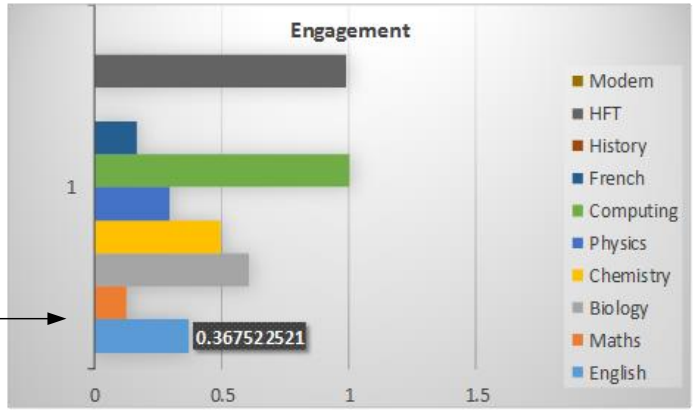


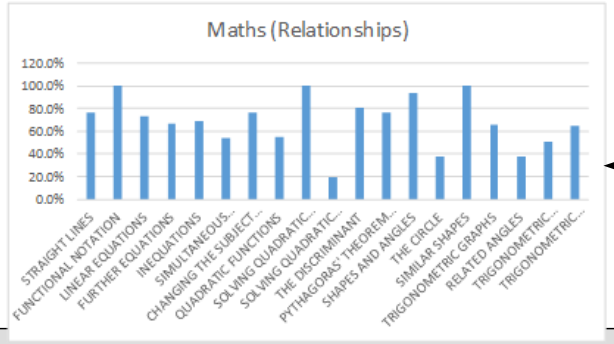
Supportive environments with solutions to problems





Knowledge-based subjects have more engagement on testing.
Strong: Modern Studies, HFT, Computing, Biology, and Chemistry.
Weaker: Maths, Physics.

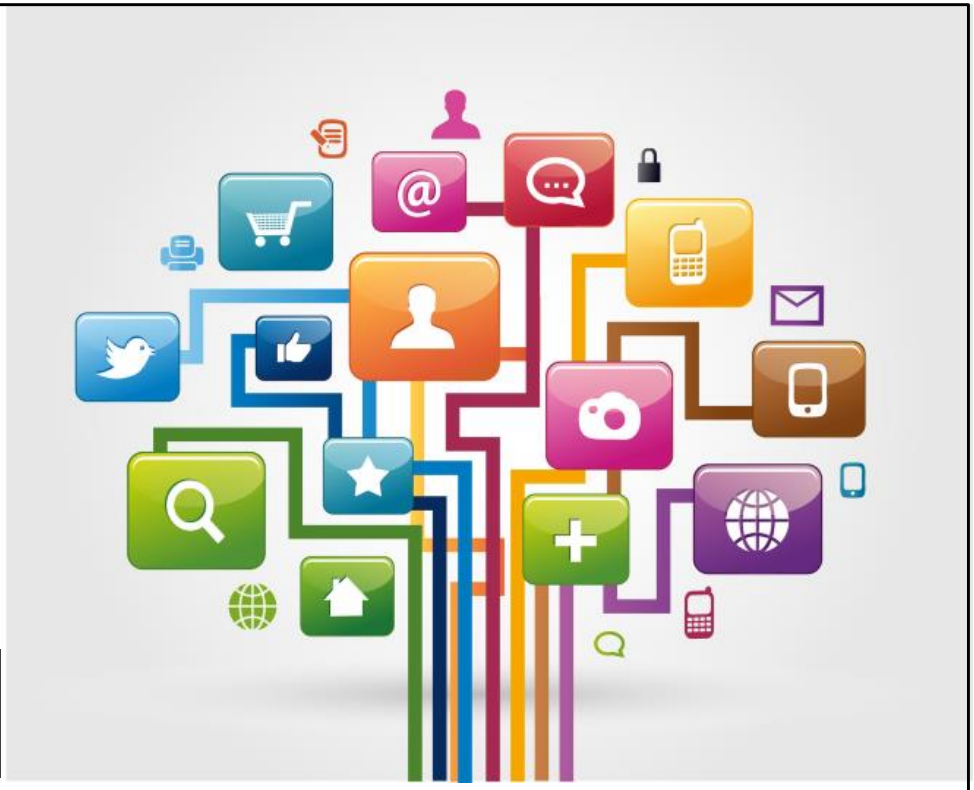




Engagement and grades can vary widely in subjects

Edinburgh Napier UNIVERSITY

Computing Science: Now and The Future



Inc. Computer Security

Prof Bill Buchanan, Twitter: @billatnapier
Web: asecuritysite.com, brightredbooks.net

Edinburgh Napier UNIVERSITY

Computing Science: Now and The Future

Inc. Computer Security

m.socrative.com Room: 504858

m.socrative.com

socrative 1.0

Please enter the room number:

Room number: 504858

Join Room

By logging in you are agreeing to our **Terms** and **Privacy Policy**

504858