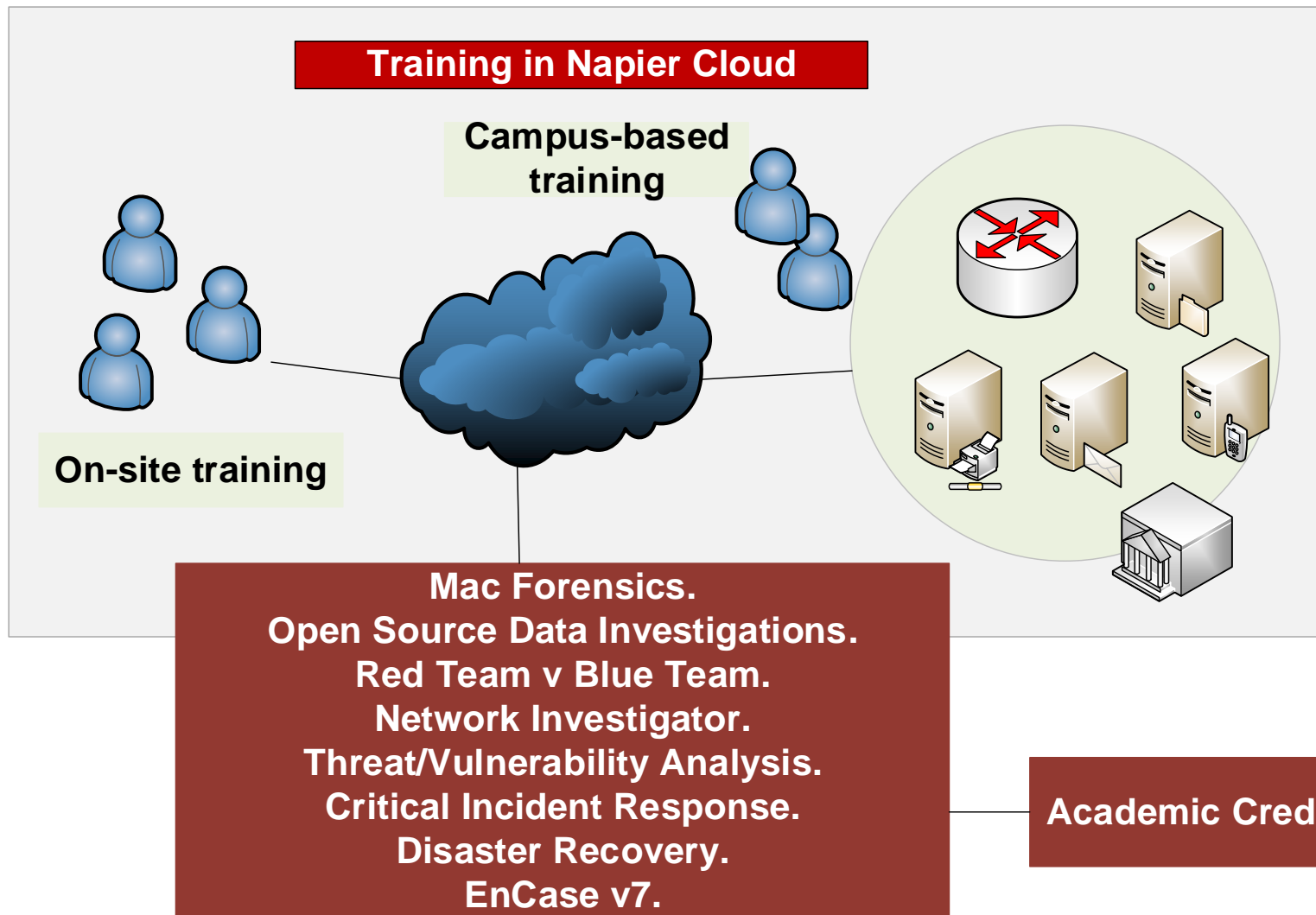


The Risks and Opportunities of Mobile Working within Cloud Environments

<http://asecuritysite.com>



Prof Bill Buchanan, Adrian Smales





Transistor



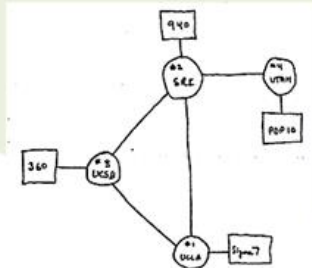
Microchip



Microprocessor



The Cloud



THE ARPA NETWORK

DEC 1969

4 nodes

The Internet



The Personal Computer

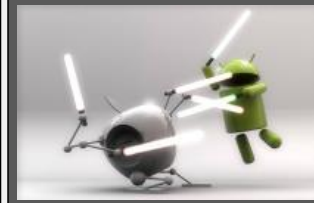


The Cloud



- 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

Gartner Trend



Mobile Device Battles

- Android 81%
- iOS 13%

In-memory Computing



Personal Cloud

Enterprise App Stores



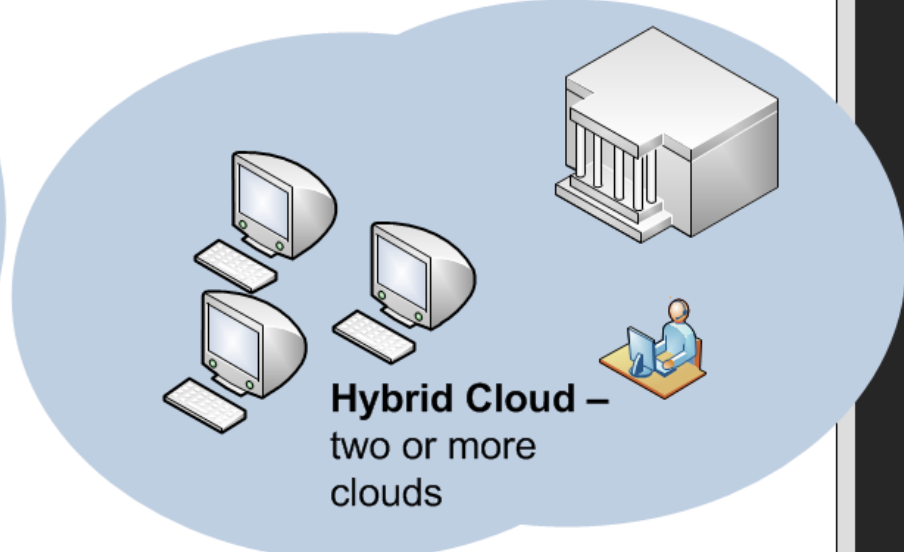
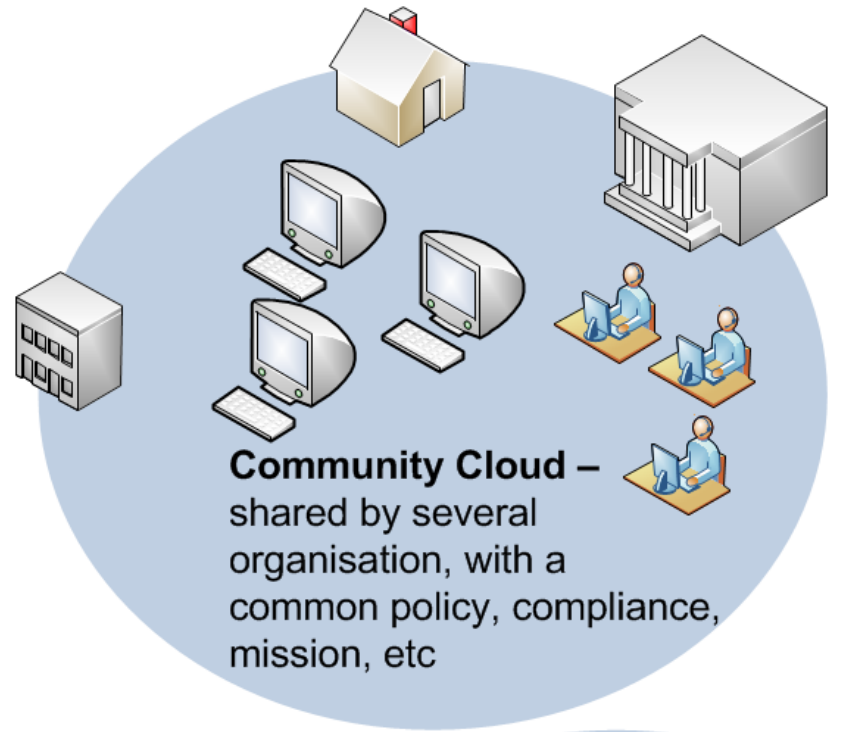
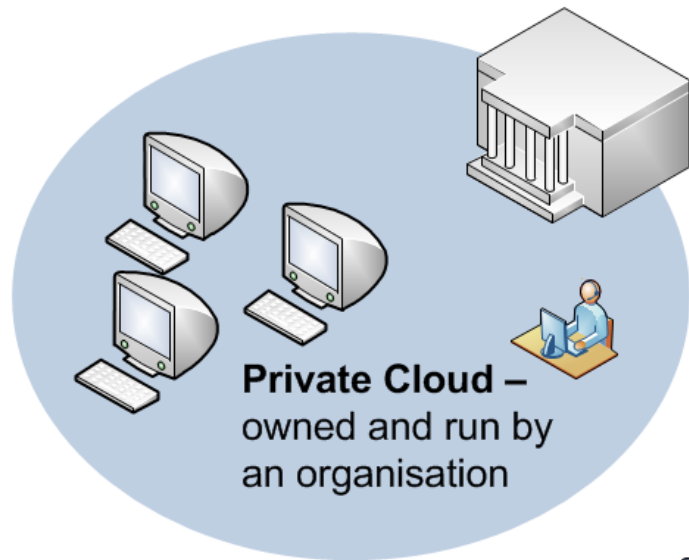
Hybrid IT and Cloud Computing

Mobile Apps and HTML 5

Integrated Ecosystems

Internet of Things

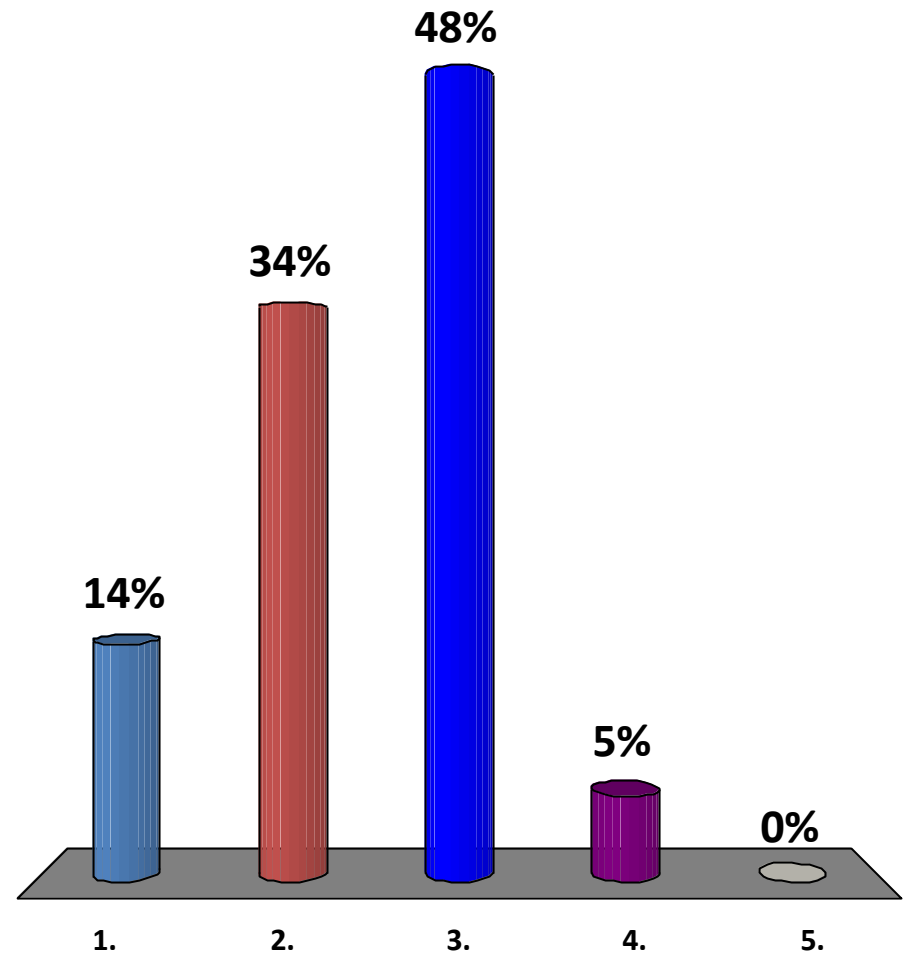
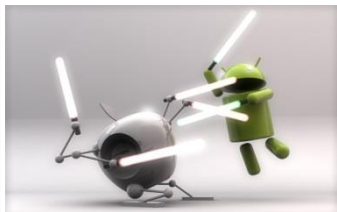
- All devices addressable





What type of phone operating system do you have?

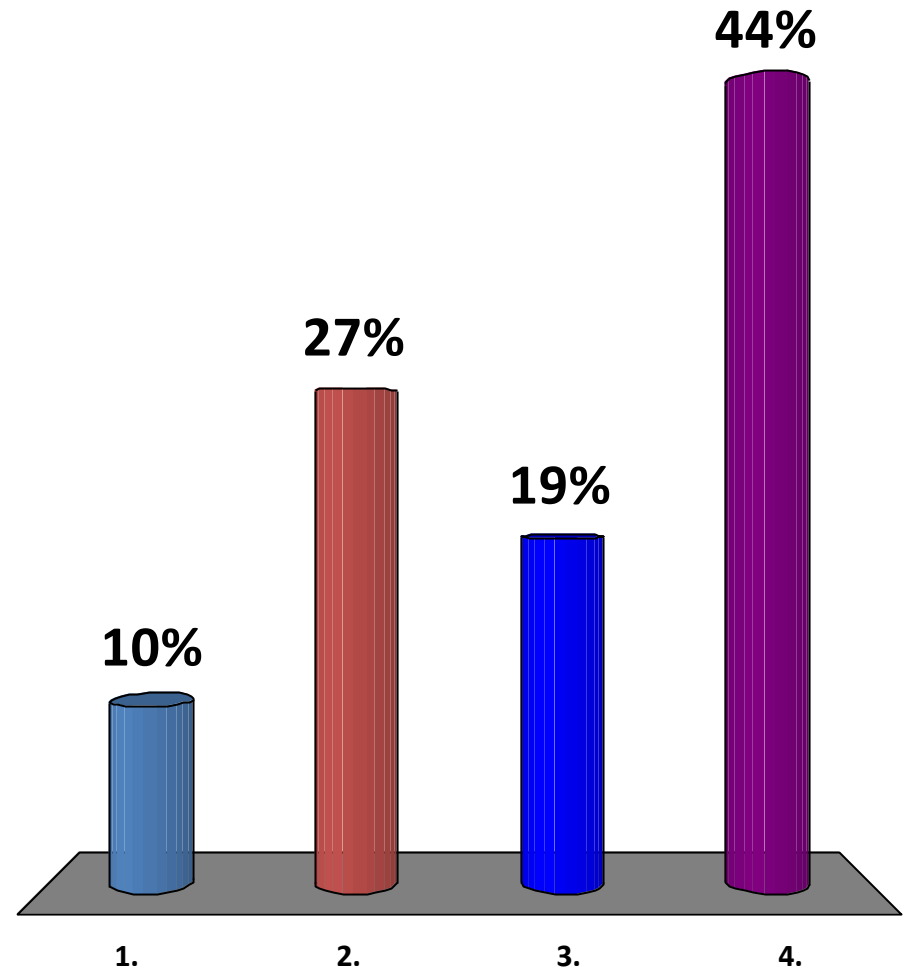
1. Blackberry.
2. Android IOS.
3. Apple IOS.
4. Windows 8.
5. None. I don't have a phone.





How many different logins do you have:

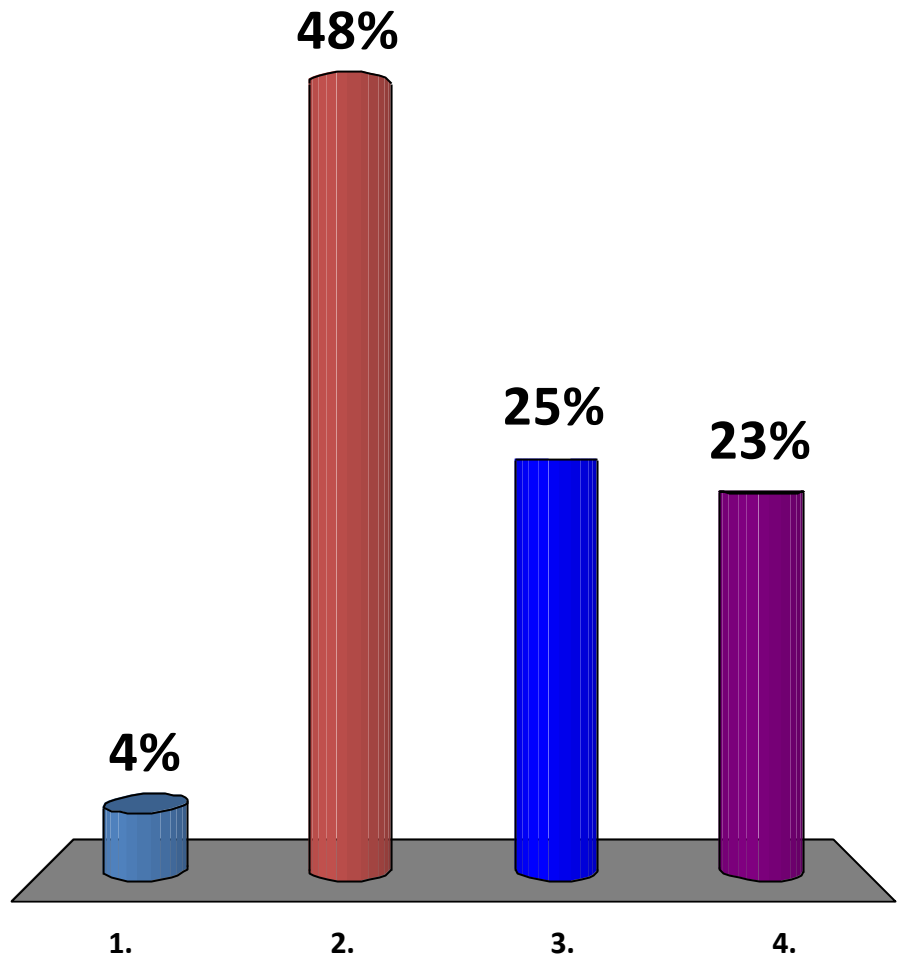
1. One
2. 2-4.
3. 4-8.
4. More than eight.





How many different passwords do you have?

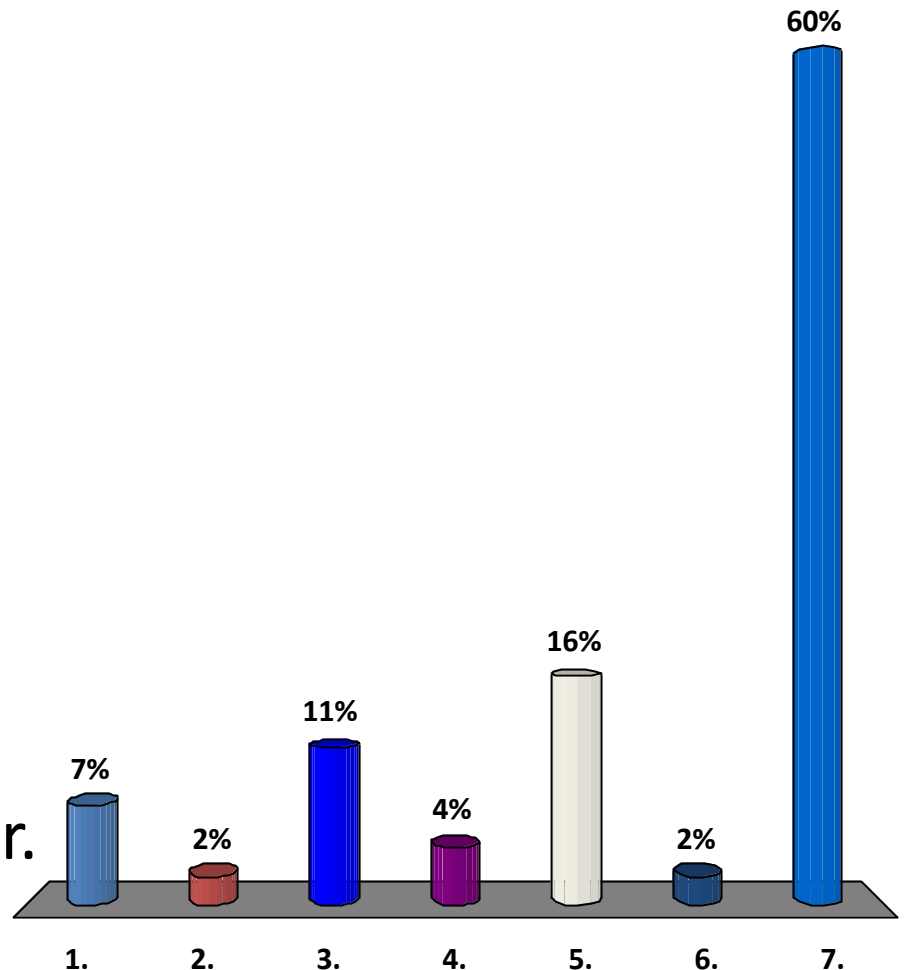
1. One
2. 2-4.
3. 4-8.
4. More than eight.





Which best matches your one of your passwords:

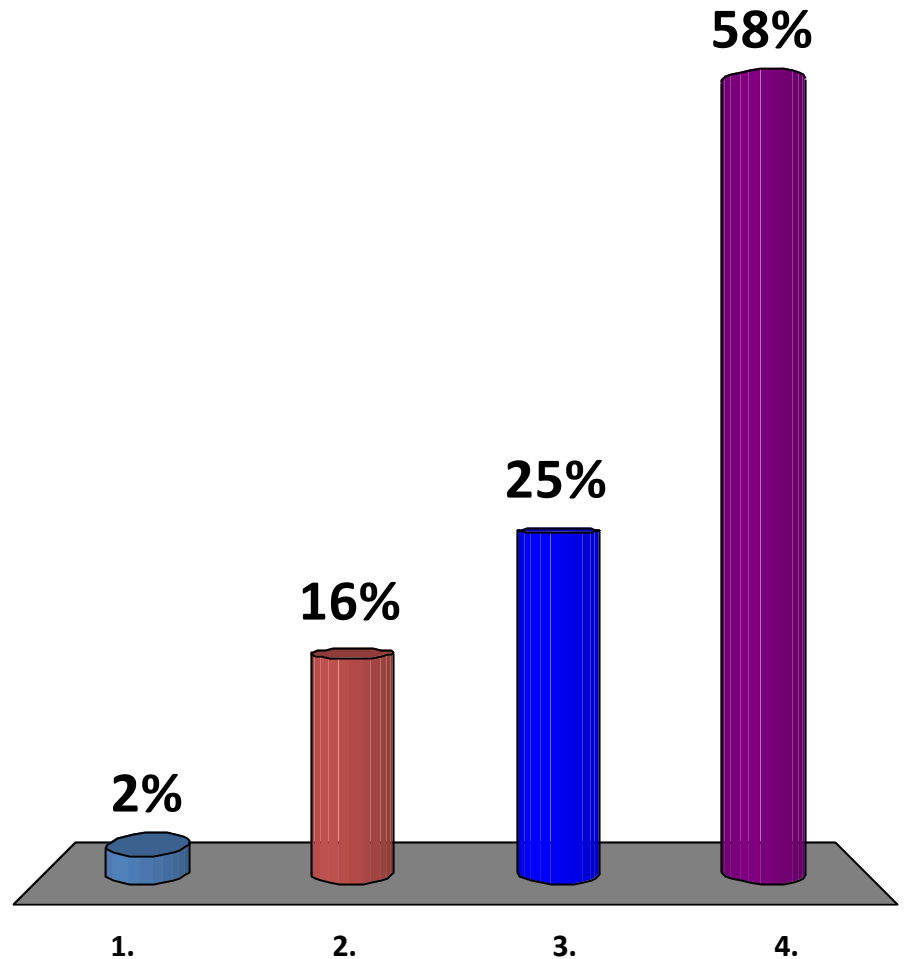
1. It is an animal/pet (past/present)
2. It is a car (past/present)
3. It is someone in my family.
4. It is my football/sports team.
5. It is a place.
6. It is a toy/game character.
7. None of the above.





What is your longest password:

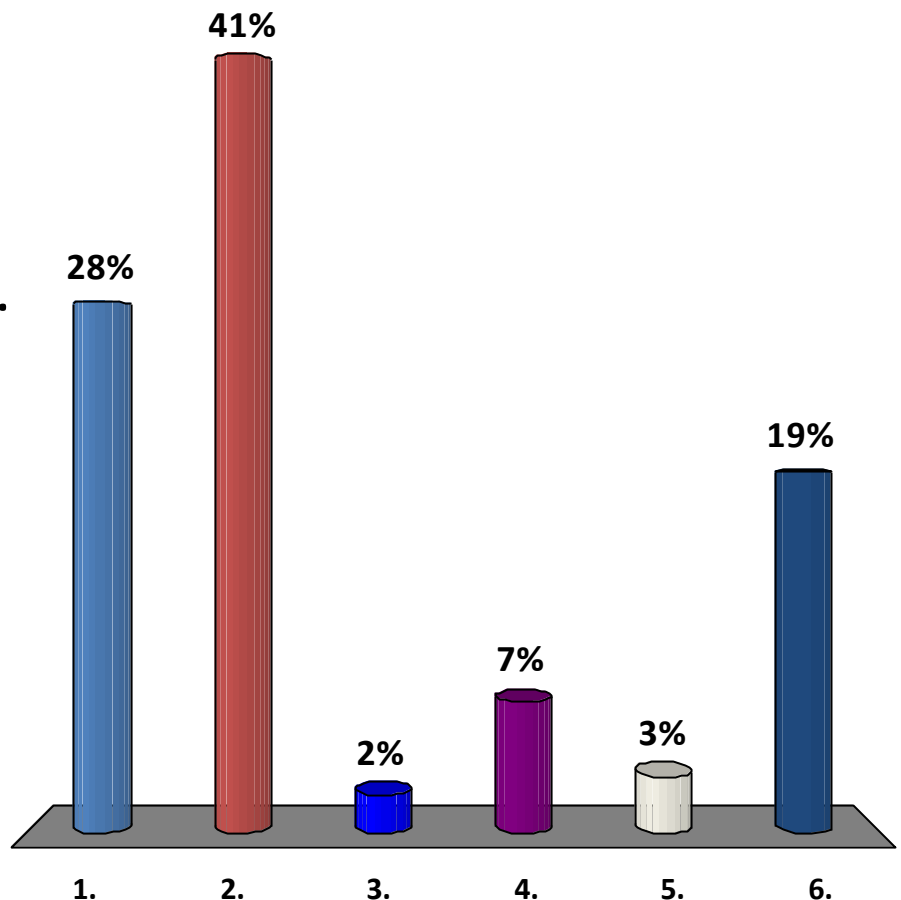
1. Up to 7 characters.
2. 8 characters.
3. 9 characters.
4. More than 9 characters.





What is your greatest worry on the Internet?

1. Someone steals my identity.
2. Someone gets my bank account/credit card details.
3. Someone tracks my location.
4. Someone gets into my computer/phone.
5. Someone tracks my Web activity.
6. Someone gets my passwords.



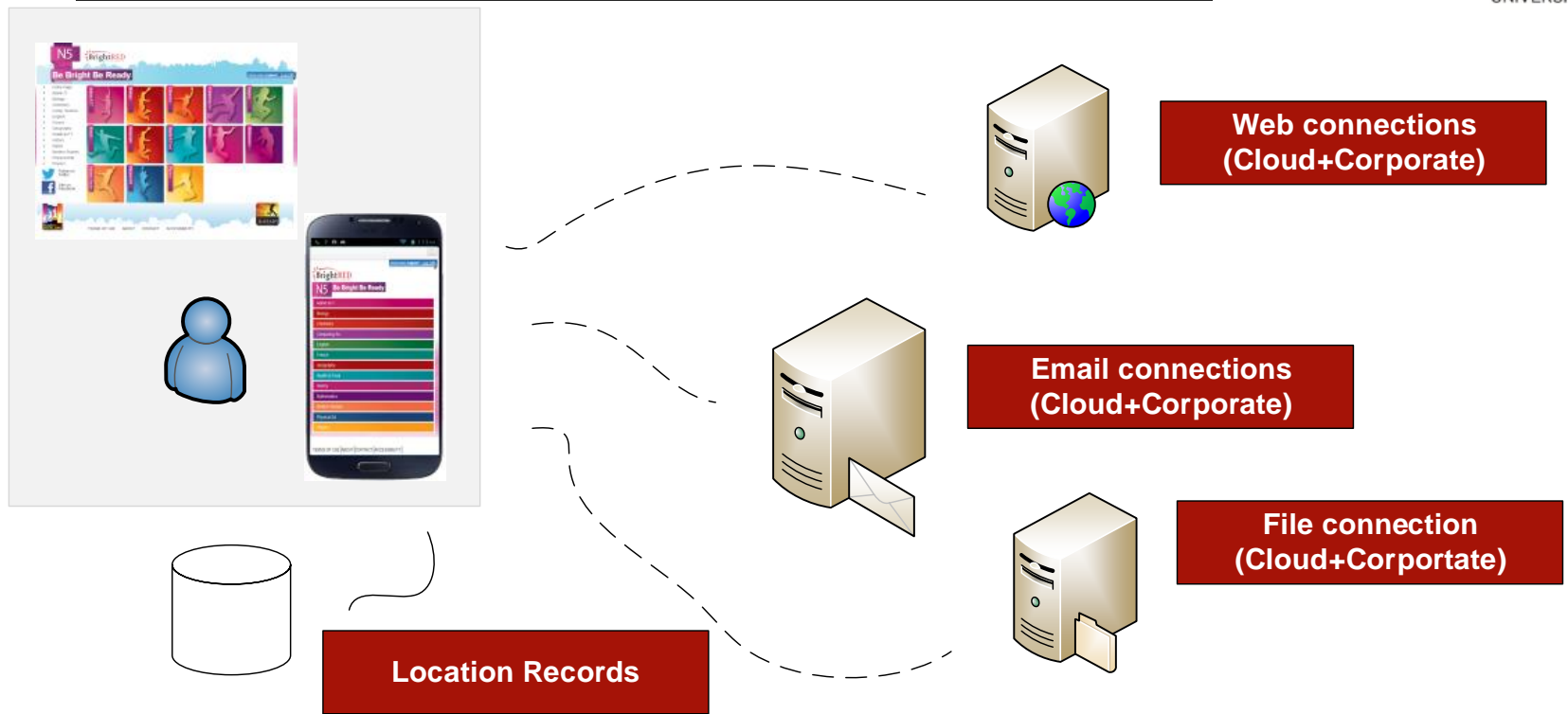
The Risks and Opportunities of Mobile Working within Cloud Environments

10 Risks...



Prof Bill Buchanan, Adrian Smales

Risk 1: Loss of Device



Phone Records

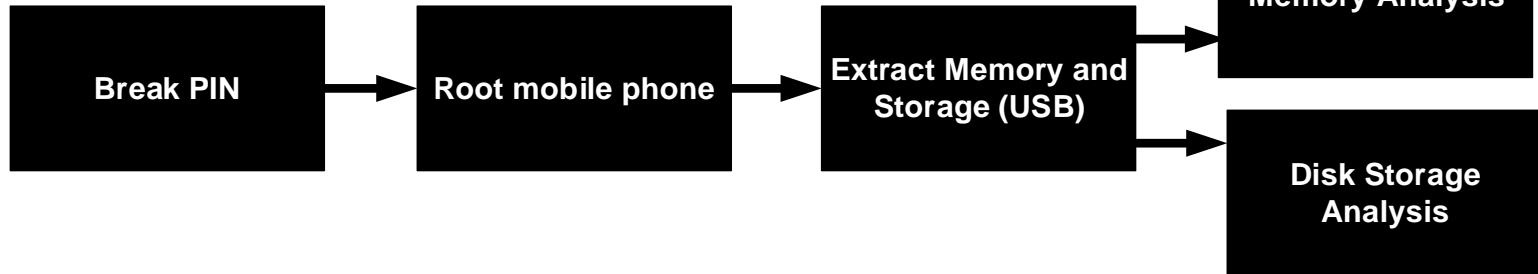
Break PIN

Root mobile phone

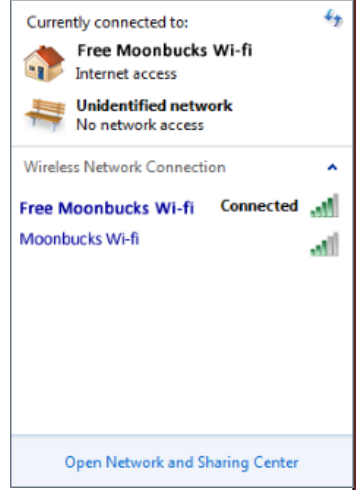
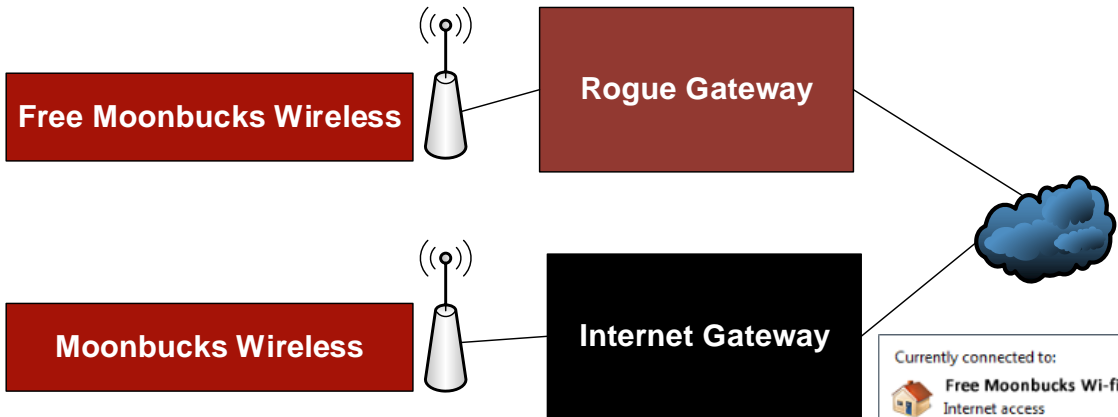
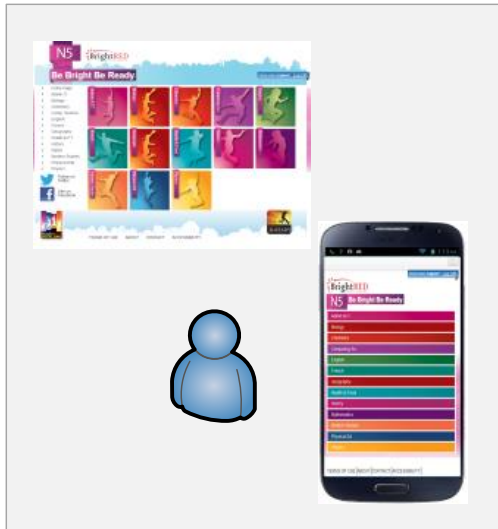
Extract Memory and Storage (USB)

Memory Analysis

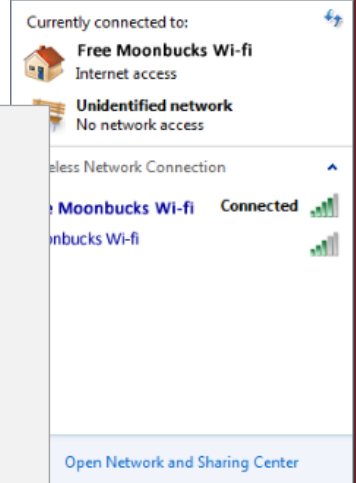
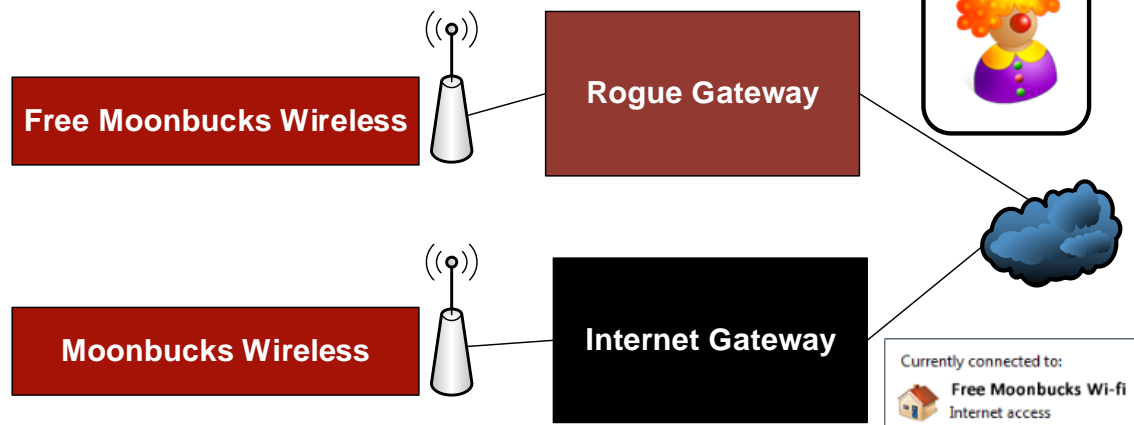
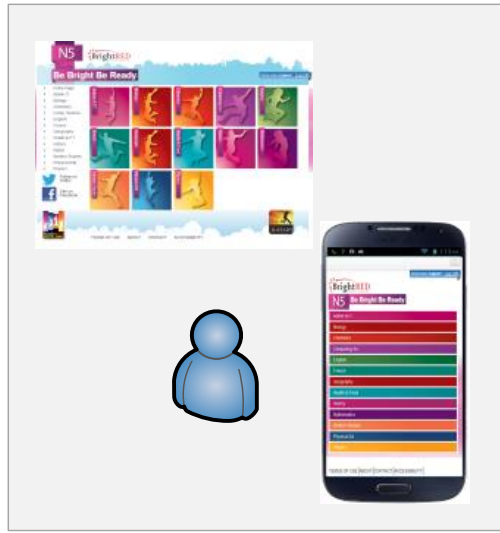
Disk Storage Analysis



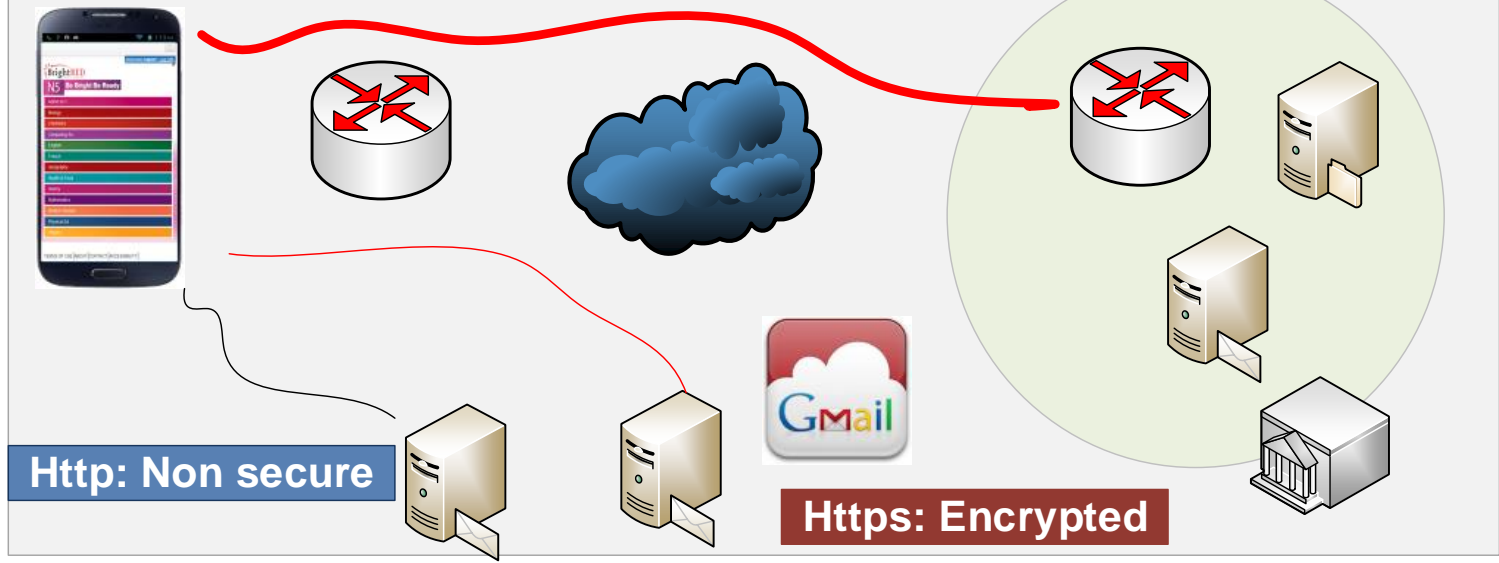
Risk 2: Rogue SSID/Gateway



Risk 2: Rogue SSID/Gateway



VPN – Tunnel's over Internet





Risk 3: Lack of Separation

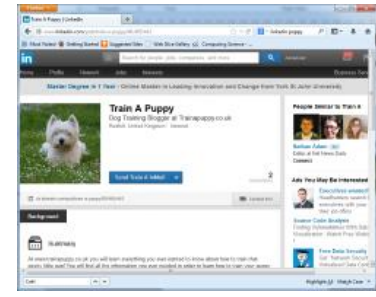
Business Life



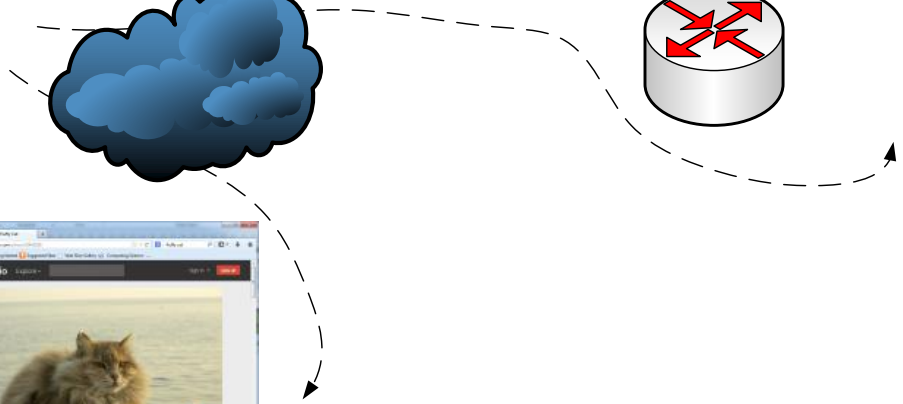
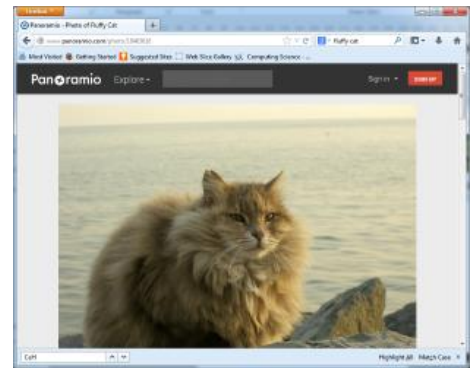
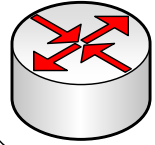
Home Life



A screenshot of a mobile application interface showing a grid of colorful icons. Below it is a smartphone displaying the same application, and a simple blue person icon.



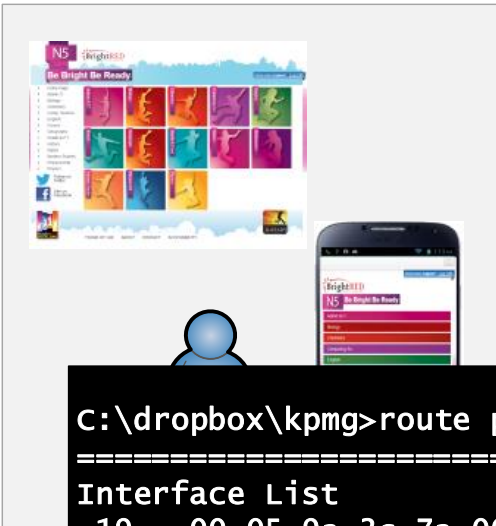
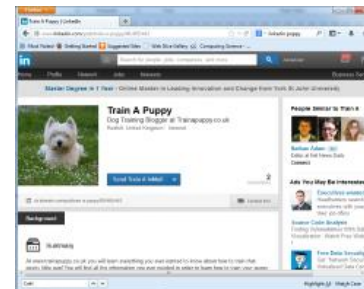
Corporate Firewall





Risk 3: Lack of Separation

Business Life



```
C:\dropbox\kpmg>route print
```

=====
Interface List

```
19...00 05 9a 3c 7a 00 .....Cisco AnyConnect Secure Mobility Client
12...c8 f7 33 4b 82 37 .....Intel(R) Centrino(R) Advanced-N 6235
=====
```

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.3	25
146.176.1.5	255.255.255.255	146.176.217.1	146.176.217.218	2	
146.176.2.5	255.255.255.255	146.176.217.1	146.176.217.218	2	
146.176.5.151	255.255.255.255	146.176.217.1	146.176.217.218	2	
146.176.32.0	255.255.255.128	146.176.217.1	146.176.217.218	2	
146.176.54.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
146.176.162.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
146.176.163.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
146.176.164.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
146.176.165.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
146.176.166.0	255.255.255.0	146.176.217.1	146.176.217.218	2	
255.255.255.255	255.255.255.255	on-link	192.168.132.1	276	
255.255.255.255	255.255.255.255	on-link	146.176.217.218	10000	

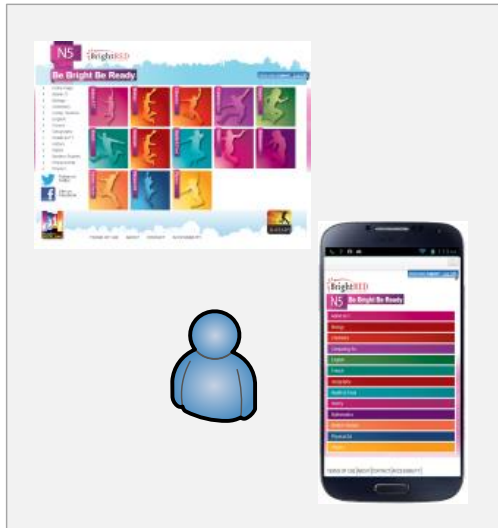


Risk 4: One Password Fits All



150 million accounts compromised

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3j13jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/i oxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYZKVeQ8I=	111111
9.	83411	PMDTbPOLZxu03SwrFUVYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123



47 million accounts



6.5 million accounts (June 2013)



One account hack ... leads to others



1 million accounts – in plain text. 77 million compromised



Dropbox compromised 2013



200,000 client accounts

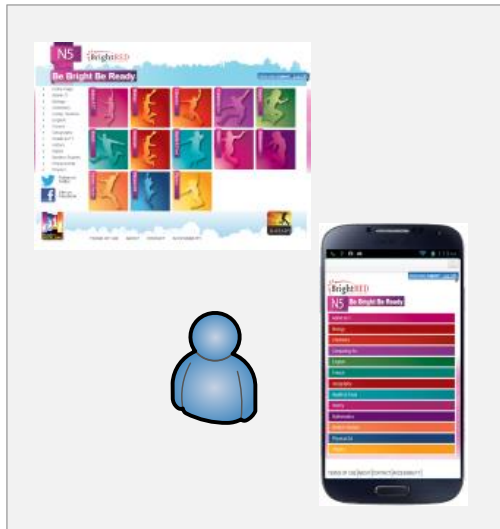


Risk 4: One Password Fits All

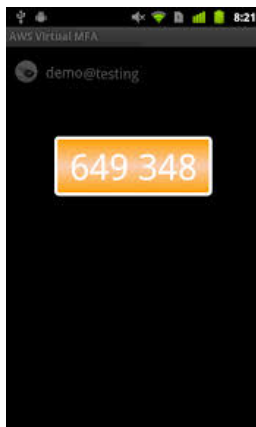


150 million accounts compromised

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLZYg==	123456789
3.	345834	L8qbAD3j13jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLi oxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/i oxG6CatHBw==	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



Enter security code

We sent a security code to your phone number ending in

6-digit code

Submit code

Trust this computer ⓘ

[Didn't receive one?](#)

[I lost my phone](#)

A cause or a fight?



Who? ... Why? ...
Where? ... When?

- One person's freedom fighter is another's terrorist.
- One person's cause is another person's fight.

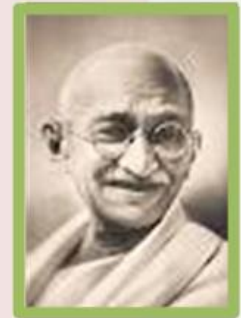
Martin Luther King



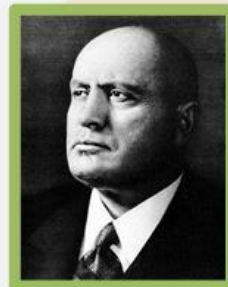
Che
Guevara



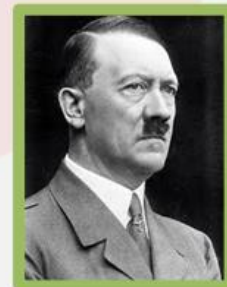
Dalai Lama



Mahatma Gandhi



Benito Mussolini



Adolf Hitler

Hacktivism



Who? ... Why? ...
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

2012

- Anonymous focus on India on censorship.
- Virgin Broadband over PirateBay block.
- SOCA (Serious and Organised Crime Agency) over arrests, also Norwegian Lottery and Bild.
- Home Office sites over Gary McKinnon case.

2010, Mastercard and Visa

- Why: Decision to stop processing payments to the whistle-blowing site Wikileaks,
- Result: DDoS attacks on Visa, Mastercard, om.nl and politie.nl

2011, Tunisian government websites

- Why: Censorship of the Wikileaks documents
- Result: DDoS attacks against sites. Some Tunisians assisting in these attacks.

2009. Climate Research Unit of East Anglia University

Why: Emails published showed conspiracy to suppress data that contradicted their conclusions on global warming (Russian FTP server)

2011, HBGary

Why: HBGary were going after Anonymous
Reward: Emails published, Web site defaced.

2010, Australian Government.

Why: Australian Government's attempt to filter the Internet.

2012. Department of Justice and the FBI. Denial of service attack

2011. Sony's PlayStation Network.

- Why: Sony were suing Geohotz, who jailbroke the PlayStation 3.
- Result: Afterwards, a group of hackers claimed to have 2.2 million credit card numbers from PSN users for sale



Hacktivism



Who? ... Why? ...
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?

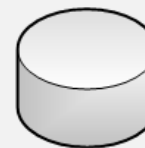


**HBGary Federal CEO
Aaron Barr to unmasked
Anonymous with a list
HBGary contacts with NSA,
Interpol, McAfee, and many
others**



**Hbgaryfederal used CMS
and comprised by:**

<http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27>



**Username, passwords
(stored as hash values),
email database**



"ranger12"

"martin12"



**CEO Aaron Barr and COO Ted
Vera had weak passwords (six
characters and two numbers) –
which were easily broken**

**Passwords broken by
Rainbow tables**



Passwords found for CEO and COO

Hacktivism



Who? ... Why? ...
Where? ... When?

- Attacks against an organisation for political reasons.
- Who?
- Why?
- Where?
- When?



“ranger12”

“martin12”

CEO Aaron Barr and COO Ted Vera used the same password for a range of systems: Twitter, email, Linked in, and so on.



Support.hbgary.com



Remote login to support.hbgary.com from Ted Vera's account



Flaw exploited in system to escalate privilege



Gigabytes of research and backup data

Aaron was a System Administrator for their Gmail Apps Hbgary account



Complete control of company email

Hacktivism



Who? ... Why? ...
Where? ... When?

- Use strong passwords.
- Never re-use passwords (30% of users do).
- Patch systems.
- Watch out for social engineering.
- Beware of unchecked Web sites.
- Get an SLA from your Cloud provider.
- Don't store emails in the Cloud.
- Restrict access from outside.



Now for another site owned by
Greg Hoglund, owner of
HBGary

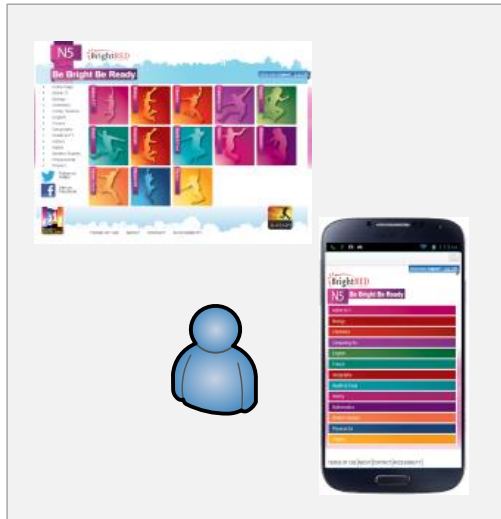
Social Engineering ... to gain
root password for Greg's site



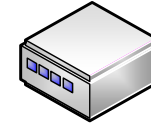
Web site taken offline and user
registration database published



Risk 5: Device Poisoning

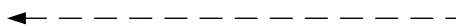


Who has this IP address (192.168.0.1)?



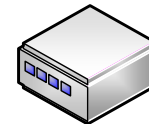
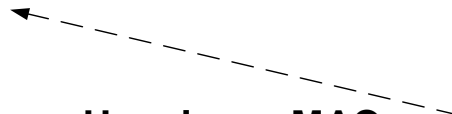
ARP Poisoning

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

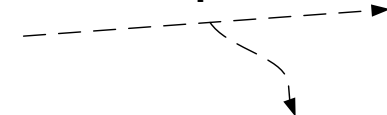


Gateway (192.168.0.1)

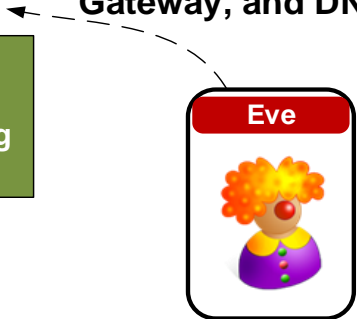
Here is my MAC address (22:33:44:55:66)



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)

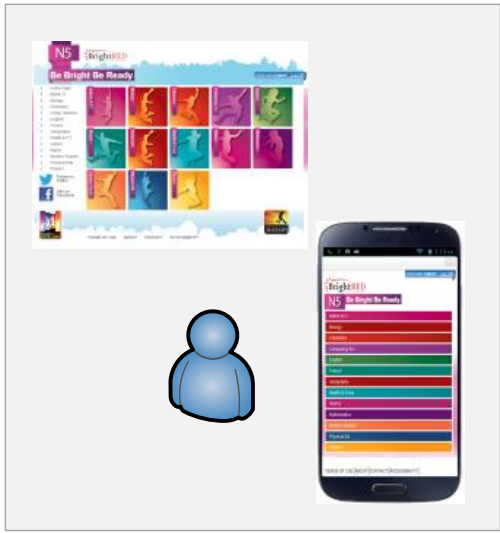
3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
Frame 3: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: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



CVE-2007-0071
Adobe Flash Player.
Integer overflow



Phoenix Exploit Kit



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



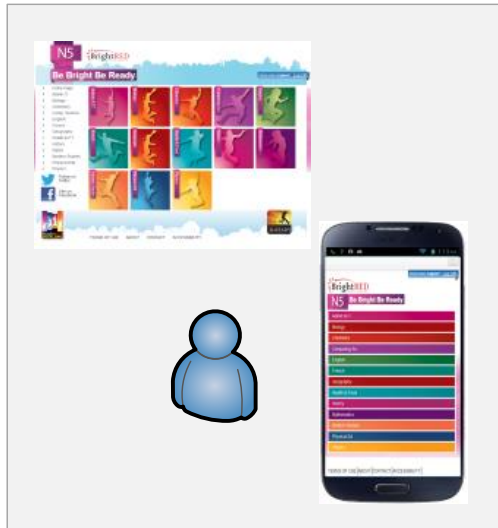
CVE-2013-1723
Java Exploit

CrimeBoss





Risk 7: Shoulder Surfing

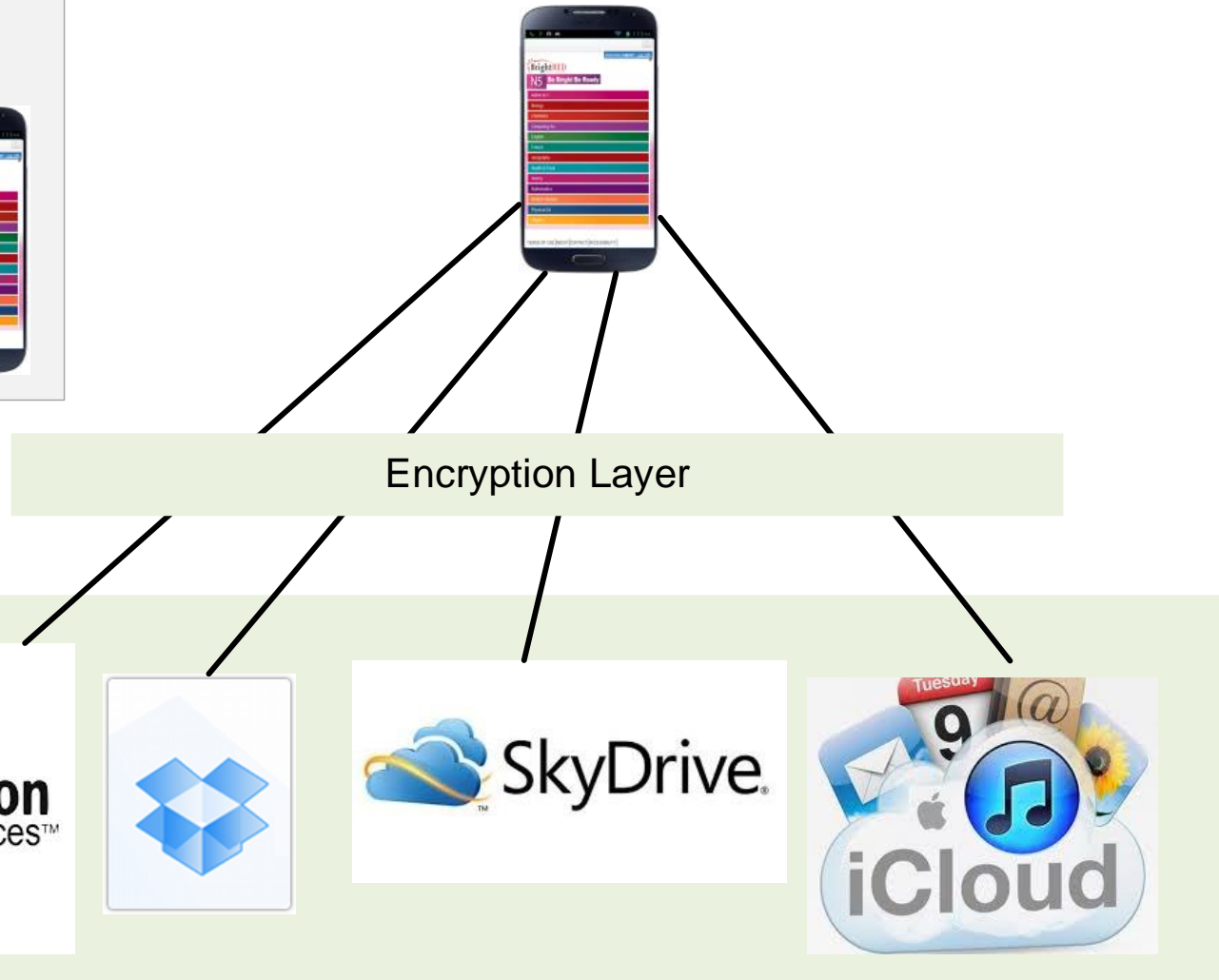
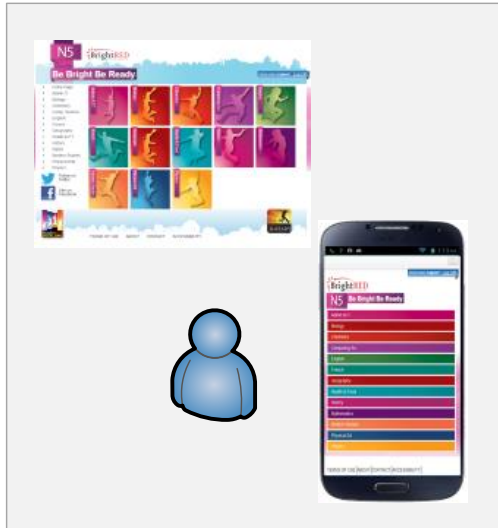


Passwords, customer details, emails, usernames, etc can all be shoulder surfed. Privacy filter is an inexpensive investment.





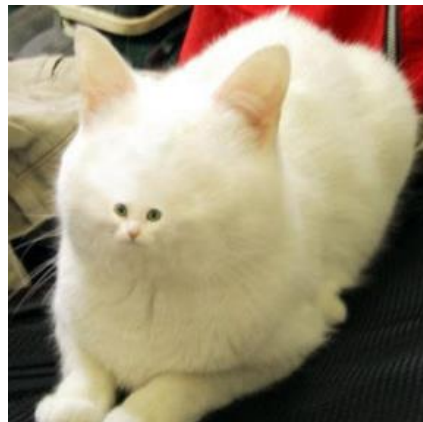
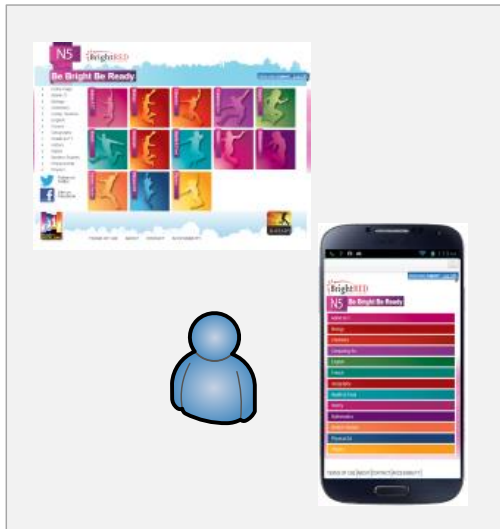
Risk 8: Storing Non-encrypted to the Cloud



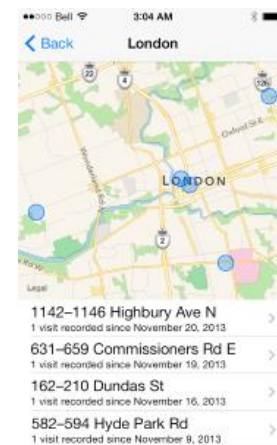
Non-UK/EU storage. Open to hack.



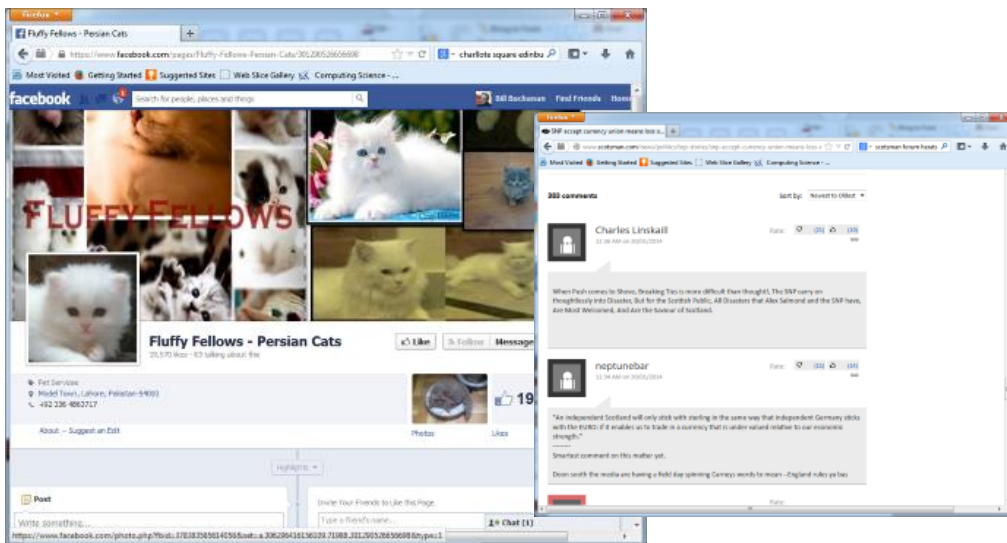
Risk 9: Digital Shadows



Photos

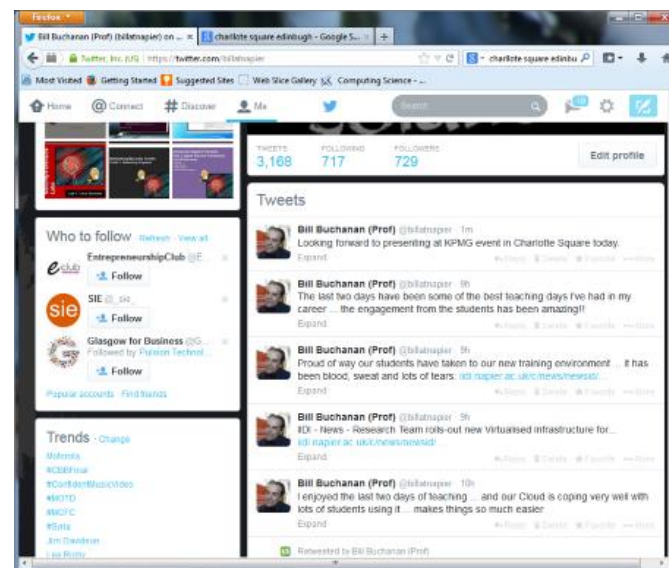


Device Records



Facebook

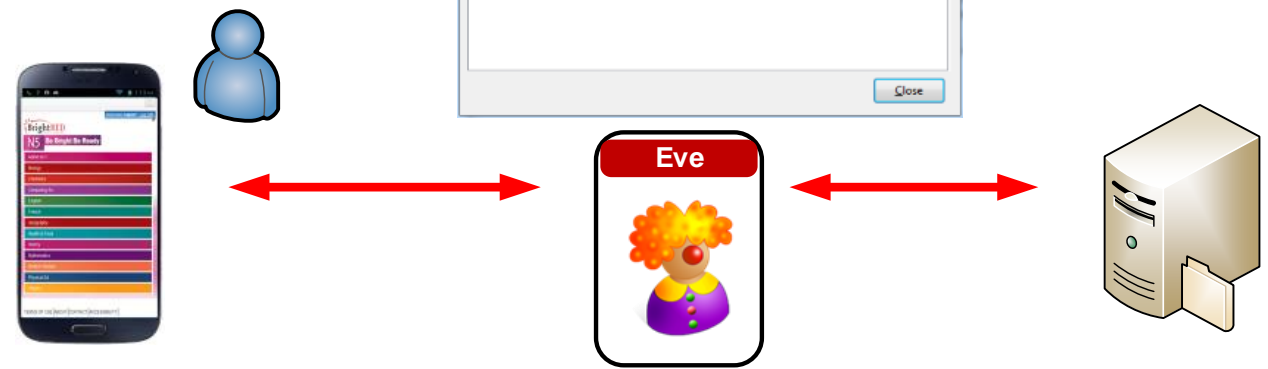
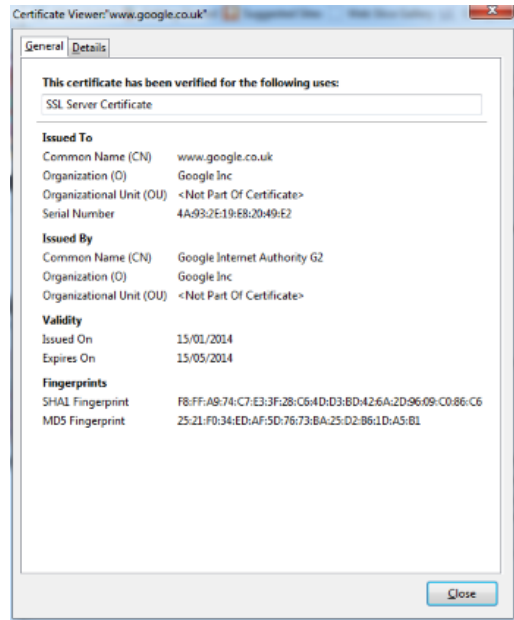
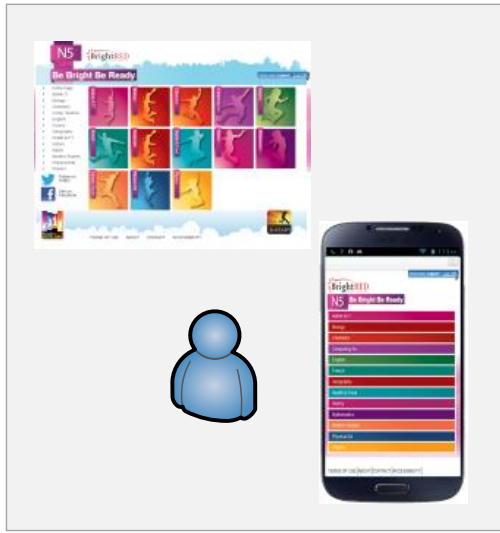
Forums



Twitter



Risk 10: Trusting https and fake cert

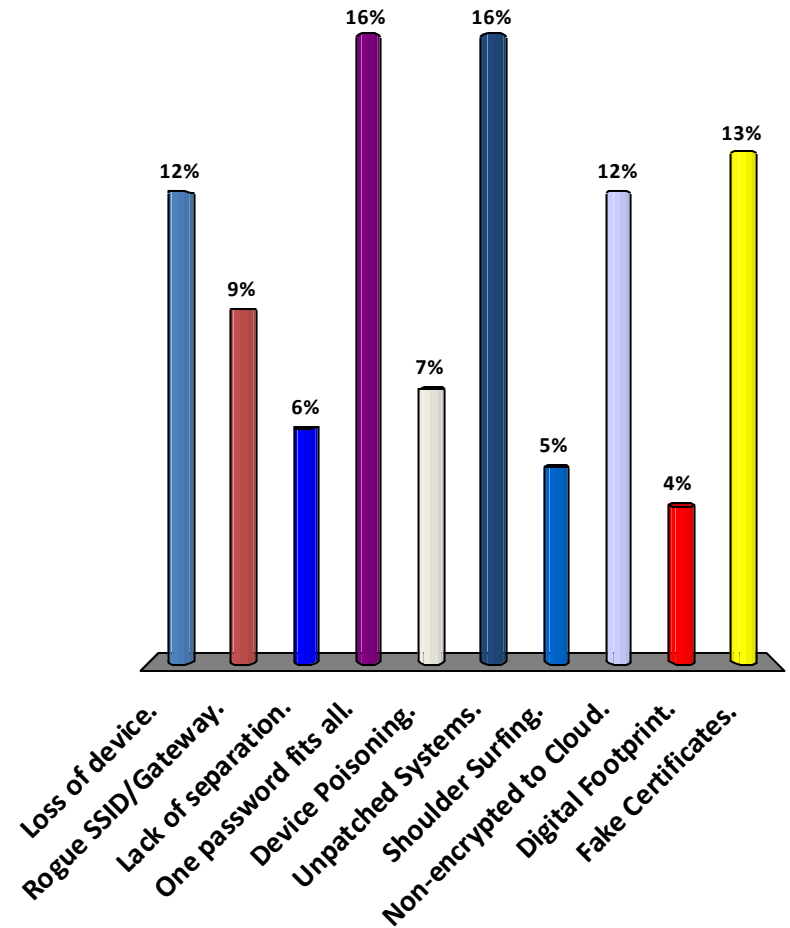


Eve-in-the-middle (Proxy/Fake Certificates)



Rank the Risks (Top 5)

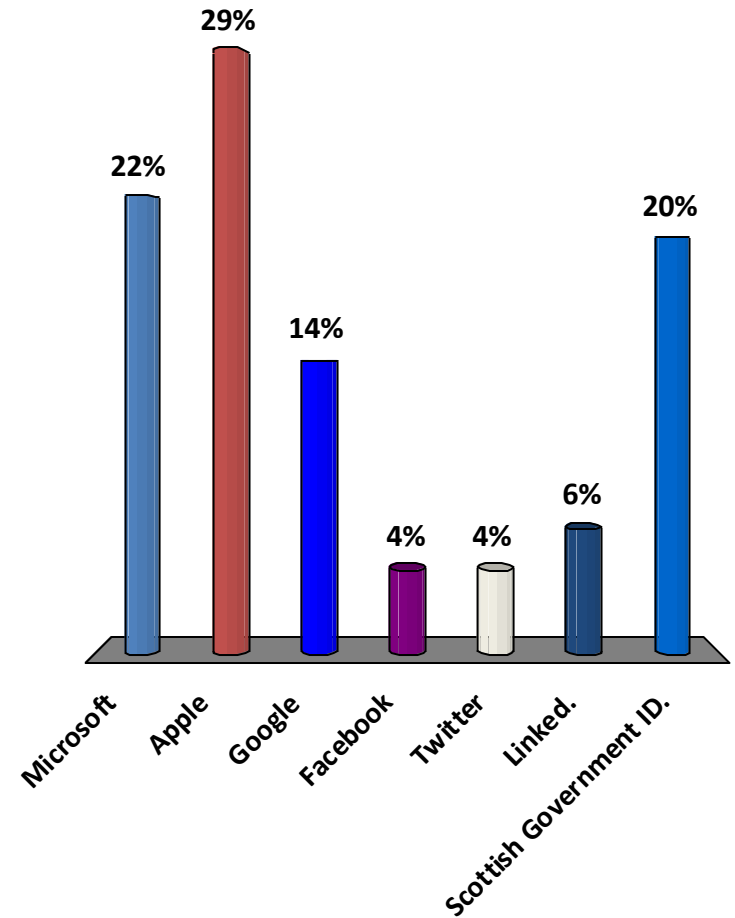
- A. Loss of device.
- B. Rogue SSID/Gateway.
- C. Lack of separation.
- D. One password fits all.
- E. Device Poisoning.
- F. Unpatched Systems.
- G. Shoulder Surfing.
- H. Non-encrypted to Cloud.
- I. Digital Footprint.
- J. Fake Certificates.





Who do you trust with your ID (Top 5)?

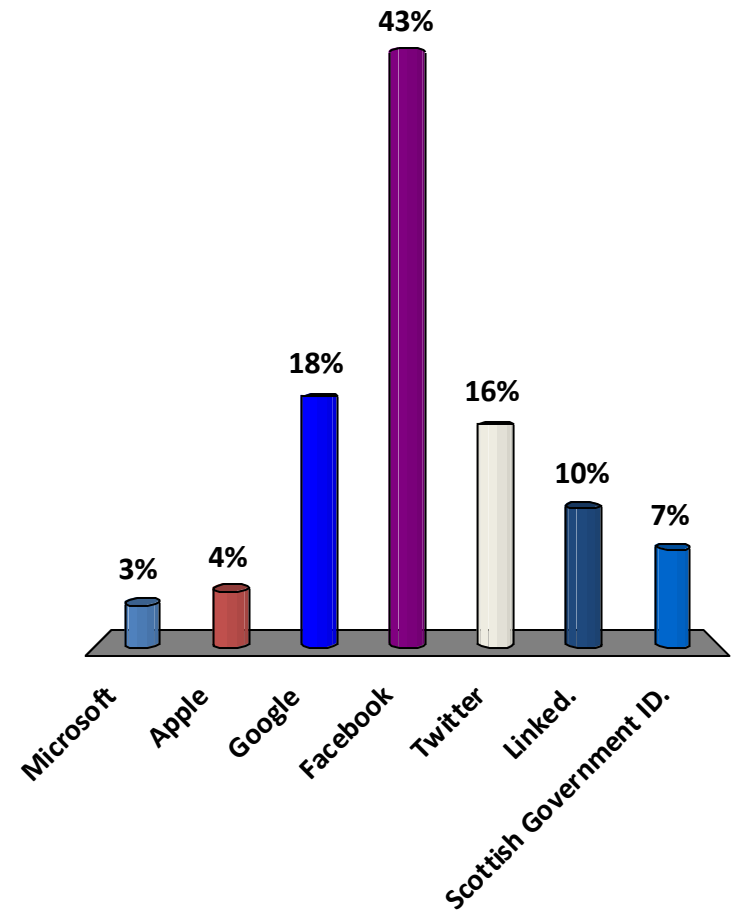
- A. Microsoft
- B. Apple
- C. Google
- D. Facebook
- E. Twitter
- F. Linked.
- G. Scottish Government ID.





Who do you trust least with your ID (Worst 5)?

- A. Microsoft
- B. Apple
- C. Google
- D. Facebook
- E. Twitter
- F. Linked.
- G. Scottish Government ID.



The Risks and Opportunities of Mobile Working within Cloud Environments

<http://asecuritysite.com>




Prof Bill Buchanan, Adrian Smales

Adrian Smales (@asmales) on Twitter | online metadata and exif viewer | meta data from photos

Home @ Connect # Discover Me

Expand

Adrian Smales @asmales · 8h
 Guess where I am... @kpmguk #cyber #mobile @billatnapier
 pic.twitter.com/dCMBkutzHk



Expand

Adrian Smales @asmales · 12h
 Take a look at the Intel infographic on #internetofthings intel...
 @IntelBiz #IoT


View conversation

Retweeted by Adrian Smales

Intel Business @IntelBiz · 13h
 Everyone's talking about the #internetofthings - but what is it
 overview> intel.ly/LkwLVG

Bill Buchanan (Prof) (@billatnapier) on ... | online metadata and exif viewer | meta data from photos

home link



Camera Copyright Location EXIF XMP Maker Notes ICC


Camera

Make	Apple
Model	iPhone 5s
Exposure	1/60
Aperture	2.2
Focal Length	4.1 mm
ISO Speed	32
Flash	Auto, Did not fire

Author and Copyright

Copyright not found.

Location



Latitude 55.951539 North
 Longitude 3.206231 West
 Altitude 65.7407182 m Above Sea Level