KF4005 Operating System Fundamentals
Information security issues

The Royal Academy of Engineering funded a Visiting Professorship in Practical Cybersecurity Insights at Northumbria University, 2019–2022. These slides are a slightly modified version of those delivered, intended to be available after the project has ended

Web `https://green-pike.co.uk/nvp`
Email p.brooke@northumbria.ac.uk (until it stops working. . .)
phil@green-pike.co.uk

Today

- IT parts of an organisation
- Identification of users across an organisation
- Incident response ("when things go wrong")

Organisations

People	are doing stuff with. . .
Technology	. . . computers, networks (and other assets, *e.g.*, paper!)
Process	how they're (meant to) do things

Phil Brooke
A *Royal Academy of Engineering Visiting Professor* in Practical Cybersecurity Insights
Northumbria University

Technology components

- Computers — desktops, laptops
- Mobile phones, tablets
- Network components — switches, routers, wireless access points, gateways
- Servers — storage and applications
- Embedded devices, “Internet of Things”
- External services — Internet and cloud

Nearly *all* of these have operating systems

User authentication

This module includes “user authentication” in the indicative content

How do users *authenticate* themselves to a computer / other device?
How do they do authenticate themselves to a device *over a network*?

Network-wide authentication

Typing in passwords repeatedly is annoying
Remembering and typing in lots of different passwords is worse
. . . this is the common user experience

Single-sign on (SSO) is a common approach
When extended beyond an organisation, this becomes *federation*

People!

People *join* an organisation, *move* roles within an organisation and *leave* an organisation ("JML")

Managing their access credentials, particularly within large organisations is a major challenge

For example, users often accumulate privileges as they move around roles

Is JML a problem for IT?

When things go wrong

The time to organise incident response is long before you need to respond...

NIST SP800-61 gives a four-step approach

1. preparation
2. detection & analysis
3. contain, eradicate, recover
4. post-incident

ISO27035 gives a similar five-phase approach

1. plan & prepare
2. detection & reporting
3. assessment & decision
4. responses
5. lessons learnt

Who should be involved?

Suppose an organisation realises it's being attacked with ransomware

Who should be involved in the response?

- ICT — specialists from all areas
- Data protection officer
- Infosec officer
- *Senior management*
- ICO (other regulators?)
- Police/NCA
- PR/corporate comms
- Legal

Often combined into an "incident response team" *a.k.a.* "computer emergency response team" (CERT) or "computer security incident response team" (CSIRT)

Who decides?

Who can decide to turn off services? Or even completely shut down?

- Could a NHS trust turn off *everything* that uses a computer?

From a (very old) .sigline:

> *"shutdown -halt now" - The final word in network security tools.*

More incident horrors

- Plan early — playbooks
- Detection is a nightmare: some surveys suggest the time from breach to detection of the breach is *months*
- Post-incident forensics: what can I find on the affected computers? All of the underlying CS theory about *how* computers work is important

Ethical question

Are we allowed to go after intruders? Should we pursue them?
Should we "counter-strike" their systems? (Ethics and legality?)

The end

Web	`https://green-pike.co.uk/nvp`
Email	p.brooke@northumbria.ac.uk (until it stops working. . .)
	phil@green-pike.co.uk

Phil Brooke
A *Royal Academy of Engineering Visiting Professor* in Practical Cybersecurity Insights
Northumbria University