KV5002 Computer networks, security and operating systems
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

- Organisations, authn and SSO
- OS / infrastructure hardening
- Incident response ("when things go wrong")

(Builds on KF4005 from last year...)

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

Classic user authentication

This is normally taught as three phrases, “something you $word”

Which words?

Can be combined with multifactor authentication
Newer options include MS’s “conditional access”

Network-wide authentication

Single-sign on (SSO) is a common approach to avoid repeatedly typing in multiple passwords and enabling a single authentication service for multiple services/systems

Typical technologies

- Kerberos
- MS Active Directory
- LDAP

Problems:

- Single point of failure
- All keys in one place
- Relates to JML management (next slide)

but can also ease problems of consistent updates, cancelling accounts promptly, . . .

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 / change roles

- What about long-term absentees?

Agility

"Modern" organisations are more likely to use some form of "DevOps". Characterised by

- frequent releases
- tighter coupling of development and operations teams and systems
- greater automation, typically involved continuous integration (CI) and continuous deployment

Makes traditional infosec types unhappy as we can't assess a single build

. . . So requires flexibility and agility of the assessment processes. . .

Virtualisation

. . . can pose similar problems.

Many variations from

- full VMs: Xen, KVM, VMware, . . .

to

- containers: docker

with complexity added by swarms or frequent movement of virtual machines, *e.g.*, Kubernetes

Takes all the operating systems content, mixes it up with networks, and adds more layers!

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.*

Plan early

Playbooks!

- Identify assets
- What could go wrong? ("wargame"?)
- How would we handle it?

Example

Consider an accountancy company that provides book-keeping, tax returns and payroll services to other companies

1. What assets do they have?
2. What could go wrong?
3. What should be done if an incident affects them?

Detection

Detection is a nightmare: some surveys suggest the time from breach to detection of the breach is *months*

How are security incidents detected?

Detection

Detection is a nightmare: some surveys suggest the time from breach to detection of the breach is *months*

How are security incidents detected?

1. Human report of anomaly
2. System crash
3. Ransom demand
4. IDS alarm
5. Log analysis

Afterwards

- Post-incident forensics: what can I find on the affected computers?
- What went well?
- What could we do better?
- Revise/review playbooks. . .

Ethical question

Are we allowed to go after intruders? Should we pursue them? Should we "counter-strike" their systems?

- What does UK law say about this?
- What collateral harm could be caused?
- Do states and/or large providers (*e.g.*, large software companies, cloud providers, major network services) have any obligations?

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