Network Security 21: Putting it Together, Taking it Apart

i.g.batten@bham.ac.uk

We’ve looked at…

- Host security (firewalls and attack-surface minimisation)
  - Firewalls
  - IDS
  - VPN
  - IPsec

We've looked at…

- Proxies
- Content Filtering
- Wireless Security
- Two Factor Authentication
- DNS Attacks

We haven’t looked at

- Virus scanners (run mostly on hosts, but can run on web proxies and mail gateways)
- DNSSec (lack of wide deployment and unclear what threats it mitigates)
- Protocol Design in detail (different course!)

Pulling from other courses/ knowledge

- NAT provides some security
- Secure applications are safe to expose to the internet
- We obviously need asset registers, risk registers and so on in order to design bespoke security solutions (TM)

Put yourself out of a job!

- 2005-style, perhaps even 2015-style, every company with a substantial web presence ran mail, web, RAS/VPN, perhaps e-commerce, perhaps e-payment.
  - Either developed in house, often by unskilled staff, or bought in and modified, or occasionally bought as a managed service.

Put yourself out of a job!

- 2018-style, forward-looking IT functions buy as much as possible as services, not products.
  - Who’s running their own mail?
  - Who’s running their own web service?
  - If your applications are in the cloud, like Salesforce and Google Apps / Office 365, do you need a VPN?

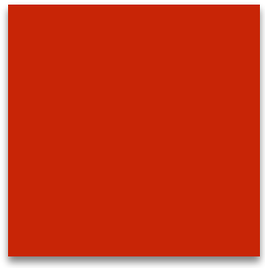
Data Centres

- No longer certain that companies will have data centres
- 10TB of storage fits in a shoebox
- And you can rent it from Amazon for a few hundred dollars a month anyway

Web Applications

- Common model is that web applications are developed to one standard for use externally, a lower standard for in-house only use, protected by VPN (SSL-VPN is enough).
- Why is this acceptable? Why not do everything to an “Internet” standard?

Old Design Pattern



Outside Firewall

Mail

Web

VPN

Inside Firewall

ERP

FIN

Stock

PMO

...

...

Bring Your Own Device (BYOD)

- Two choices for a business
  - Staff bring their own kit and you manage the risks in an appropriate manner in collaboration with your auditors and other stakeholders
  - Staff bring their own kit anyway, and use it anyway, and you don’t get a say
  - Senior and middle management **will not back you** if you attempt to ban iPads.

Home Working

- Ability to isolate home devices reducing
  - people won’t accept devices that don’t split tunnel
- People want full functionality from home
  - including telephony, printing, CTI, etc
- IT Directors and CSOs that say “no” will be saying “no” to their recruitment agency.

Financial Reality

- When laptops were expensive, only senior management and salesmen had laptops
  - As IT Director in all but name, I didn't get a laptop until about 1997, and (from memory) at meetings in Silicon Valley in 1995–2000 laptops were nothing like universal for technical people (to be fair, these were technical meetings at server vendors!)
- Now, everyone either has a laptop from work or owns a laptop/iPad at home, and laptops are widely issued: massive capital cost

“Generation Y”, Digital Natives, etc

- For people under 30, their digital life **is** their life.
- Boundaries between work and play blurred
- Portfolio of digital skills one of the things they are selling
- Companies that issue large black Windows 10 (or 7!) machines in locked-down state

  a.not making best use of staff skills

  b.not best at recruiting staff
- If you want the best people, you need the best environment

Take-away quote

- **In five years' time, we'll only be issuing laptops to people to whom we issue trousers**
- Essential to issue locked-down machines to emergency and uniformed services, plus receptionists, field engineers, some call centres, etc.
- And people will also use supplied systems (dealing floor displays, CAD, HPC, etc).
- But for many staff, they will also have a personal machine on their desk or in their hand, and that machine will blend work and personal.

As go computers, so go phones. Double.

- Many companies still issuing Blackberry devices (in particular)
- No appetite amongst staff for this, everyone wants to have their work phone be their personal phone (or their personal phone be their work phone)
- Phones now join internal WiFi networks

BYOD has to happen

- In universities, *de facto* already here: few laptops purchased and centrally managed for academics, every academic has a laptop
- Ditto development shops, start-ups, tech companies
- Corporates still exercising control but cannot last forever

Consequences for Network Security

- Take five minutes, in groups of two or three, and come up with three issues which arise from people having a laptop/phone device on the corporate network which they control.

Borderless Networks

Inside Firewall

ERP

FIN

Stock

PMO

…

…

What should we do?

- Take another five minutes and come up with three improvements we need to make to standard network architectures.

Implications

- Host security
- Single Sign On / Two Factor
- Virtualisation
- “Islands”
- Networking

Host Security

- All machines are exposed to the Internet, in the form of user devices which have Internet connectivity
  - In reality, has been true for ten and more years
- On campus, and in large offices, not inter-penetrated with third-party WiFi.
- Hosts containing sensitive data have to be secured, as in the first few lectures.

Single Sign On / Two Factor

- Devices are going to store corporate credentials, and those credentials will be useful remotely
  - Used to joke we could safely publish root password on front page of newspaper: not any more.
- Two factor with hardware devices will become critical
  - But is cumbersome
- SSO was the big corporate “thing” ten years ago, then died a messy death. Has to be solved.

Virtualisation

- You’re running Linux and Solaris instances to get access to particular facilities on a range of devices
- One option for companies is to ship a single build of the corporate environment as a virtual machine, for users to run on their own systems
  - Different security model, for example attacks in the network layer of the host system
  - Not perfect, but a good transition aid

“Islands”

- In large enterprises, the “outer, proxy, inner, secure” model may be replicated in miniature.
- Secure offices, secure cells within the organisation
- Access by VPN servers dedicated to the island

Islands

User Devices

Outside Firewall

Mail

Web

VPN

Inside Firewall

ERP

FIN

Stock

PMO

…

…

Outside F

Mail

Web

Inside Fi

ERP

FIN

Stoc
k

Networking

- Much more need for VPNs (remote working, distributed workplaces)
- Architecture of those VPNs much harder (endpoints not trusted)
- IPsec may also be needed as data centre moves to cloud

Issues to Ponder

- Territoriality (legal actions, interception, search warrants, Anton Pillar orders)
- Data Protection (US rules considerably looser than ours, German rules considerably tighter)
- Accountability (if you have a contract with Amazon and it goes wrong, is the money enough?)
- Auditability (Sarbox, JSox, SSAP, ISO 27001, etc)