ENTERPRISE CYBER SECURITY

PRE-HISTORY

University of Glasgow

OVERVIEW

- understand the evolving architectures of enterprise over the decades.
- security incidents that happened alongside the evolution and the response of enterprise.
- understand the modern-day complex architecture that involves many different elements and connections.

ENTERPRISE CONCERNS

PRODUCTIVITY

- computers were introduced into the enterprise with the aim of boosting productivity.

- replacing human calculators with mechanical machines, that did not get sick or need comfort breaks.

- 1960s introduced enterprises to the possibilities of computers with the adoption of mainframes.

- prior to the 1960s, computers were too expensive for organisations to be confident on Return On Investment.

CORE COMPETENCY

- motivation of enterprise is to focus on their core competency.
- outsource those areas that are important but not what they want to focus on.
- outsource distribution to another organisation, for example, or outsource HR requirements to another organisation.
- enterprises can form agreements about how this happens, but prefer fixed numbers to plan for each period.

SYSTEMS AND NETWORKS

- systems can be used to improve productivity, they can also support individuals in completing tasks.

- networks can pull these systems together to achieve business processes.

- networks can also pull together systems and resources across various domains supporting outsourcing.

CYBER SECURITY

- cyber security concerns have not necessarily been paramount in the early motivation for these tasks.

- wonderment of whether things are possible are the first task, rather than how to transition it into a dependable, secure solution.

- transitioning from experts to every day users.

ENTERPRISE ARCHITECTURES

1955 TELEPHONE SYSTEM COMPROMISED

TELEPHONE NETWORK

- telephone networks represented one of the most complex systems in the world, usable by individuals.

- telephone networks were a mixture of human and mechanical elements.

- operators who were fallible, slow and untrustworthy were replaced with automatic switches.

- switches that could be manipulated by frequencies.

PHREAKING

- switches relied on tone-dealing that the network provider could use to open and close calls.
- Joe Engressia in 1957, is one such example where he used pitch perfect tones to close calls.
- subsequently and along with John Draper, the pair began to grasp an understanding of how the network operated.
- John Draper discovered that a toy whistle, distributed with a cereal recreated the same tones and these could be used to place calls.

COUNTERMEASURES

- switches relying on the frequencies were slowly replaced at great expense over a period of time.

- debatable whether such a transition would have happened if it was not for the lack of competition.

- network providers also put increasing pressure for individuals to be convicted and fined.

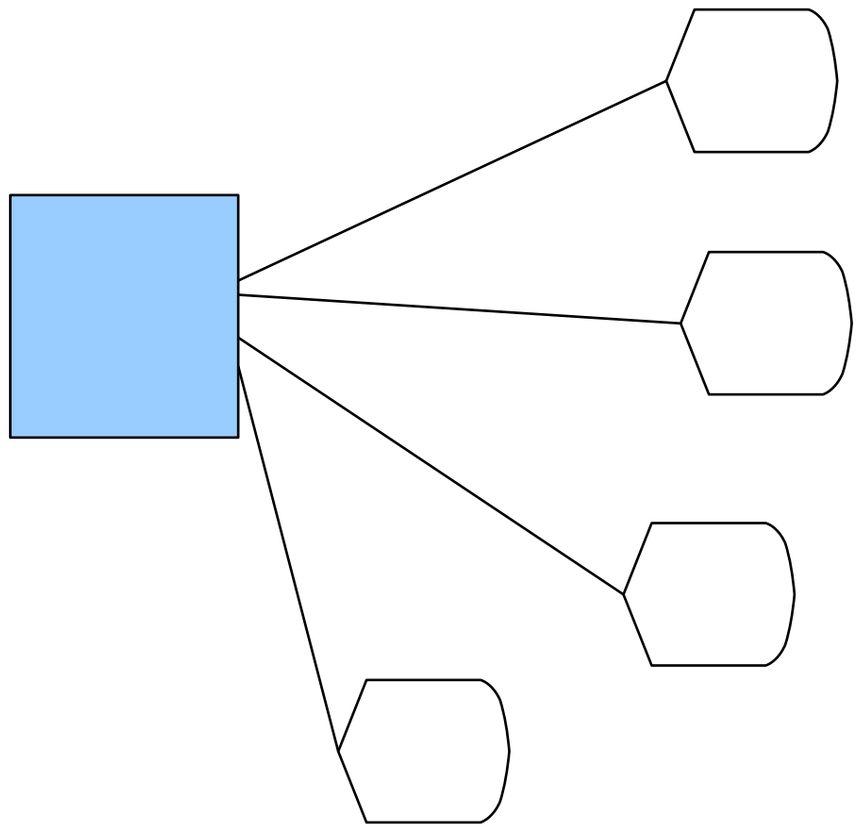
- the network providers had simply not accounted for the curiosity of individuals, never mind malicious attackers.

"The fact the phone company had set it up that way… flabbergasted me."

–JOHN DRAPER

MAINFRAME ERA

MAINFRAME ERA (1950S-70S)



MAINFRAMES

- enterprises started to invest in mainframes, large computers that could be physically secured in a room.

- such systems could be managed and maintained by professionals with others queuing to gain access to them.

- not physical access, but resource access - many individuals in the 1960s would queue up with punched cards.

- as the decade progressed individuals could have these cards read remotely by machines connected by cable to the mainframe.

MAINFRAMES

- security at this stage would be to make sure the lock on the door is working and staff would physically trace cables.

- managers were less concerned about the security of information, in terms of confidentiality, but more in terms of integrity.

- computer systems were constantly failing and collapsing, modern software engineering practices were not in effect.

- computer crime was starting to emerge significantly, even being discussed in the media.

“It had all the glamour and excitement of dropping one's clothes off at a laundromat.”

–FERNANDO J. CORBATÓ

MAINFRAMES

- electronic input slowly started to replace punched cards as form of interaction.

- individuals started to get computers in their system, connected to the larger system.

- security professionals would again physically trace all connections to make sure only authorised systems connected.

- business logic presented illusion of security with individuals presented screen specific to their task.

MAINFRAMES

- customer service agents could create reservations but purchasing would happen at another system
- security challenges started to become obvious issues for enterprises to address.
- enterprises could start rely on systems, but the confidentiality of data become more of a challenge.

GOVERNMENT

- cryptography became of interest as elements of government came online, such as the Internal Revenue Service (IRS).

- reason for this is that machines started to be connected intimately to an individual

- confidentiality became more an issue and National Institute for Standards and Technology (NIST) launched 1974 Privacy and Security act.

- the act concerned itself with government machines and use of personally identifiable information (PII).

1965 COMPATIBLE TIME-SHARING SYSTEM (CTSS)

COMPATIBLE TIME-SHARING SYSTEM

- mainframes individuals would have to wait in a queue and wait for it be batch processed over night.

- if there was any error in the punch cards, any mistake the job would be abandoned and would likely not know until the next morning

- time-sharing system was about dividing up resources to offer real-time interaction mainly for the purpose of debugging.

- CTSS is considered the first system to embrace passwords to restrict access to resources for users.

“Putting a password on for each individual user as a lock seemed like a very straightforward solution.

Fernando Corbató

1961

COMPATIBLE TIME-SHARING SYSTEM

- passwords were likely used as they are inexpensive to implement
- each individual had their own user directory containing files.
- system itself was a ‘quasi-user’ containing numerous applications, files and ‘message of the day’.

PASSWORD PROBLEM

- system programmers convinced Corbató to allow the system directory to be an exception.

- two system programmers accessed the system directory simultaneously.

- both used the text editor application to edit files, namely the ‘password file’ and ‘message of the day’.

- design of system led to the data from the password file being associated with the message of the day file.

LESSONS LEARNED

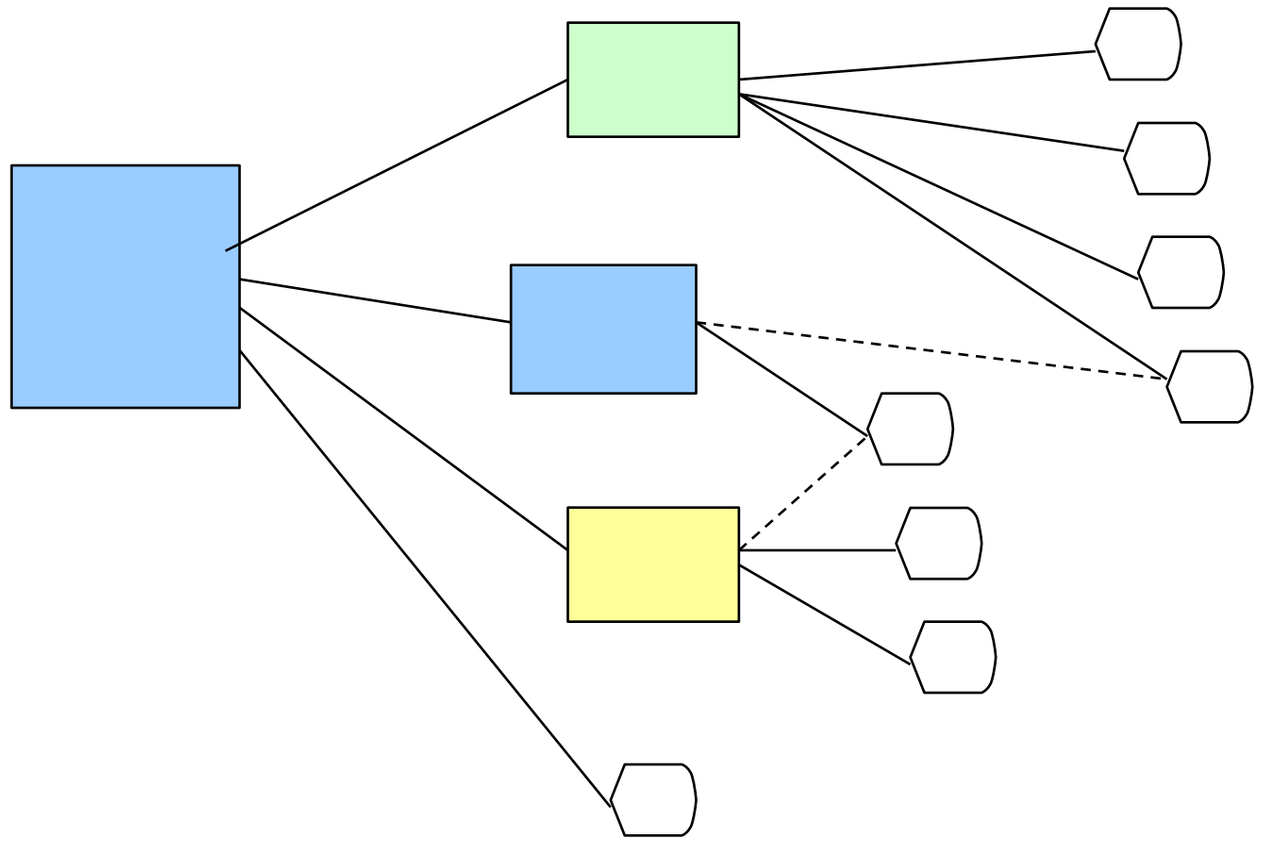
- challenges in secure design or just good design of software.
- there is no clear language in terms of how discuss security concern
- how to secure password files and how to secure access without issues of division.
- problems of password, Corbató knew this from the start - even discussed in his Turning lecture.

MAINFRAME ERA (1950S-70S)

- few mainstream supplier choices (IBM, ICL, Amdahl, Burroughs, Univac, Honeywell, Fujitsu etc).
- simple architecture with centralised tight control with low autonomy.
- back office automation and transaction processing, relying on dumb terminals.
- the approach had very high costs and the emergence of siloed applications.

MINICOMPUTER ERA

MINICOMPUTER ERA (1970S, 80S)



MINICOMPUTER ERA (1970S, 80S)

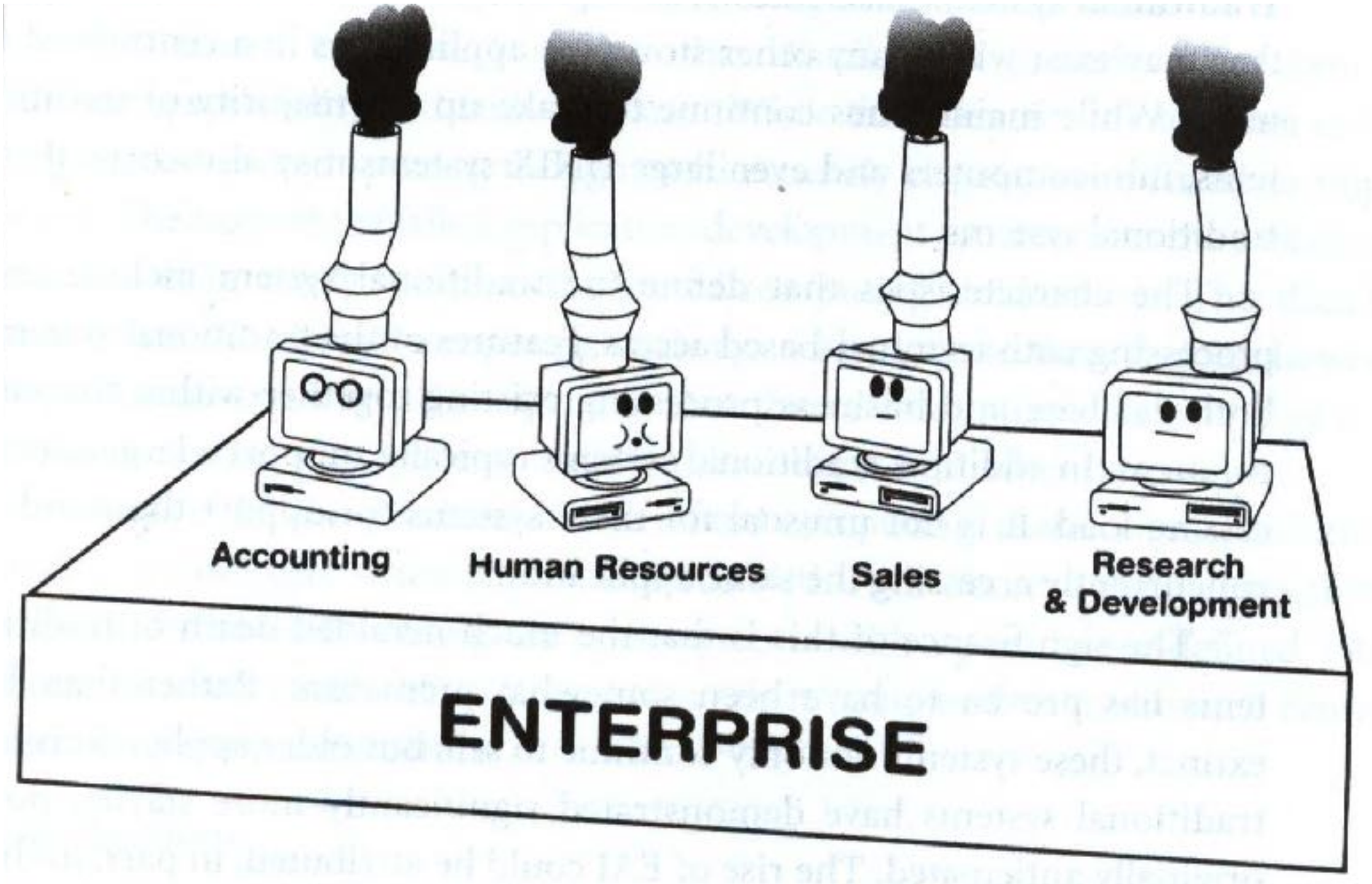
- several mainstream supplier choices from 1960s (IBM, ICL, DEC, NCR etc.)

- architecture remains simple with dumb terminals, but the focus is still transaction processing.

- silo applications, ‘islands of automation’, mismatching data as well as strategy.

- distributed autonomy starts to emerge with the approach still representing significant costs and concerns.

SILOS


Accounting
Human Resources
Sales
Research
& Development
ENTERPRISE

STOVEPIPES

- stovepipe systems are typically designed to fulfil a specific purpose and specific set of users.

- stovepipe systems were typically implemented with in-fashion approaches and technologies.

- no real consideration of integration of different users or different systems.

- business units, such as logistics or human resources, may have their own systems and applications that do not integrate.

PROBLEMS WITH STOVEPIPES

- many problems with stovepipes, designed without much thought to integration.

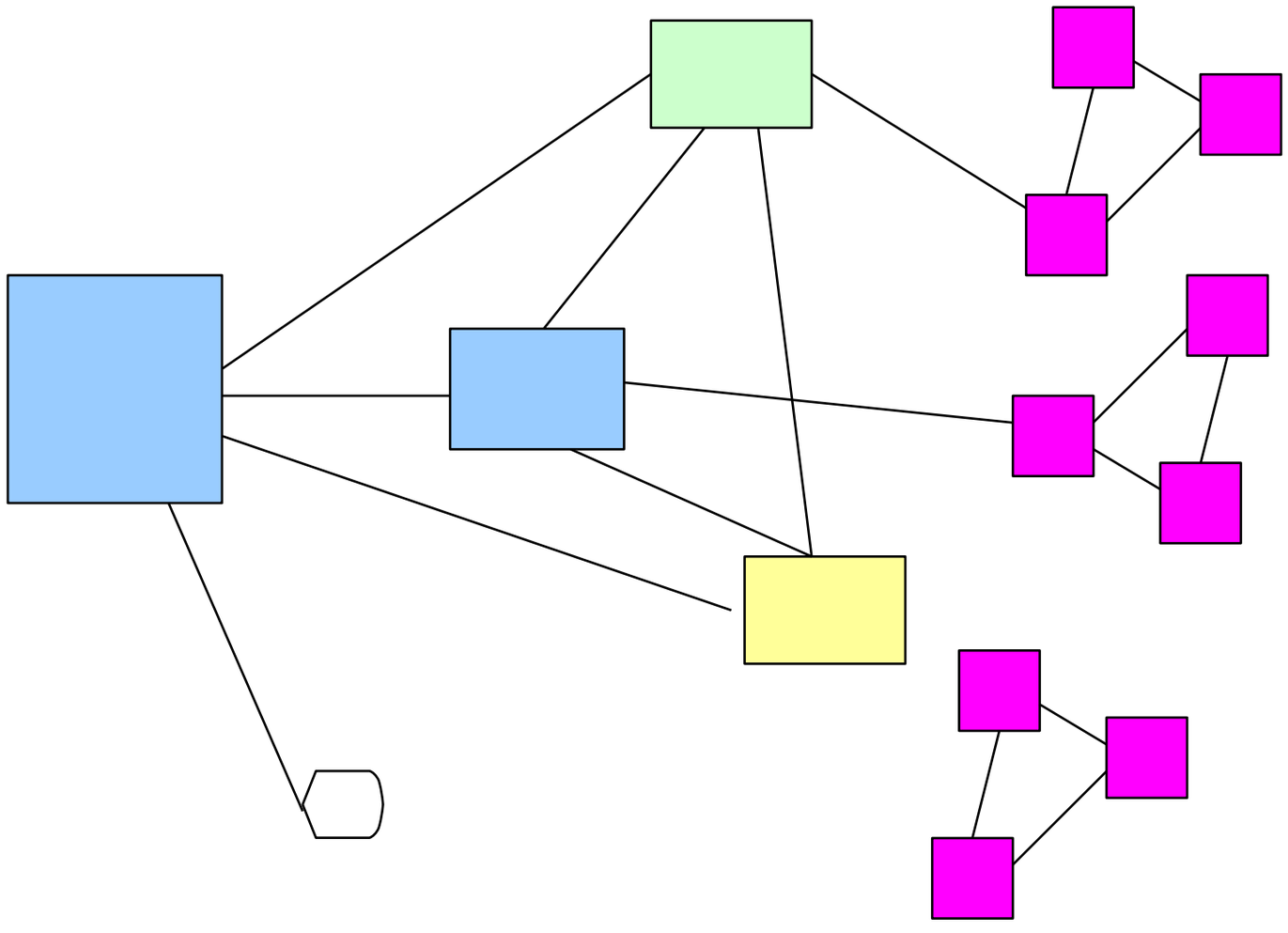
- they do not share data, with data exchange, difficult to determine a coherent understanding of enterprise.

- some senses easier to secure as less complex, but less useful as well.

- stovepipes can represent many processes and unseen challenges with integration.

DISTRIBUTED/PC ERA

DISTRIBUTED/PC ERA (1980S, 90S)



DISTRIBUTED/PC ERA (1980S, 90S)

- burgeoning market for personal computers with many different suppliers and varied capabilities.

- complex architectures evolves with far more autonomy for units, down to departmental level.

- integration still remains poor, becoming greater challenge with emerging technologies (voice, data etc).

- associated cost is still and need to evolve to support ever more complex organisational structures.

1983 WARGAMES

WARGAMES

- interesting film released in the Summer of 1983.
- teenagers unwittingly access the systems related to defences, thinking the systems belonged to a video game developer.
- technical details of the film, may be inaccurate, but does provide an entertaining consideration of various security concerns.
- teenagers randomly trying to access several systems to play games was not actually that unusual.

414S

- group of young individuals that compromised access to various systems with the motivation to play games.
- compromised high-profile systems including Los Alamos National Laboratory, Sloan Kettering Cancer Center and Security Pacific Bank.
- for the most part they performed pranks, printing off paper etc.
- in the case of Sloan Kettering Cancer Center, they deleted records to cover tracks.

"We were like, wow, that sounds kind of fun, and you know how it is: one gets going, then the next person tries to see what they can get into. It starts to become a game."

– NEIL PATRICK

LESSONS LEARNED

- enterprises became more aware of the importance of security data to maintain integrity as well as confidentiality.

- incidents such accessing Sloan Kettering Cancer Centre prompted enterprises to strongly consider securing of information through cryptography.

- enterprises were still focused on strengthening physical security as well as improving password strength.

1988 MORRIS WORM

MORRIS WORM

- computer worms can be considered self-replicating programs that spread through systems.
- Robert Morris released a payload free worm on the nascent Internet in 1988.
- Morris claimed to be curious about the scale of the Internet and designed the program to gain insight.
- Morris released the worm from MIT, even though he was a Cornell student.

MORRIS WORM

- Morris utilised vulnerabilities within Unix so that the program could spread itself.

- the program could copy itself to a compromised system, effectively allowing the program to propagate.

- Morris was mindful that resources could be consumed if propagation continued uncontrolled.

- Morris built in a control step that would cause self-destruct if a copy of the program was already executing.

MORRIS WORM

- control step could be manipulated with a system basically stating the program was already executing.
- Morris added an additional, random step, that every seven times the program would execute regardless.
- problem was that as the program propagated, resources were slowly consumed until systems could not service any requests.
- the original denial of service attack, compromised approximately 6000 systems.

LESSON LEARNED

- US Government estimated and reported clear-up costs for the worm, providing insight for other organisations.

- Defense Advanced Research Projects Agency (DARPA) created the CERT Coordination Center (CERT/CC) to research software vulnerabilities and security.

- First conviction under the Computer Fraud and Abuse Act 1986 (CFAA) with language altered due to disputes within the case.

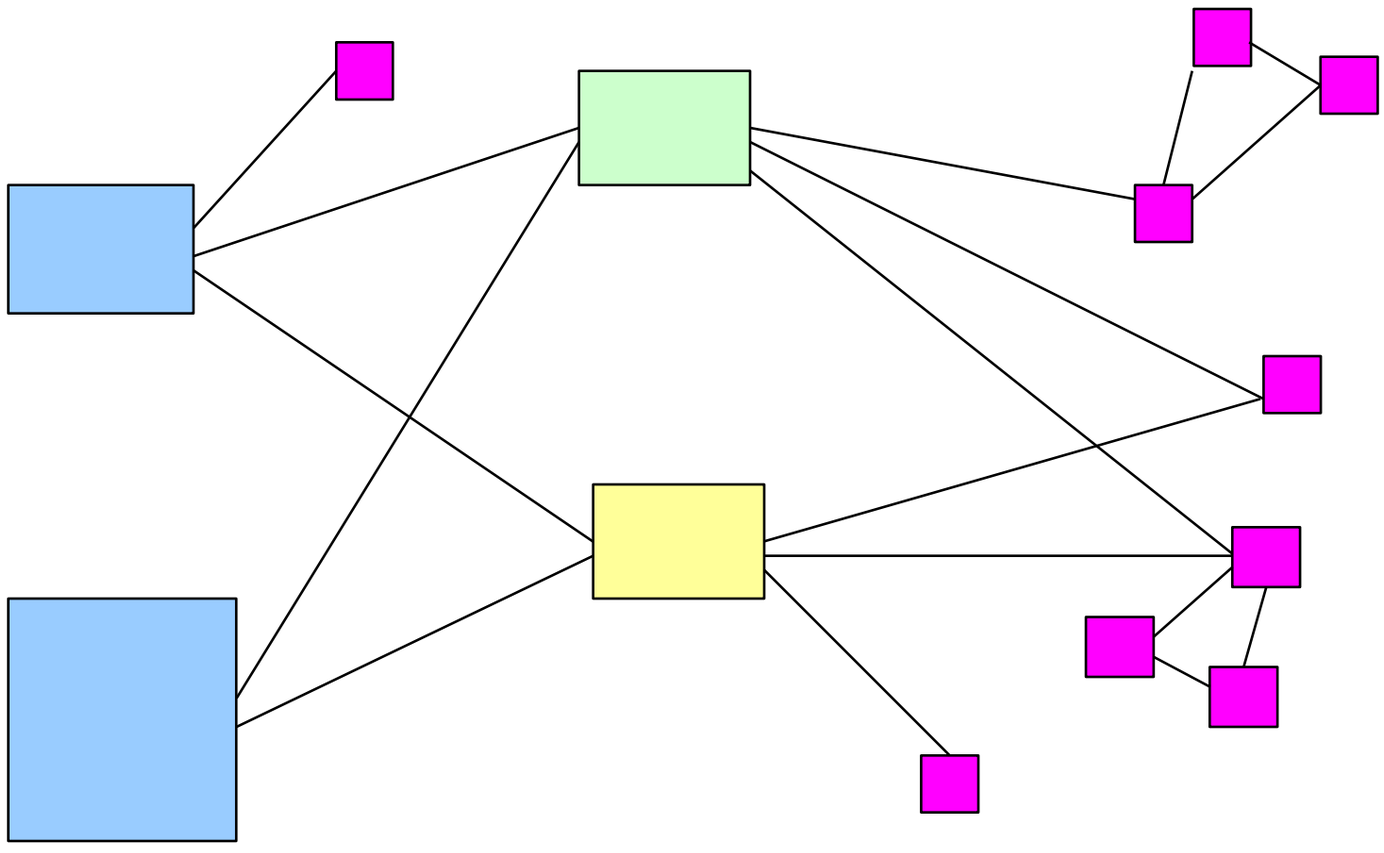
- the dangers of weak passwords could be compromised via a bruce-force attack.

"I was there when it was cooked up, and this was the recipe: someone guessed that there were about 60,000 computers attached to the Internet, and that the worm might have infected ten percent of them."

– PAUL GRAHAM

CLIENT SERVER ERA

CLIENT-SERVER ERA (1990S)



CLIENT-SERVER ERA (1990S)

- enterprises had a wealth of suppliers to choose from, but choice was restricted in terms of proprietary and open standards.

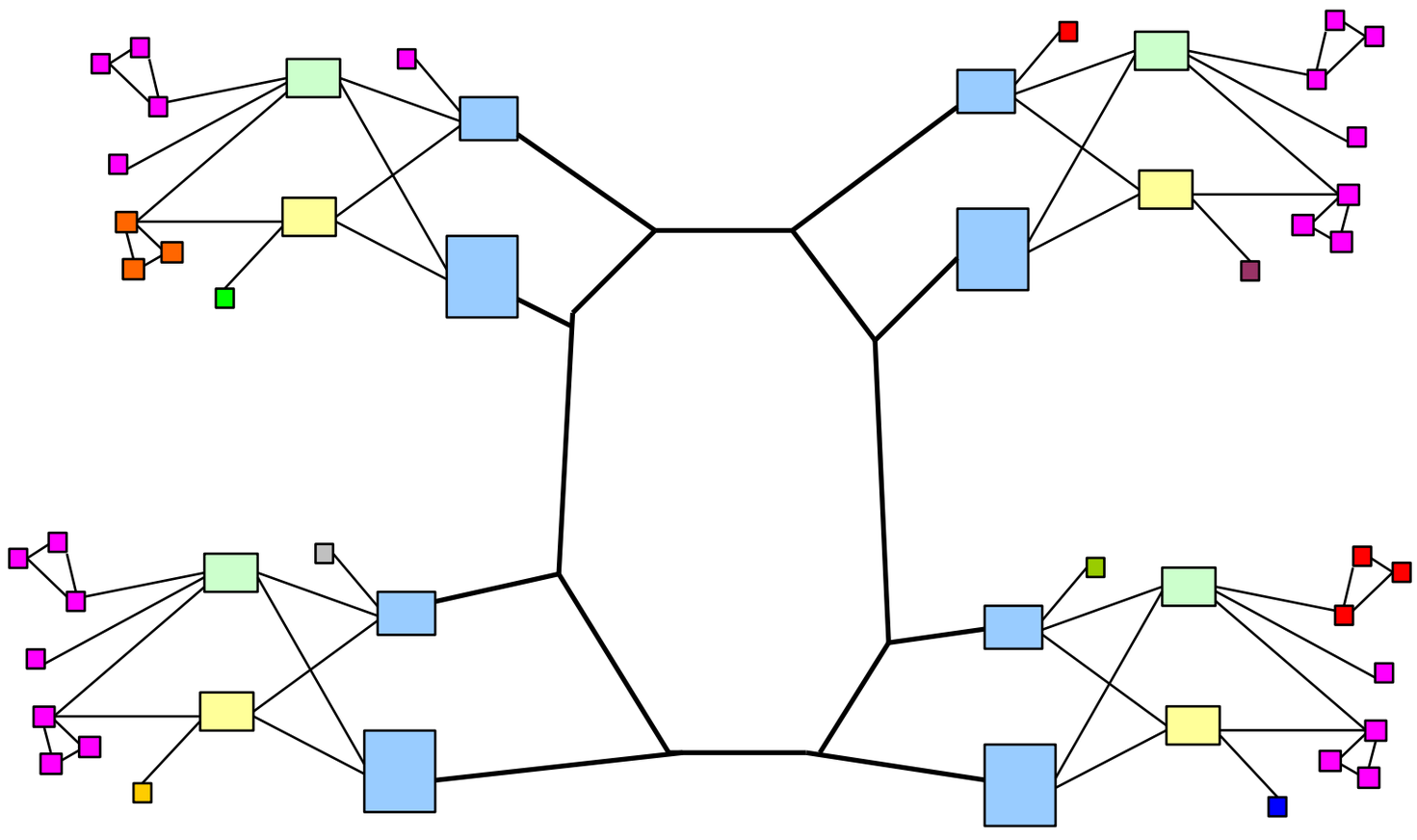
- the Internet became of greater interest and challenge to the enterprise, importantly it standardised communication.

- business units had incredible autonomy, but this can be even more as concern as more and more data was captured.

- enterprise investment still represented a significant consideration and cost.

NETWORK ERA

NETWORK ERA (2000S)



NETWORK ERA (2000S)

- emergence of connecting various systems together to achieve business processes.

- supplies offered more outsourcing choices, potentially to meet legal and compliance needs.

- decreasing costs in technology ensure more capable hardware is available to more business units.

- capable hardware to capture data within business units as well as harness resources from other areas of the enterprise.

CLOUD ERA

- enterprises can consider renting resources from various providers, effectively executing applications ‘in the cloud’.

- legal and location issues with making use of such service providers and infrastructure.

- relatively simple Application Programming Interface (APIs), compared to the needs of some enterprises.

- can form Service Level Agreements (SLAs) and afford enterprise flexibility in scale.

CLOUD ERA

- enterprises can take advantage of technology, potentially, without significant up-front investment, but this is not always the case.

- affords efficient resource utilisation with the ability to scale up and down in line with the demands of the enterprise.

- enterprises can potentially outsource challenging competencies to external organisations (e.g. time and resource management).

TODAY

TODAY

- considerable choice available for enterprises to achieve business processes.

- enterprises have not necessarily all evolved to current trends, they often represent a **mixture** of various periods.

- technology, along with globalisation, is affording enterprises complex and mixed architectures.

TODAY

- enterprises often comprise of complex architectures, connected to the Internet.

- complex integrated applications across different business units as well as partnering organisations.

- enterprises often have their own legacy systems that represent significant investment.

- bespoke applications costs considerable investment, including in terms of security, and impact on competitiveness.

2013 TARGET

ADVANCED PERSISTENT THREAT

ADVANCED PERSISTENT THREAT

- pragmatic and well organised campaigns against an enterprise or organisation.
- campaign can exist for several years and is potentially well funded.
- involves considerable research and analysis in terms of extracting the data.
- concerning due to the increasingly complex nature of enterprise architectures.

40,000,000

CREDIT CARDS STOLEN

70,000,000

CUSTOMER RECORDS STOLEN

1 / 3

AMERICANS

$61,000,000

EXPENSES

47%

DROP IN TRANSACTIONS DURING CHRISTMAS

FAZIO

Actors tested technology on a few service points during busy periods.

Why give the company such access?

How did the actors behind the APT determine the connection between the two companies?

SUMMARY

- understand the evolving architectures of enterprise over decades.
- security incidents that happened alongside the evolution and the response of enterprise.
- understand the modern-day complex architecture that involves many different elements and connections.

ENTERPRISE CYBER SECURITY

PRE-HISTORY

University of Glasgow