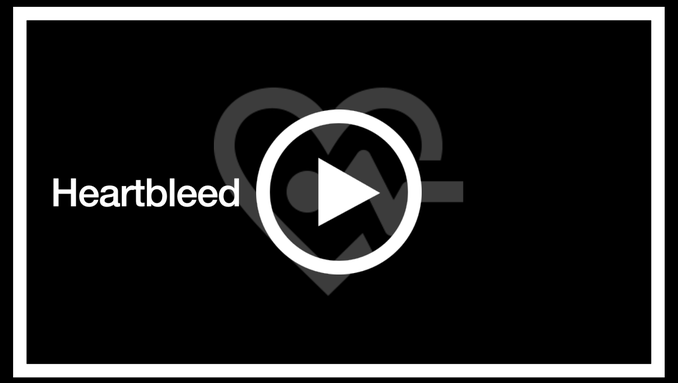
Legacy Systems

Enterprise Cyber Security

What are legacy systems?

Legacy systems

- Definition of a legacy system often **depends on viewpoint** of the person you ask within the enterprise.
- Often **pejorative** reference to ageing systems that are **resistant to evolution**.
- Recall the different periods of evolution, depending on the perspective, **systems from any period could be considered legacy**.
- Typically they are sprawling, complex, isolated systems and **considered outdated by modern standards**.
- Some legacy systems will have been designed and developed with the expectation of a **trusted environment**.


Heartbleed

Legacy Systems as an Asset

Legacy Systems as an Asset

Legacy systems

- Contain **business critical information** that represent considerable business knowledge and processes.
- Legacy systems are only **interesting because enterprises rely** on and utilise them.
- They often represent a **significant investment** in terms of time and money.
- Companies have **expectations of the lifecycle** of their investment, e.g. laptops versus Industrial Control Systems (ICS) (typically more than 25 years for ICS).
- Due to level of investment, typical criticality to business and lack of understanding, **interfering with legacy systems can have significant consequences**.

Characteristics

Characteristics

Legacy systems

- Legacy systems are **susceptible to modern day cyber security concerns**, even if cyber security was not considered when they were designed and implemented.
- Design quality in terms of **software is typically poor** and **does not respond to change** easily.
- **Difficult to integrate and migrate** due to a lack of understanding among staff.
- **Performance is often undesirable** and can impact on the performance of business processes.
- **Poorly documented**, rarely understood widely and are often inaccessible to the larger system.

““The biggest vulnerabilities faced by the banking industry resides within the use of legacy systems that run outdated software, yet these systems are still critical to the performance of daily business operations. When legacy systems are in use, the network topology should ensure sufficient segregation from any other public networks or devices.”

Alex Heid

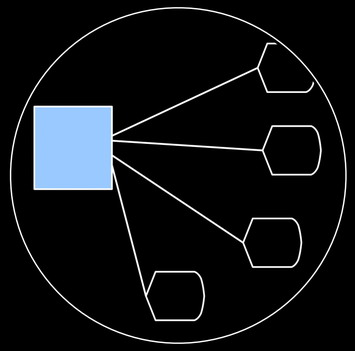
Dilemma

Dilemma

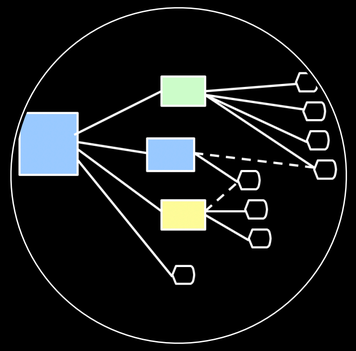
Legacy Systems

- Legacy systems are complex, poorly understood, crucial to business processes and represent a significant investment.
- Expensive to maintain and manage, but a poor approach to evolution could have significant consequences.
- Enterprises need to assess the challenges and associated costs, inline with the given risks.

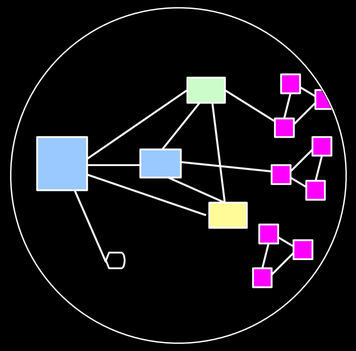
Legacy Systems



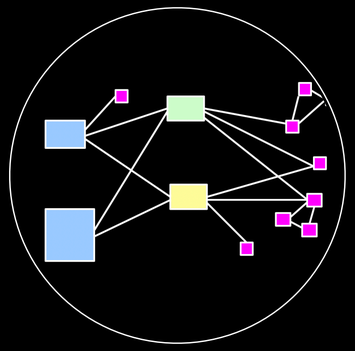
Mainframe Era



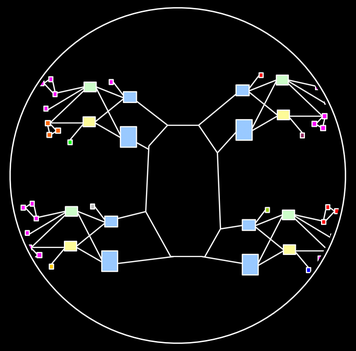
Minicomputer Era



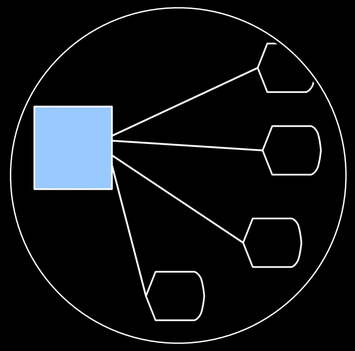
Distributed/PC Era



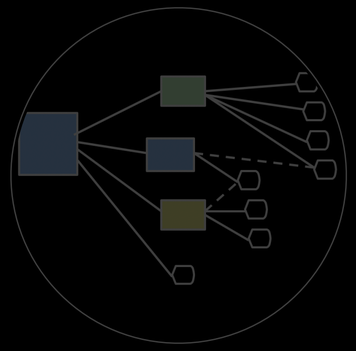
Client-server Era



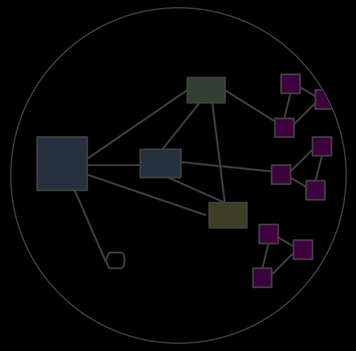
Networked Era



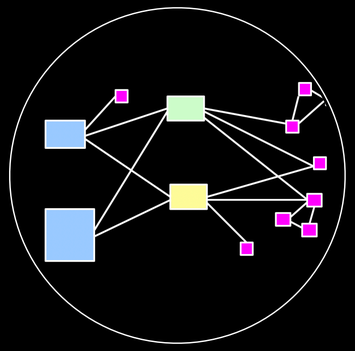
Mainframe Era



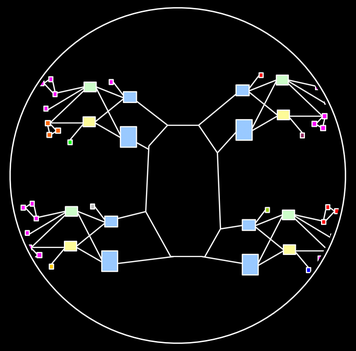
Minicomputer Era



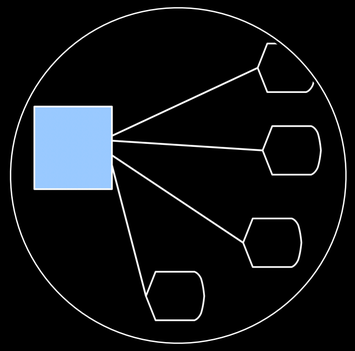
Distributed/PC Era



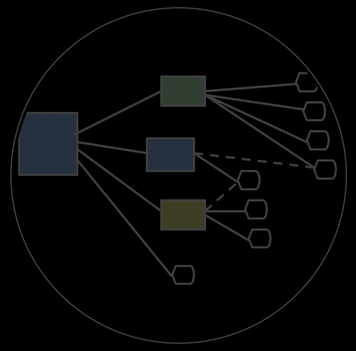
Client-server Era



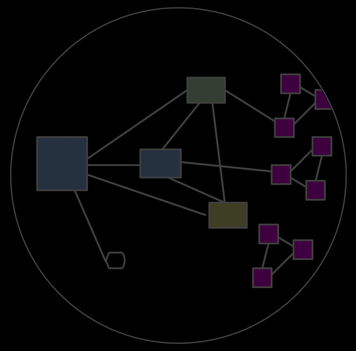
Networked Era



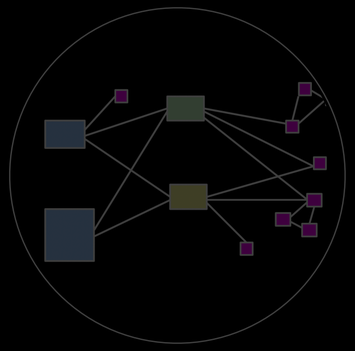
Mainframe Era



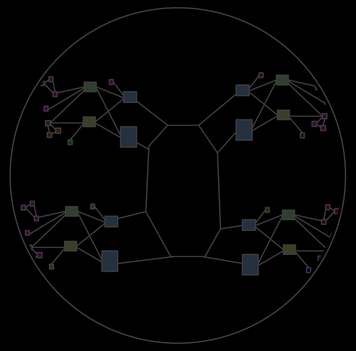
Minicomputer Era



Distributed/PC Era



Client-server Era



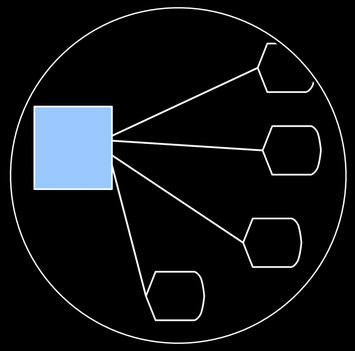
Networked Era

Semi-Automatic Business Research Environment (SABRE)

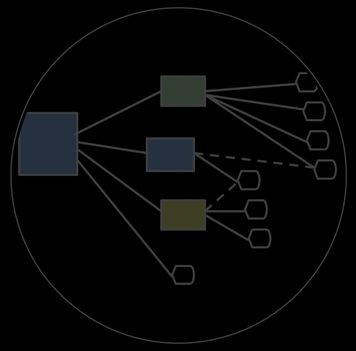
AMERICAN AIRLINES

SABRE

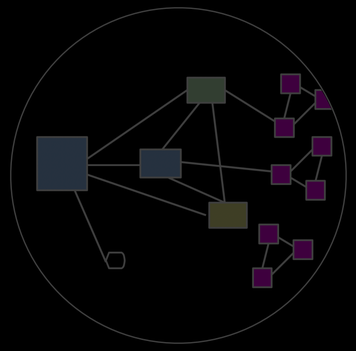
Reservation System by IBM



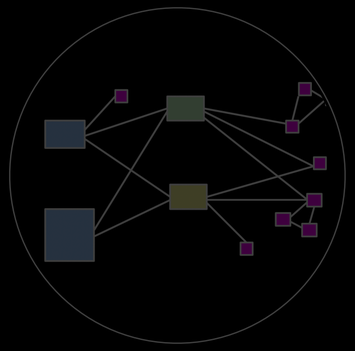
Mainframe Era



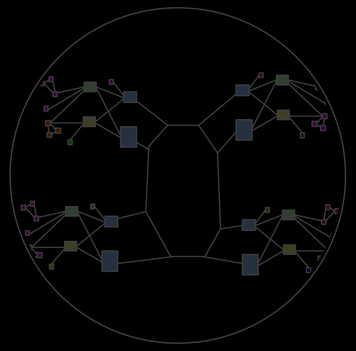
Minicomputer Era



Distributed/PC Era



Client-server Era



Networked Era

Strengths
Mainframe Era

- **Dumb terminals** have no sophisticated processing or capability
- Forces architects and developers to **restrict complexity to the mainframe**, potentially making it easier to secure
- **Limited user interface** with very limited command driven approach and based on users
- These strengths provided some relief but **there are still problems.**

Concerns

Mainframe Era

- Primary security concern during the period was the **physical connection** between mainframe and terminal.
- Software developers are unlikely to have spent energy considering **security at the application level**.
- Several **assumptions would have been made** by architects, system programmers and application developers.
- Focus was not so much security but the challenge of distributing resources among the enterprise.

Access Control

Mainframe Era

- **Authentication is handled by the mainframe** rather than the dumb terminal.
- **Credentials may be sent over the network** in the clear, susceptible to observation from a third-party.
- **File and resource access may be with fine-grained granular** access based on user identification.
- Specific concerns with such access is that privileges of a particular individual may **not be properly maintained by the human element**.

Access Control

Mainframe Era

- **Access control logic may be handled by the operating system** or application.
- Compromising access control logic may allow attackers access to restricted functions and data.
- Access control logic is often targeted by attackers attempting to utilise vulnerabilities.
- Strengthening such logic can be challenging, especially if staff no longer have knowledge of how it operates.

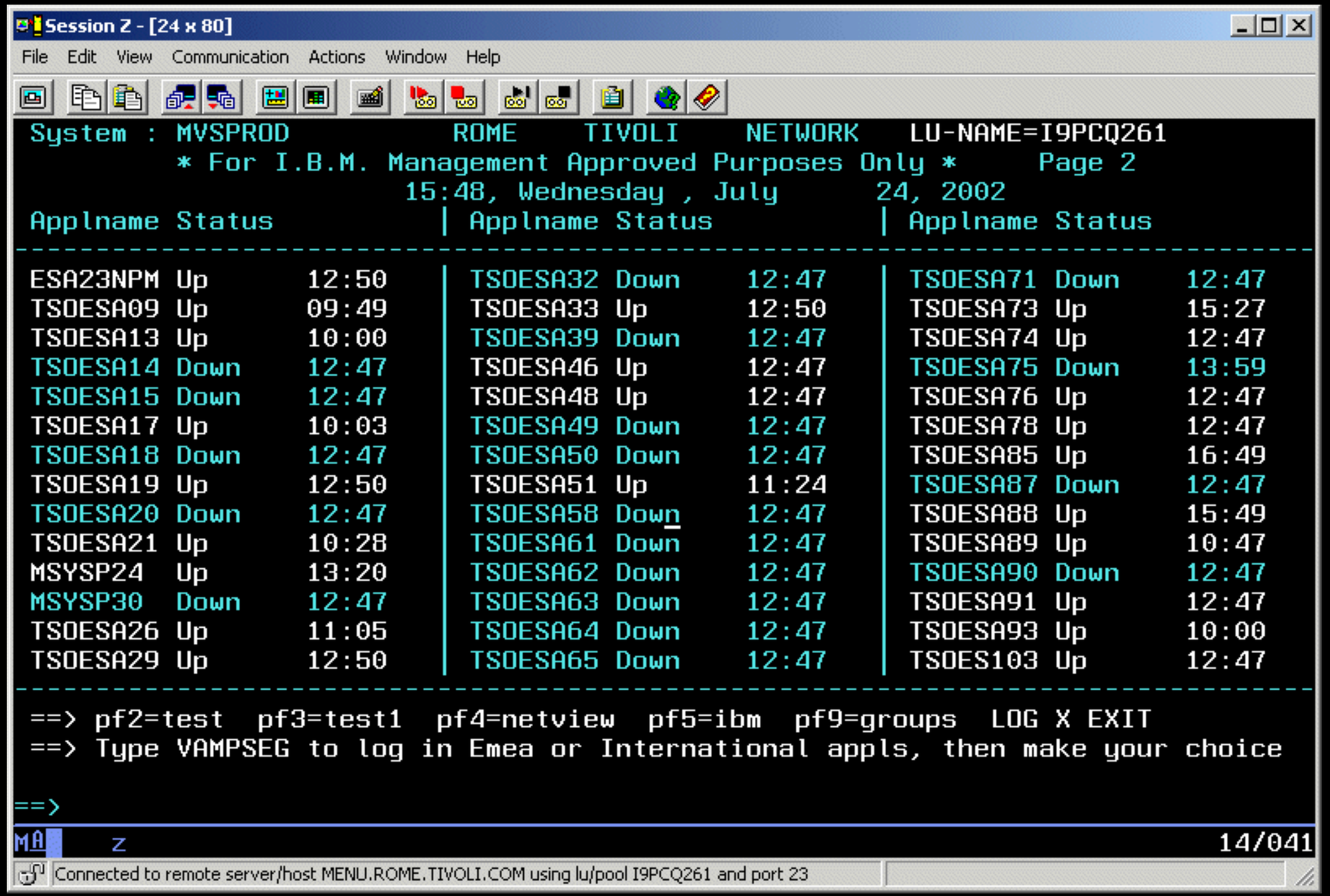
Input Validation

- **Local validation is often non-existent** on dumb terminals, but some legacy mainframe application may assume expected data.
- Developers must ensure that **extreme, expected and unexpected data cases** are properly handled.
- Unanticipated cases could result in system failures that could be utilised by attackers.
- Software developers need to process the stream of characters.

Screen Scraping

Mainframe Era

- Enterprises are motivated to ensure time and money invested in legacy mainframe applications are accessible.
- Mainframe applications can be accessed using terminal emulation on different display architecture.
- Individuals can use green screen applications on modern day systems.
- IBM 3270 is common dumb terminal example, that can be used to access applications on IBM mainframes.

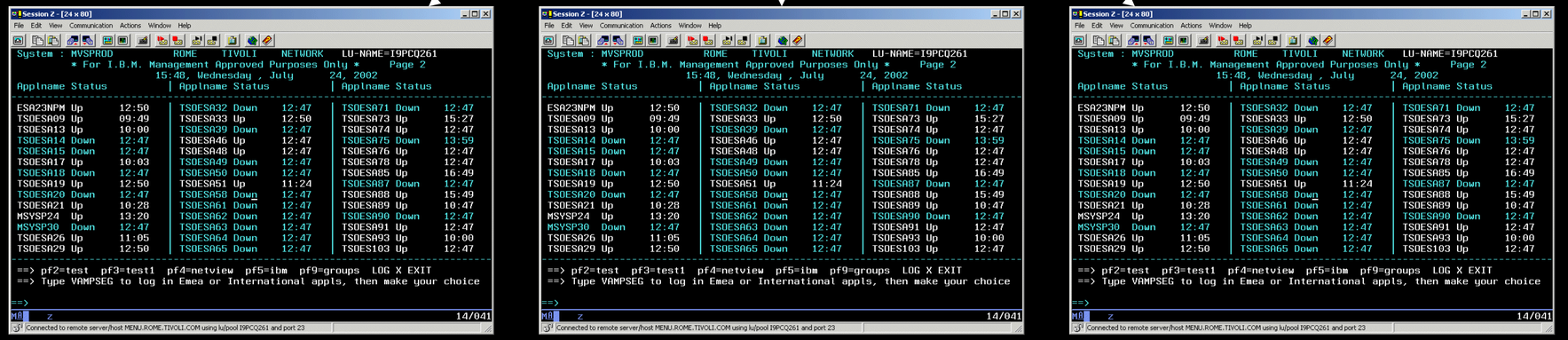

Session Z - [24 x 80]
File Edit View Communication Actions Window Help
System : MVSPROD ROME TIVOLI NETWORK LU-NAME=I9PCQ261
* For I.B.M. Management Approved Purposes Only * Page 2
15:48, Wednesday , July 24, 2002
Applname Status | Applname Status | Applname Status
ESA23NPM Up 12:50 | TSOESA32 Down 12:47 | TSOESA71 Down 12:47
TSOESA09 Up 09:49 | TSOESA33 Up 12:50 | TSOESA73 Up 15:27
TSOESA13 Up 10:00 | TSOESA39 Down 12:47 | TSOESA74 Up 12:47
TSOESA14 Down 12:47 | TSOESA46 Up 12:47 | TSOESA75 Down 13:59
TSOESA15 Down 12:47 | TSOESA48 Up 12:47 | TSOESA76 Up 12:47
TSOESA17 Up 10:03 | TSOESA49 Down 12:47 | TSOESA78 Up 12:47
TSOESA18 Down 12:47 | TSOESA50 Down 12:47 | TSOESA85 Up 16:49
TSOESA19 Up 12:50 | TSOESA51 Up 11:24 | TSOESA87 Down 12:47
TSOESA20 Down 12:47 | TSOESA58 Down 12:47 | TSOESA88 Up 15:49
TSOESA21 Up 10:28 | TSOESA61 Down 12:47 | TSOESA89 Up 10:47
MSYSP24 Up 13:20 | TSOESA62 Down 12:47 | TSOESA90 Down 12:47
MSYSP30 Down 12:47 | TSOESA63 Down 12:47 | TSOESA91 Up 12:47
TSOESA26 Up 11:05 | TSOESA64 Down 12:47 | TSOESA93 Up 10:00
TSOESA29 Up 12:50 | TSOESA65 Down 12:47 | TSOES103 Up 12:47
==> pf2=test pf3=test1 pf4=netview pf5=ibm pf9=groups LOG X EXIT
==> Type VAMPSEG to log in Emea or International appls, then make your choice
==>
MA Z 14/041
Connected to remote server/host MENU.ROME.TIVOLI.COM using lu/pool I9PCQ261 and port 23

Screen Scraping

Mainframe Era

Legacy Mainframe

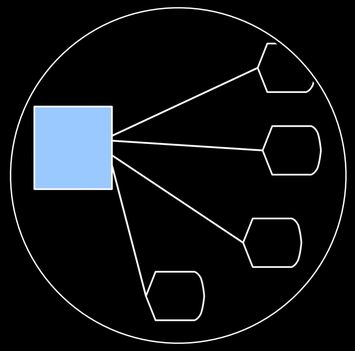
Terminal Emulation Server



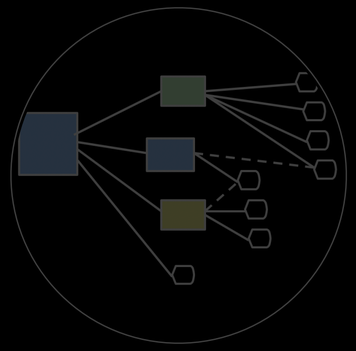
Screen Scraping

Mainframe Era

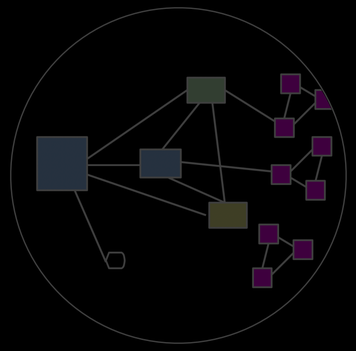
- Attackers can potentially compromise systems designed to support emulation.
- IBM 3270 terminal can limit values entered into specific fields as well as the length of input string length.
- An attacker can potentially circumvent any legacy application that assumes that input has been validated in this way.



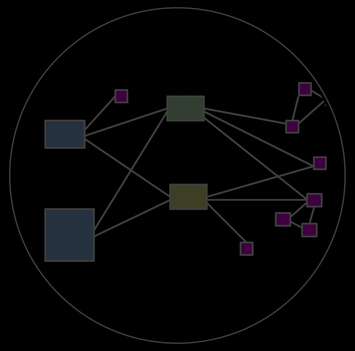
Mainframe Era



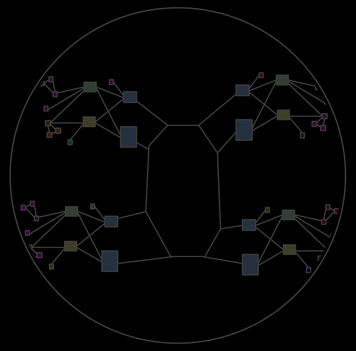
Minicomputer Era



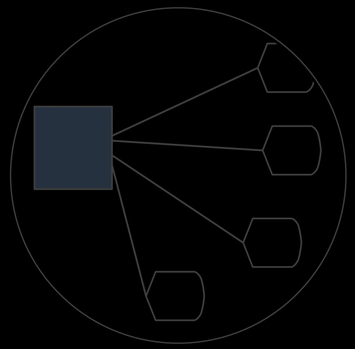
Distributed/PC Era



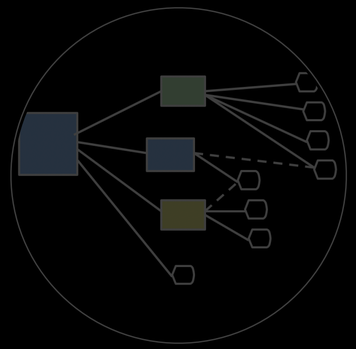
Client-server Era



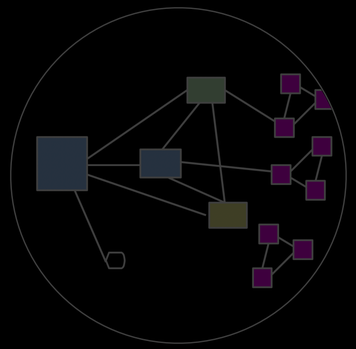
Networked Era



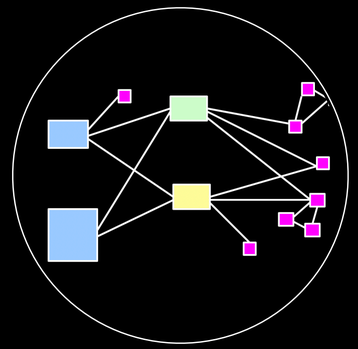
Mainframe Era



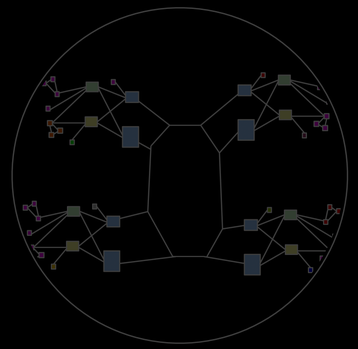
Minicomputer Era



Distributed/PC Era



Client-server Era



Networked Era

Strengths

Client-server Era

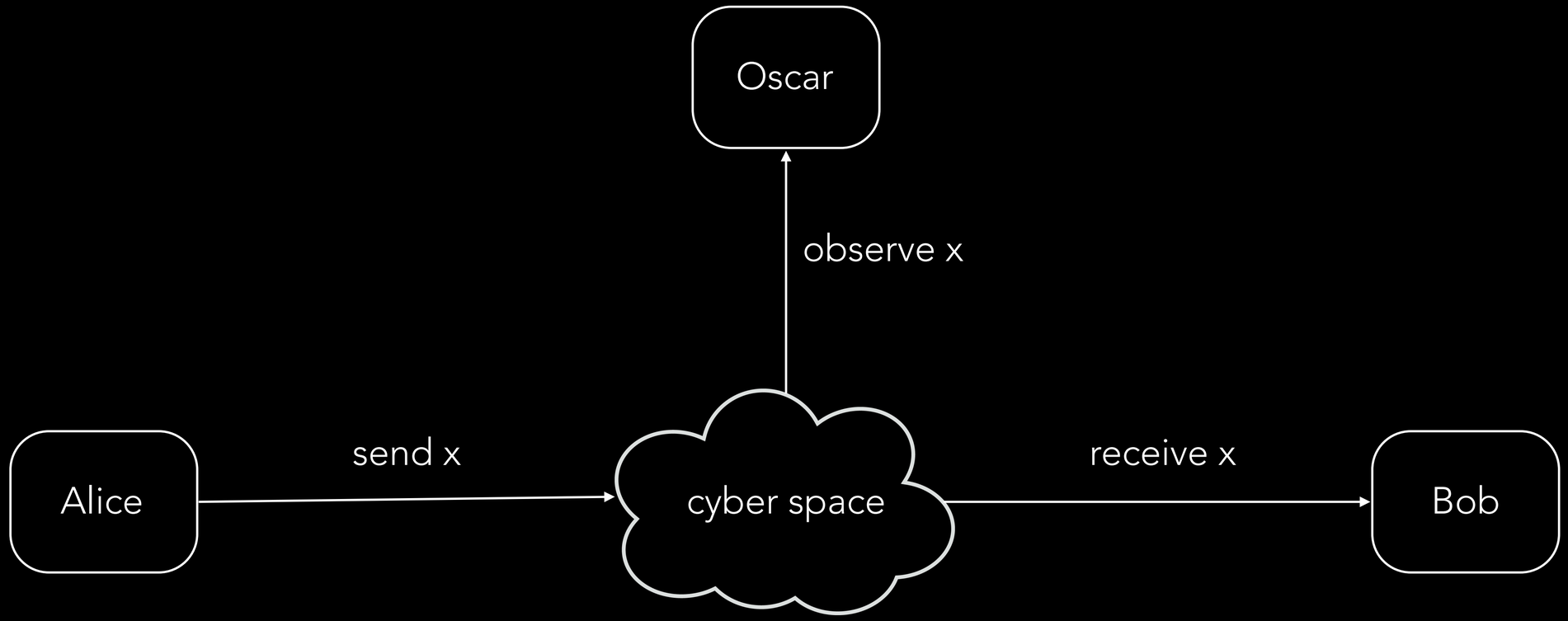
- Clients are sophisticated and support more functionality between elements.
- Encryption is possible on the client, affording secure communication between client and service.
- Potentially more can done on the client itself, reducing demands on the network.

Insecure communication

Legacy systems

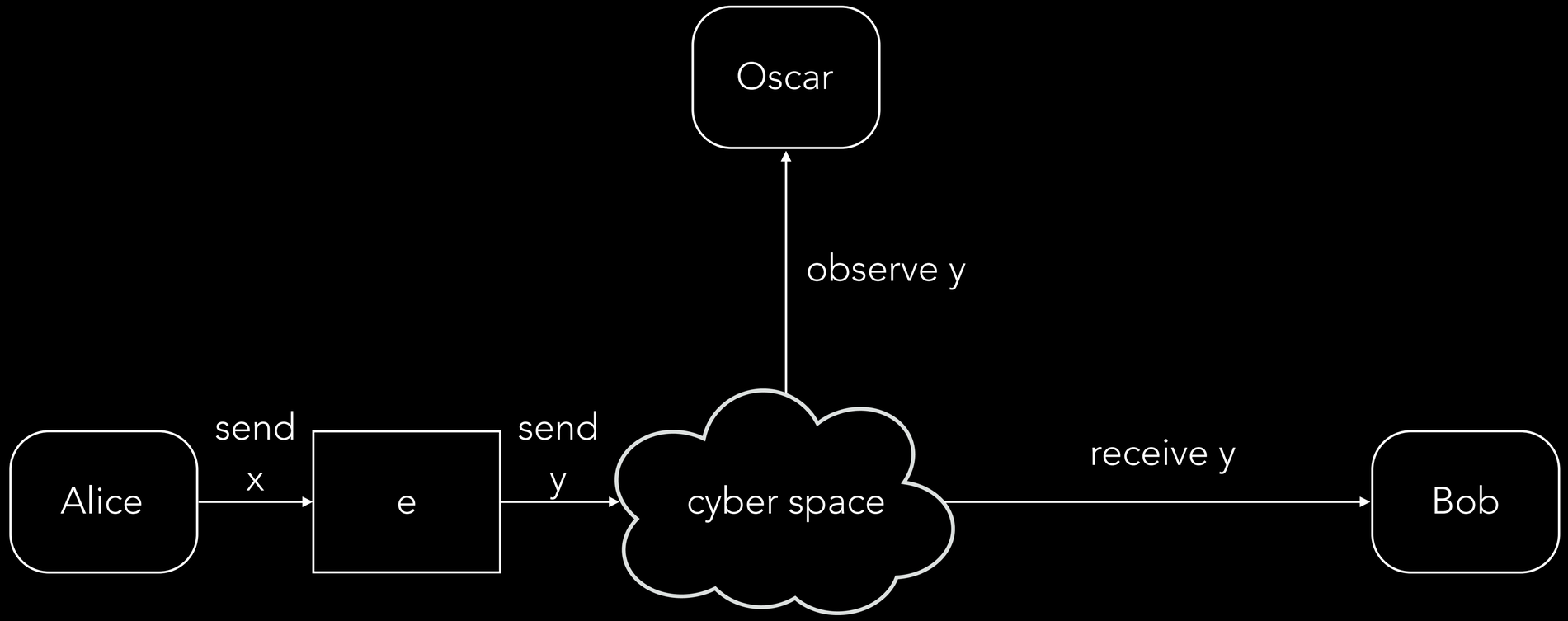
Insecure communication

Legacy systems



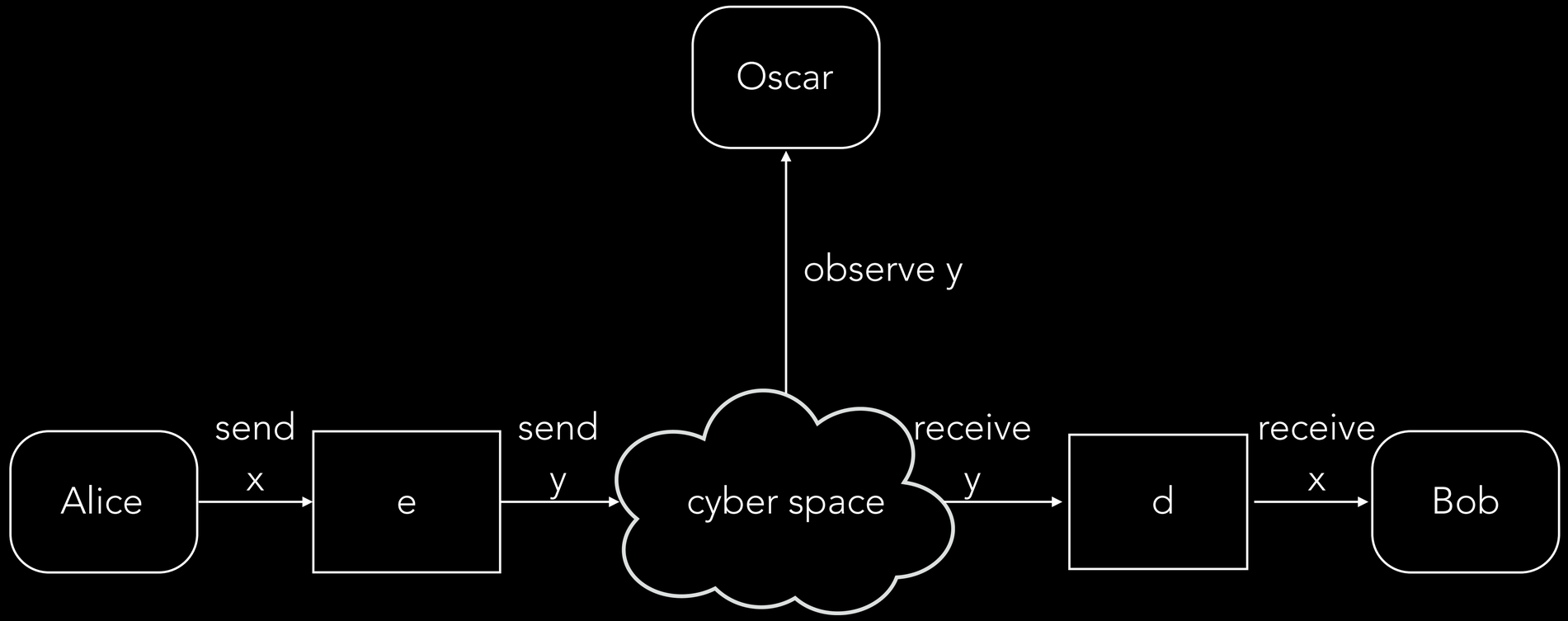
Insecure communication

Legacy systems



Insecure communication

Legacy systems



Concerns

Client-server Era

- Complexity ensures the architecture becomes a ballet between elements.
- Significant expense in terms of initial investment and maintenance.
- Ideally, an attacker should gain no real insight by gaining accessing to a client.
- Potentially poor visibility in terms of what actions and data is residing on the client.

Concerns

Client-server Era

- Network-level connection to server become the primary concern within client-server architecture.
- Concerns that an attacker may gain access to the network beyond the perimeter of the enterprise.
- Client should be dumb, containing no sensitive data or specialised processing.
- Sophisticated clients afford developers opportunity to compensate with slow network connections.

Client Software

Client-server Era

- Attackers can gain considerable insight into an enterprise and architecture through client software.
- Attackers understanding the data and systems by decompiling and analysing client software.
- Distribution of the client software represents a significant challenge for enterprises.
- Concerns that some clients may execute older versions of the client software.

Client Software

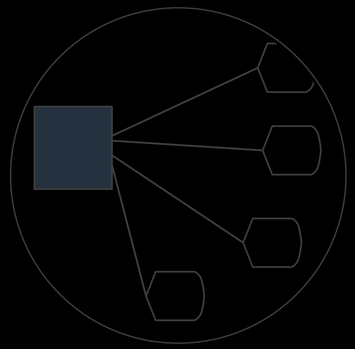
Client-server Era

- Distribution of client software can be handled automatically using various mechanisms.
- Concerns that attackers can compromise such mechanisms and insert their own variant of client software.
- Alternative attacker variant of client software can provide insight into the operation of individual users.
- Also affords the attacker an understanding of the system itself and the purpose of each business unit.

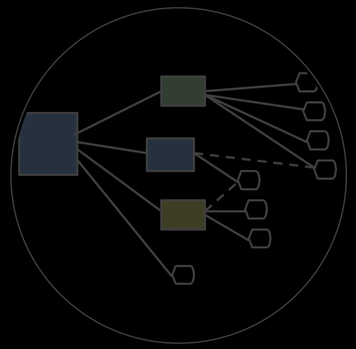
Client Software

Client-server Era

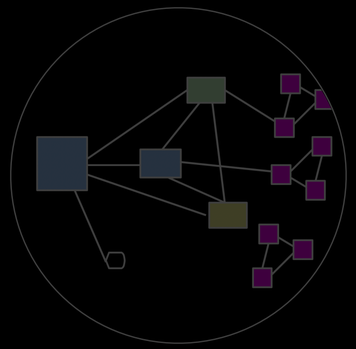
- Server support for client software is also a concern as enterprises may not operate on the same version.
- Server can support backwards compatibility to earlier versions of client software.
- Communicating vulnerabilities of client software is difficulty while supporting backwards compatibility.
- Attacker can use earlier, vulnerable version of client software to gain access to server.



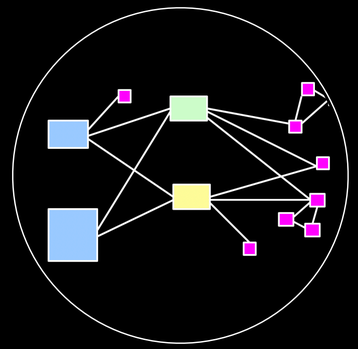
Mainframe Era



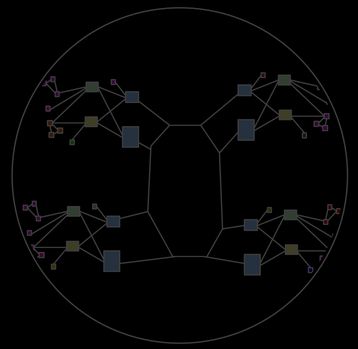
Minicomputer Era



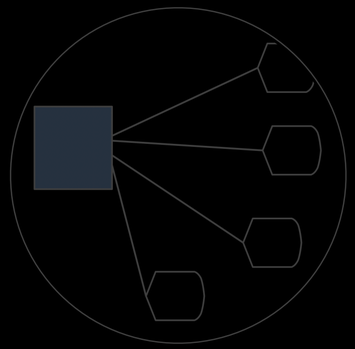
Distributed/PC Era



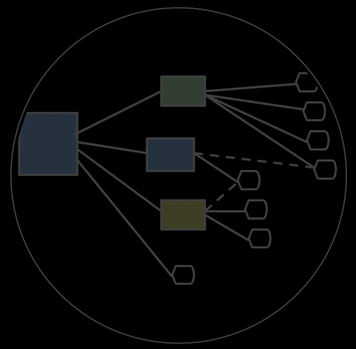
Client-server Era



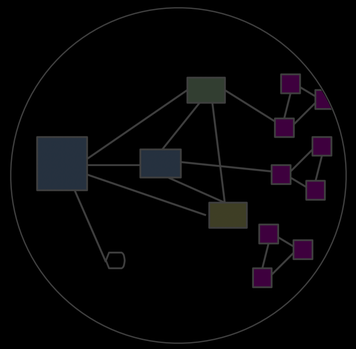
Networked Era



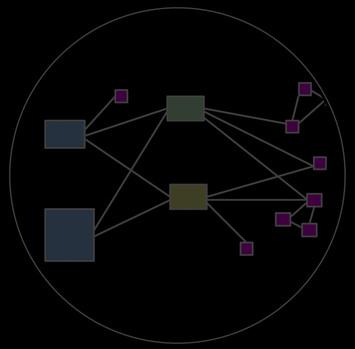
Mainframe Era



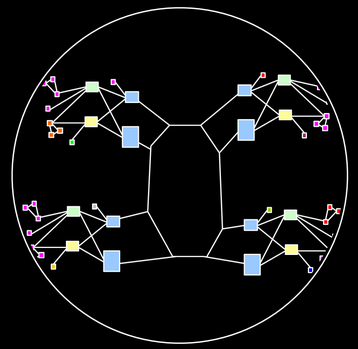
Minicomputer Era



Distributed/PC Era



Client-server Era

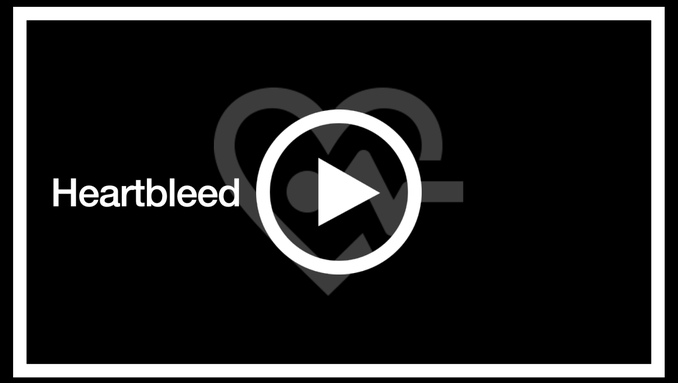


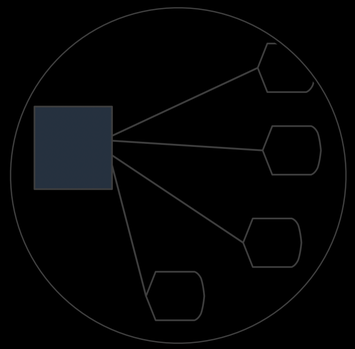
Networked Era

Concerns

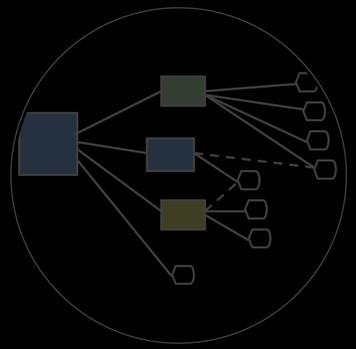
Networked Era

- Physical constraints are limited and focus must become logical isolation.
- Attackers seek to remain anonymous to ensure they can use system uninterrupted, e.g anonymous proxy.
- Inputs must be validated to reduce likelihood of SQL injection and other such attacks.
- Vulnerabilities will depend on the implementation of the server-side technology, e.g. framework vs. bespoke.

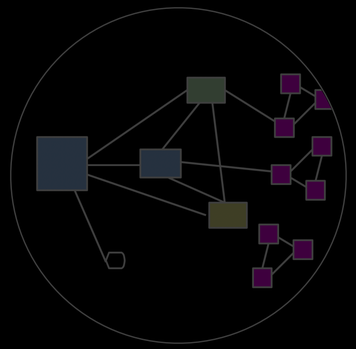

Heartbleed



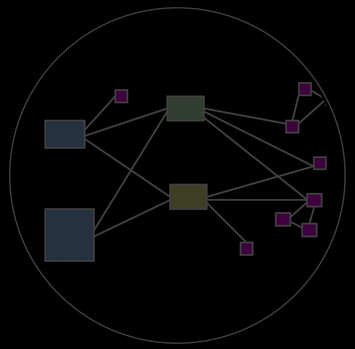
Mainframe Era



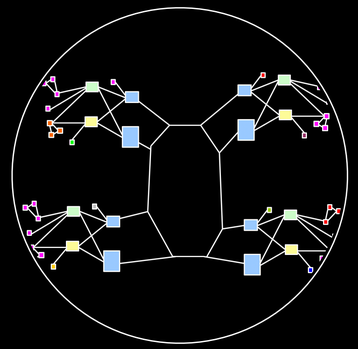
Minicomputer Era



Distributed/PC Era



Client-server Era



Networked Era

Legacy Systems

Enterprise Cyber Security