ENTERPRISE CYBER SECURITY

LEGACY SYSTEMS

University of Glasgow

OVERVIEW

- defining and understanding the types of legacy system.
- understanding potential cyber security concerns related to legacy systems.
- evolving legacy systems to ensure they do not represent significant risk to enterprise.

LEGACY SYSTEMS

LEGACY SYSTEMS

- 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- typically they are sprawling, complex, isolated systems and **considered outdated by modern standards**.

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.

- legacy systems are only **interesting because enterprises rely** on and utilise them.

- they often represent a **significant investment** in terms of time and money.

LEGACY SYSTEMS

- 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.

LEGACY SYSTEMS

- contain **business critical information** that represent considerable business knowledge and processes.

- **poorly documented**, rarely understood widely and are often inaccessible to the larger system.

- critical to business but often poorly understood, **interfering with legacy systems can have significant consequences**.

“The biggest vulnerabilities faced by the banking industry resides within the use of legacy systems that run outdated software, yet these systems are still critical to the performance of daily business operations.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

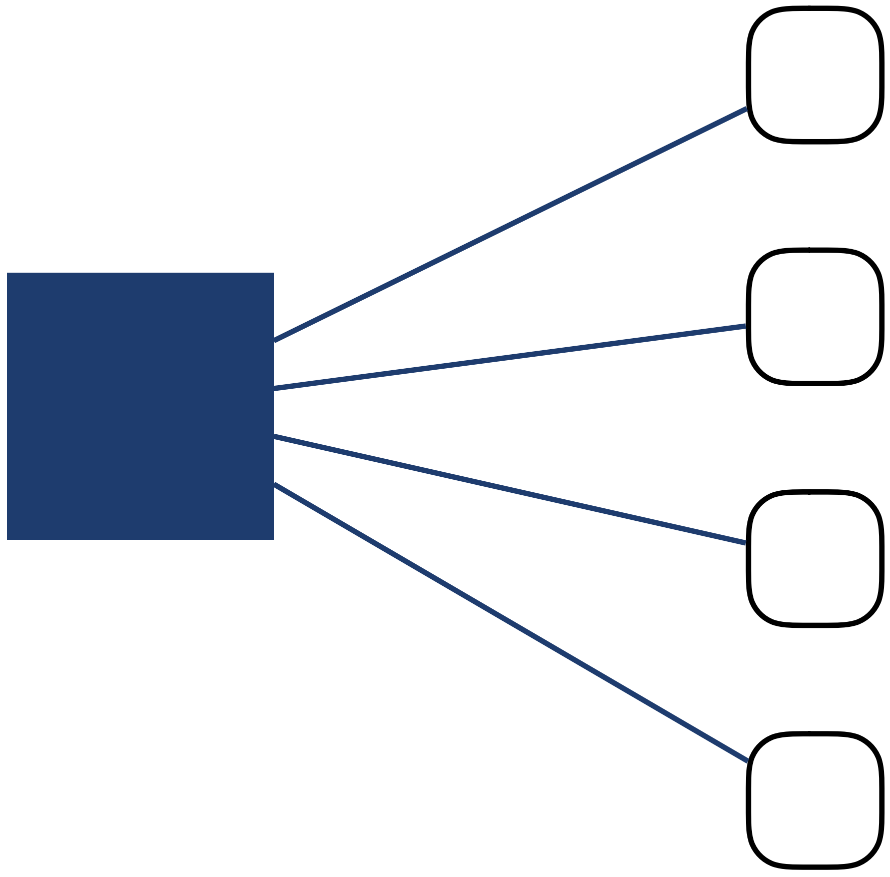
DILEMMA

- 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.

MAINFRAME ERA (1950S-70S)



SABRE AIRLINE RESERVATION SYSTEM

- Semi-automated Business Research Environment was developed between IBM and American Airlines.

- IBM used a defence research project, Semi-automated Ground Environment (SAGE) as the basis of the new research system.

- SAGE was an earlier, connected, electronic brain used to defend against Soviet attack.

SABRE AIRLINE RESERVATION SYSTEM

- SAGE was used to coordinate information coming from radar sites and redirect it to inceptors.

- teleprinters would produce information coming from various sites and then subsequent commands would be sent to teleprinters in inceptor bases.

- IBM and American Airlines felt the technology used to defend against Soviet attacks could be used to reserve seats.

- research system was developed (~$350,000,000) and by the 1970s, IBM was offering the fully developed system to several airlines.

STRENGTHS

- 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
- this provides some relief but does not mean there are not problems.

CONCERNS

- 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 is on the challenge of distributing resources among the enterprise.

ACCESS CONTROL

- 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.

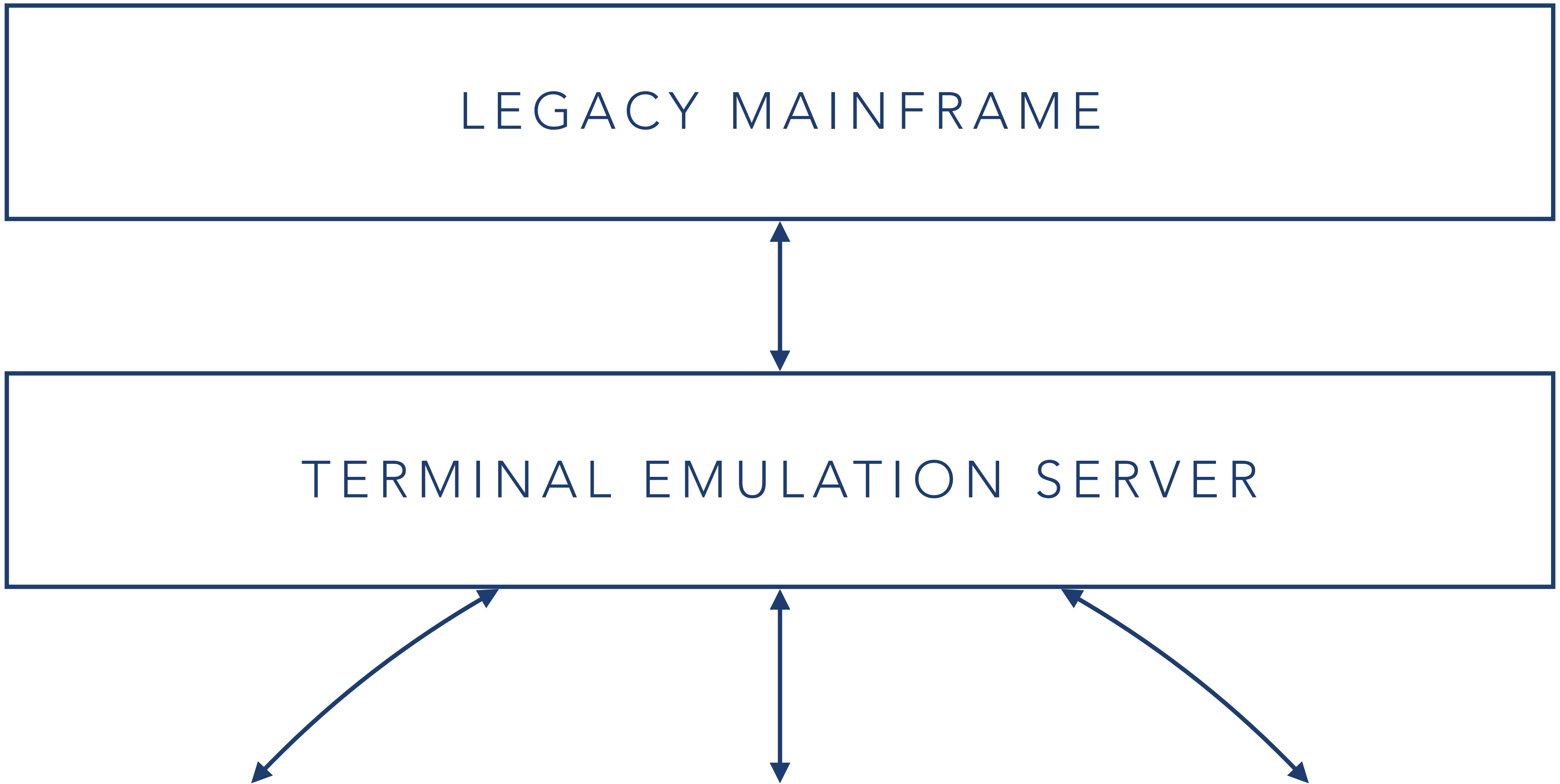
ACCESS CONTROL

- 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

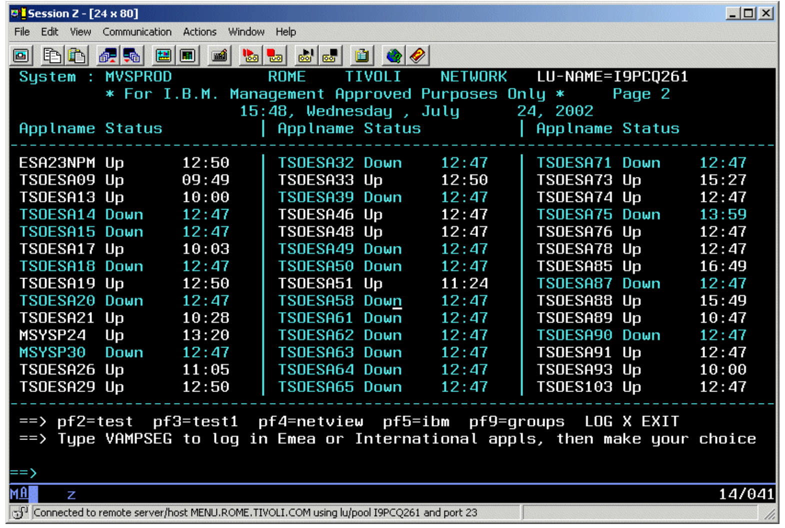
- local validation is often non-existent on dumb terminals, but some legacy mainframe application may assume expected data.
- developers must ensure that extreme, expected and unexpected data cases are properly handled.
- unanticipated cases could result in system failures that could be utilised by attackers.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

SCREEN SCRAPING



LEGACY MAINFRAME

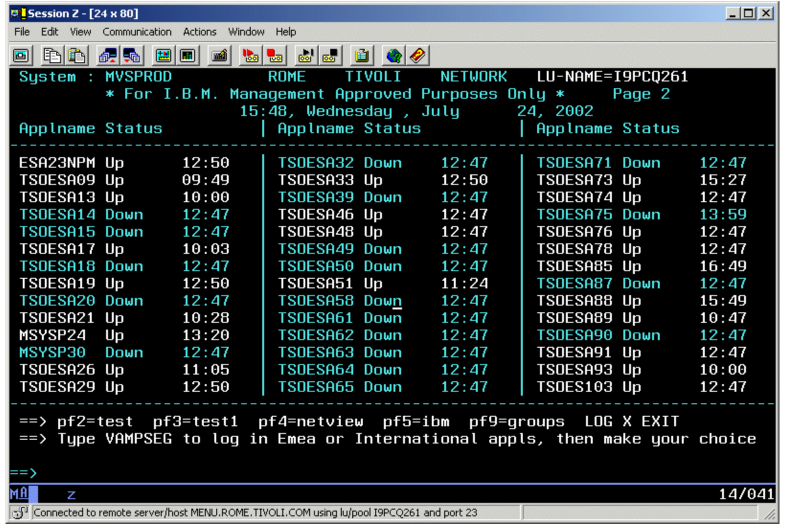
TERMINAL EMULATION SERVER



```
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

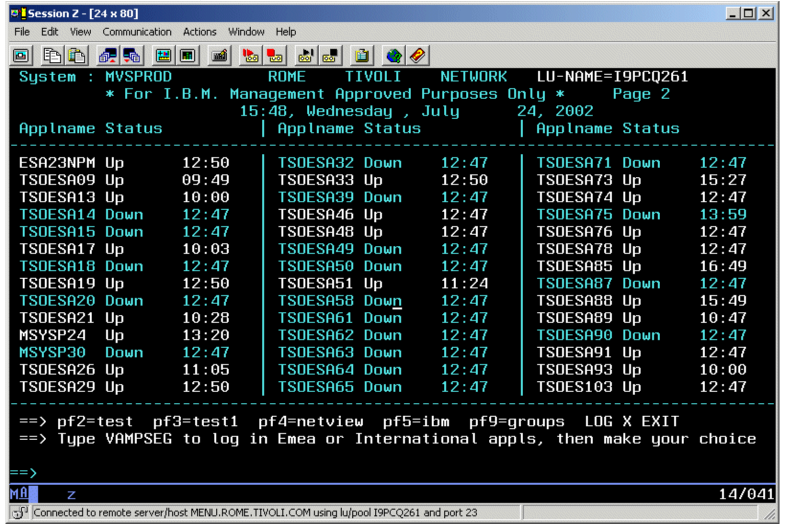


Session Z - [24 x 80]
File Edit View Communication Actions Window Help

```
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



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

- 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.

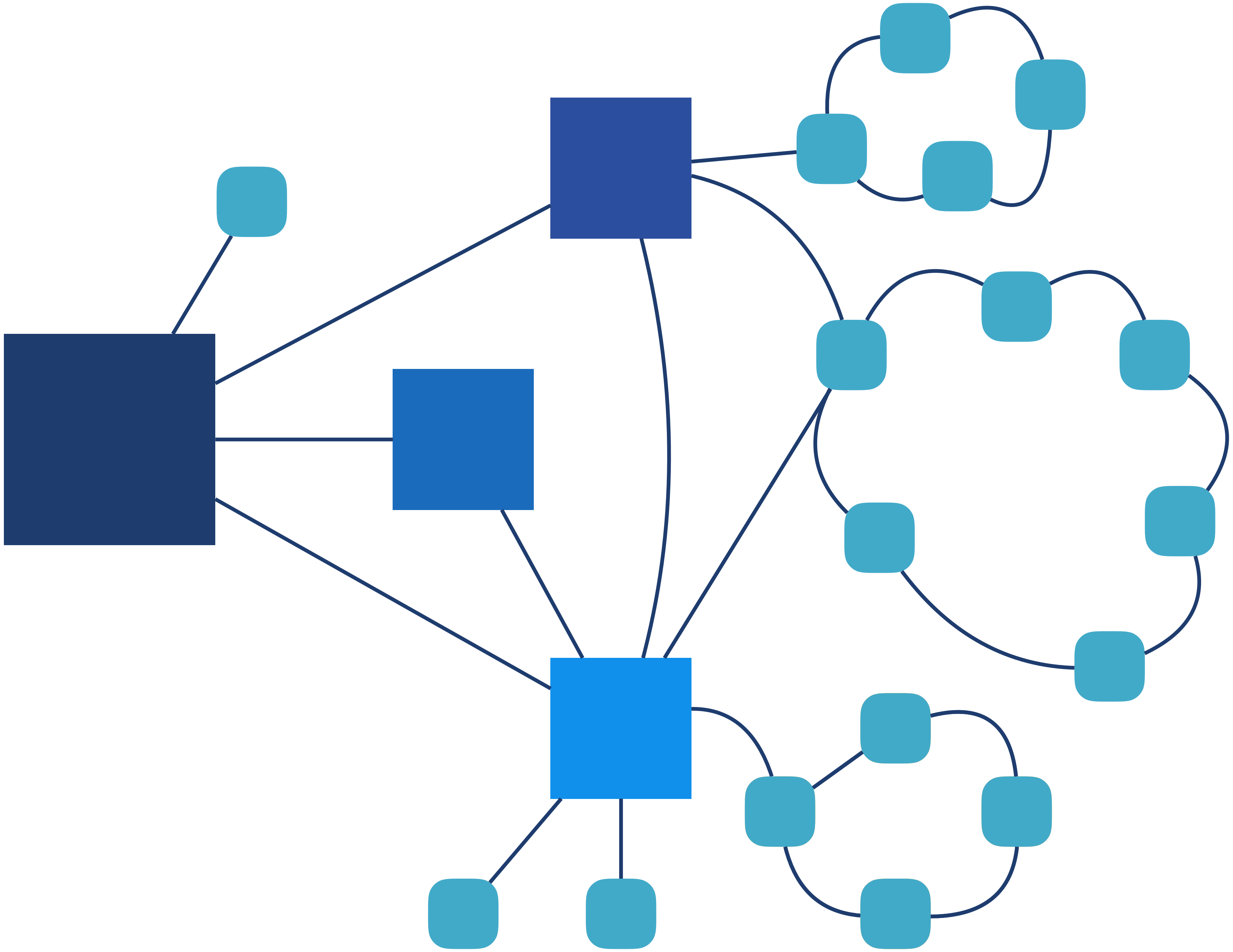
SCREEN SCRAPING

- 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.

CLIENT-SERVER ERA (1990S)



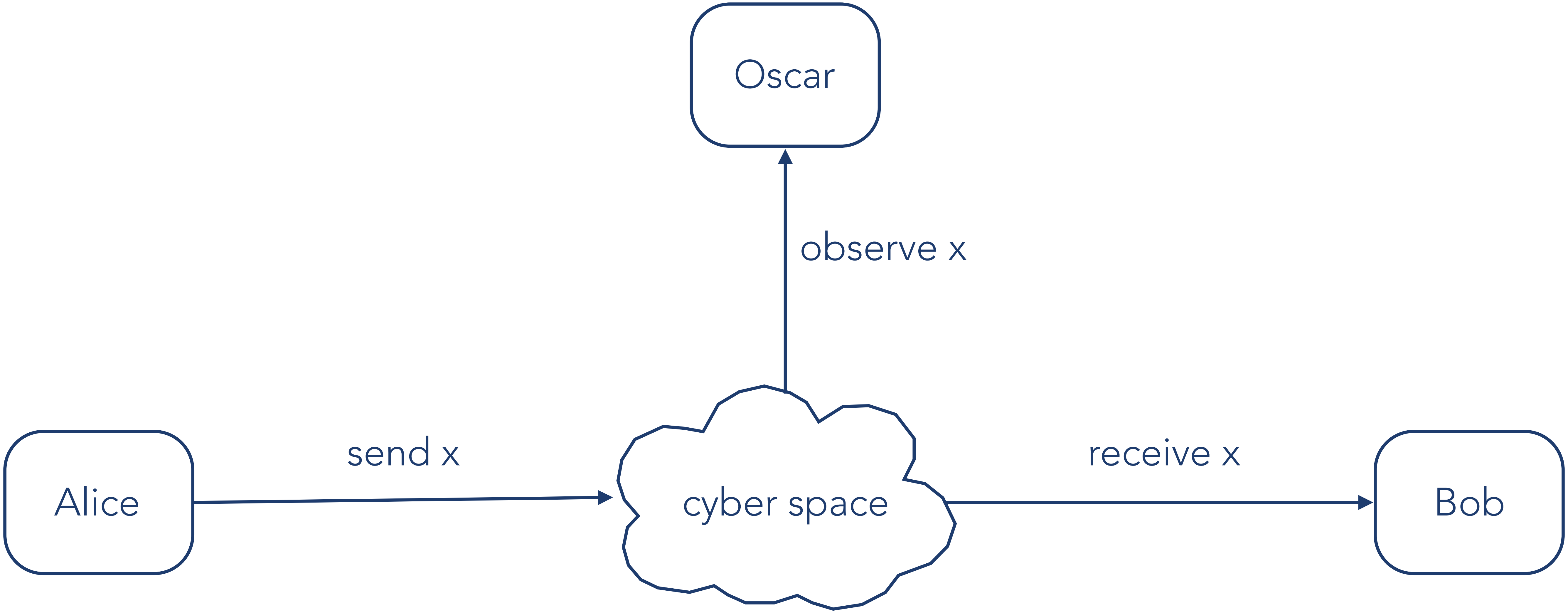
STRENGTHS

- clients are sophisticated and support more functionality between elements.

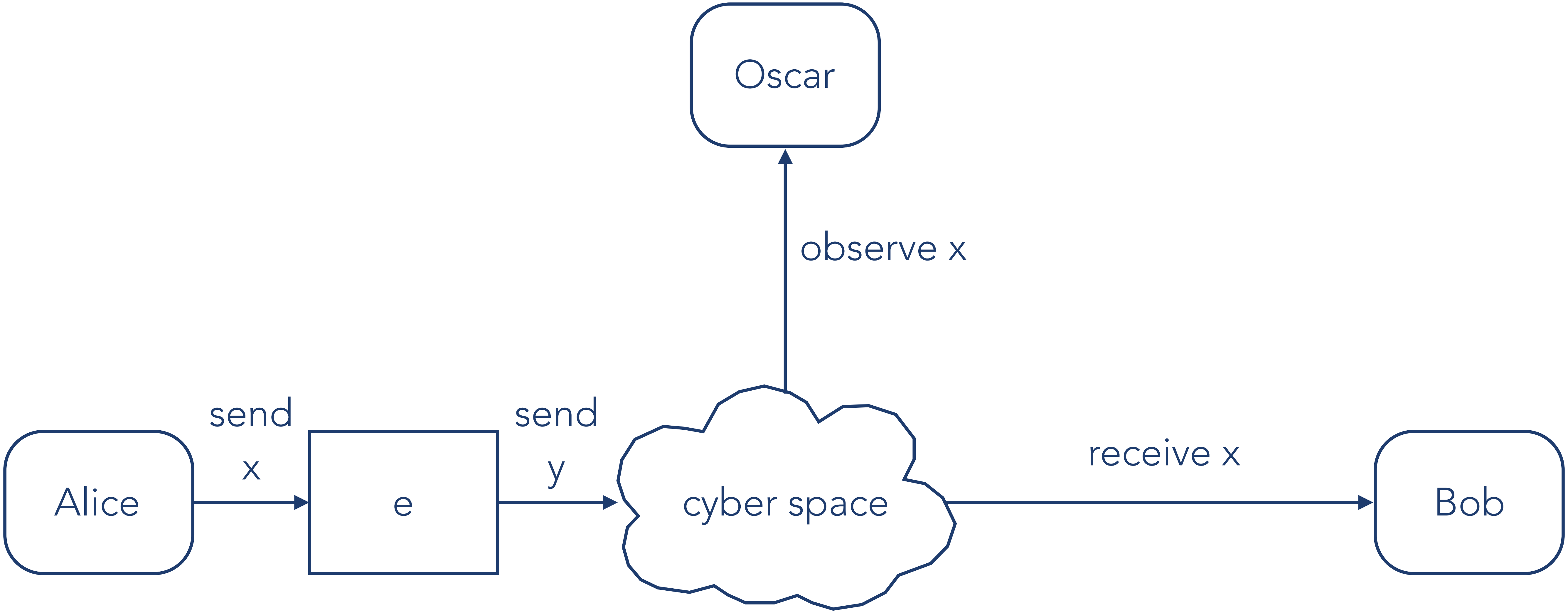
- encryption is possible on the client, affording secure communication between client and service.

- potentially more can done on the client itself, reducing demands on the network.

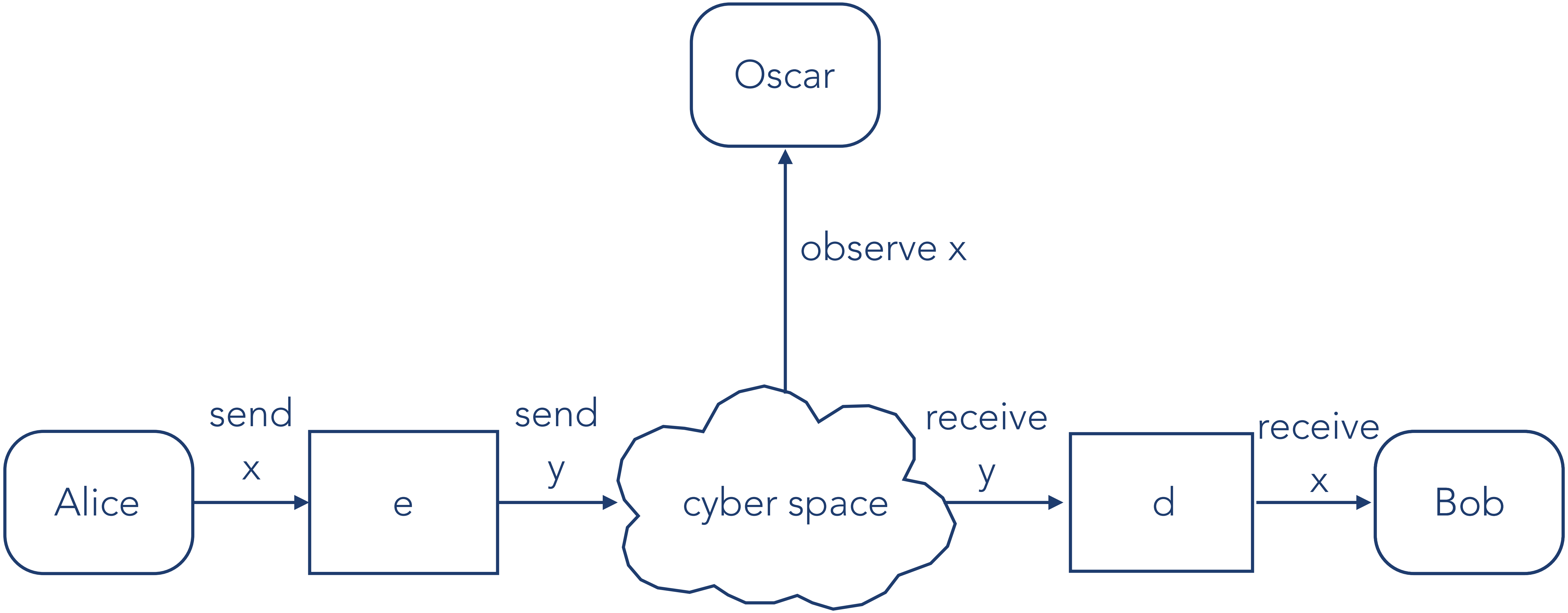
INSECURE COMMUNICATION



INSECURE COMMUNICATION



INSECURE COMMUNICATION



CONCERNS

- 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

- 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.
- clients should be dumb, containing no sensitive data or specialised processing.
- sophisticated clients afford developers opportunity to compensate with slow network connections.

CLIENT SOFTWARE

- 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

- 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

- 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.

DATABASE

- attackers have little motivation to terminate a client within the enterprise system.
- crashing central database server has high motivation, as it can undermine several clients.
- also need to consider configuration and data stored on client.
- how are database access credentials stored and managed on the client?

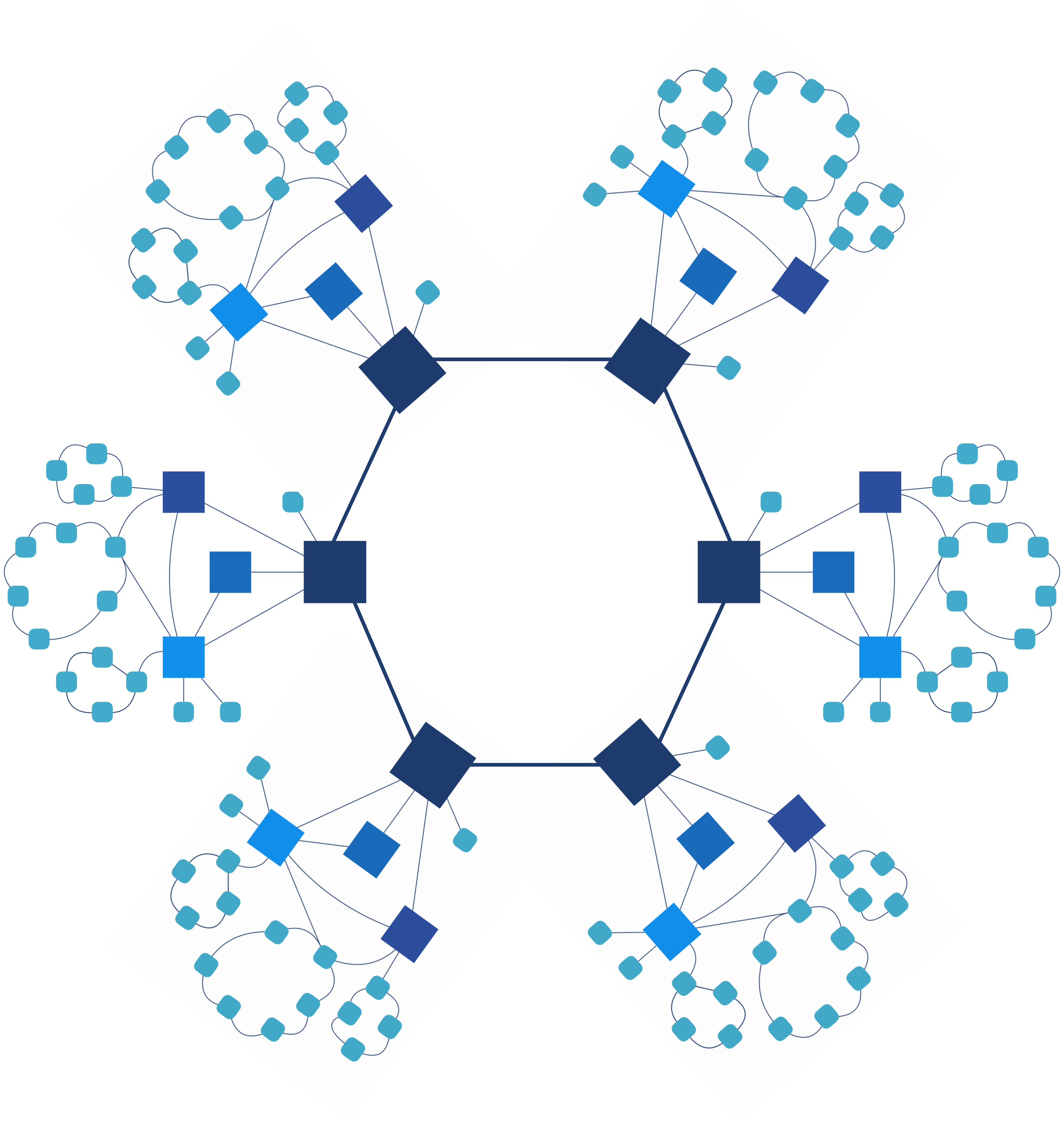
SESSIONS

- sessions are considered a conversation between the client and server.
- starting such conversations is expensive in terms of time and resources.
- application initiate session with the server and leaves it open.
- attackers can masquerade as the legitimate client to gain access to server function and data.

TRANSACTIONS

- database interactions are typically transaction-based with clients.
- transaction should be committed swiftly and not remain open.
- non-committed transactions result in rollback to the previous state.
- attackers are motivated to interfere with transmission at opportune moments to ensure integrity is undermined.

NETWORK ERA (2000S)



CONCERNS

- 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 suck attacks.
- vulnerabilities will **depend on the implementation** of the server-side technology, e.g. framework vs. bespoke.

EVOLVING LEGACY SYSTEMS

SABRE EVOLVES

- legacy system prioritised seat availability over all other functions.
- information pertaining to departures, meal upgrades or even maintenance request were very slow - couple with the increase of users.
- Sabre outsourced operations ~$2.2 billion to an external organisation and sold-off legacy assets $778,000,000.
- primary concern is not cyber security but the concern of rebel business units losing independence.

EVOLVING LEGACY SYSTEMS

- create an **inventory** of the legacy systems that exist within the enterprise.
- prioritise and **identify high-risk legacy systems** to the enterprise.
- **assess** identified legacy system to determine the actual level risk.
- **define** and develop plans to evolve high-risk legacy systems.

INVENTORY

- essentially list all the legacy systems that are accessible to individuals and other systems.
- creating an inventory appears trivial but can be complex, due to some systems simply going out of use.
- similarly, some systems may be masked by modern systems but are still in use.
- a solid foundation of legacy assessment is based from a complete inventory.

INVENTORY

- observe the system to understand and determine the actual purpose of the legacy system.
- research development history and understand inception, design and implementation decisions.
- determine the type of legacy system, relevant knowledgable staff and the sensitive data as well as functions it provides and processes.
- understand accessibility of the legacy system, i.e. open to public access, specific staff etc.

IDENTIFICATION

- determine the importance of the legacy subsystem to the overall enterprise system.

- investigate the implementation and design approach adopted, understand the common vulnerabilities for any associated platform.

- understand the development cycle of the legacy system.

- systems are frequently developed over several years that may lack the discipline of the original implementation.

IDENTIFICATION

- testing approach and how security was considered during implementation.
- type of data and the level of sensitivity, the legacy systems may be processing medical material or credit card numbers.
- accessibility of the system in terms of employees as well as connections to external systems.

PRIORITISING

- verify purpose of the legacy system and information related to its development.
- perform thorough analysis of the legacy system and understand the wider impact of the system to the enterprise.
- understand what risks the organisations is taking by relying on the legacy system.

EVOLVING

- enterprises may opt to handle any concerns with legacy systems by developing **policies**.
- legacy system can be **harden** against attackers by reducing vulnerabilities or wrapping some components.
- **enhancing** the legacy system by developing and integration new hardware and software.
- **replace** legacy system with alternative system to serve the needs of the enterprise.

HARDEN

- **address vulnerabilities** in the legacy system by improving software and wrapping components.
- **restrict scope** and remain focused on the specific concern.
- **costs** are difficult to define as may not be clear how many hours will be required to address the problems.
- difficult to position arguments for hardening as alternative to replacing as costs are difficult to estimate.
- software alterations can introduce further complications that could severely impact on the enterprise.

ENHANCE

- many of the concerns of hardening apply to enhancement.
- enhancement differs from hardening in that considerable software is generally added to the system.
- functionality of legacy system components can be reconsidered.
- enhancement affords the enterprise the option of retaining the significant investment of a legacy system.

REPLACE

- costs associated with hardening or enhancement may be as significant as replacement.
- security concerns are rarely significant enough to justify full replacement of a legacy system.
- transitioning between legacy systems and new system will require thought and considerable planning to minimise impact.

SUMMARY

- defining and understanding the types of legacy system.
- understanding potential cyber security concerns related to legacy systems.
- evolving legacy systems to ensure they do not represent significant risk to enterprise.