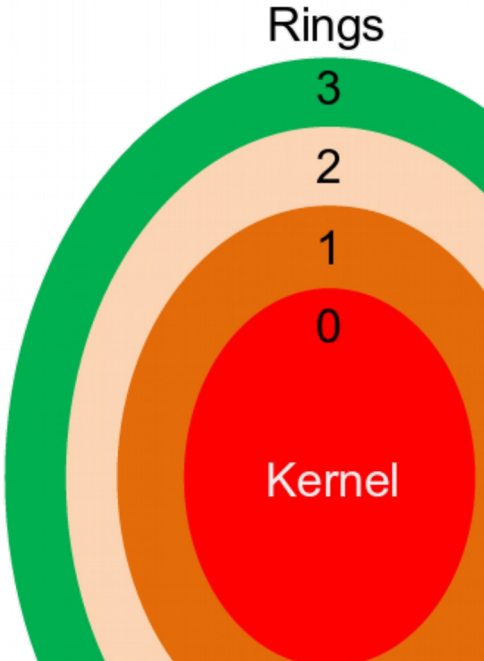
Information Technology
Security Evaluation
Criteria (ITSEC)

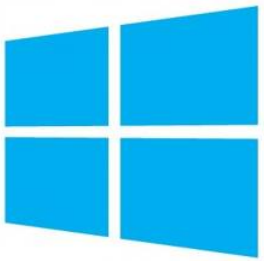
Security Architecture And Design



CISSP®
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Operating Systems and Security



CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Operating Systems and Security

- Many OS include some level of security.
- Security is based on the two ideas that give access to a number of resources
  - files on a local disk
  - privileged system calls
  - personal information about users
  - services offered by programs.
- The OS must distinguishing between authorised and non authorised requests.

Graphical user interfaces

- Most modern OSs contain a Graphical User Interface (GUI).
- Original Mac OS and Microsoft Windows tightly integrated the GUI to the kernel.
- Modern OSs are modular, separating the graphics subsystem from the kernel as is the case with GNU/Linux and Mac OS X.
- GNU/Linux / BSD UNIX
  - Options; X Windows System with a desktop environment
    - Gnome, KDE, Cinnamon, MATE, Xfce, LXDE, ...

Device drivers

- Specific software to allow OS and program interaction with hardware devices via specific computer bus or communications subsystem.
  - USB, Serial, SCSI, IDE/ATA, SAS, SATA, ...
- Provides commands to and/or receiving data from the device.
- OS specific.
- Enables the OS or applications to interact transparently with a hardware device.
- Provides interrupt handling.

Operating Systems

- **UNIX**
  - Sun Solaris, HP UX, SCO UNIX, BSD UNIX

- **Apple Macintosh OS X**

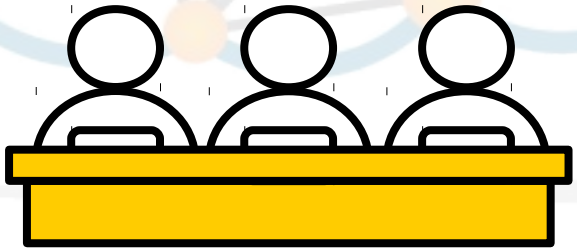
- **GNU/Linux**

- **Microsoft Windows**

Operating Systems

- Group exercise

- In your group discuss the Advantages and Disadvantages of each OS type;
  - UNIX
  - OS X
  - GNU/Linux
  - Microsoft Windows



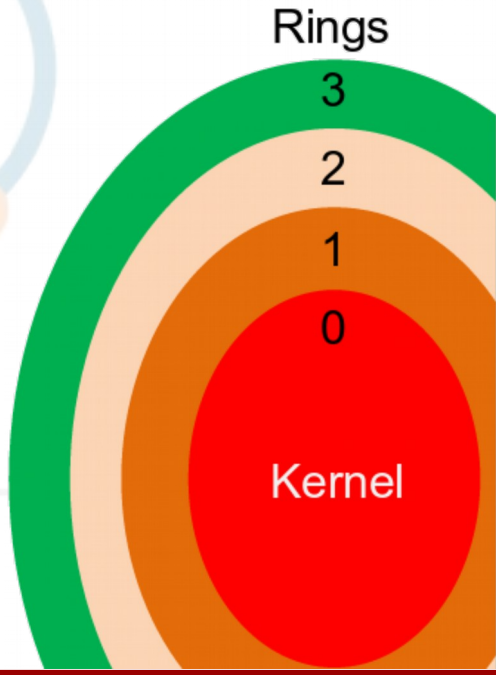
Execution Types

- **Multi-tasking**
  - Multiple processes, share common processing resources such as a CPU.
- **Multi-processing**
  - Multi-processing is the use of two or more CPUs within a single computer system.
- **Multi-programming**
  - This is similar to Multi-tasking and comes from an era where CPU time was expensive, and peripherals were very slow.
- **Multi-threading**
  - Multi-threading computers have hardware support to efficiently execute multiple threads.
  - Multi-threading aims to increase utilisation of a single core by leveraging thread-level as well as instruction-level parallelism.

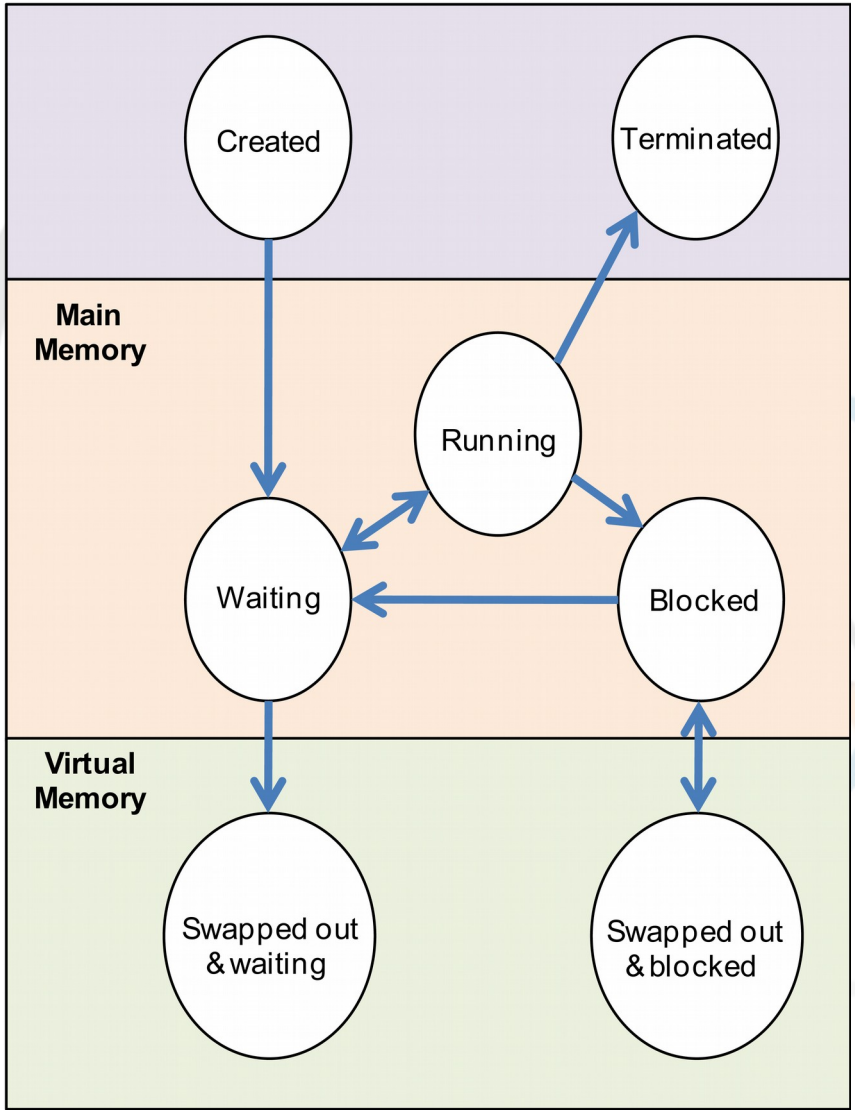
Protection Mechanisms

- Ring 0: OS Kernel / Memory
- Ring 1: Other OS components
- Ring 2: Drivers
- Ring 3: User-level programs and applications

- Rings 0 – 2 run in privileged mode
- Ring 3 runs in user mode



Process states



Security modes

- Information systems security modes of operations used in **Mandatory Access Control (MAC)** systems.
- The mode of operation is determined by:
  - **Type of users**
    - directly or indirectly accessing the system.
  - **Type of data**
    - including classification levels, compartments, and categories, that are processed on the system.
  - **Type of levels of users**
    - their need to know, and formal access approvals that the users will have.

Security modes

Mode	Signed NDA for	Proper clearance for	Formal access approval for	A valid need to know for
Dedicated security	ALL information	ALL information	ALL information	ALL information
System high security	ALL information	ALL information	ALL information	SOME information
Compartmented security	ALL information	ALL information	SOME information	SOME information
Multilevel security	ALL information	SOME information	SOME information	SOME information

Zachman Enterprise Architecture framework

- Enterprise Architecture framework
- Provides a formal and highly structured way of viewing and defining an enterprise.
- Two dimensional classification matrix based on the intersection of six communication questions
  - What, Where, When, Why, Who and How
  - Six rows of transformations.

Zachman Enterprise Architecture framework

	Why	How	What	Who	Where	When
Contextual	Goal list	Process list	Material list	Organisational unit and roles list	Geographical locations list	Event list
Conceptual	Goal relationship	Process relationship	Entity relationship model	Organisational unit and roles relationship model	Location model	Event model
Logical	Rules diagram	Process diagram	Data model diagram	Role relationship diagram	Location diagram	Event diagram
Physical	Rules specification	Process functional specification	Data entity specification	Role specification	Location specification	Event specification
Detailed	Rules details	Process details	Data details	Role details	Location details	Event details

Sherwood Applied Business Security Architecture

- SABSA framework
- Developed independently from Zachman, similar.
- Model and methodology for:
  - developing risk-driven enterprise information security architectures
  - delivering security infrastructure solutions that support critical business initiatives.
- Everything must be derived from an analysis of the business requirements for security.

Sherwood Applied Business Security Architecture

	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The business	Business risk model	Business process model	Business organisation and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strageties and architectural layering	Security entity model and trust framework	Security domain model	Security related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	User applications and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and execution
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application, user management and support	Security of sites and platforms	Security operations schedule

ISO 7498 – Part 2 (7498-2)

- Basic Reference Model - Part 2: Security Architecture
  - provides a general description of security services and related mechanisms
  - defines the positions within the Reference Model where the services and mechanisms may be provided.
  - extends the field of application of ISO 7498, to cover secure communications between open systems.

ISO/IEC 42010:2007

- Addresses the activities of architectures of software-intensive systems:
  - creation
  - Analysis
  - Sustainment
  - Recording.
  -
- Establishes a conceptual framework for:
  - Architectural description
  - Defines the content of an architectural description.

The Open Group Architecture Framework

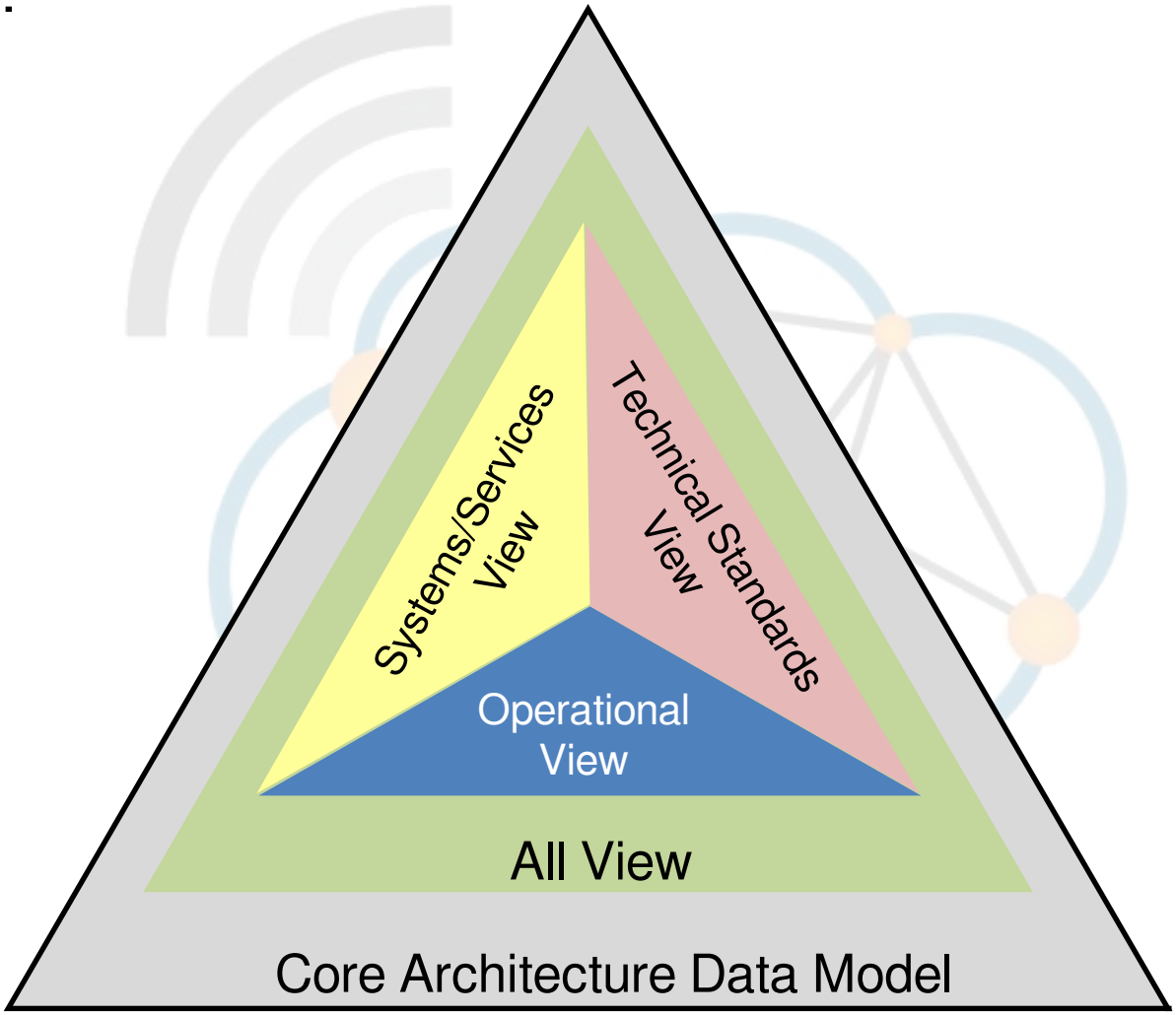
THE Open GROUP
Making standards work®

- Comprehensive approach to the design, planning, implementation, and governance of enterprise information architectures.
- Four levels or domains:
  - **Business**
    - Business strategy, governance, organisation, and key business processes.
  - **Application**
    - Provides a blueprint for the individual application systems to be deployed and the interactions between them.
  - **Data**
    - The structure of an organisation's logical and physical data assets and their data management resources.
  - **Technology**
    - The hardware, software and network infrastructure needed to support the deployment of core, mission-critical applications.

DoD Architecture Framework

- DoDAF organises the Enterprise Architecture (EA) into complementary and consistent views.
- Defines a set of products that act as mechanisms for visualising, understanding, and assimilating an architecture description through graphic, tabular, or text.
- **All View (AV)**
  - Overarching descriptions of the entire architecture.
- **Operational View (OV)**
  - Descriptions of the tasks and activities, operational elements, and information exchanges required to accomplish tasks.
- **Systems and Services View (SV)**
  - Set of graphical and textual products that describe systems and services and interconnections providing for, or supporting functions.
- **Technical Standards View (TV)**
  - Technical standards, implementation conventions, business rules and criteria.

Department of Defence Architecture Framework

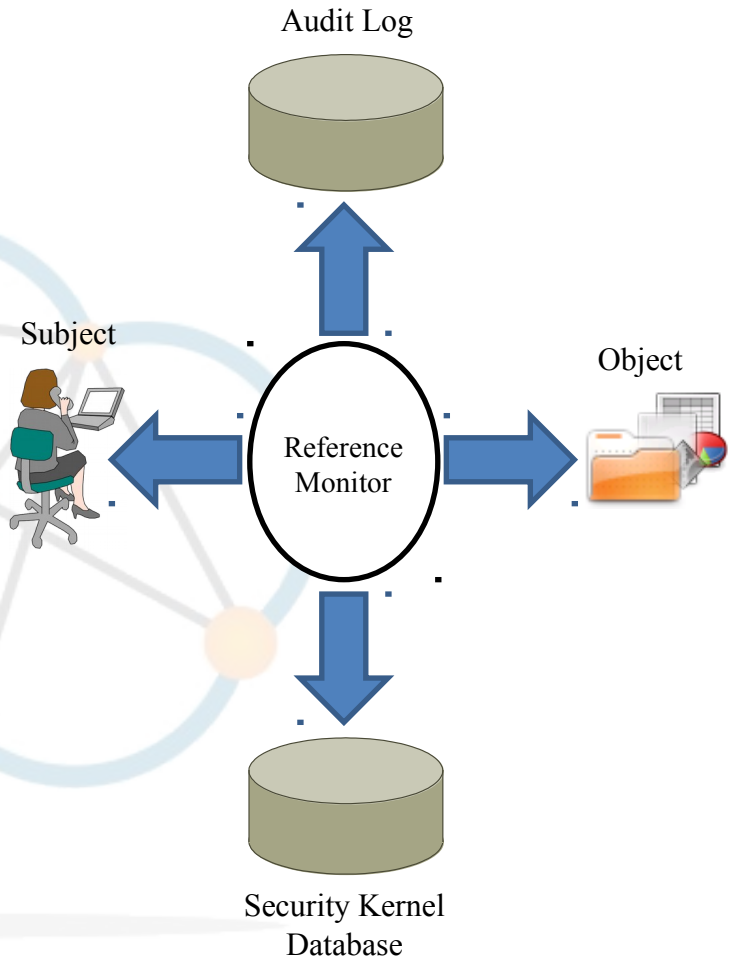


Trusted Computing Base

- TCB is the set of all hardware, firmware, and/or software components that are critical to its security.
- Bugs or vulnerabilities occurring inside the TCB might jeopardise the security properties of the entire system.
- Parts of the system outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the security policy.
- The careful design and implementation of a system's TCB is paramount to its overall security.
- Modern OSs strive to reduce the size of the TCB so that an exhaustive examination of its code base becomes feasible.

DoD Architecture Framework

- **Security Perimeter**
  - Imaginary boundary that separates the TCB from the rest of the system.
- **Reference Monitor**
  - Tamperproof, always invoked module of the TCB that controls all software access to data objects or devices.
  - Verifies the nature of the request against a table of allowable access types for each process.
- **Security Kernel**
  - This is the hardware and software of the TCB that implements the reference monitor.

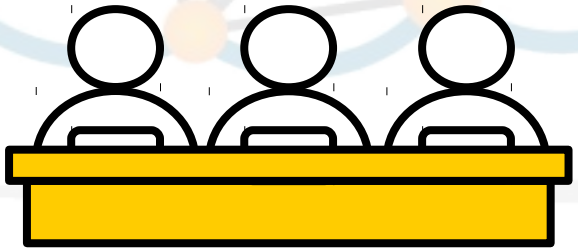


Security models

- Group exercise

- In your group discuss these words in terms of Security models, which is more important ? Why ?
- What specifics would you include in your Security model to protect files and directories ?

Integrity	Confidentiality



Security model summary

Integrity	Confidentiality
Clark Wilson	Bell-la Padula
Biba	Chinese Wall
Graham Denning	Brewer & Nash
G&M	
Sutherland	

Bell-La Padula (BLP) Model

- BLP is a state machine model used for enforcing access control in US government and military applications.
- It focuses on data **confidentiality** and **access** to classified information.
- The entities in the system are divided into:
  - Subjects
  - Objects.
- The notion of a "***secure state***" is defined.
- Each state transition preserves security by moving from secure state to secure state.
- Controls
  - Mandatory
  - Discretionary.

Bell-La Padula Model - Mandatory Access Control (MAC)

- **Simple** Security Property – **no read-up**
  - A subject at a given security level may not READ an object at a higher security level.
- ***-property – no write-down**
  - A subject at a given security level must not WRITE to any object at a lower security level.
- **Strong *-property – no RW-up or RW-down**
  - A subject with RW properties is restricted to RW at their level of security but cannot RW.

Bell- La Padula Confidentiality Model

Security Access Level			
Higher Secrecy	X	OK	X
	Read Only	Write Only	Read & Write
Lower Secrecy	OK	X	X
Security Property	**Simple**	**Star**	**Strong Star**
	(Read down)	(Write up)	Constrained

Bell-La Padula Model - Discretionary Access Control (DAC)

- Additional to the three MACs model has a DAC
- Provides a specific access matrix to specify the discretionary access permissions.

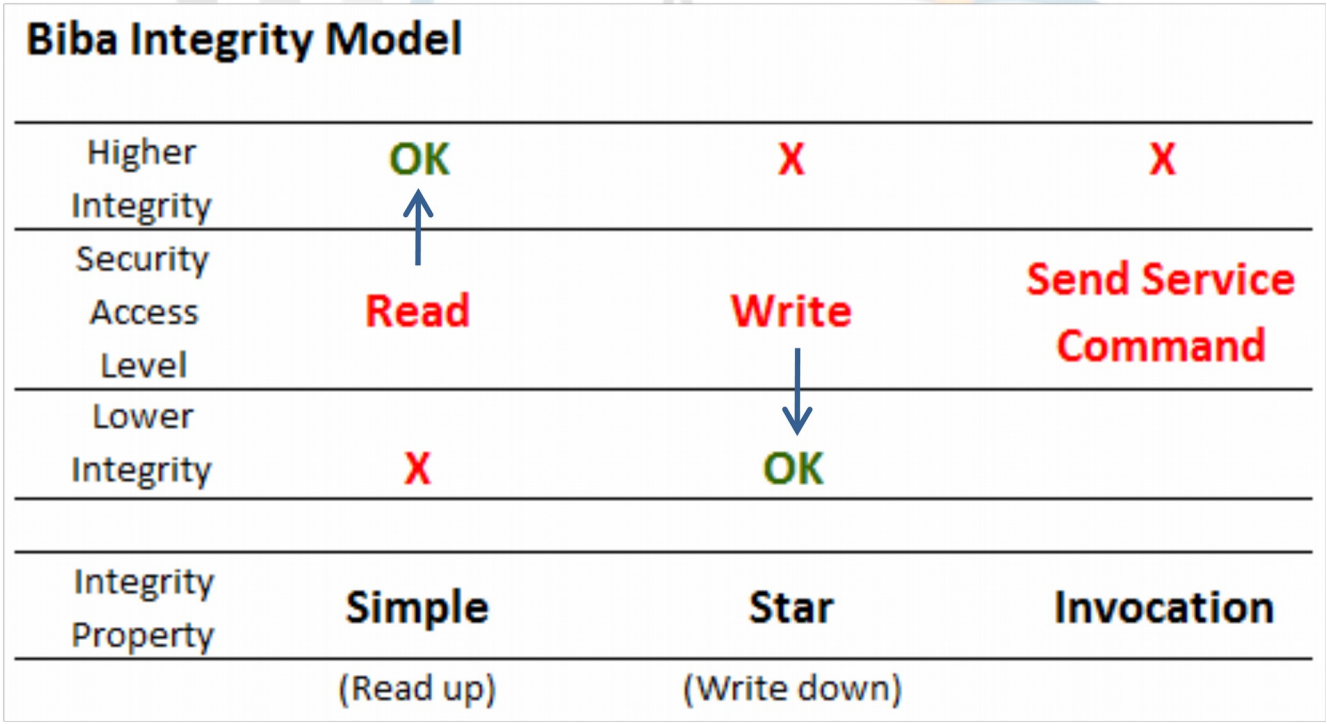
	Application A	Application B	File A	Device A
Role A	R, W, X, O	X	read	write
Role B	R, X	R, W, X, O		

Biba Integrity Model

- Describes access control rules that ensure data **Integrity**.
- Data and subjects are grouped into levels of **integrity**.
- Subjects may not
  - corrupt data in a level ranked higher than the subject
  - be corrupted by data from a lower level than the subject.
- Developed to circumvent a weakness in the BLP Model which only addresses data **confidentiality**.
- Defines a set of security rules similar to BLP model.
- The MAC rules are the reverse of the BLP rules.

Biba Integrity Model

- **Simple – no read-down**
  - A subject at a given level of integrity must not read an object at a lower integrity level.
- ***-property – no write-up**
  - A subject at a given level of integrity must not write to any object at a higher level of integrity.
- The **Invocation** property
  - Prevents a process from below requesting access at a higher integrity level.

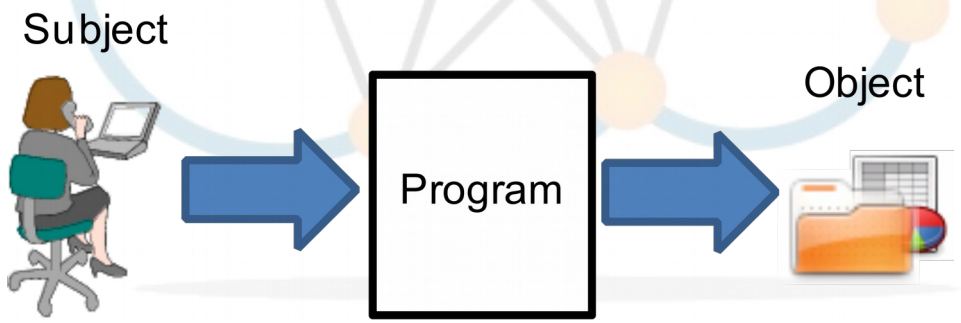


Clark-Wilson model

- Foundation for specifying and analysing an **integrity** policy for a computing system.
- Describes how the data items should be kept valid from one state to the next and specifies the capabilities of various principals in the system.
- The model defines enforcement rules and certification rules.
- Based on the notion of a transaction:
  - A **well-formed transaction,** series of operations that transition a system from one consistent state to another consistent state.
  - The integrity policy addresses the integrity of the transactions.
  - The principle of Separation of Duty (SoD) requires that the certifier of a transaction and the implementer be different entities.

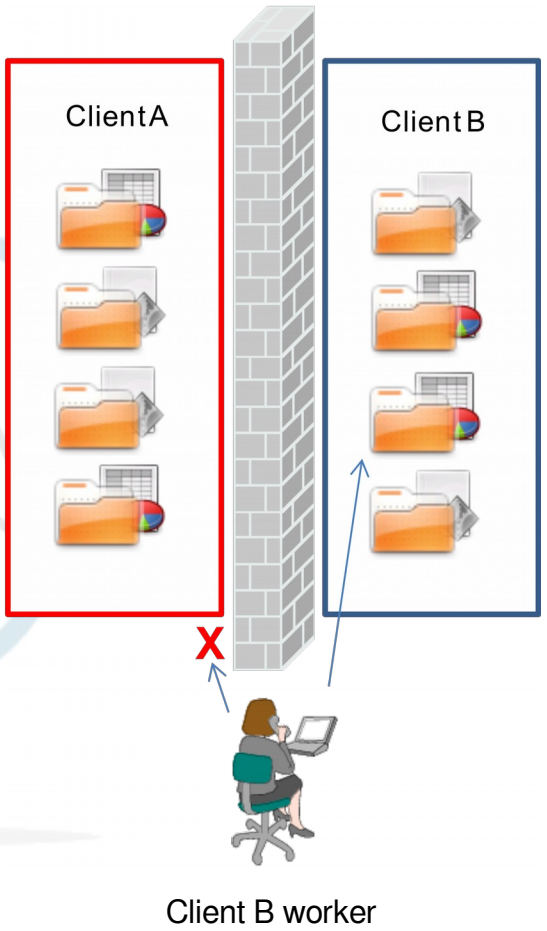
Clark-Wilson model

- Access Triple – **SUBJECT – PROGRAM – OBJECT** relationship.
- The **subject** making a change to the **object** must comply with the **restrictions** built into the program which prevents the subject making an inappropriate adjustment of the object.
- A well formed transaction is one where the changes requested by the subject meet the integrity rules.



Brewer and Nash model

- This model was constructed to provide information security access controls that can change dynamically.
- **Chinese wall** model to provide controls that mitigate conflict of interest in commercial organisations, and is built upon an information flow model.
- No information can flow between the **subjects** and **objects** in a way that would create a conflict of interest.



Evaluation Models

Evaluation standards which can be used to evaluate systems security.

- Trusted Computer System Evaluation Criteria (**TCSEC**)
  - US DoD
  - Orange book
- Information Technology Security Evaluation Criteria (**ITSEC**)
  - European Union (EU)
- Common Criteria (**CC**) for Information Technology Security Evaluation
  - ISO/IEC 15408

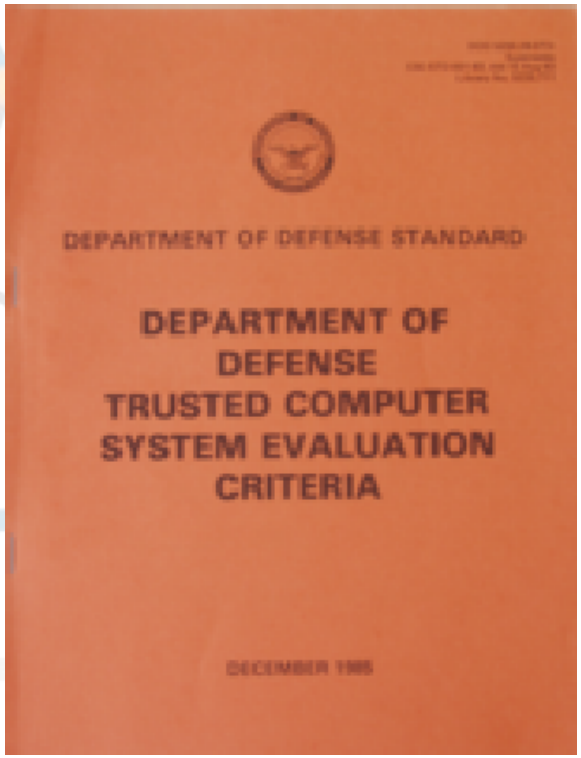
Trusted Computer System Evaluation Criteria

- TCSEC, US DoD standard that sets basic requirements for assessing the effectiveness of computer security controls.
- It is an implementation of the BLP security model.
- Used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.
- TCSEC, or the Orange Book, is the centrepiece of the DoD Rainbow Series publications issued in 1983 by the NSA, and then updated in 1985.
- Replaced by the CC international standard originally published in 2005.

Trusted Computer System Evaluation Criteria

Each division represents a significant difference in the trust an individual or organisation can place on the evaluated system.

- D — Minimal protection
- C — Discretionary protection
  - C1 — Discretionary Security Protection
  - C2 — Controlled Access Protection
- B — Mandatory protection
  - B1 — Labelled Security Protection
  - B2 — Structured Protection
  - B3 — Security Domains
- A — Verified protection
  - A1 — Verified Design

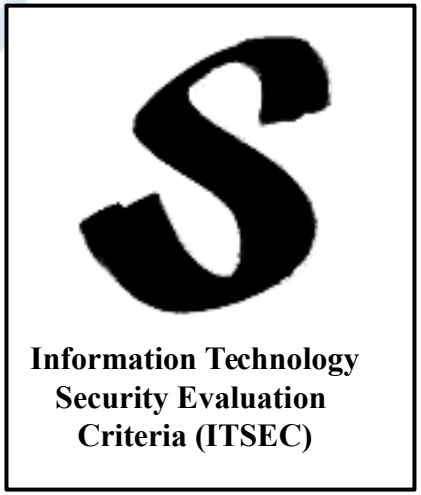


IT Security Evaluation Criteria

- ITSEC set of criteria for evaluating computer security within products and systems.
- First published in May 1990 in France, Germany, the Netherlands, and the UK based on existing work in their respective countries.
- v1.2 was subsequently published in June 1991 by the EU for operational use within evaluation and certification schemes.
- Replaced by the CC international standard originally published in 2005.

ITSEC Classes

- ITSEC defines two ratings:
  - Assurance (E0 – E6)
  - Functionality (F-C1, F-C2, F-B1, F-B2, F-B3)
- ITSEC defines evaluation levels, denoted E0 through E6.
- Higher evaluation levels involve more extensive examination and testing.
- Unlike TCSEC, ITSEC did not require evaluated targets to contain specific technical features in order to achieve a particular assurance level.
- An ITSEC target might provide authentication or integrity features without providing confidentiality or availability.
- Each target's security features are documented in a Security Target document, whose contents have to be evaluated and approved before the target itself is evaluated.
- Each evaluation is based exclusively on verifying the security features identified in the Security Target.



Common Criteria

Common Criteria for Information Technology Security Evaluation

- CC for IT Security Evaluation, an international standard (ISO/IEC 15408) for computer security certification.
- CC is a framework in which:
  - Computer system users can specify their security functional and assurance requirements
  - Vendors can then implement and/or make claims about the security attributes of their products
  - Testing laboratories can evaluate the products to determine if they actually meet the claims.
- CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

CC Evaluation Assurance Level (EAL)

- The EAL (EAL1 through EAL7) of an IT product or system, assigned after a CC security evaluation.
- Increasing assurance levels reflect added assurance that must be met to achieve CC certification.
- Higher levels provide higher confidence that the system's principal security features are reliably implemented.
- The EAL level does not measure the security of the system itself, it simply states at what level the system was tested to see if it meets all the requirements of its Protection Profile.

CC Flaw remediation

Additional to the EAL level an evaluation of flaw remediation can be added to the assurance level which further provides assurance as to the quality of the product.

- ALC_FLR.1
  - Provides for the identification of security measures where developers provide documented flaw remediation procedures.
- ALC_FLR.2
  - Further to documenting flaws, a flaw reporting procedural mechanism to ensure that any reported flaws are corrected.
- ALC_FLR.3
  - This flaw remediation demonstrates that a systematic flaw remediation mechanism exists.

Certification and Accreditation of Systems

- Phase 1 : **Definition**
  - Assignment of project personnel
  - Documentation of need
  - System Security Authorisation Agreement (SSAA).
- Phase 2 : **Verification**
  - Refinement of SSAA
  - Systems development activity
  - Certification analysis.
- Phase 3 : **Validation**
  - Further refinement of SSAA
  - Certification evaluation of the integrated system
  - Development of a recommendation for Designated Approving Authority (DAA)
  - DAA's accreditation decision.
- Phase 4 : **Post Accreditation**
  - Maintenance of SSAA
  - Systems operation
  - Change management
  - Compliance validation.

Example OS products with CC certification

Name	Company	Assurance Level
Apple Mac OS X 10.6	Apple Inc.	EAL3+
Citrix XenServer 6.0.2 Platinum Edition	Citrix Systems, Inc.	EAL2+,ALC_FLR.2
Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers	Dell, Inc.	EAL4+,ALC_FLR.3
HP HP-UX 11i v3 (using CCv3.1)	HP Company	EAL4+,ALC_FLR.3
Red Hat Enterprise Linux, v3 Update 3	HP Company	EAL3+,ALC_FLR.3
IBM AIX 7 for POWER V7.1 with optional IBM Virtual I/O Server V2.2	IBM Corporation	EAL4+,ALC_FLR.3
Microsoft Windows 8 and Windows RT	Microsoft Corporation	None
Microsoft Windows 8 and Windows Server 2012	Microsoft Corporation	None
Microsoft Windows Server 2008 R2 Hyper-V Release 6.1.7600	Microsoft Corporation	EAL4+,ALC_FLR.3
Microsoft Windows Mobile 6.5	Microsoft Corporation	EAL4+
Microsoft Windows Vista and Windows Server 2008	Microsoft Corporation	EAL1
Oracle Solaris 11.1	Oracle Corporation	EAL4+,ALC_FLR.3
Oracle Enterprise Linux v5 Update 1	Oracle Corporation	EAL4+,ALC_FLR.3
Oracle Enterprise Linux v4 Update 5	Oracle Corporation	EAL4+,ALC_FLR.3
Red Hat Enterprise Linux on 32 bit x86 Architecture, v6.2	Red Hat, Inc.	EAL4+,ALC_FLR.3
Red Hat Enterprise Linux v6.2 on IBM Hardware	Red Hat, Inc.	EAL4+,ALC_FLR.3
Red Hat Enterprise Linux, v3 Update 2	Red Hat, Inc.	EAL3+,ALC_FLR.3
SUSE Linux Enterprise Server 11 Service Pack 2 on IBM System z	SUSE Linux Gmbh	EAL4+,ALC_FLR.3
VMware ESX 4.0 Update 1 and vCenter Server 4.0 Update 1	VMware, Inc.	EAL4+,ALC_FLR.2
VMware ESXi 4.0 Update 1 and vCenter Server 4.0 Update 1	VMware, Inc.	EAL4+,ALC_FLR.2

Thank you

Class Assignment

As the Chief Information Security Officer (CISO) for a firm called "***Mtoto Lishe Limited***" in Ntinda, Nakawa, Kampala exploiting research from the Makerere University College of Health Sciences (CHS) on baby food.

This discovery from CHS is considered a commercial secret and the information is sought after for commercial purposes by a number of pharmaceutical firms from around the world and therefore it is essential that the Server and Desktop products used consider security adequately.

Write a short report considering possible alternative solutions with particular reference to their security features.

Note:
It is important that you research beyond the limits of the associated text to this slidedeck.