Week 4

MIS-5903

Domain 3:

Security Architecture & Engineering

https://community.mis.temple.edu/mis5903sec711summer2021

Last Revised 6/01/21

1

1

ISO/IEC 42010:2011 Vocabulary

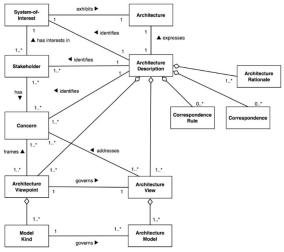
- Architecture
  - Organization of a system/components
  - Relationship between components and environment
  - Principles guiding design and evolution
- Architecture Description (AD) – documents in a formal manner
- Stakeholder - have interests in the system
  - Users
  - Maintenance staff, operators
  - Developers
  - Suppliers
- View – Representation of system from perspective of concerns
- Viewpoint -
  - Specification of the conventions for constructing and using a view
  - Template from which to develop individual views (purposes, audience for a view, techniques)

6/1/21 MIS5903 - Domain 3 2

2

Example Viewpoints

- Logical
- Physical
- Structural
- Behavioral
- Management
- Cost
- Security



6/1/21 MIS5903 - Domain 3 3

3

Central Processing Unit

- Registers (locate instructions, data in memory)
  - General – variables, temporary work results
  - Special – program counter, stack pointer, program status word
    - User Mode (aka problem state)
    - Privileged Mode (aka kernel or supervisor)
- Control Unit
  - Control Bus
  - Data Bus (retrieve data)
  - Address Bus (pass from CPU to RAM, ROM, I/O)
- Arithmetic Logit Unit (ALU)
- Multi-tasking – processor completes individual tasks
- Multiprocessing
  - Symmetric mode (scheduler determines and balances processor loads)
  - Asymmetric mode (dedicated processor for user time-sensitive threads)

4

Memory – Random Access Memory (RAM)

- Static RAM – does not require refreshing; used for cache.
- Dynamic:
  - Synchronous DRAM – synchronized signal input and output
  - Extended Data Out DRAM – access next block of data ("look ahead")
  - Burst EDO SDRAM – reads and sends up to four memory addresses.
  - Double Data Rate SDRAM – utilizes both rising and falling cycles of a clock pulse

5

Memory – Other Types

- Read Only Memory
  - Software stored in ROM referred to as firmware
  - Programmable Read-Only Memory (only once)
  - Erasable Programmable Read-Only Memory (EPROM) – ultraviolet
  - Electrically Erasable Programmable Read-Only Memory (EEPROM)
- Flash Memory
  - SD-Card is an example
- Cache Memory
  - Level 3 on motherboard
  - Level 1, Level 2 inside processor/controller.

6

Memory Issues

- Mapping
  - Physical memory is an absolute address
  - Indexed addresses used by software are logical addresses.
- Buffer Overflow
  - Programmer doesn't check input value type
- Memory Leaks
  - Operating System becomes "starved"
  - Memory no longer in use/needed not released.

7

Operating Systems

- Process Management
  - Cooperative multitasking (Windows 3.x, early Mac) – controlled by process
  - Preemptive multitasking – controlled by operating system
- Thread Management – portions of process
- Process Scheduling – affinity levels
- Process Activity
  - Process isolation
  - If not encapsulated, could accept malicious instructions
  - Time Multiplexing – processes use same resources

8

Operating System Memory Management

- Goals:
  - Provide abstraction level for programmers
  - Maximize performance with limited memory
  - Protect OS and applications in memory
- Relocation: swap from RAM to hard drive. Provide Pointers
- Protection: limit processes to assigned memory segments
- Sharing: allow shared memory segments
- Logical Organization: Segment all memory types
- Physical Organization: Separate memory space for OS versus apps.

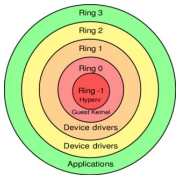
9

Input/Output Device Management

- Interrupts
  - Programmable I/O – checks for device
  - Interrupt-Driven I/O – waits for subsequent request
  - I/O using Direct Memory Access (DMA) – DMA controller (unmapped I/O)
  - Premapped I/O – I/O device provided memory address of requesting process
  - Fully Mapped I/O – Operating System acts as broker.

10

CPU Architecture



- Ring 3 – Applications
- Ring 2 – Operating system utilities, File system drivers
- Ring 1 – Operating System
- Ring 0 – Operating system Kernel
- Ring -1 – Virtualized Environments

- Available Ring(s) Determined by CPU

11

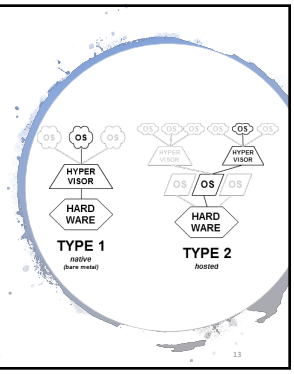
Operating System Architectures

- Monolithic – all processes run in kernel mode
- Layered
- Microkernel – core processes run in kernel mode; remaining processes run in user mode.
- Hybrid microkernel – All operating system processes run in kernel mode. Processes divided between microkernel or client/server model.

12

Virtualization

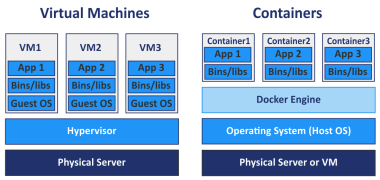
- Type 1 – Vmware ESXi, Microsoft Hyper-V
- Type 2 – VirtualBox, VMWare Workstation, Vmware Fusion, Virtual PC



13

Another Virtualization Option - Containers

- Container contains the application, as well as any of its dependencies to run that are outside of the operating system.
- Docker is a common example of Containerization



14

Security Policy

- Access Control
- Least Privilege
- Separation of Duties (SoD)
  - More than one person required to complete a task
- Auditing
- Trusted Paths
- Does not contain covert channels

15

Access Control

- Mandatory Access Control – based on discrete levels
- Role Based Access Control – based on roles
- Discretionary Access Control – set at the resource (not necessary tied to role)
- Content Based Access Control – based on the sensitivity of data
- Context Based Access Control – based on the sequence of events or other factors

6/1/21

16

Trusted Computer System Evaluation Criteria (TCSEC)

Trusted computing Base (TCB)

- Collection of all hardware, software, and firmware within a system that provides security and enforces security policy.

Security Perimeter

Reference Monitor

Security Kernel

- Hardware, software, and firmware that fall within the TCB

6/1/21 MIS5903 - Domain 3 17

17

Security Models – Bell-LaPadula

First mathematical model of a multilevel security policy

Confidentiality Focused

Simple Security Rule – cannot read data at higher security levels (no read up)

* (star) property rule – cannot write lower levels (no write down)

Strong Star property rule – to be able to read and write, subject and object must be equal.

6/1/21 MIS5903 - Domain 3 18

18

Security Models – Biba

- Set of access rules designed to ensure data integrity
- Simple Integrity – subject cannot read data at lower levels (no read down)
- * (star) integrity axiom – subjects cannot modify objects at higher integrity level (no write up)

19

Security Models – Clark-Wilson

Protect the integrity of data and ensure properly formatted transactions

Three goals of integrity:

- Subjects can access objects only through authorized programs (access triple)
- Separation of duties is enforced
- Auditing is required.

20

Security Models – Others

- Noninterference – multilevel security model states that commands and activities performed at one level should not be seen by, nor affect subjects or objects at other security levels.
- Brewer-Nash – dynamically changing access controls protect against conflicts of interest. (also known as Chinese Wall)
- Graham-Denning – model shows how subjects and objects should be created and deleted. Addresses how to assign specific access rights.
- Harrison-Ruzzo-Ullman – model shows how a finite set of procedures can be available to edit the access rights of a subject.

21

Systems Evaluation – ISO/IEC 15408 (CC)

- Common Criteria has seven assurance levels
  - EAL1 – Functionally tested
  - EAL2 – Structurally tested
  - EAL3 – Methodically tested and checked
  - EAL4 – Methodically designed, tested, and reviewed
  - EAL5 – Semi formally designed and tested
  - EAL6 – Semi formally verified design and tested
  - EAL7 – Formally verified design and tested

22

Common Criteria Components

- PP - Protection Profile – request for a specific solution
- TOE - Target of Evaluation – proposed product
- ST – Security Target – vendor's written explanation
- Security functional requirements – individual security functions provided by the product
- Security assurance requirements – measures taken during development and evaluation of product to ensure compliance with claimed functionality
- Packages – What must be achieved to achieve specific EAL.

23

Certification versus Accreditation

- Certification tests and documents good and bad results
- Accreditation is the formal acceptance of the system
- Requirement of Federal Information Security Management Act of 2002 (FISMA)
- "Authorization to Operate"
- Major Changes require re-certification, and thus re-accreditation

24

Open versus Closed Systems

- Open systems are built upon standards, protocols, interfaces that have published specifications
  - Windows, OS X, Linux, Unix
- Closed Systems do not follow industry standards
  - Proprietary

6/1/21

25

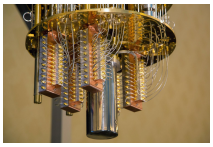
Parallel Computing (Parallelism)

- Bit-Level– each bit processed separately through parallel gates
- Instruction-Level – two or more instructions executed simultaneously (multi-core)
- Task-Level – divide the program into tasks or threads and run in parallel
- Data – distribute data among different nodes to process in parallel

6/1/21

26

New Technologies – Quantum Computing



- IBM and others developing this technology.
- Quantum states
  - Superposition
  - Entanglement
- Instead of binary (0 or 1), a quantum bit is "fluid" / "on the spectrum"
- Sample Applications:
  - Encryption
  - Healthcare – Medication Development
  - Future Quantum Internet

6/1/21 MIS5903 - Domain 3 27

27

Industrial Control Systems

- NIS 800-82 "Guide to Industrial Control Systems (ICS) Security
- Programmable Logic Controllers
- Distributed Control Systems
- Supervisory Control and Data Acquisition (SCADA)
  - Remote Terminal Unit (RTU) (endpoint)
  - Data Acquisition Servers (back ends)
  - Human-Machine Interface (user station, displays interface)

28

Cyber Physical Systems

Embedded Systems

Digital thermometers, other specialized devices

Internet of Things

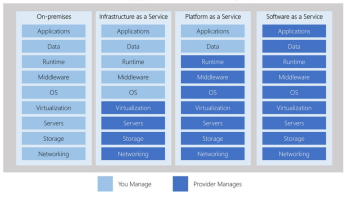
Global network of connected embedded systems
Each device is uniquely addressable
Issues to address:

- Authentication
- Encryption
- Updates

29

Cloud Computing

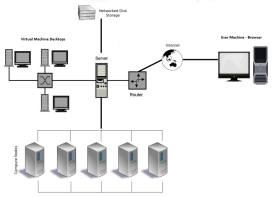
- SaaS – Software as a Service – ready to use application
- PaaS – Platform as a Service – Operating system, Database Engine, etc., but not a ready-to-use application
- IaaS – Infrastructure as a Service – full access to the underlying system; full responsibility for the customer



30

High Performance Computing (HPC)

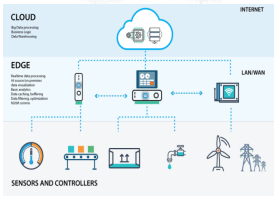
- Utilization of multiple computers to achieve more as a group than individually.
- Orchestrator / Controller



31

Edge Computing

- Refers to Topology
- Derived from Content Delivery Networks
  - Web and video – closer to users
- Low latency close to the requests



32

Mobile Security

- False base stations can be created
- Confidential data can be stolen
- Camera and/or microphones can capture data
- Internet sites accessed in violation of policies
- Malicious code downloaded
- Encryption can be weak, not end-to-end.

33

System Attacks

Maintenance Hooks

Type of back door
Used during development
Should be removed

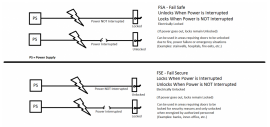
Time-of-Check/Time-of-Use

Race Condition – attacker makes processes execute out of sequence to control the result

TOCTOU – attacker jumps in between two tasks, modifies the temporary value to control the result

34

Failure Modes



- Fail Open – "fail safe"
- Fail Closed – "fail secure"

35

Site and Facility Threats

- Natural environmental – floods, earthquakes, storms, tornadoes, fires, temperature
- Supply system – power distribution outages, communication interruptions, also water, gas, air filtration, etc.
- Manmade – unauthorized access (internal or external), explosions, damage by disgruntled employees, employee errors, accident, vandalism, fraud, theft, etc.
- Politically motivated threats – strikes, riots, civil disobedience, terrorist attacks, bombings, etc.

36

Physical Security Program

- Deter crime and disruption – fences, security guards, signs
- Reduction of damage by delaying – layered defenses, locks, security personnel, barriers
- Detection – smoke or motion detectors, CCTV
- Incident assessment – security guards dispatched
- Response procedures – internal as well as outside security professionals

37

Building the Program

38

Building a Facility

- Combustibility (wood, steel, concrete)
- Fire Rating
- Walls – Reinforcement for secured areas

39

Building a Facility - Doors

- Resistance to forcible entry
- Emergency Marking
- Placement
- Locked or Controlled
- Alarms
- Secure hinges
- Directional opening
- Electric door locks (fail safe)
- Type of glass – shatterproof or bulletproof
- Hollow-Core or Solid-Core

40

Building a Facility – Ceilings & Floors

- Weight-bearing rating
- Drop Ceilings
  - "true floor" to "true ceiling"
- Floors - Nonconducting surface and material

41

Building a Facility – Windows

- Translucent or opaque
- Alarms
- Placement
- Accessibility to intruders
- Strength - Shatterproof?
  - Standard
  - Tempered
  - Acrylic
  - Wired
  - Laminated
  - Solar or Security film

42

Building a Facility – HVAC

Positive Air Pressure

Protected intake vents

Dedicated power lines

Emergency shutoff valve and switches

Placement

Considerations:

- Computer systems: 175 degrees
- Magnetic Storage Devices: 100 degrees
- Paper Products: 350 degrees

43

Designing a Facility - Supplies

Electric

- Backup and alternative power supplies
- Clean and steady power source
- Dedicated feeders to required areas
- Placement and access to distribution panels and circuit breakers
- Electromagnetic Interference (EMI)
- Radio Frequency Interference (RFI)
- UPS / Online UPS / Generators

Water & Gas

- Shutoff valves – labeled for visibility
- Positive flow (material flows out of building)
- Placement – properly located

44

Electric Power Fluctuations

Excess:

- Spike – momentary high voltage
- Surge – prolonged high voltage

Loss:

- Fault – momentary
- Blackout – prolonged, complete loss

Degradation:

- Sag/Dip – momentary – from one cycle to a few seconds
- Brownout – prolonged below normal voltage
- In-Rush current – initial surge required to start a load

45

Designing a Facility – Fire Detection & Suppression

- Placement of sensors and detectors
  - Smoke
  - Heat / Rate of Rise
- Placement of suppression systems
- Type of detectors and suppression agents

46

Fire Suppression

Class	Type of Fire	Elements	Suppression
A	Common combustibles	Wood products, paper, and laminates	Water, foam
B	Liquid	Petroleum products and coolants	Gas, CO2, foam, dry powders
C	Electrical	Electrical equipment and wires	Gas, CO2, dry powders
D	Combustible metals	Magnesium, sodium, potassium	Dry powder

47

Substance Interactions

Combustion Element	Suppression Method	How Suppression Works
Fuel	Soda acid	Removes fuel
Oxygen	Carbon dioxide	Removes oxygen
Temperature	Water	Reduces temperature
Chemical combustion	Gas – Halon substitute (FM-200)	Interferes with the chemical reasons between elements

48

Fire Suppression

Turn off HVAC

- Reduces oxygen
- Minimizes spread of smoke

Sprinklers

- Wet pipe
- Dry pipe
- Preaction
- Deluge – large volume of water

49

Next Steps

Complete Discussion Questions / Participation

Complete online quiz – (graded)

Complete Domain #3 Practice Exam (submit best result)

Begin Week 5 Reading

50