Security Architecture and Models

Ed Crowley CISSP

Spring ‘05

Topics

- Computer and system architecture
- Open, Closed, and Distributed systems
- Security Models
  - Confidentiality models
  - Integrity models
  - Information flow models
- Evaluation and Assurance
  - TCSEC, TNI
  - DITSCAP, NIACAP
  - Common Criteria
- Certification and accreditation

Computer Architecture

- A computer system's structure and organization.
  - Originally defined as the way the computer appears to a machine language program. (IBM 360 Series.)
  - Defines interfaces and arrangements of a system's basic components
  - Includes physical and logical components

Security Model

- Security Model
  - Defines a security implementation's structure
  - Articulates requirements necessary to support an appropriate security level.
- Orange Book defines a Security Policy Model as:

  A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.
  - *Note that this is a confidentiality model*

Formal Security Model Definition
(NCSC-TG-004-88)

- A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model must be supported by, a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. …

Fundamental Computer Components

- Central Processing Unit (CPU)
- Memory
- Input/Output
- Communications buses connects major components. Typical bus components:
  - Address bus –Memory addresses
  - Data bus – Data
  - Control bus – Control signals

Central Processing Unit (CPU)

- Two major components:
  - Arithmetic Logic Unit (ALU)
  - Control Unit (CU)
- Registers – basic unit of operation
- Performance related to Word Size, Clock Speed, and I/O
- Normally, CPU chip contains a small amount of fast memory called Cache RAM

Instruction Execution Cycle

- Two phases in a basic machine cycle.
  1. Fetch
  2. Execute.
- Instructions may require multiple machine cycles.

CPU Instruction Sets

- Complex-Instruction Set Computer (CISC)
  - Uses instructions that perform many operations per instruction.
- Reduced Instruction Set Computer (RISC)
  - Uses simple instructions with a goal of one operation per instruction.
- Pipelining increases performance by overlapping the steps of different instructions.

CPU Instruction Set Terms

- Scalar Processor
  - Processor that executes one instruction at a time.
- Superscalar Processor
  - Processor that enables concurrent execution of multiple instructions in the same pipeline stage as well as in different pipeline stages
- Very Long Instruction Word Processor (VLIW)
  - Processor in which a single instruction specifies more than one concurrent operation.

IC Based Memory

- Cache
  - Generally, a small amount of very high speed RAM that holds instructions and data from primary memory
- Random Access (RAM)
  - Directly addressed
  - Volatile (Dynamic)
  - Fast (relatively)
- ROM
  - Non volatile directly addressable storage

Memory Types

- Real or Primary Memory aka RAM
- Secondary Memory aka DASD
- Sequential Memory aka Tape
- Virtual Memory
  - Created by using hard disk to simulate additional random-access memory.
  - Utilizes a memory manager to map virtual addresses into real addresses

Memory Addressing Modes

- Register addressing -- Within CPU
- Direct addressing -- By address
- Absolute addressing -- Using primary address
- Indexed addressing -- Index register based addressing (8086 Family)
- Implied addressing -- Internal to processor
- Indirect addressing -- Using pointer

Memory Protection

- Means to prevent a program, process, or user, from accessing and modifying memory contents belonging to another entity.

Terms

- Multitasking
  - Executing two or more programs or tasks at the same time.
    - Cooperative
    - Pre-emptive
- Multiprocessing
  - Utilizing multiple processors.

Input/Output

- I/O adapters provide buffering, timing, and interrupt controls.
- Memory mapped I/O shares CPU memory address space aka programmed I/O
- With Direct Memory Access (DMA), data is transferred directly to and from memory without going through a CPU.

I/O Concepts

- Channel
  - The data transfer path between memory and a peripheral device.
- Interrupt processing occurs when a signal interrupts normal program flow to request service.
- By nesting interrupt service routines, multiple interrupts can be handled concurrently.

Software Generations

- Machine Language 1st Gen
- Assembler 2ND Gen
  - Source and object code
- High level language 3RD Gen
  - Fortran, COBOL, PL-1
- Program Generator 4th Gen
  - FOCUS
- Artificial Intelligence 5TH Gen

Operating System

- Program, or set of programs, that control the computer's real resources.
- Controller
  - Device that interfaces system and peripheral.
  - Runs specialized software that manages device communications.

Open and Closed Systems

- Open systems
  - Vendor independent systems with published specifications and interfaces that permit operations with the other products.
  - Source code available.
  - Multiple types of open source licenses.
- Closed systems
  - Vendor dependent proprietary hardware and/or software that may not be compatible with other products.
  - Source code not available.

Distributed Architecture

- As computing evolved from centralized paradigm to a client server paradigm, new security issues also evolved.
- In general, distributed architecture refers to collaborative processing among multiple systems.
  - The Web is an example of a distributed architecture.

Distributed Architecture Vulnerabilities

- Desktops may:
  - Contain sensitive information.
  - Not be physically secure.
  - Not be regularly backed up my their users.
  - Provide access into other critical systems
  - Have modems.
  - Have users that lack security awareness
- Internet access increases risk of malicious code.

Protection Mechanisms

- Protection Domain
  - Each process has the ability to access certain memory locations and to execute a subset of the computer's instruction set.
- Trusted Computer Base (TCB)
  - Total combination of protection mechanisms within a computer system. Hardware, software, and firmware
  - Must be tamperproof.
  - If you don't have a TCB, you don't have security.
- Security Perimeter
  - Separates the TCB from the remainder of the system.

Trusted Path and Trusted Computer System

- Trusted path enables a user to access TCB without being compromised by other processes or users.
- Trusted computer system is one that employs the necessary hardware and software assurance measures to enable its use in processing multiple levels of classified or sensitive information.

Object Oriented Programming

- In object oriented programming, methods and data are encapsulated within an object.
- Objects can be viewed as abstractions that have certain characteristics, including:
  - Inheritance
  - Methods
  - Encapsulation
  - Reuse

Protection Rings

- Rings provide isolation and protection among user and system processes.
- Most privileged domain located in the center ring
  - Kernel in Ring 0.
  - Least privileged domain in outermost ring.
- Originally Implemented in MULTICS.
  - Enhanced for secure applications.

Security Kernel

- A trusted computing base's hardware, firmware, and software.
- Implements reference monitor concept.
- Security Kernel
  - Mediates all access
  - Protected from modification
  - Verifiable as correct

Reference Monitor

From the Rainbow Series:

> An access-control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Kernel Based Security Approaches

- Implementing a virtual machine monitor.
- Each virtual machine can run at a different security level

Modes of Operation

- A description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized:
- Dedicated mode
  - All users have a clearance and a need to know
- Compartmented
  - All users have a clearance for the highest level of information but not necessarily a need to know

Security Modes

- System High
  - Each subject must have a clearance and a formal approval for all info and for their information a valid need to know.
- Multilevel
  - Some users do not have a valid clearance
  - All have a need to know for their information.
  - All have formal approval for their information.

Threats

- Covert channel
  - An unintended communication path between two or more subjects sharing a common resource.
- Lack of parameter checking aka buffer overflow
- Maintenance hook aka back door
- Time of Check to Time of Use attack aka race condition

Covert Channels

- Covert Channel: a communications channel that allows transfer of information in a manner that violates the system's security policy.
- Covert storage channels: e.g. through operating system messages, file names, etc.
- Covert timing channels: e.g. through monitoring system performance

Recovery Procedures

- The actions necessary to restore a system's computational capability and data files after a system failure.*(Aqua Book)*
- Whenever a trusted system has a hardware of software component failure, it should not compromise security.
- Fault tolerance is when a system component fails and the system continues to function.

Fallover

- Refers to real time switching to a duplicate ‘hot’ backup component when a hardware or software failure occurs

Failsafe and Failsoft

- Failsafe
  - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.
- Failsoft
  - Pertaining to the selective termination of affected nonessential processing when a hardware or software failure is detected in a system.

From the Aqua Book (NCSC-TG-004-88)

Assurance

- A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. (*Aqua Book*)
- In 1985 the National Computer Security Center (NCSC), developed the Trusted Computer System Evaluation Criteria (TCSEC).
  - Provides guidelines for evaluating vendor's products for the specified security criteria.
  - aka Orange Book
  - Historically important

AIS means automated information system

Trusted Computer System Evaluation Criteria

- Provides specific criteria based guidelines for evaluating vendor products.
  - aka Orange Book
- Addresses Confidentiality
- Does not Integrity
- Does not address availability

TCSEC (Orange Book) Provides

- A basis for establishing security requirements in acquisition specifications
- A standard of the security services that should be provided by vendors for the different classes of security requirements.
- A means to measure an information system's trustworthiness.

TCSEC Levels

- A1 -- verified protection
- B1, B2, and B3 -- Mandatory protection
- C1 and C2 -- Discretionary protection
- D -- Minimal protection

  Level D protections indicate that the system did not qualify for a higher level.

Trusted Network Implementation (Red Book)

- Developed in ‘87
- Extends TCSEC specific security features to networks.
  - Assurance requirements
  - Rating structure.

ITSEC

- European Information Technology Security Evaluation Criteria addresses:
  - Confidentiality
  - Integrity
  - Availability.
- Evaluates functionality and assurance separately.
  - Target of Evaluation (TOE) – system to be evaluated
  - TOE must have a security target – including security enforcing mechanisms and security policy

What is the Common Criteria?

- The Common Criteria for Information Technology Security Evaluation (CCITSE) is a multinational effort to write a successor to the TCSEC and ITSEC that combines the best aspects of both.
- The CCITSE has a structure closer to the ITSEC than the TCSEC and includes the concept of a "profile" to collect requirements into easily specified and compared sets and the concept of a Security Target.

http://www.radium.ncsc.mil/tpep/library/ccitse/

Certification

- The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
  - *From Aqua Book*

Accreditation

- A formal declaration by the Designated Approving Authority (DAA) that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.
  - *From Aqua Book*

DITSCAP

- U.S. Defense Information Technology Security Certification and Accreditation Process
- Establishes:
  - A standard process
  - A set of activities, general tasks descriptions
  - A management structure
- Certifies and accredits IT systems that will maintain the required security posture.

Four DITSCAP Phases

- Phase 1
  - Focuses on understanding the mission, the environment, and the architecture
- Phase 2
  - Verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement

DITSCAP Phases

- Phase 3
  - Validates compliance
- Phase 4
  - Post Accreditation activities that are necessary for the continuing operation … and for addressing the changing threats a system faces through its life cycle.

NIACAP

- National Information Assurance Certification and Accreditation Process
- Establishes minimum national standards for certifying and accrediting national security systems.
- Establishes requirements for federal departments and agencies to implement a C&A process for national security systems under their operational control.

Security Models

- Formalization of security policies.
  - Security model is a formal description of a security policy.
- Used in security evaluation, accreditation, and certification.
- May be used to provide a formal security proof.

Security Models

- Access Control Models
  - Access Matrix
  - Bell LaPadula
  - Take Grant
- Integrity Models
  - Biba
  - Clark Wilson
- Information Flow Models
  - State Machine

Access Control Models

- Access Matrix
  - Access Matrix Columns are called Access Control Lists
  - Rows called capability lists.
- Supports Discretionary Access Control (DAC).

Take-Grant Model

- Uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can transfer to another subject.

Bell LaPadula (BLP)Model

- Formalizes DOD's multilevel security policy. (Orange Book)
  - Confidentiality model
- Access permissions are defined through an access control matrix and through a partial ordering of security levels.
- Security policies prevent information flowing downwards from a high security level to a low security level.

BLP Multilevel Properties

- Simple Security Property (SSP)
  - Reading of information by a subject at a lower level is not permitted-- No read up
- Star Security Property (*)
  - Writing of information by a subject at a higher level of sensitivity is not permitted -- No write down
- Discretionary Security Property
  - Uses an access matrix to specify discretionary Access Control

BLP Trusted Subject

- When the * property is too restrictive, the transfer of information is permitted through a Trusted Subject.
- A Trusted Subject can violate the * property, yet it cannot violate its intent.

BLP Notes

- Discretionary portion of the Bell-LaPadula model is based on the access matrix
- Authorization is concerned with how access rights are defined and how they are evaluated.
- Has several serious limitations
  - No mechanism for changing access rights
  - Does not address covert channels
  - Does not deal with client/server model
- Historically important

BLP Observations

- If the initial state of a system is secure and if all state transactions are secure, then the system will always be secure.
  - Converse is also true!
- N.B. a state machine model
- Has no provisions for changes

State Machine Models

- Based upon system state
  - States changes only at discrete points in time, e.g. triggered by clock or other event.
- Basic state machine theory focuses on state transitions. Specifically:
- If security is preserved by all state transitions, the system will always be `secure'.

Integrity Models

- In many organizations, data integrity is as important or more important than confidentiality.
- Biba
- Clark Wilson

Biba Integrity Model

- Goals
  - Protect data from modification by unauthorized users
  - Protect data from unauthorized modification by authorized users
  - Internally and externally consistent data
- Like the BLP model, this is a state machine model.
- Unlike the BLP, the Biba model focuses on integrity.

Three Integrity Axioms

- Simple Integrity Axiom
  - A subject at one level of integrity is not permitted to read an object of a lower integrity
- * Integrity Axiom
  - An object at one level is not permitted to write to an object at a higher level.
- A subject at one level of integrity cannot invoke a subject at a higher level of integrity.

Clark Wilson Integrity Model

- Application level integrity model developed for commercial environments.
  - Emphasis is on maintaining internal and external data consistency
- Deals with:
  - Constrained Data items
  - Integrity verification
  - Transaction procedure
  - Unconstrained data items

Clark Wilson

- Requires integrity labels to determine the integrity level of a data item and to verify that this integrity was maintained after an application of a transaction process.
- Principle of a well formed transaction
  - Transaction where users cannot arbitrarily manipulate data.
- Principle of Separations of Duties
  - Ensures internal and external consistency by preventing any one person from corrupting data integrity.

Comparison

- BLP is a general purpose confidentiality model
- Biba added integrity to BLP model
- Clark-Wilson is an application orientated integrity model

Information Flow Model

- An information flow model is based on a state machine.
- Consists of:
  - Objects
  - State transitions
  - Lattice states.
- Information flow is described in terms of conditional entropy.

Noninterference model

- Noninterference model
- Covers methods that prevent subjects operating in one domain from affecting each other in violation of security policy
- Chinese Wall Model

Questions?