Computer Security: Principles and Practice

Chapter 13: Trusted Computing and Multilevel Security

Computer Security Models

- Two fundamental computer security facts
  - All complex software systems have eventually revealed flaws or bugs that need to be fixed
  - It is extraordinarily difficult to build computer hardware/software not vulnerable to security attacks

Confidentiality Policy

- Goal: prevent the unauthorized disclosure of information
  - Deals with information flow
  - Integrity incidental
- Multi-level security models are best-known examples
  - Bell-LaPadula Model basis for many, or most, of these

Formal Security Models

Problems involved both design and implementation led to development of formal security models

- Initially funded by US Department of Defense
- Bell-LaPadula (BLP) model very influential

Bell-LaPadula (BLP) Model

- Security levels arranged in linear ordering
  - Top Secret: highest
  - Secret
  - Confidential
  - Unclassified: lowest
- Levels consist of security clearance L(s)
- Objects have security classification L(o)

Bell-LaPadula (BLP) Model

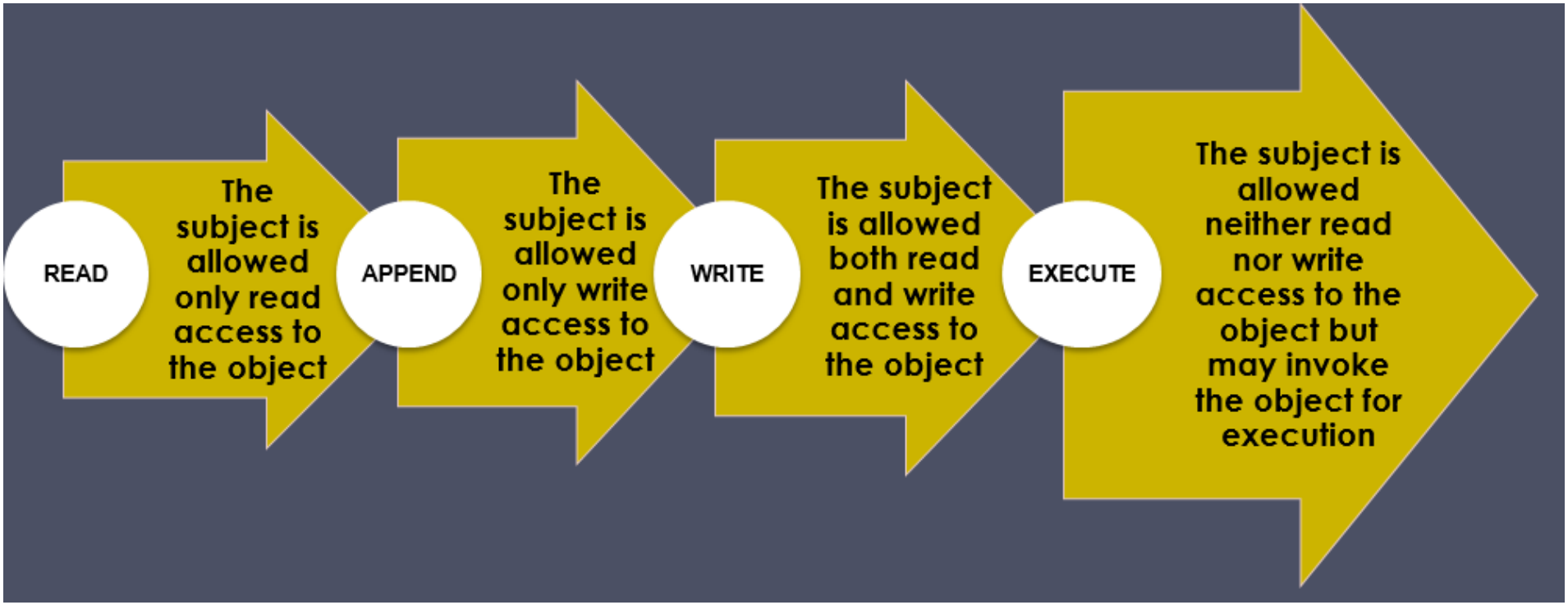
- Developed in 1970s
- Formal model for access control
- Subjects and objects are assigned a security class
- Form a hierarchy and are referred to as security levels
- A subject has a security **clearance**
- An object has a security **classification**
- Security classes control the manner by which a subject may access an object

A BLP Example

Security level	***Subject***	***Object***
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	James	Telephone Lists

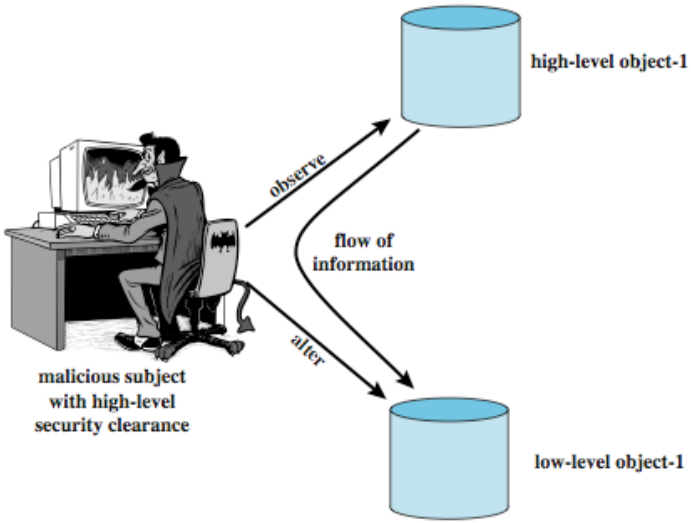
- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- James can only read Telephone Lists

Access Privileges



Multilevel Security

- Multiple levels of security and data
- Subject at a high level may not convey info to a subject at a non-comparable level:
  - No read up (ss-property): a subj can only read an obj of less or equal sec level
  - No write down (*-property): a subj can only write into an obj of greater or equal sec level



BLP Formal Description

- Based on current state of system (***b***, ***M***, ***f***, ***H***):
  - Current access set ***b (subj, objs, access-mode);*** it is the ***current*** access (not permanent)
  - Access matrix ***M*** (same as before)
  - Level function ***f: assigns sec level to each subj and obj;*** a subject may operate at that or lower level
  - Hierarchy ***H: a directed tree whose nodes are objs:***
    - ***Sec level of an obj must dominate (must be greater than) its parents***

BLP Properties

- Three BLP properties: *(c = current)*
  1. ss-property: $(S_i, O_j,$ read) has $f_c(S_i) \geq f_o(O_j)$
  2. *-property: $(S_i, O_j,$ append) has $f_c(S_i) \leq f_o(O_j)$ and
     $(S_i, O_j,$ write) has $f_c(S_i) = f_o(O_j)$
  3. ds-property: (S_i, O_j, A_x) implies $A_x \in M[S_i, O_j]$

- BLP give formal theorems
  - Theoretically possible to prove system is secure

BLP Operations

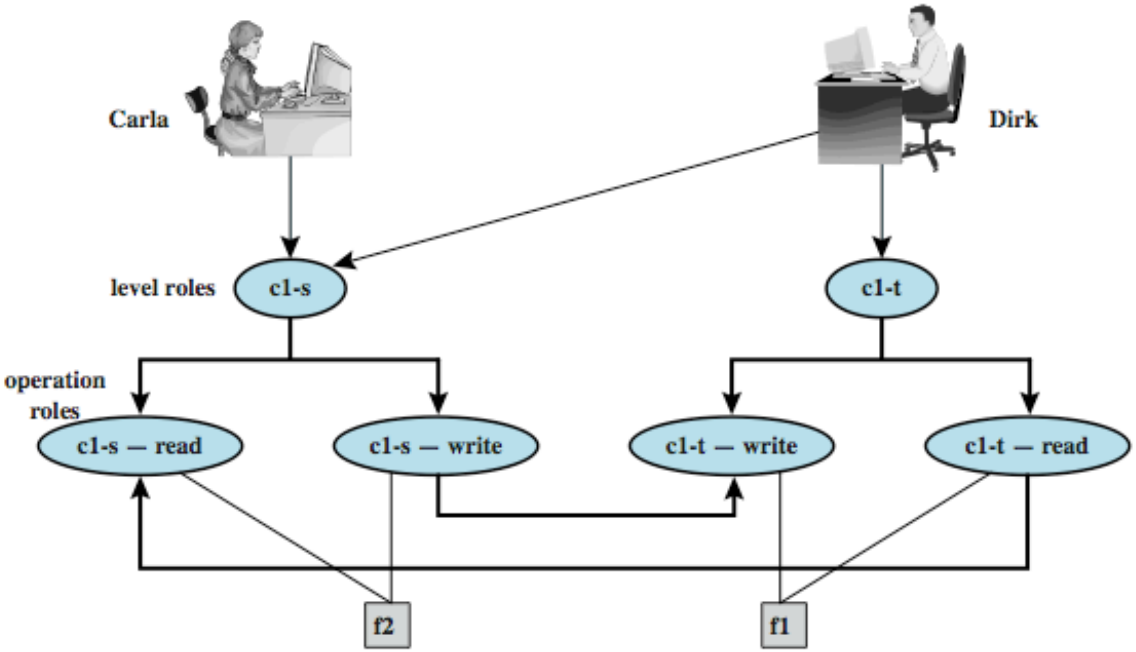
1. **get access**: add (subj, obj, access-mode) to b
   - used by a subj to initiate an access to an object
2. **release access**: remove (subj, obj, access-mode)
3. **change object level**
4. **change current l**evel
5. **give access permission**: Add an access mode to M
   - used by a subj to grant access to on an obj
6. **rescind access permission**: reverse of 5
7. **create an object**
8. **delete a group of objects**

BLP Example

- A role-based access control system
- Two users: Carla (student) and Dirk (teacher)
  - Carla (Class: s)
  - Dirk (Class: T); can also login as a students thus (Class: s)
- A student role has a lower security clearance
- A teacher role has a higher security clearance

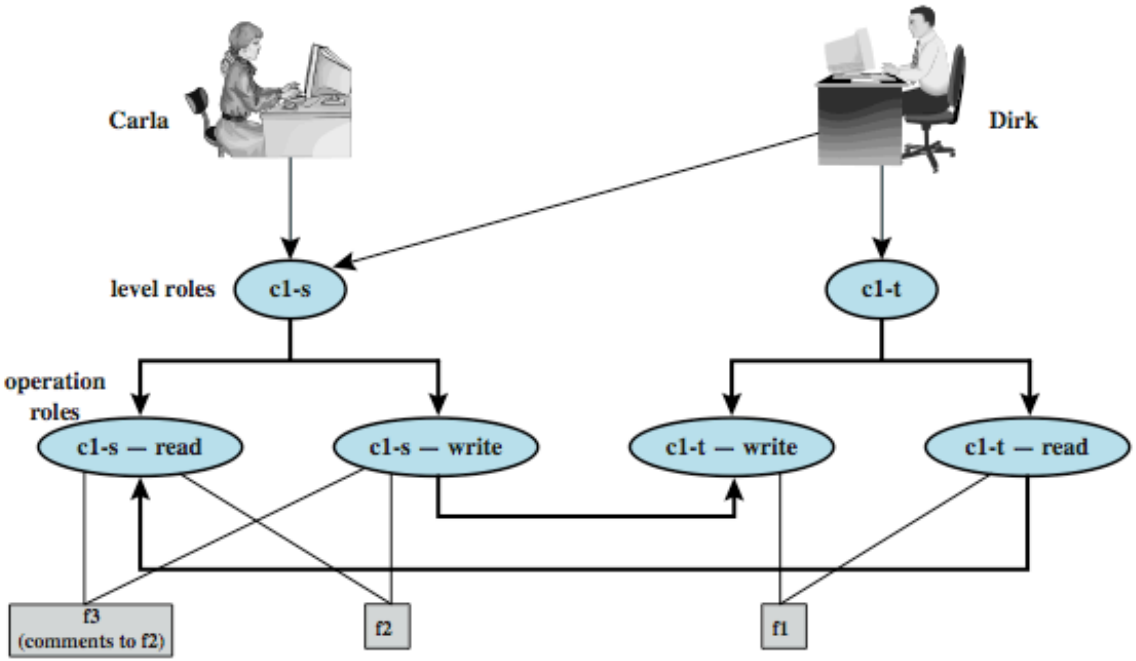
BLP

Dirk creates f1; Carla creates f2
Carla can read/write to f2
Carla can't read f1
Dirk can read/write f1
Dirk can read f2 (if perm)
Dirk can read/write f2 only as a stu



(a) Two new files are created: f1: c1-t; f2: c1-s

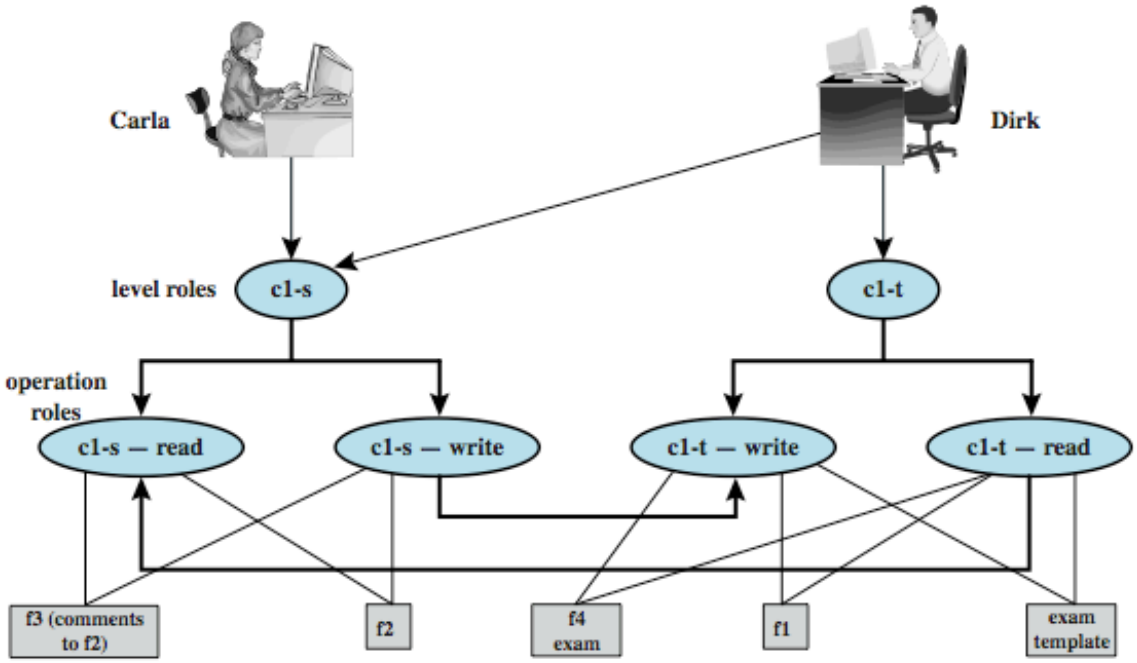
Dirk reads f2; want create f3 (comments)
Dirk signs in as a stu (so Carla can read)
As a teacher, Dirk cannot create a file at stu classification



(b) A third file is added: f3: c1-s

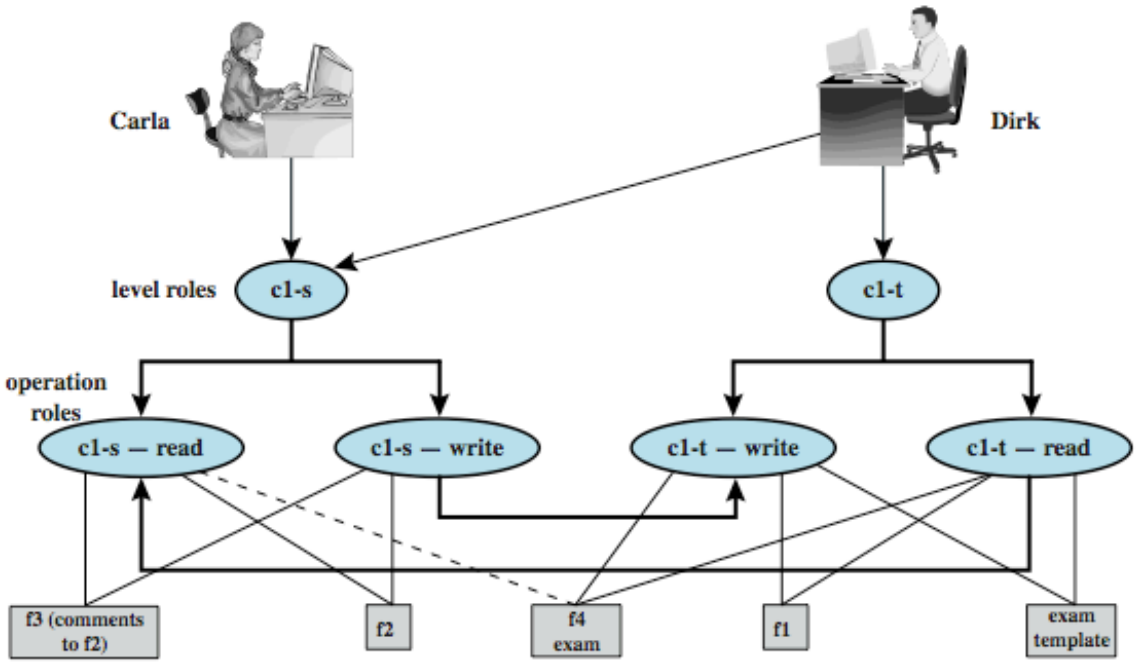
BLP Example cont.

Dirk as a teacher creates exam (f4)
Must log in as a teacher to read template



(c) An exam is created based on an existing template: f4: c1-t

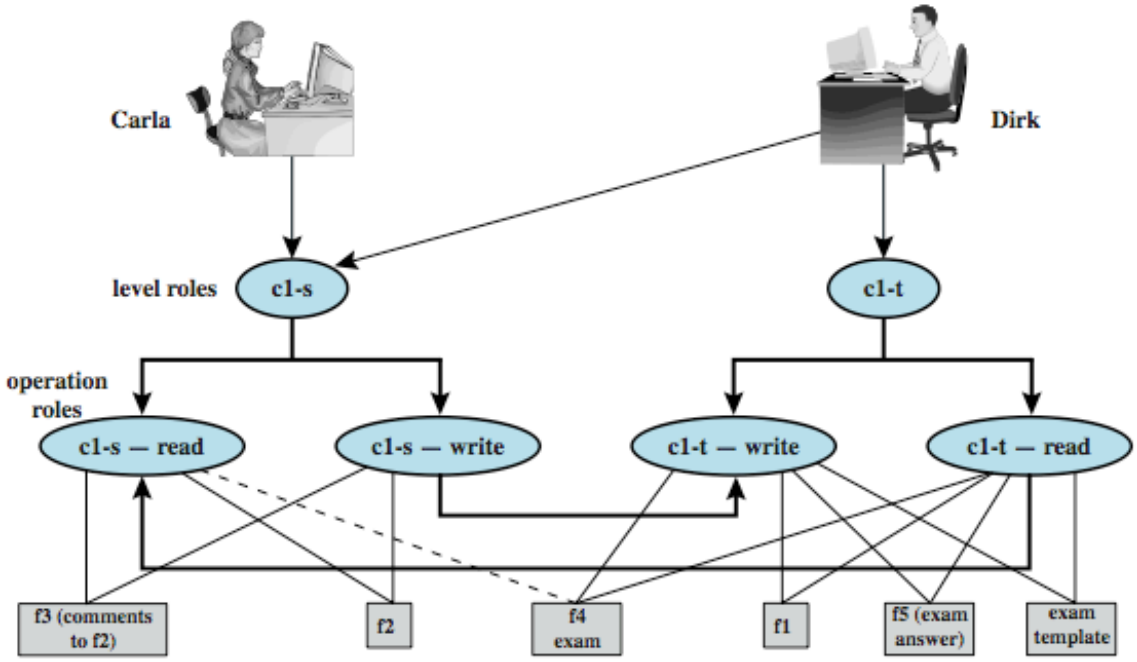
Dirk wants to give Carla access to read f4
Dirk can't do that; an admin must do
An admin downgrades f4 class to c1-s



(d) Carla, as student, is permitted acess to the exam: f4: c1-s

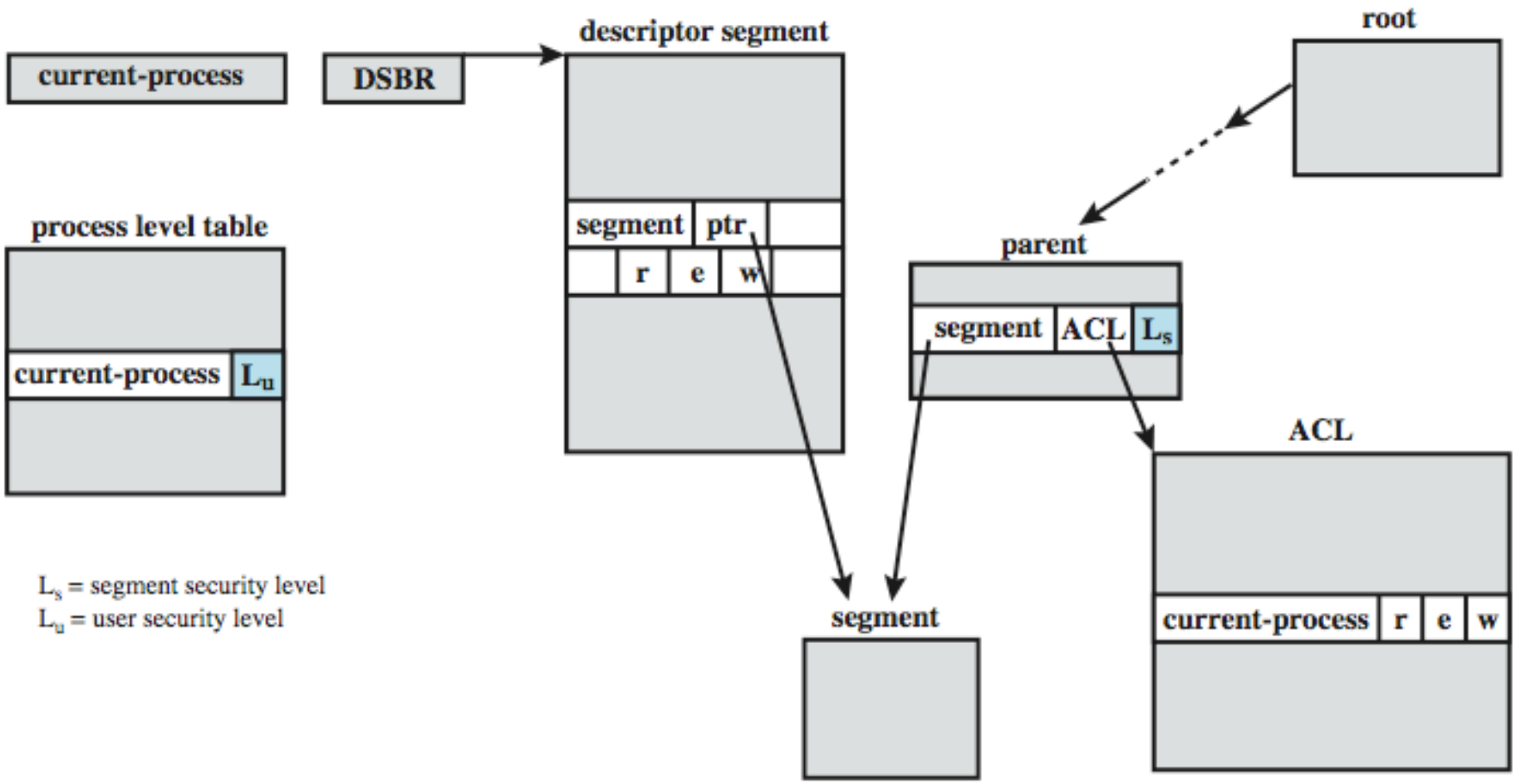
BLP Example cont.

Carla writes answers to f5 (at c1-t level)
-- An example of write up
Dirk can read f5



(e) The answers given by Carla are only accessible for the teacher: f5: c1-t

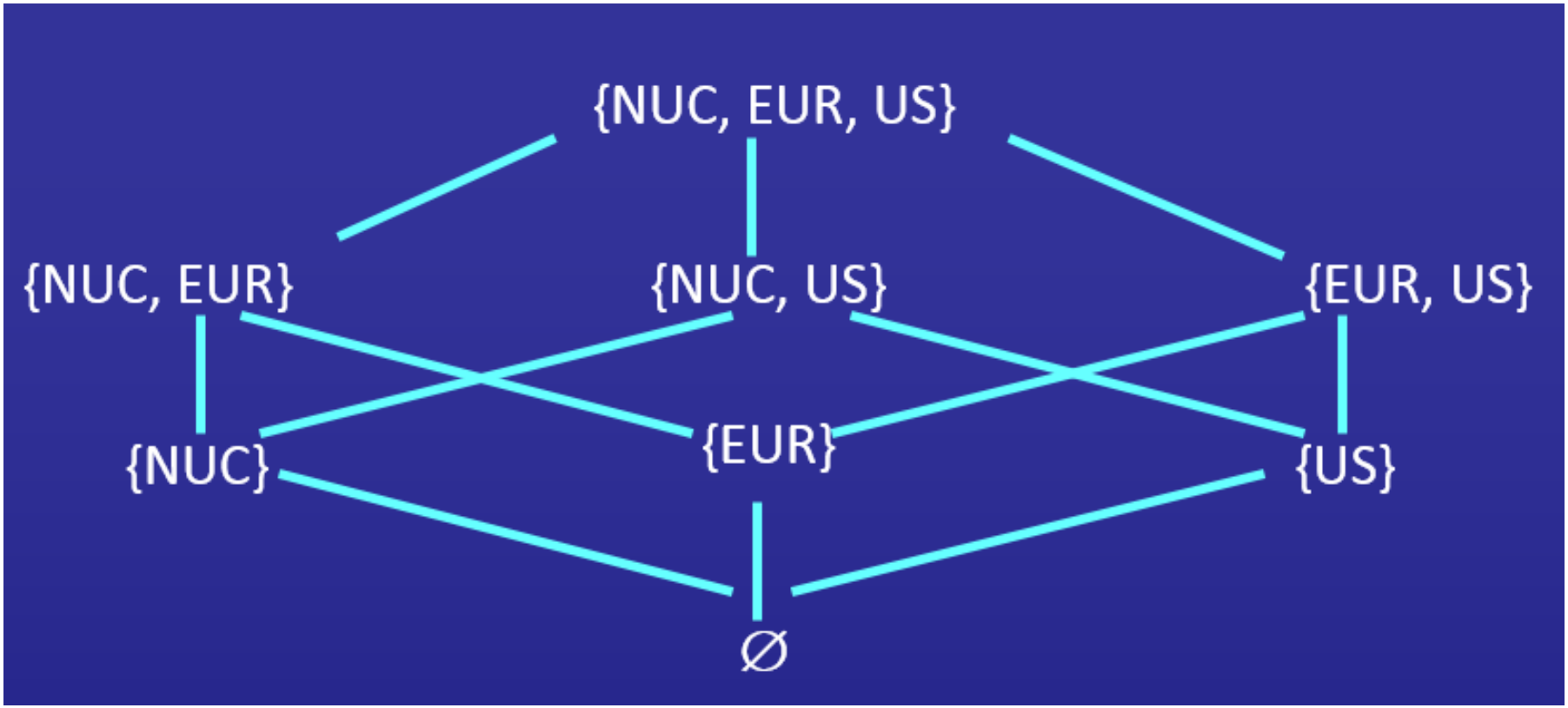
MULTICS Example



BLP Categories

- Expand the model to add categories to each security classification
- Objects placed in multiple categories
- Based on “need to know” principle
- Example categories: NUC, EUR, US
  - One can have access to any of these: none, {NUC}, {EUR}, {US}, {NUC, EUR}, … {NUC, EUR, US}
  - Categories form a lattice under the “subset of” operation

The Lattice Hierarchy



BLP Dominate (dom) Relationship

- Captures the combination of security classification and category set
- (A, C) ***dom*** (A', C') iff $A' \leq A$ and $C' \subseteq C$
- Examples
  - (Top Secret, {NUC, ASI}) ***dom*** (Secret, {NUC})
  - (Secret, {NUC, EUR}) ***dom*** (Confidential,{NUC, EUR})
  - (Top Secret, {NUC}) ¬***dom*** (Confidential, {EUR})

An Example of dom Relationship

- George is cleared into security level (S, {NUC, EUR})
- `DocA` is classified as (C, {NUC})
- `DocB` is classified as (S, {EUR, US})
- `DocC` is classified as (S, {EUR})
- George dom `DocA`
- George ¬dom `DocB`
- George dom `DocC`

Reading Information - New

- Information flows ***up***, not ***down***
  - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition
  - Subject ***s*** can read object ***o*** iff ***L***(***s***) ***dom*** ***L***(***o***) and ***s*** has permission to read ***o***
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no reads up" rule

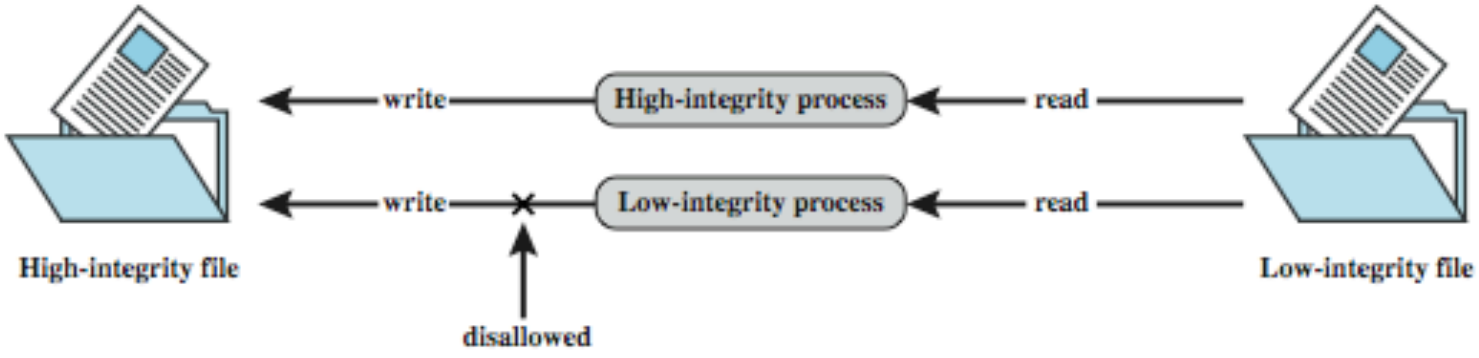
Writing Information - New

- Information flows up, not down
  - "Writes up" allowed, "writes down" disallowed

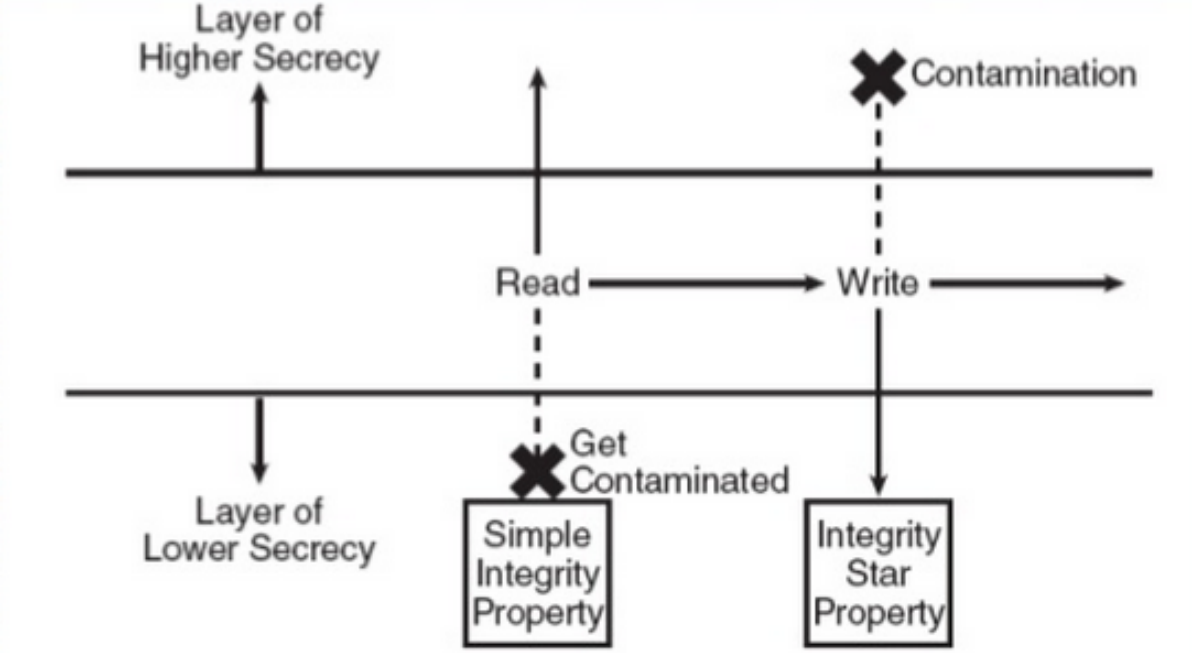
- *-Property (Step 2)
  - Subject ***s*** can write object ***o*** iff ***L*(*o*)** ***dom*** ***L*(*s*)** and ***s*** has permission to write ***o***
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no writes down" rule

Biba Integrity Model

- Various models dealing with integrity
- Strict integrity policy:
  - Simple integrity: *modify only if* $I(S) \geq I(O)$
  - Integrity confinement: *read only if* $I(S) \leq I(O)$
  - Invocation property: *invoke/comm only if* $I(S_1) \geq I(S_2)$



Biba Integrity Model



- Simple integrity: *modify only if* $I(S) \geq I(O)$
- Integrity confinement: *read only if* $I(S) \leq I(O)$
- Invocation property: *invoke/comm only if* $I(S_1) \geq I(S_2)$

Clark-Wilson Integrity Model

- Two concepts
  - Well-formed transactions: a user can manipulate data in constrained ways
  - Separation of duty: one can create a transaction but not execute it
- CDI: constrained data items (loan app; checks)
- UDI: unconstrained items
- IVPs: procedures that assure all CDIs conform to integrity/consistency rules
- TPs: transactions that change CDIs
- Very practical; used in commercial world

Certified and Enforcement Rules

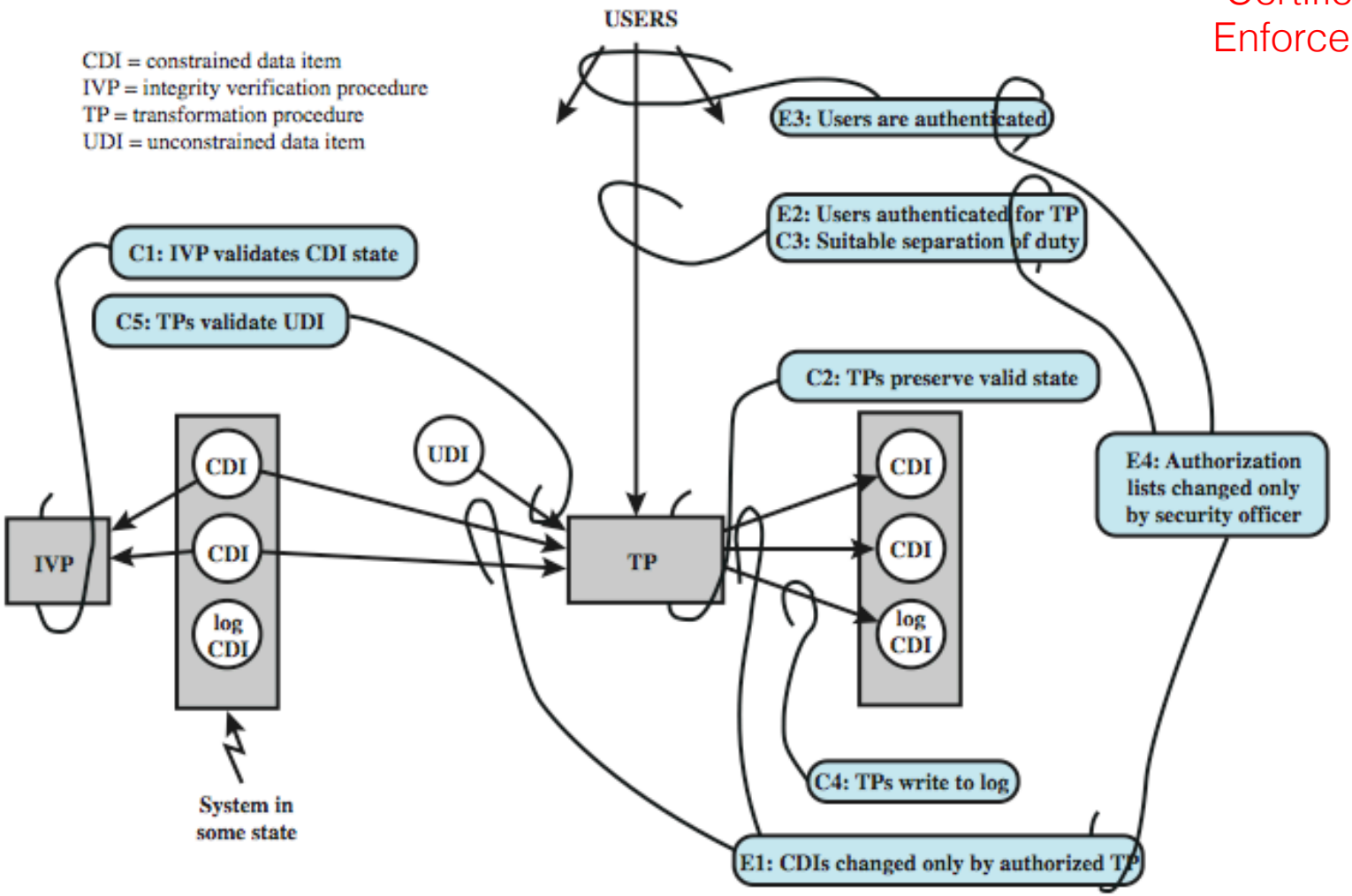
- C1: IVPs must ensure that all CDIs are in valid states
- C2: All TPs must be certified (must take a CDI from a valid state to a valid final state)
  - (Tpi, CDIa, CDIb, CDIc, …)
- E1: The system must maintain a list of relations specified in C2
- E2: The system must maintain a list of (User, Tpi, (CDIa, CDIb, …))

Certified and Enforcement Rules

- C3: The list of relations in E2 must be certified to meet separation of duties
- E3 The system must authenticate each user when executing a TP
- C4: All TPs must be certified
- C5: Any TP that takes UDI as in input value must be certified to perform valid transaction
- E4: Only the agent permitted to certify entitles is allowed to do so

Clark-Wilson Integrity Model

Certification (C) and Enforcement (E) rules



The Chinese Wall Model

- Hybrid model: addresses integrity and confidentiality
- Addresses conflict of interest (CI or CoI)
- Model elements
  - **subjects: active entities interested in accessing protected objects**
  - **information**
    - objects: individual data items, each about a corp
    - datasets (DS): all objects concerning one corp
    - CI class: datasets whose corp are in competition (conflict of interest or CI)
  - **access rules: rules for reading/writing data**

The Chinese Wall Model

- Not a true multilevel secure model
  - the history of a subject's access determines access control

- Subjects are only allowed access to info that is not held to conflict with any other info they already possess

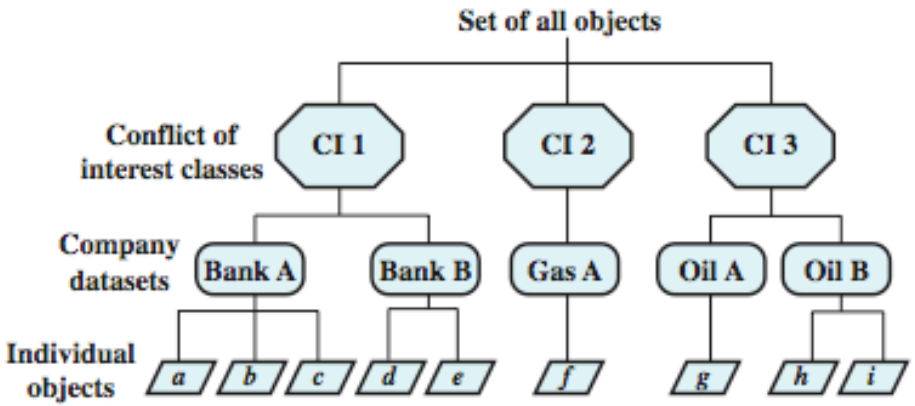
- Once a subject accesses info from one dataset, a ***wall*** is set up to protect info in other datasets in the same CI

Chinese Wall Model

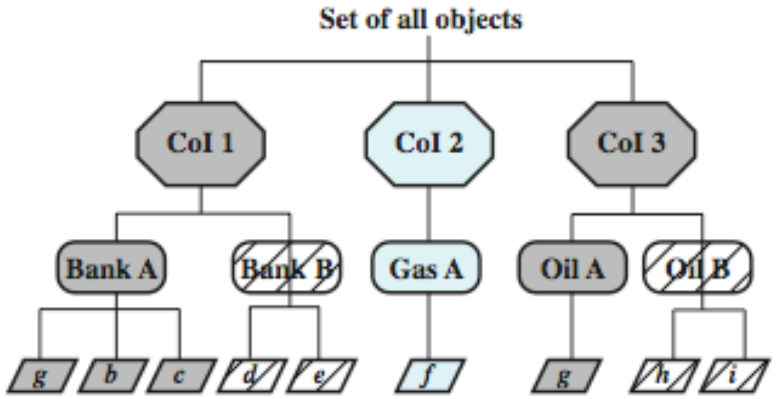
Simple sec rule (read): S can read O if O is in the same DS as an object already accessed by S OR O belongs to a CoI from which S has not yet accessed any info

***-property (write):** S can write O only if S can read O and all objects that S can read are in the same DS as O.

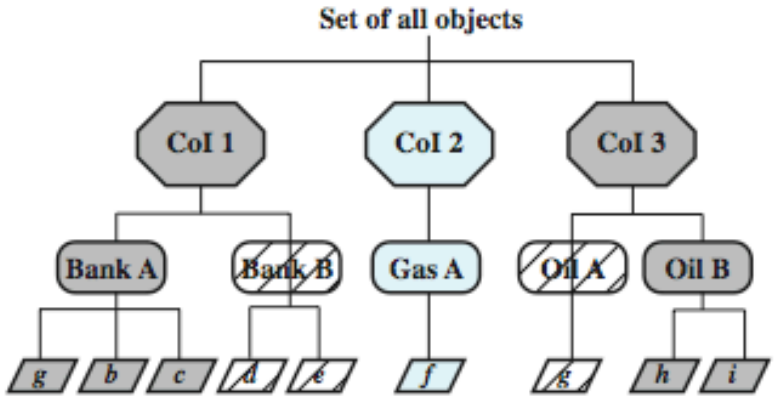
Question: what can John or Jane write to?



(a) Example set

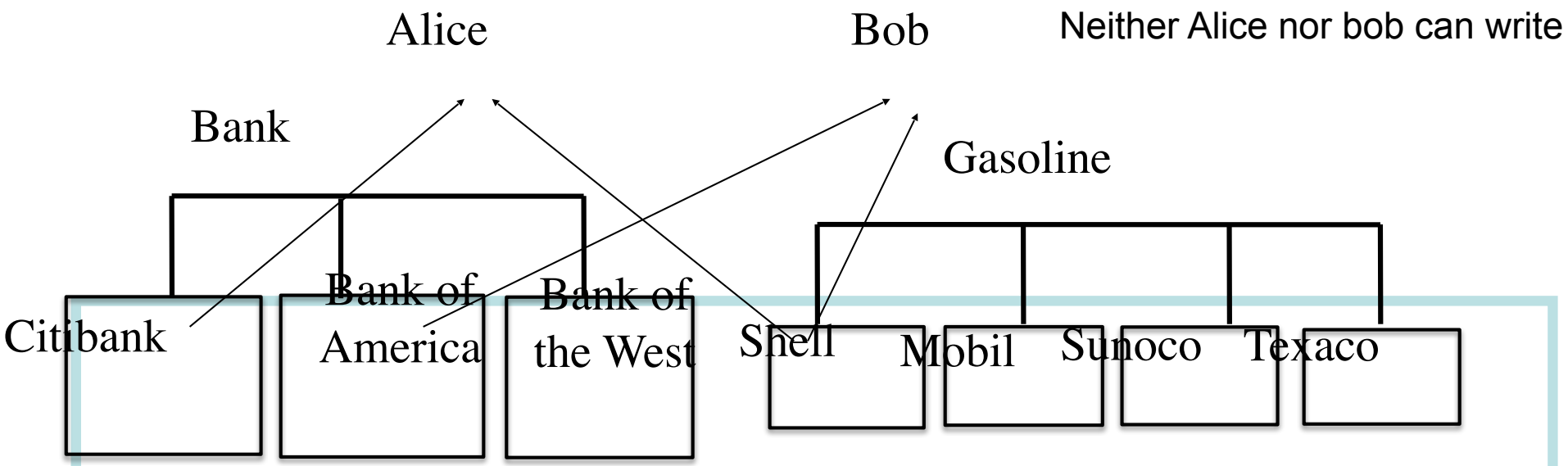


(b) John has access to Bank A and Oil A



(c) Jane has access to Bank A and Oil B

CW-*-Property



s can write to *o* iff both of the following hold:

1. The CW-simple condition permits *s* to read *o*
2. For all ***unsanitized*** objects *o′*, if *s* can read *o′*, then ***CD*** (*o′*) = ***CD*** (*o*)

- All *s* can read are either within the same CD, or sanitized

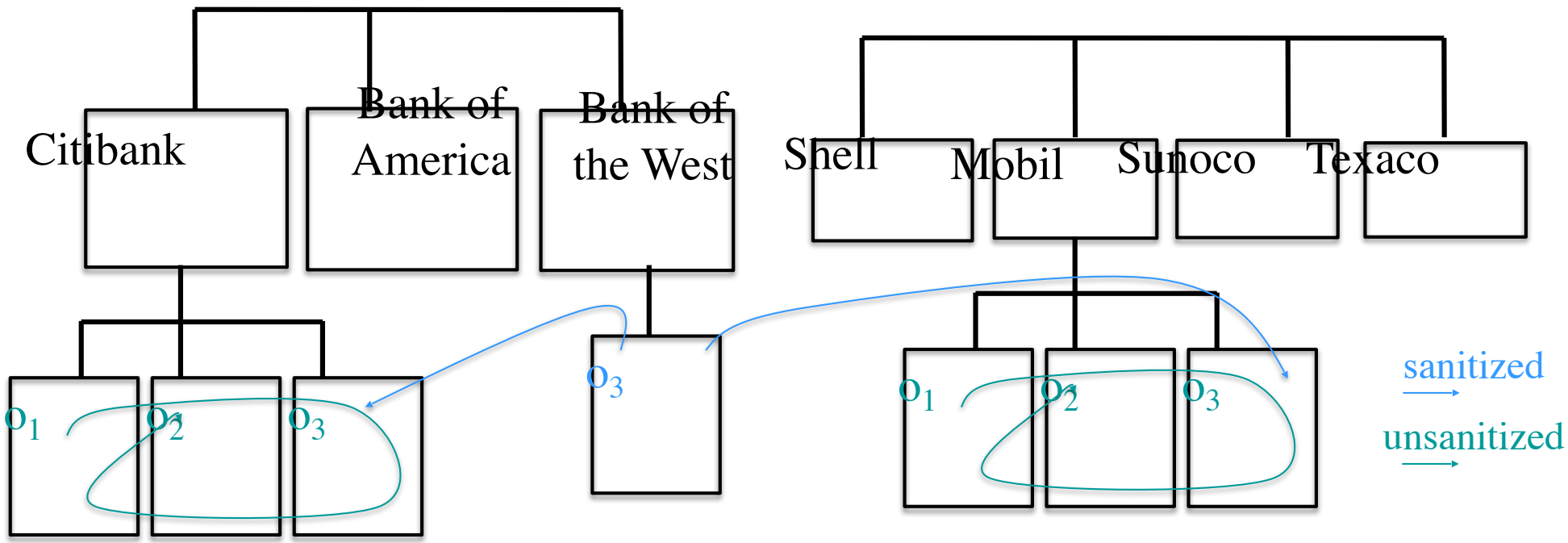
How Does Information Flow?

- With the two conditions (CW simple security condition and CW *-property) in place, how can information flow around the system?

- Main Results
  - In each COI class (e.g. Bank), a subject can only read objects in a single CD (e.g. Citibank)
  - At least ***n*** subjects are required to access all objects in a COI class with totally ***n*** CDs

How Does Information Flow? (Cont'd)

- Information flows from ***o*** to ***o'*** if ***s*** reads ***o*** and writes ***o'***
- information in an unsanitized object can only flow inside that CD; information in sanitized objects can flow freely



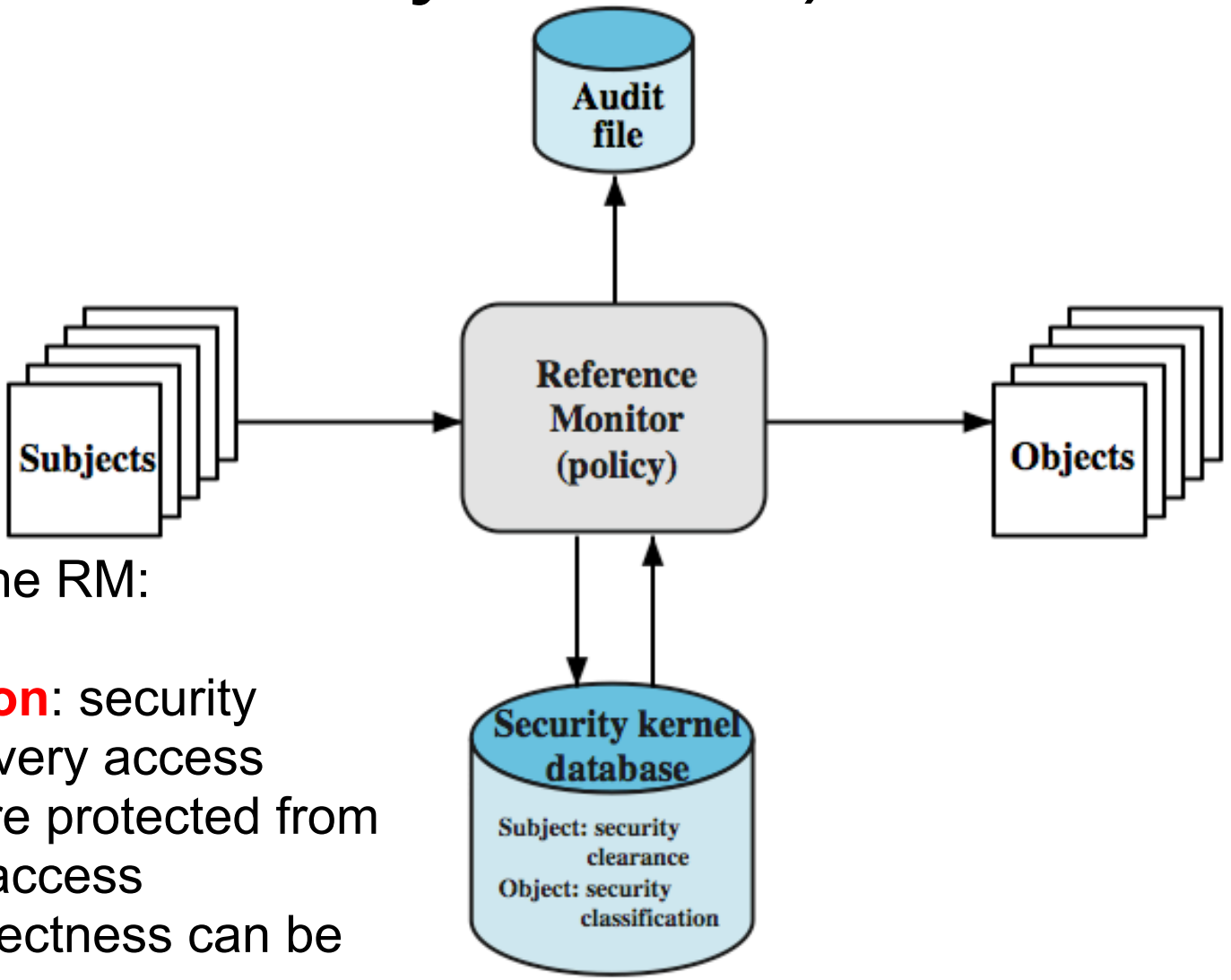
Compare CW to Bell-LaPadula

- CW is based on access history, BLP is history-less
- BLP can capture CW state at any time, but cannot track changes over time
  - BLP security levels would need to be updated each time an access is allowed

Trusted Systems

- **Trusted system**: A system believed to enforce a given set of attributes to a stated degree of assurance
- **Trustworthiness**: Assurance that a system deserves to be trusted, such that the trust can be guaranteed in some convincing way, such as through formal analysis or code review
- **Trusted computer system**: A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information

Reference Monitors (Trusted Systems)



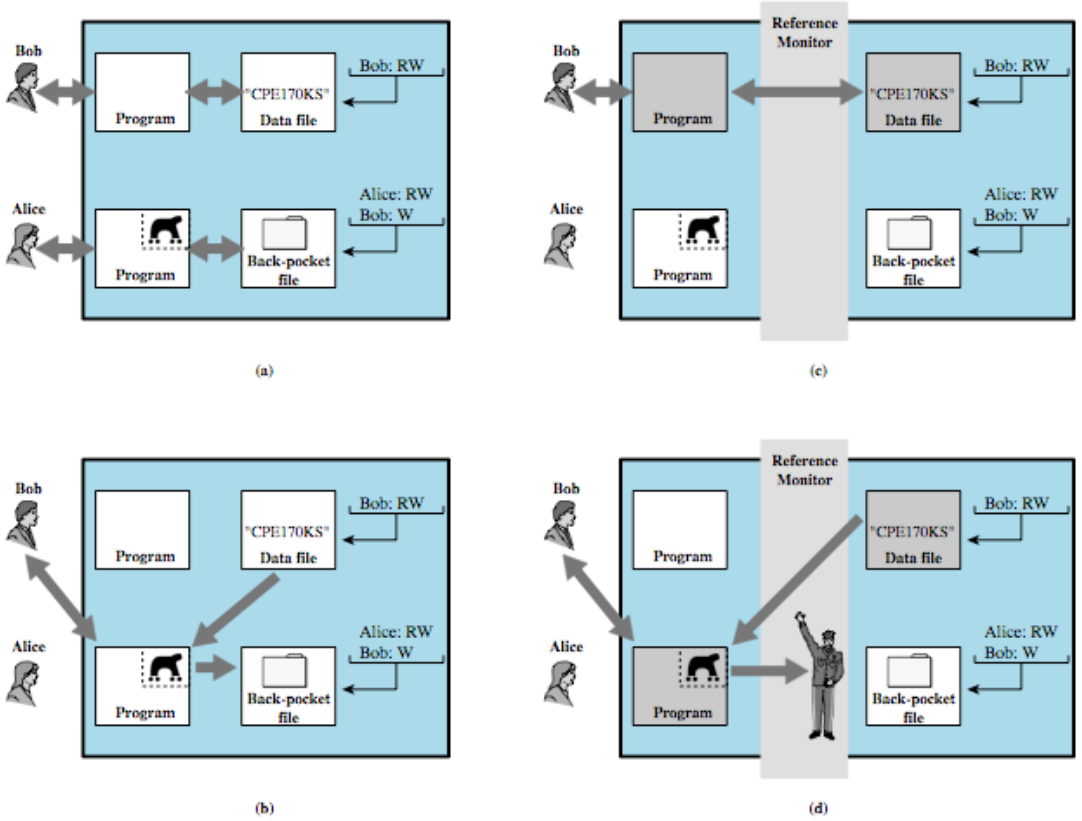
Properties of the RM:

Complete mediation: security rules enforced on every access

Isolation: RM and DB are protected from unauthorized access

Verifiability: RM's correctness can be proven

Trojan Horse Defense



security levels are assigned at login
sec levels: sensitive and public data
Trojan must have the same sec level

A “normal” OS vs a trusted OS with RM
(sec levels assigned at login thus can’t
write down)

MLS Security for Role-Based Access Control

- Role-based access control (RBAC) can implement BLP MLS rules given:
  - Security constraints on users:

  For all users u, sec-level(u) is defined
  - Constraints on read/write permissions:

  All objects have a defined r and w access permission
  - Read and write level role access definitions

  Each role r defined has r-level(r) and w-level(r)
  - Constraint on user-role assignments

  Clearance of a user must dominate the r-level and be dominated by the w-level

Database Security: Read Access

- DBMS enforces simple security rule (no read up)
- Easy if granularity is entire database or at table level
- Inference problems if have column granularity
  - If can query on restricted data can infer its existence
  - `SELECT Ename FROM Employee`
  - `SELECT Ename FROM Employee WHERE Salary > 50K`
  - Solution is to check access to all query data
- Also have problems if have row granularity
  - Null response indicates restricted/empty result
- No extra concerns if have element granularity

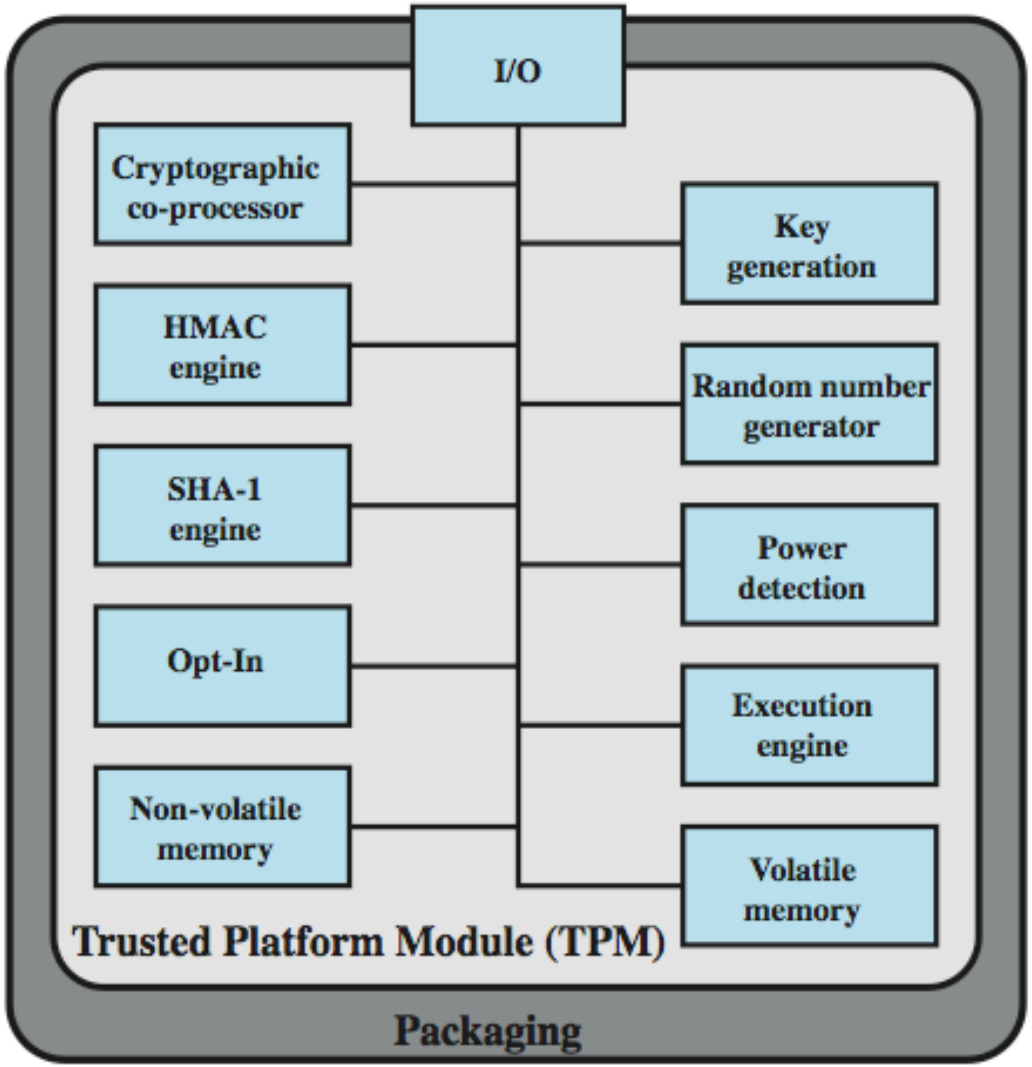
Database Security: Write Access

- Enforce *-security rule (no write down)
- Have problem if a low clearance user wants to insert a row with a primary key that already exists in a higher level row:
  - Can reject, but user knows row exists
  - Can replace, compromises data integrity
  - Polyinstantiation and insert multiple rows with same key, creates conflicting entries but plausible (and implemented in many DBs)
- Same alternatives occur on update
- Avoid problem if use database/table granularity

Trusted Platform Module (TPM)

- Concept from Trusted Computing Group
- Hardware module at heart of hardware/ software approach to trusted computing
- Uses a TPM chip on
  - motherboard, smart card, processor
  - working with approved hardware / software
  - generating and using crypto keys
- Has 3 basic services: authenticated boot, certification, and encryption

TPM Functions



Common Criteria (CC)

- ISO standards for security requirements and defining evaluation criteria to give:
  - Greater confidence in IT product security
  - Formal actions during process of:
    - development using secure requirements
    - evaluation confirming meets requirements
    - operation in accordance with requirements
- Evaluated products are listed for use

CC Requirements

- Have a common set of potential security requirements for use in evaluation
- Target of evaluation (TOE) refers product/system subject to evaluation
- Functional requirements
  - define desired security behavior
- Assurance requirements
  - that security measures effective correct
- Requirements: see pages 471-472

Assurance

- “Degree of confidence that the security controls operate correctly and protect the system as intended”
- Applies to:
  - product security requirements, security policy, product design, implementation, operation
- various approaches analyzing, checking, testing various aspects

Common Criteria (CC) Assurance Levels

- EAL 1: functionally *independently* tested
- EAL 2: structurally tested *(includes review of design and vulnerability analysis)*
- EAL 3: methodically tested and checked *(design testing)*
- EAL 4: methodically designed, tested, and reviewed *(high level to low level vulnerability analysis)*
- EAL 5: semiformally designed and tested
- EAL 6: semiformally verified design and tested
- EAL 7: formally verified design and tested (formal analysis and formally showing correspondence)

Evaluation Parties & Phases

- Evaluation parties:
  - sponsor - customer or vendor
  - developer - provides evidence for evaluation
  - evaluator - confirms requirements satisfied
  - certifier - agency monitoring evaluation process
- Phases:
  - preparation (initial contact)
  - conduct of evaluation (structured process)
  - conclusion (final evaluation)
- Government agency regulates: NIST, NSA jointly operate Common Criteria Eval and Validation Scheme (US CCEVS)

Chapter 14 – IT Security Management and Risk Assessment

Overview

- security requirements means asking
  - what assets do we need to protect?
  - how are those assets threatened?
  - what can we do to counter those threats?

- IT security management answers these
  - determining security objectives and risk profile
  - perform security risk assessment of assets
  - select, implement, monitor controls

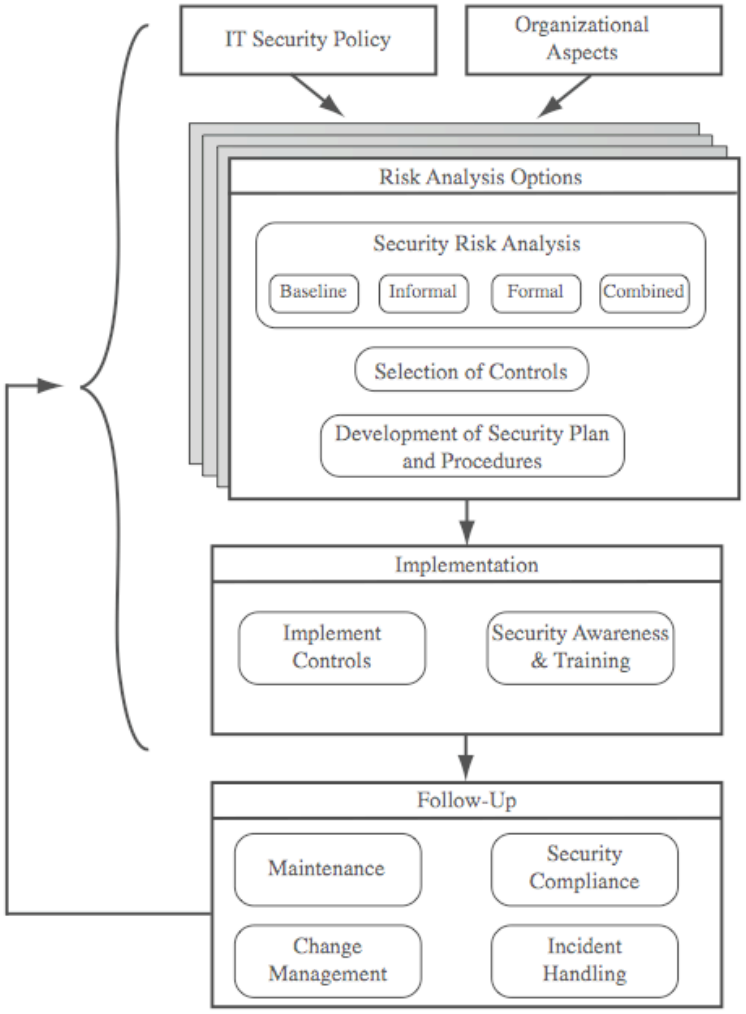
IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

ISO 27000 Security Standards

ISO27000	a proposed standard which will define the vocabulary and definitions used in the 27000 family of standards.
ISO27001	defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2.
ISO27002 (ISO17799)	currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best-practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1.
ISO27003	a proposed standard containing ***implementation guidance*** on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008.
ISO27004	a draft standard on information security ***management measurement*** to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007.
ISO27005	a proposed standard on information ***security risk management***. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/9.
ISO13335	provides guidance on the ***management of IT security***. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1-5.

IT Security Management Process



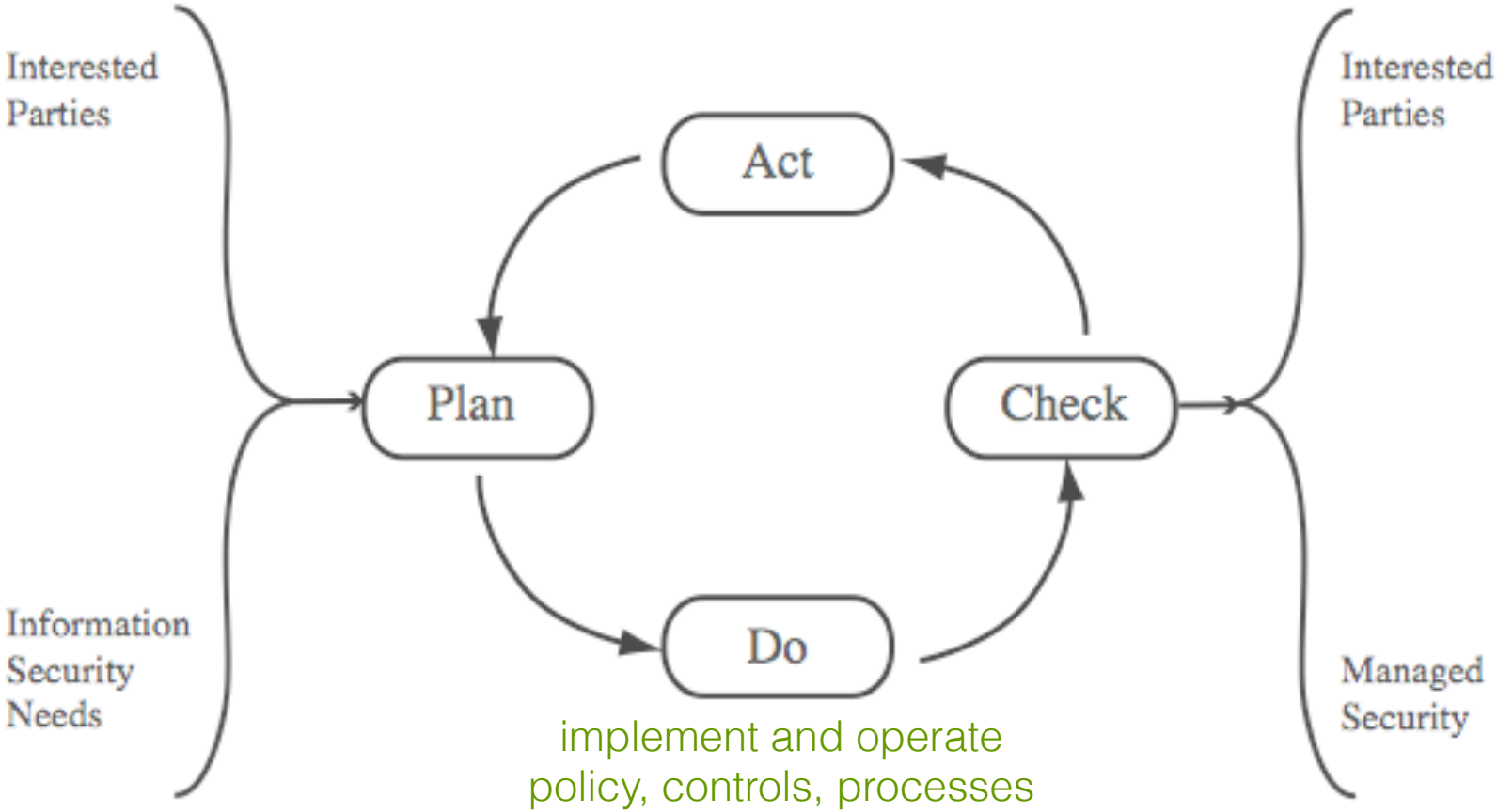
Plan - Do - Check – Act

(Deming Cycle)

establish policy; define objectives and processes

take corrective and preventative actions (based on audits)

assess and measure and report results



implement and operate policy, controls, processes

Organizational Context and Security Policy

- first examine organization's IT security:
  - objectives - wanted IT security outcomes
  - strategies - how to meet objectives
  - policies - identify what needs to be done
- maintained and updated regularly
  - using periodic security reviews
  - reflect changing technical/risk environments

Security Policy: Topics to Cover

- needs to address:
  - scope and purpose including relation of objectives to business, legal, regulatory requirements
  - IT security requirements
  - assignment of responsibilities
  - risk management approach
  - security awareness and training
  - general personnel issues and any legal sanctions
  - integration of security into systems development
  - information classification scheme
  - contingency and business continuity planning
  - incident detection and handling processes
  - how when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- need IT security officer
  - to provide consistent overall supervision
  - manage process
  - handle incidents
- large organizations needs IT security officers on major projects/teams
  - manage process within their areas

Security Risk Assessment

- critical component of process
  - else may have vulnerabilities or waste money
- ideally examine every asset vs risk
  - not feasible in practice
- choose one of possible alternatives based on organization's resources and risk profile
  - baseline
  - informal
  - formal
  - combined

Baseline Approach

- use “industry best practice”
  - easy, cheap, can be replicated
  - but gives no special consideration to org
  - may give too much or too little security
- implement safeguards against most common threats
- baseline recommendations and checklist documents available from various bodies
- alone only suitable for small organizations

Informal Approach

- conduct informal, pragmatic risk analysis on organization's IT systems
- exploits knowledge and expertise of analyst
- fairly quick and cheap
- does address some org specific issues
- some risks may be incorrectly assessed
- skewed by analysts views, varies over time
- suitable for small to medium sized orgs

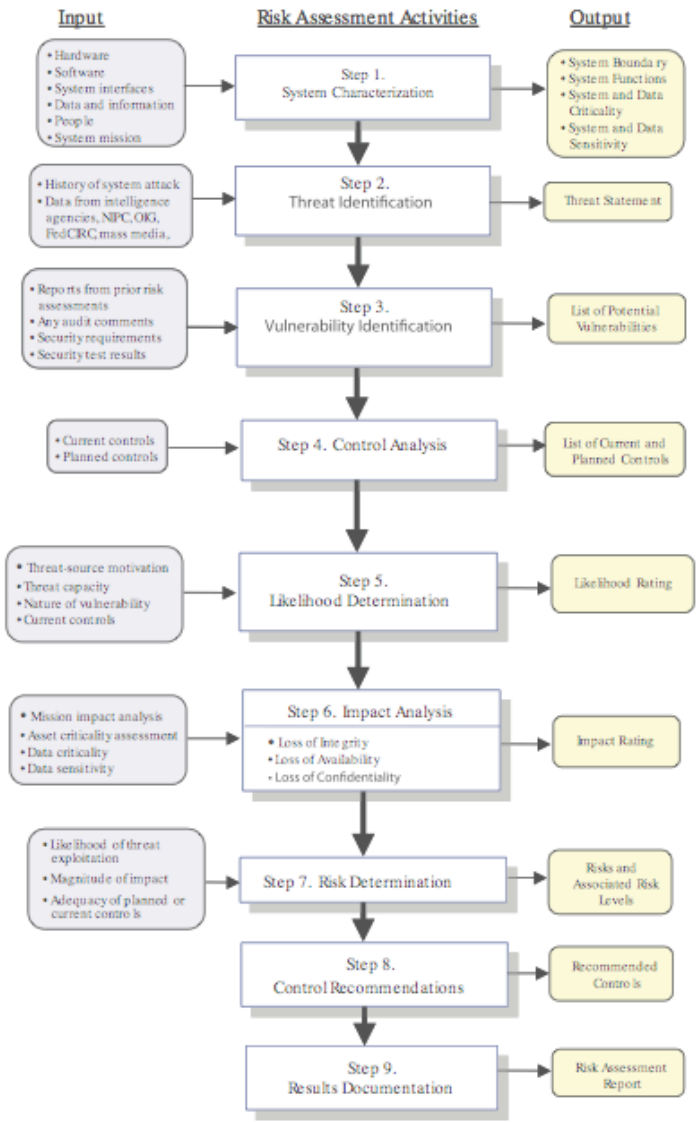
Detailed Risk Analysis

- most comprehensive alternative
- assess using formal structured process
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- costly and slow, requires expert analysts
- may be a legal requirement to use
- suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- combines elements of other approaches
  - initial baseline on all systems
  - informal analysis to identify critical risks
  - formal assessment on these systems
  - iterated and extended over time
- better use of time and money resources
- better security earlier that evolves
- may miss some risks early
- recommended alternative for most orgs

Detailed Risk Analysis Process



Establish Context

- determine broad risk exposure of org
  - related to wider political/social environment
  - legal and regulatory constraints
- specify organization's risk ***appetite***
- set boundaries of risk assessment
  - partly on risk assessment approach used
- decide on risk assessment criteria used

Asset Identification

- identify assets
  - “anything which needs to be protected”
  - of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- draw on expertise of people in relevant areas of organization to identify key assets
  - identify and interview such personnel
  - see checklists in various standards

Terminology

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification

- to identify threats or risks to assets asK
  - who or what could cause it harm?
  - how could this occur?

- threats are anything that hinders or prevents an asset providing appropriate levels of the key security services:
  - confidentiality, integrity, availability, accountability, authenticity and reliability

- assets may have multiple threats

Threat Sources

- threats may be
  - natural “acts of god”
  - man-made and either accidental or deliberate
- should consider human attackers
  - motivation
  - capability
  - resources
  - probability of attack
  - deterrence
- any previous history of attack on org

Threat Identification

- depends on risk assessors experience
- uses variety of sources
  - natural threat chance from insurance stats
  - lists of potential threats in standards, IT security surveys, info from governments
  - tailored to organization's environment
  - and any vulnerabilities in its IT systems

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems or processes
- hence determine applicability and significance of threat to organization
- need combination of threat and vulnerability to create a risk to an asset
- again can use lists of potential vulnerabilities in standards etc

Analyze Risks

- specify likelihood of occurrence of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce exposure of org to some risks
- specify consequence should threat occur
- hence derive overall risk rating for each threat
  risk = probability threat occurs x cost to organization
- in practice very hard to determine exactly
- use qualitative not quantitative, ratings for each
- aim to order resulting risks in order to treat them

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Determine Consequence

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last ***up to 2 weeks*** and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last ***4-8 weeks*** and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for ***3 months or more*** and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

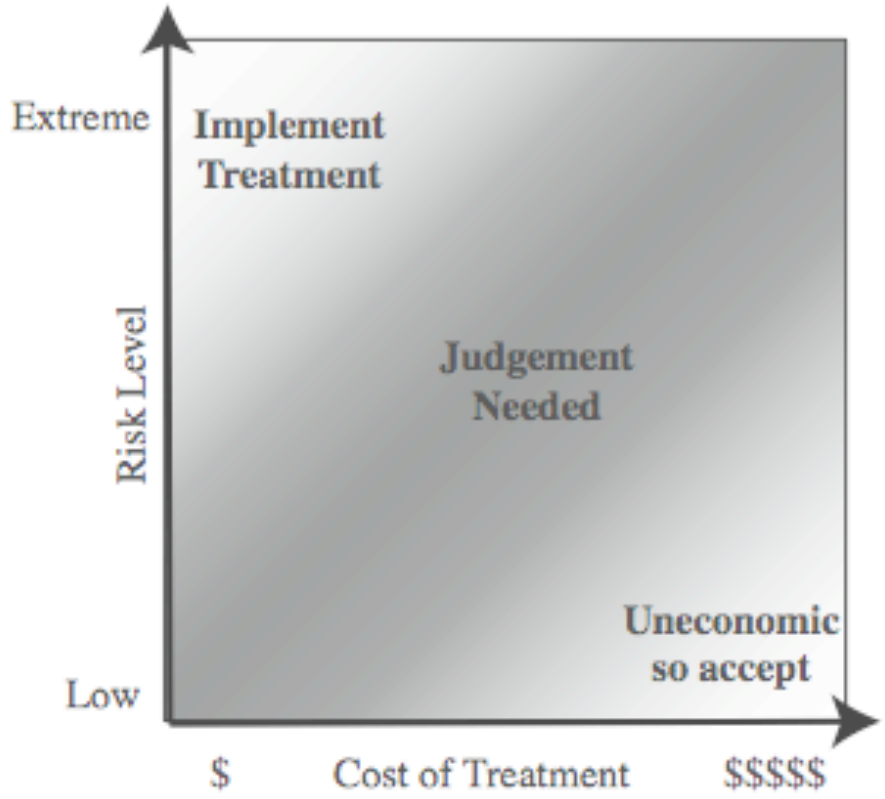
	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed r esearch and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Document in Risk Register and Evaluate Risks

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment



Risk Treatment Alternatives

- **risk acceptance**: *accept risk (perhaps because of excessive cost of risk treatment)*
- **risk avoidance**: *do not proceed with the activity that causes the risk (loss of convenience)*
- **risk transfer**: buy insurance; outsource
- **reduce consequence**: *modify the uses of an asset to reduce risk impact (e.g., offsite backup)*
- **reduce likelihood**: *implement suitable controls*

Case Study: Silver Star Mines

- fictional operation of global mining company
- large IT infrastructure
  - both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked
- decided on combined approach
- mining industry less risky end of spectrum
- management accepts moderate or low risk

Assets

- reliability and integrity of SCADA nodes and net
- integrity of stored file and database information
- availability, integrity of financial system
- availability, integrity of procurement system
- availability, integrity of maintenance/production system
- availability, integrity and confidentiality of mail services

Threats & Vulnerabilities

- unauthorized modification of control system
- corruption, theft, loss of info
- attacks/errors affecting procurement system
- attacks/errors affecting financial system
- attacks/errors affecting mail system
- attacks/errors maintenance/production affecting system

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Summary

- detailed need to perform risk assessment as part of IT security management process
- relevant security standards
- presented risk assessment alternatives
- detailed risk assessment process involves
  - context including asset identification
  - identify threats, vulnerabilities, risks
  - analyse and evaluate risks
- Silver Star Mines case study