[l04] solutions

[l04_t01] policies

wim mees

introduction

learning objectives

- know and understand different policies for protecting security characteristics of information:
  - for confidentiality and integrity,
  - as well as for specific business constraints

policies

policies

why ?

- why security ? protection of assets against threats
- based on a high-level risk management process
- this is translated into
  "security requirements" or *"security objectives"*

what is a *"policy"* ?

set of rules that implement security requirements or goals

policies

policies at different levels

- **"meta-policy":** overall security goals
  - expressed in terms of confidentiality, integrity, and availability of business processes and information
  - too general to provide practical guidance as such
- **"policy":** system-specific refinement of a meta-policy
  - different policy solutions can exist for implementing the same meta-policy
  - provides specific and enforceable guidance to system developers, administrators, and users
  - expressed in terms of mechanisms like access control, firewall rules, encryption, ...
  - may seem arbitrary if you do not know the overarching meta-policy

example

De Regie der Gebouwen heeft gevoelige informatie over gevangenissen, justitiehuizen en -paleizen en Europese gebouwen zonder beveiliging op haar site laten rondslingeren. Hoe is het mogelijk dat belangrijke gegevens zo slecht beveiligd zijn?

De Regie der Gebouwen, de vastgoedbeheerder van de federale overheid, maakt een bijzonder slechte beurt. Lange tijd stonden gedetailleerde grondplannen van belangrijke gebouwen in ons land op haar website. De Regie haalde die informatie pas offline toen De Morgen haar contacteerde. Via het intussen offline gehaalde internetadres buildingsagency.be/bestekken was informatie over een waslijst van gebouwen voor iedereen toegankelijk.

Figure 1: http://www.demorgen.be/binnenland/zo-raakt-u-toch-binnen-in-zwaar-beveiligde-gebouwen-b74f4f44/

example

De Regie der Gebouwen zette per abuis plattegronden van gevangenissen en justitiepaleizen online. Het is nu 48 uur later en toch kan de vastgoedspecialist nog steeds niet zeggen hoelang dat al zo was, en hoe vaak ze zijn gedownload. "We zijn een onderzoek gestart."

Zaterdagochtend was er crisisoverleg tussen leden van het kabinet van minister van Binnenlandse Zaken Jan Jambon (N-VA) en Laurent Vrijdaghs, de administrateur-generaal van de Regie der Gebouwen. "Hij viel net als iedereen uit de lucht", zegt Olivier Van Raemdonck, de woordvoerder van Jambon. "Het is nog steeds niet duidelijk waarom deze documenten online zijn komen te staan.

Figure 2: http://www.demorgen.be/binnenland/regie-der-gebouwen-kan-nog-niet-zeggen-hoelang-plattegronden-online-stonden-bd6b8f1a/

example

Opnieuw staan er plannen van belangrijke gebouwen in ons land zomaar online. Tot het militaire legerhoofdkwartier in Evere en een federale politiekazerne toe, deze keer. Hoe is het mogelijk dat de overheid zo blijft blunderen met zeer gevoelige informatie?

Veel wranger kan het niet, het document dat te vinden is op de website van de Regie der Gebouwen. "Ter beschikking stelling van een consultant (voltijds) voor bijstand bij het beheer van de informaticasystemen van de Regie der Gebouwen", zo luidt de titel van het pdf-bestand. Het gaat om een openbare aanbesteding waarvoor geïnteresseerde IT-consultancybedrijven zich op 30 oktober van dit jaar mogen aanmelden bij de overheidsdienst.

Figure 3: http://www.demorgen.be/binnenland/overheid-blijft-blunderen-met-gevoelige-informatie-bc5a5c90/

example

- there were probably a lot of “policies” in place
  - firewall policies
  - access control policies
  - ...
- perhaps there was no overarching meta-policy that was translated into a comprehensive set of policies ?

access control

some definitions

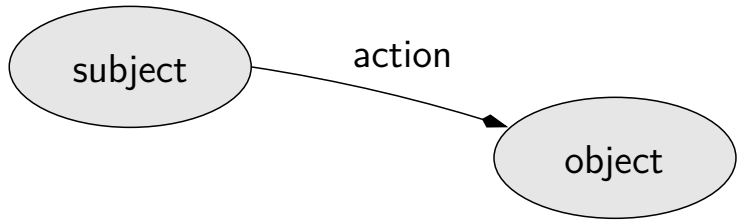

Figure 4: *"subject" performs "action" on "object"*

definitions

- **"objects:"** information containers protected by the system (files, directories, databases, records in a database, . . .)
- **"subjects:"** entities (users, processes, . . .) that request access to and execute activities on objects
- **"actions:"** operations, primitive (open file) or complex (pay invoice), executed on behalf of subjects that affect objects

access control policy

access control policy

rules that control which actions subjects are allowed to take with respect to objects

access control matrix

any access control policy can be represented by an ***"access control matrix"*** *(ACM)*

	O_1	...	O_N
S_1	A_i, A_j		$\emptyset$
...			
S_M	A_l		A_i, A_m

access control policy

some approaches

- **"mandatory access controls"** (MAC):
  - a set of (general) rules is enforced on every attempted access, based on specific attributes of subject and object
- **"role-based access controls"** (RBAC):
  - a set of (general) rules is enforced on every attempted access, based on the subject's current role
- **"attribute-based access controls"** (ABAC):
  - allowed actions are derived from a combination of attributes (user, device, environment, . . .)
- **"discretionary access controls"** (DAC):
  - access rules are at the discretion of individual system users
  - popular in GPOS with file ACLs configured by file's owner

multi-level security (MLS)

confidentiality in a military/government setting

11 DECEMBRE 1998. - Loi relative à la classification et aux habilitations, attestations et avis de sécurité <Intitulé remplacé par L 2005-05-03/33, art. 2, 004 ; En vigueur : 07-06-2005>
(NOTE : Consultation des versions antérieures à partir du 07-05-1999 et mise à jour au 29-04-2016)

Source : DEFENSE NATIONALE
Publication : 07-05-1999 numéro : 1999007004 page : 15752 IMAGE
Dossier numéro : 1998-12-11/61
Entrée en vigueur : 01-01-2001 (ART. 11) * 01-06-2000 (ART. (29))**

Figure 5: law of 98

CHAPITRE I. - Dispositions générales.

Article 1. La présente loi règle une matière visée à l'article 78 de la Constitution.

Figure 6: law of 98 art 1

confidentiality in a military/government setting

the objects

CHAPITRE II. - De la classification.

Art. 2. Par classification, on entend l'attribution d'un degré de protection par ou en vertu de la loi ou par ou en vertu d[illegible] traités ou conventions liant la Belgique.

Art. 3.[1 § 1er.]1 Peuvent faire l'objet d'une classification : les informations, documents ou données, le matériel, les matériaux ou matières, sous quelque forme que ce soit, dont l'utilisation inappropriée peut porter atteinte à l'un des intérêts suivants :
a) la défense de l'intégrité du territoire national et des plans de défense militaire;
b) l'accomplissement des missions des forces armées;
c) la sûreté intérieure de l'Etat, y compris dans le domaine de l'énergie nucléaire, et la pérennité de l'ordre démocratique et constitutionnel;
d) la sûreté extérieure de l'Etat et les relations internationales de la Belgique;
e) le potentiel scientifique et économique du pays;
f) tout autre intérêt fondamental de l'Etat;
g) la sécurité des ressortissants belges à l'étranger;
h) le fonctionnement des organes décisionnels de l'Etat.
(i) la sécurité des personnes auxquelles en vertu de l'article 104, § 2, du Code d'instruction criminelle, des mesures de protection spéciales sont octroyées.) <L 2002-07-07/42, art. 7, 002; En vigueur : 20-08-2002>

Figure 7: law of 98 art 2-3

confidentiality in a military/government setting

labelling the objects

Art. 4. La classification visée à l'article 3 comprend trois degrés : TRES SECRET, SECRET, CONFIDENTIEL.
Le degré TRES SECRET est attribué lorsque l'utilisation inappropriée peut porter très gravement atteinte à un des intérêts visés à l'article 3.
Le degré SECRET est attribué lorsque l'utilisation inappropriée peut porter gravement atteinte à un des intérêts visés à l'article 3.
Le degré CONFIDENTIEL est attribué lorsque l'utilisation inappropriée peut porter atteinte à un des intérêts visés à l'article 3.
L'utilisation susvisée comprend notamment la prise de connaissance, la détention, la conservation, l'utilisation, le traitement, la communication, la diffusion, la reproduction, la transmission ou le transport.

Figure 8: law of 98 art 4

confidentiality in a military/government setting

labelling the objects - high watermark

Art. 5. Le degré de classification est déterminé d'après le contenu.
Pour l'ensemble à classifier, il ne peut être donné qu'un seul degré de classification général. La classification de l'ensemble aura au moins le même degré que le degré de classification le plus élevé des composantes. L'ensemble peut, le cas échéant, recevoir un degré de classification général supérieur à celui de chacune des parties qui le composent.
L'autorité ou la personne, désignée en application de l'article 7, qui décide de la classification, décide de sa révision ou de sa suppression.

Figure 9: law of 98 art 5

confidentiality in a military/government setting

subjects

Art. 8. Nul n'est admis à avoir accès aux informations, documents ou données, au matériel, aux matériaux ou matières classifiés s'il n'est pas titulaire d'une habilitation de sécurité correspondante et s'il n'a pas besoin d'en connaître et d'y avoir accès pour l'exercice de sa fonction ou de sa mission, sans préjudice des compétences propres des autorités judiciaires (, de celles de la Cellule de traitement des informations financières et de celles des membres de l'organe de recours visé par la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité). <L 2005-05-03/33, art. 3, 004; En vigueur : 07-06-2005. Voir également son art. 8>
L'accès aux locaux, bâtiments ou sites où se trouvent des informations, documents, données, matériels, matériaux et matières classifiés peut être soumis aux mêmes conditions par les autorités désignées par le Roi.

Figure 10: law of 98 art 8

confidentiality in a military/government setting

least privilege

Art. 9. Le niveau de l'habilitation de sécurité est déterminé par le degré de classification des informations, documents ou données, du matériel, des matériaux ou matières auxquels le titulaire de l'habilitation peut devoir avoir accès pour l'exercice de sa fonction ou de sa mission.

Figure 11: law of 98 art 9

confidentiality in a military/government setting

good intentions are not enough. . .

Art. 11. Le titulaire d'une habilitation de sécurité qui, dans l'exercice de ses fonctions, utilise ou laisse utiliser au sens de l'article 4 des informations, documents ou données, du matériel, des matériaux ou matières classifiés, de manière inappropriée sera, même si cette utilisation est la conséquence d'une négligence, pour autant que celle-ci soit grave, puni d'un emprisonnement d'un mois à cinq ans et d'une amende de cent francs à cinq mille francs ou d'une de ces peines seulement.

Figure 12: law of 98 art 11

confidentiality in a military/government setting

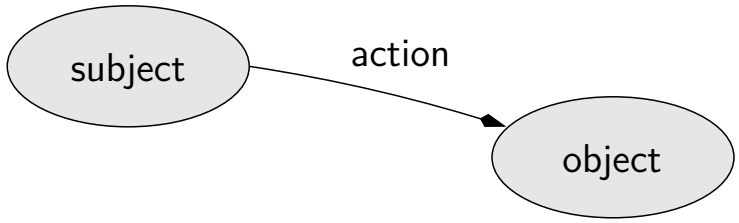

Figure 13: *"subject" performs "action" on "object"*

problem

- information (objects) at various sensitivity levels
- users (subjects) with various degrees of trustworthiness

confidentiality in a military/government setting

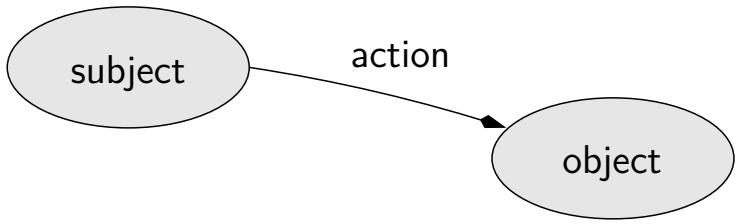

Figure 14: *"subject" performs "action" on "object"*

solution

- principle of **"least privilege"**

  a subject should have access to the minimum sufficient amount of information needed to do its job

- implemented using **"multi-level security" (MLS)**

MLS - objects

multi-level security (MLS) applied to objects

- each object is assigned
  - a single **"classification level"** L from a *linearly ordered set* (e.g. "UNCLASS", "CONFIDENTIAL", "SECRET", "TOP SECRET")
  - a subset C with one or more **"need-to-know categories"** from an *unordered set* representing all the possible interest groups ("NUCLEAR", "CRYPTO", "HR", "FINANCIAL", R&T", ...)
- example
  - docA is labelled ("SECRET", { "CRYPTO", "R&T"})
  - docB is labelled ("TOP SECRET", { "CRYPTO" })

MLS - objects

some questions

- who determines the level and categories of a document ?
  - security officer produces guidelines on how to label
  - creator/owner of document selects its level and categories
- how to label a document with "mixed information" ?
  - the highest appropriate hierarchical level
  - the union of all relevant categories
- can the level of a document be modified ?
  - "downgrading" or "upgrading" is possible when justified
  - is typically an expensive manual process

MLS - subjects

multi-level security (MLS) applied to subjects

- each subject is assigned
  - a hierarchical security level (“*clearance*”) that indicates the degree of trustworthiness to which the subject has been vetted
  - a set of need-to-know categories indicating domains of interest in which the subject is authorized to operate

MLS - relations

(l_1, C_1) dominates (l_2, C_2) iff

1. $l_1 \geq l_2$ in the ordering on levels, and
2. $C_1 \supseteq C_2$

notes

- this is usually written as $(l_1, C_1) \geq (l_2, C_2)$
- domination is a *"partial order"* ; there are labels A and B such that neither $A \geq B$ nor $B \geq A$ (they are *"incompatible"*)

MLS - simple security property

simple security property

- subject S with clearance (l_S, C_S) may be granted **read access** to object O with classification (l_O, C_O) only if $(l_S, C_S) \geq (l_O, C_O)$
- this captures our intuition about when a subject is to be allowed to **read** an object

remaining problem

- someone with access to a "SECRET" file could copy (part of) its content to an "UNCLASS" file
  - simple security property has **not** been violated
  - however, confidentiality has certainly been violated!
- may seem obvious to a human user, but what about a program running with his privileges (possibly a malware)?

MLS - the *-property

*-property

- subject S with clearance (l_S, C_S) may be granted **write access** to object O with classification (l_O, C_O) only if $(l_S, C_S) \leq (l_O, C_O)$

remaining problems

- commanding general with "TOP SECRET" clearance cannot email a soldier with a lower clearance...
- soldier with a lower clearance can overwrite a "TOP SECRET" war plan...
  note: this is an integrity problem, not a confidentiality problem

MLS

note

- “simple security property” also known as **“no read up”**
- "*-property" also known as **“no write down”**

remaining problem

- these rules do not prevent a change of the label assigned to an object, for instance from (“TOP SECRET”, { “ATOMAL” }), to (“UNCLASS”, {})

MLS - tranquillity properties

strong tranquillity property

subjects and objects do not change labels during the lifetime of the system

weak tranquillity property

subjects and objects do not change labels in a way that violates the "spirit" of the security policy

MLS - Bell-LaPadula Model

Bell and LaPadula have formalized (1973–75) the **"Bell-LaPadula Model"** (BLP) that consists of

- the simple security property
- the *-property
- the tranquillity property

It is a cornerstone of modern computer security
and is still very widely used as a policy.

MLS - example

BLP system with "H" $>$ "L"

subject	level	object	level
S_1	$(H, \{A, B, C\})$	O_1	$(L, \{A, B, C\})$
S_2	$(L, \{\})$	O_2	$(L, \{\})$
S_3	$(L, \{A, B\})$	O_3	$(L, \{B, C\})$

access control matrix

	O_1	O_2	O_3
S_1	?	?	?
S_2	?	?	?
S_3	?	?	?

MLS - example

BLP system with "H" $>$ "L"

subject	level	object	level
S_1	$(H, \{A, B, C\})$	O_1	$(L, \{A, B, C\})$
S_2	$(L, \{\})$	O_2	$(L, \{\})$
S_3	$(L, \{A, B\})$	O_3	$(L, \{B, C\})$

access control matrix

	O_1	O_2	O_3
S_1	R	R	R
S_2	W	R,W	W
S_3	W	R	-

BLP in a single drawing

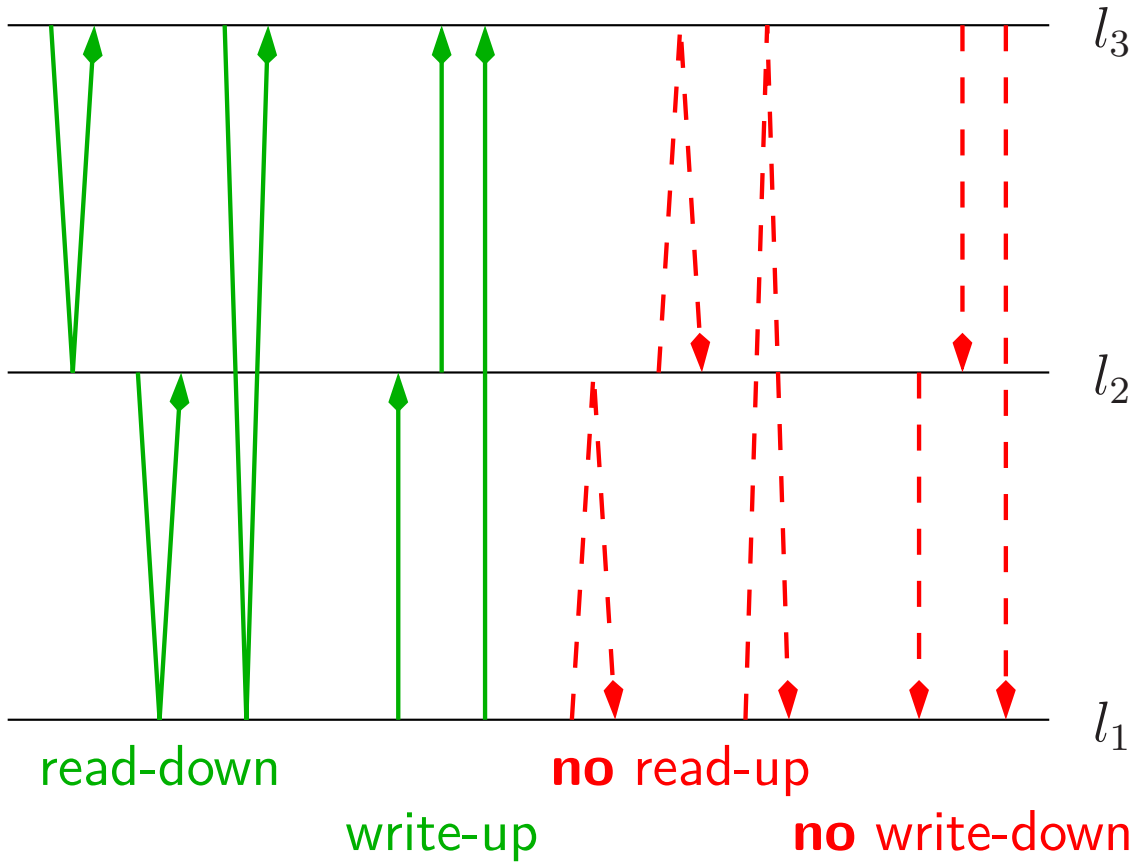

Figure 15: confidentiality policy with $l_1 < l_2 < l_3$

covert channels

simple BLP system

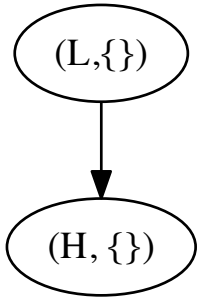

Figure 16: simple lattice with two labels and no need-to-know categories

policy: information is allowed to flow from “L” to “H”

simple BLP system

implementation:

- READ(S, O) operation
  - if object O exists and $l_S \geq l_O$
  - then return its current value
  - else return NULL
- WRITE(S, O, V) operation
  - if object O exists and $l_S \leq l_O$
  - then change the value of object O to value V
  - else do nothing

this is compatible with BLP

simple BLP system

an object O needs to be created and destroyed, therefore we add:

- CREATE(S, O) operation
  - if no object with name O exists
  - then create a new object O at level l_S
  - else do nothing
- DESTROY(S, O):
  - if an object with name O exists and $l_S \leq l_O$
  - then destroy it
  - else do nothing

this seems acceptable, **but is it really ?**

in other words, can a subject S_H (at level "H") still send information to a subject S_L (at level "L") and violate the meta-policy ?

covert channel

a subject S_H can signal one bit of information to a subject S_L:

	S_H transmits a "0"	S_H transmits a "1"
S_H does:	CREATE(S_H, F)	*nothing*
S_L does:	CREATE(S_L, F)	CREATE(S_L, F)
	WRITE(S_L, F, 1)	WRITE(S_L, F, 1)
	X = READ(S_L, F)	X = READ(S_L, F)
	DESTROY(S_L, F)	DESTROY(S_L, F)

in the first case X = NULL, in the second $X = 1$

$\Rightarrow$ **violation of the meta-policy !**

covert channel

covert channel

a path for the illegal flow of information between subjects within a system, utilizing system resources that were not designed to be used for inter-subject communication

note: *"illegal"* means in violation of the security meta-policy (e.g. there shall be no information flowing from "H" to "L"), but not necessarily in violation of a policy implementation

covert channel

main types of covert channels

- *"storage channel":* information is recorded within the system state, e.g.:
  - when S_L tries to a access a high level resource this results in one of two error messages: "resource not found" or "access denied"
  - S_H can then send a bit of information to S_L by modulating the status of this resource
- *"timing channel":* information is recorded in the ordering or duration of events on the system, e.g.:
  - S_H sends a bit by either consuming its total time-slice or by relinquishing the processor immediately
  - S_L reads the bit by consulting the system clock to see how long it gets interrupted

covert channel

some other types of covert channels

- "*implicit*": what control path does the program take?
- "*termination*": does a computation terminate?
- "*probability*": what is the distribution of system events?
- "*resource exhaustion*": is some resource depleted?
- "*power*": how much energy is consumed?

covert channel

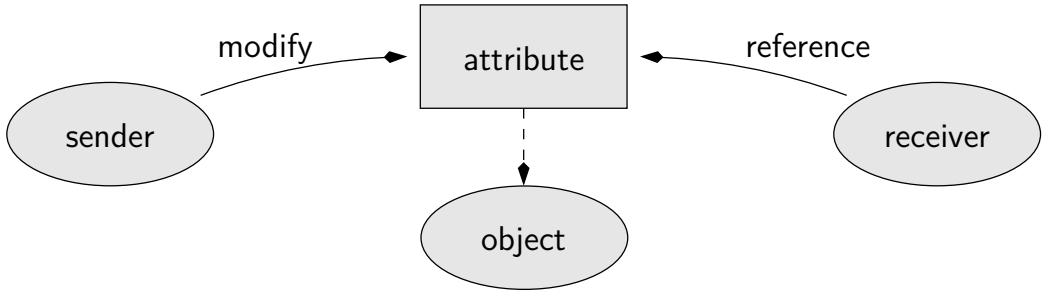

Figure 17: covert channel

conditions for a covert (storage) channel

- both sender and receiver have access to some attribute of a given object
- sender is able to modify the attribute
- receiver is able to reference (view) the attribute
- mechanism exists for initiating both processes, and sequencing their accesses to the shared resource

integrity

remember

we know the CIA triad:

- *confidentiality:* control who can read information
- *integrity:* control who can write or modify information
- *availability:* mechanisms to ensure that resources are available when needed

BLP is used for ensuring confidentiality,
but what about integrity ?

integrity

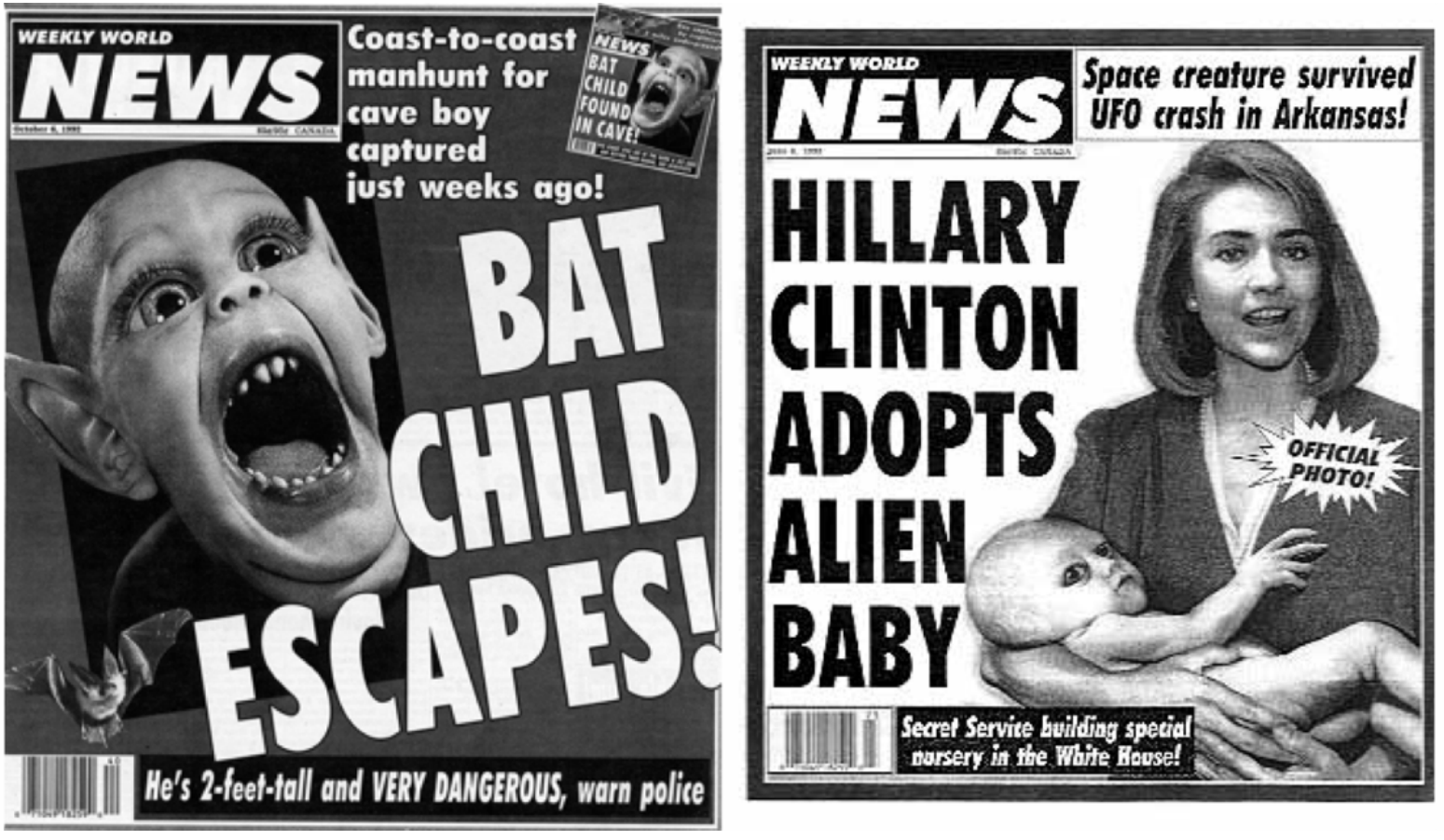

Figure 18: fake news

integrity

note:

- integrity labels are separate from classification labels: information may be of dubious validity but very sensitive, or highly reliable and of little sensitivity
- unlike confidentiality, violations of integrity do not require external action
- in some applications, particularly in the commercial world, integrity is more important than confidentiality

integrity

some principles of operation related to integrity

- *"separation of duty":* several different subjects must be involved to complete a critical function (e.g. developers of a new software version "make sure it works", and someone else "makes it live")
- *"separation of function":* if functions do not require the same resources, they do not share resources (e.g. do not develop a new version of the web site on the live system)
- *"auditing":* recoverability and accountability require maintaining an audit trail

integrity

integrity labels

- object's label: characterizes degree of trustworthiness of the information contained in the object
- subject's label: characterizes the trustworthiness of a subject to produce, protect, or modify information

integrity labels consist of (similar to BLP labels):

- a hierarchical component: gives the level of trustworthiness
- a set of categories: provides a list of domains of relevant competence

example: a physics professor could have the labels:

- ("EXPERT": { "PHYSICS" })
- ("NOVICE": { "FOOTBALL" })

integrity

"dominates" relationship can be defined as for BLP

label 1	label 2	dom?
("EXPERT": { "PHYSICS" })	("STUDENT": { "PHYSICS" })	yes
("NOVICE": { "PHYSICS", "ART"})	("EXPERT": { "PHYSICS" })	no
("STUDENT": { "ART" })	("NOVICE": { })	yes

integrity

meta-policy

"don't allow bad information to *taint* good information"

or in other words:

"don't allow information to *flow up* in the integrity hierarchy"

resulting rules in analogy with BLP

- low integrity subject is not allowed to write bad information into a high integrity object $\rightarrow$ **"no write up"**
- high integrity subject is not allowed to read bad information from a low integrity object $\rightarrow$ **"no read down"**

integrity model

Ken Biba (1977) proposed 3 integrity access control policies:

- low water mark integrity policy
- ring policy
- strict integrity policy

integrity model

low water mark integrity policy

the integrity level either

- monotonically automatically floats up (high water mark) or
- monotonically automatically floats down (low water mark), and
- may be "reset" at some point

the low water mark integrity policy consists of 2 rules:

1. if subject S reads object O then S is assigned a new integrity level $I'(S) = \min(I(S), I(O))$
2. subject S can write to object O only if $I(O) \leq I(S)$

problem: this results in an overly conservative *"label creep"* where a subject's integrity level continuously decreases

integrity model

ring policy

the ring policy consists of 2 rules:

1. any subject can read any object, regardless of integrity levels
2. subjects S can write to object O only if $I(O) \leq I(S)$

ring policy is more trusting of the subject, assuming that a subject can properly filter the information it receives

integrity model

strict integrity policy (Biba)

- **"simple integrity property":** subject S can read object O only if $I(S) \leq I(O)$
- **"integrity * -property":** subject S can write to object O only if $I(O) \leq I(S)$

example

access control policy

subjects	level	objects	level
S_1	(H,{A,B,C})	O_1	(L,{A,B,C})
S_2	(L, {})	O_2	(L, {})
S_3	(L,{A,B})	O_3	(L,{B,C})

represented as an access control matrix

	O_1	O_2	O_3
S_1	?	?	?
S_2	?	?	?
S_3	?	?	?

example model

access control policy

subjects	level	objects	level
S_1	(H,{A,B,C})	O_1	(L,{A,B,C})
S_2	(L, {})	O_2	(L, {})
S_3	(L,{A,B})	O_3	(L,{B,C})

represented as an access control matrix

	O_1	O_2	O_3
S_1	W	W	W
S_2	R	R,W	R
S_3	R	W	-

Biba in a single drawing

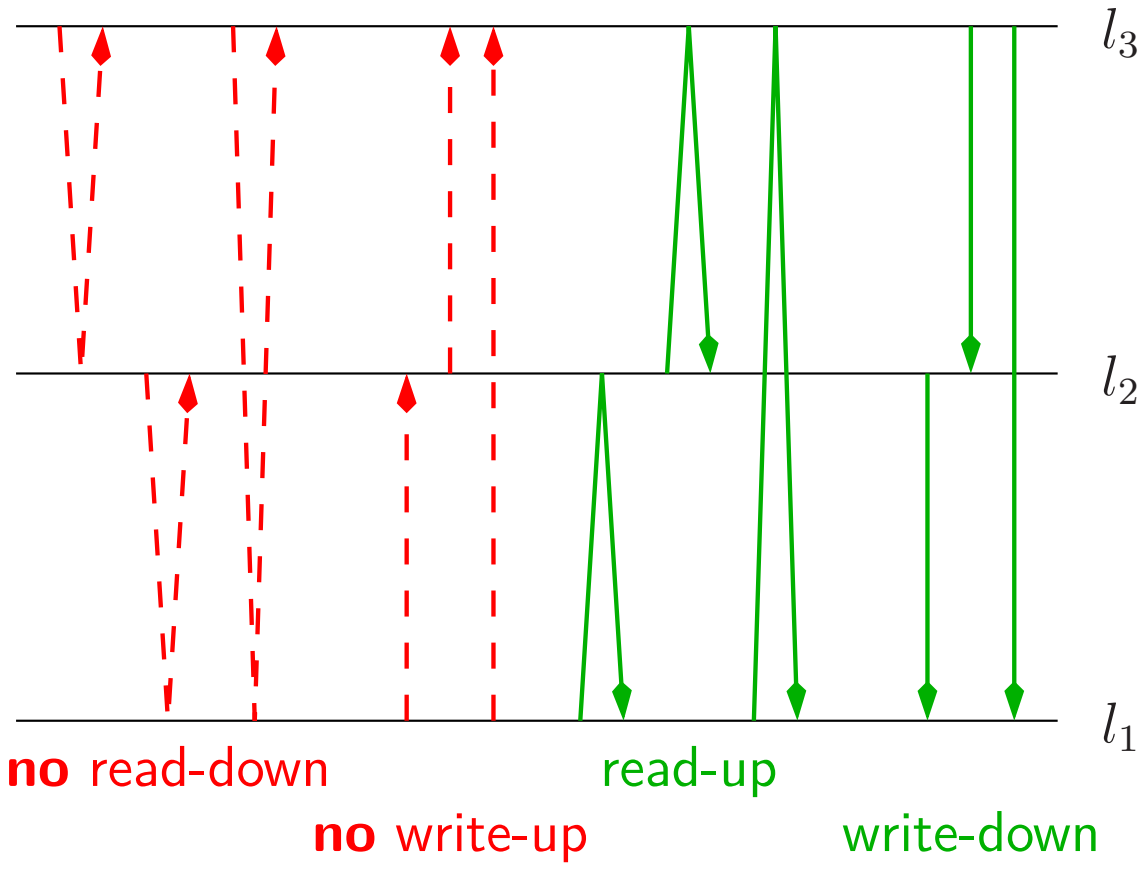

Figure 19: integrity policy with $l_1 < l_2 < l_3$

specific constraints

protecting specific business objectives

- **Chinese wall model**
  preventing conflicts of interest
- **Steve Lipner's model**
  separating software development from software usage
- **Clark-Wilson model**
  protecting business process integrity

Chinese wall model

Chinese wall policy

problem: potential for conflict of interest and inadvertent disclosure of information by a consultant or contractor

example: lawyer office specializing in product liability

- is working for Bosch (or has worked for them in the recent past)
- starts working for Siemens $\rightarrow$ conflict of interest
- starts working for Carpet Land $\rightarrow$ no conflict

solution: an appropriate access control policy

$\rightarrow$ the **Chinese wall policy**

Chinese wall policy

three levels of abstraction

- *"objects"* containing information about a single company (e.g. files, emails)
- *"company groups"* collect all *objects* concerning a particular company
- *"conflict classes"* cluster the *company groups* for competing companies

examples of conflict classes:

- { Porsche, Mercedes, Audi, VW, Ford, Open, ... }
- { BNP Fortis, KBC, ING, ... }
- { Carrefour, Delhaize, Spar, Colruyt, ... }
- { Microsoft, Apple, ... }

Chinese wall policy

two properties

- **simple security rule:** subject S can be granted access to object O only if the object:
  - is in one of the *company groups* already accessed by S before (in other words "within the Wall"), or
  - belongs to an entirely different *conflict class*
- **the * -property:** write access is only permitted if:
  - access is permitted by the simple security rule, and
  - no object can be read which is in a different *company group* than the one for which write access is requested, and contains un-sanitized information

Chinese wall policy

why is the *-property necessary ?

example:

- user A has access to FIAT and to KBC
- user B has access to AUDI and to KBC

when for instance FIAT has an account at KBC, user A might read information in the FIAT company group and write about it in objects within the KBC company group, where it then becomes accessible to user B

Lipner's model

Lipner's model

Steve Lipner (Microsoft) describes a number of concerns in a commercial data processing environment:

1. users do not write their own programs,
   but rather use existing production software
2. programmers develop and test applications
   on non-production systems
3. moving applications from development to production
   requires a special process
4. this process must be controlled and audited
5. managers and auditors must have access to system state
   and to system logs

Lipner's model

- confidentiality levels (high to low):
  - *audit manager* (AM): system audit and management
  - *system low* (SL): all other processes
- confidentiality categories:
  - *production* (SP): production code and data
  - *development* (SD): programs under development
  - *system development* (SSD): system programs in development

Lipner's model

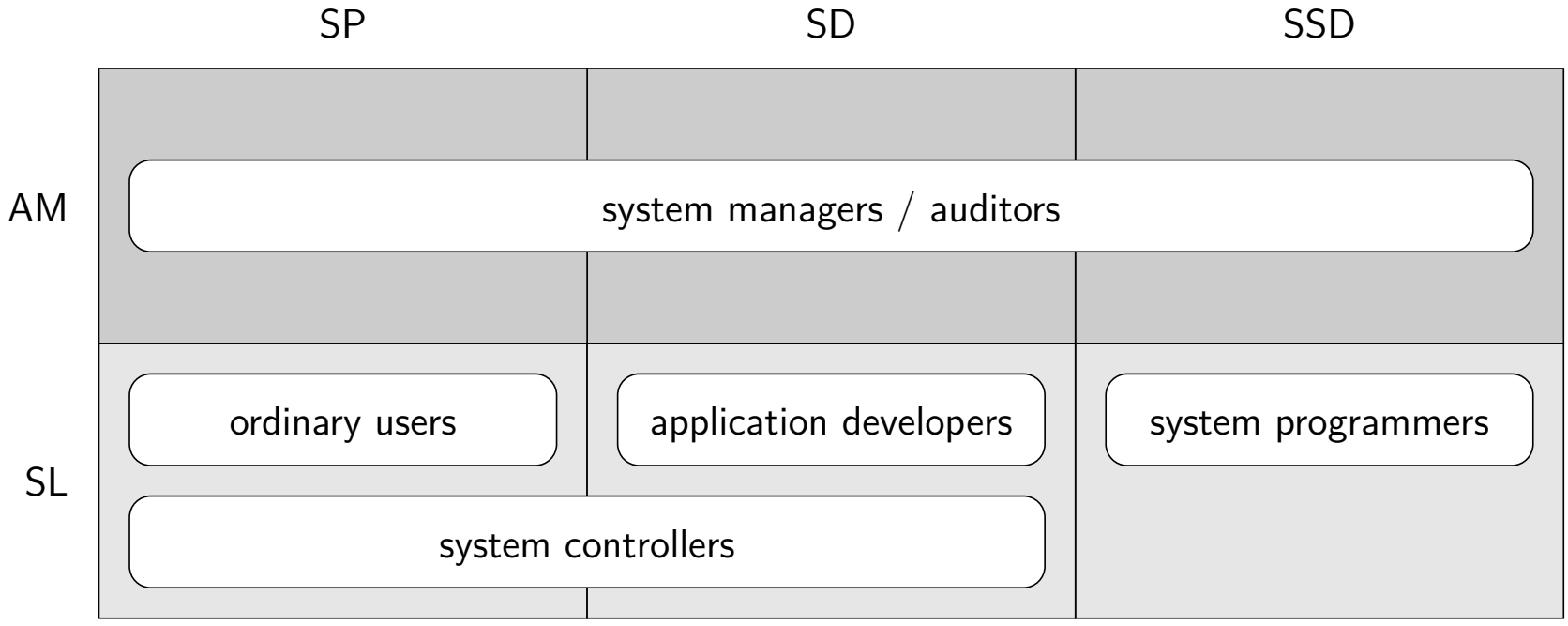

Figure 20: Lipner's use of confidentiality for subjects

Lipner's model

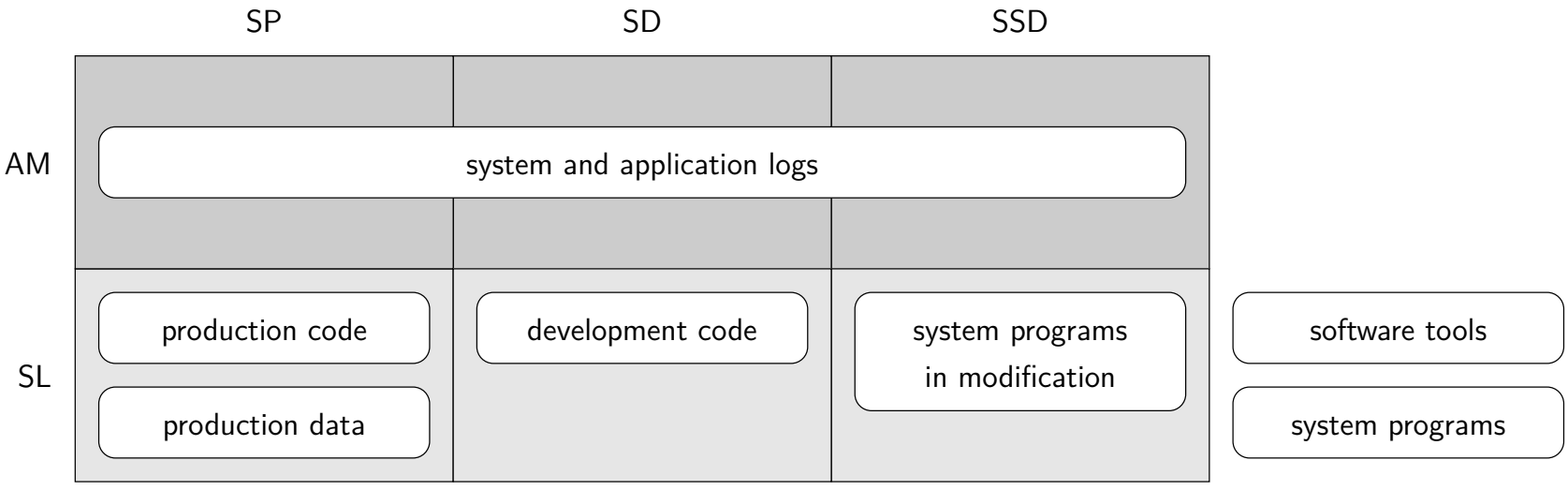

Figure 21: Lipner's use of confidentiality for objects

Lipner's model

- integrity levels (high to low):
  - *system program* (ISP): system software
  - *operational* (IO): production programs and development software
  - *system low* (ISL): user level behaviour
- integrity categories:
  - *development* (ID)
  - *production* (IP)

(additional permission: system controllers can move software objects from development to production)

Lipner's model

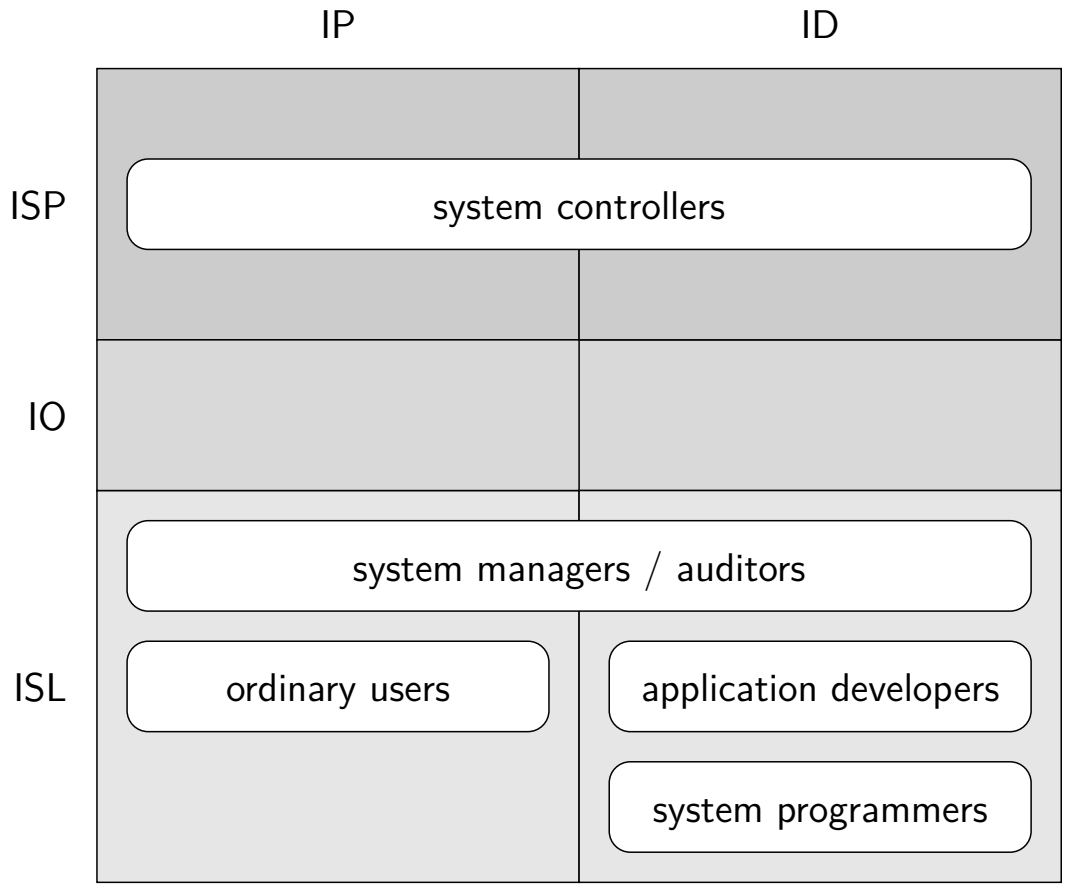

Figure 22: Lipner's use of integrity for subjects

Lipner's model

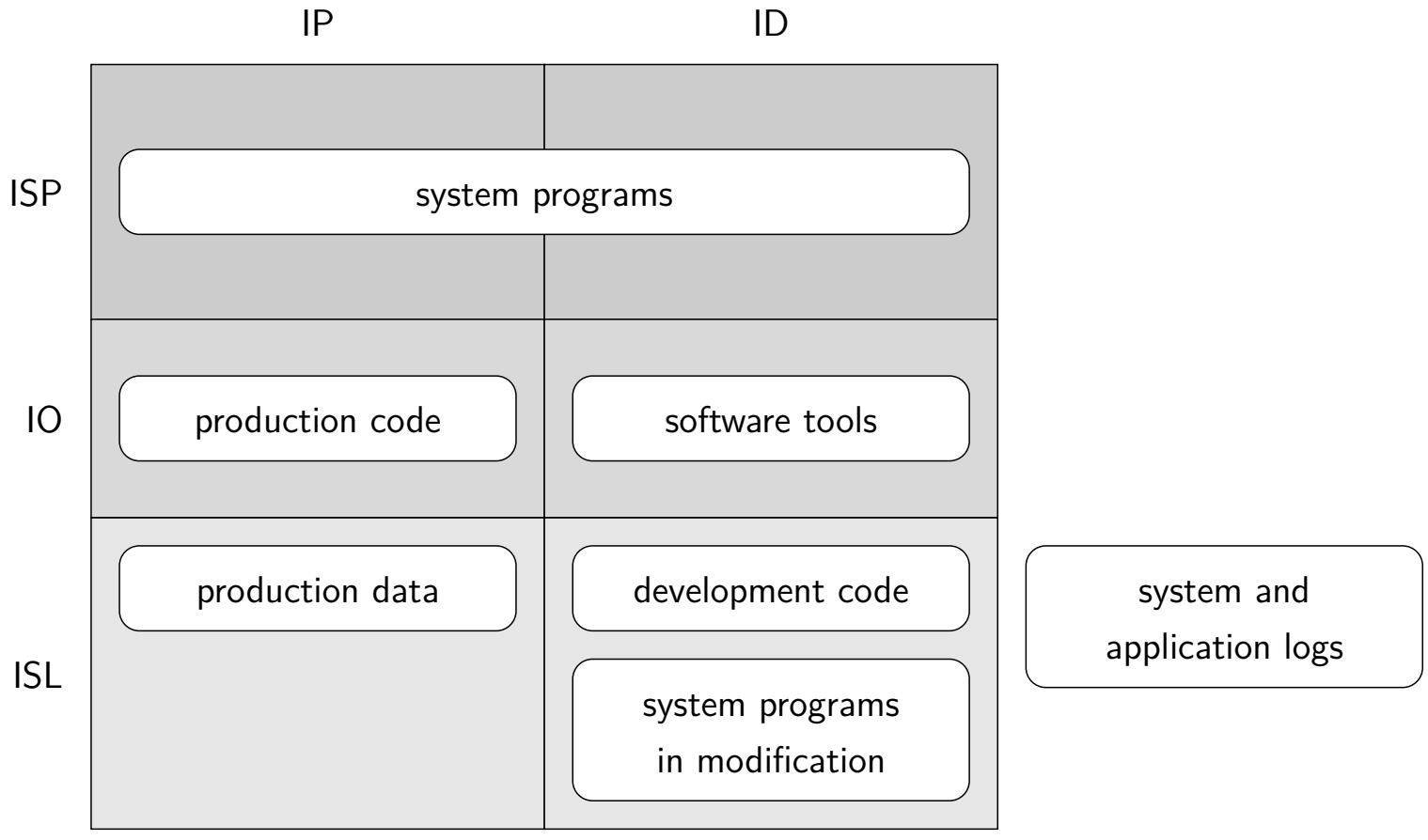

Figure 23: Lipner's use of integrity for objects

Lipner's model

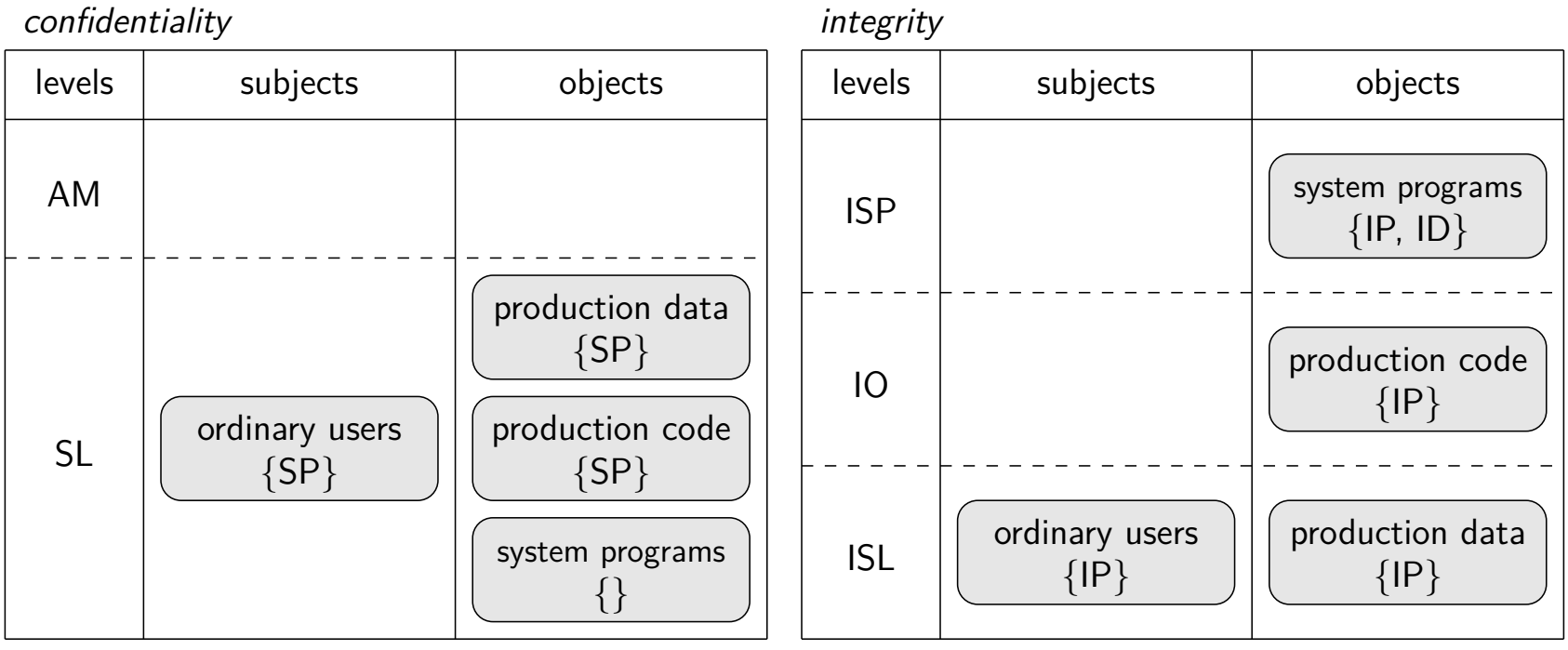

Figure 24: ordinary users as subjects

Clark-Wilson model

Clark-Wilson model

David Clark and David Wilson proposed specific model for commercial activities where consistency among various components of the system state is often more of a concern than confidentiality.

example for a bank

funds at the end of the day must be equal to funds at the beginning of the day plus the funds deposited minus the funds withdrawn

Clark-Wilson model

four fundamental concerns for a commercial integrity model

1. **authentication:** all users must be properly identified and authenticated
2. **audit:** all modifications must be logged (program executed, when, by whom, ...) in a way that cannot be subverted
3. **well-formed transactions:** users manipulate data only in constrained ways; only legitimate accesses are allowed
4. **separation of duty:** the system associates with each user a valid set of programs they can run and prevents unauthorized modifications

Clark-Wilson model

data items

- *"constrained data items"* (CDI): objects whose integrity is to be protected by the policy
- *"unconstrained data items"* (UDI): objects not covered by the integrity policy (e.g. user or network input)

procedures

- *"transformation procedures"* (TP): only procedures allowed to modify CDIs, or to take UDIs and create new CDIs; TPs are designed to take the system from one valid state to another
- *"integrity verification procedures"* (IVP): are procedures meant to verify the integrity of the CDIs in a given state

Clark-Wilson rules

there are *"certification rules"* (Cx) and *"enforcement rules"* (Ex)

- ensuring internal consistency:
  - **C1** when an IVP is executed, it must ensure the CDIs are valid
  - **C2** for some associated set of CDIs, a TP must transform those CDIs from one valid state to another
- protecting internal integrity by ensuring objects can only be changed by a specific set of trusted programs, and only specifically authorized users can use each program:
  - **E1** system must maintain a list of certified relations and ensure only TPs certified to run on a CDI change that CDI
  - **E2** system must associate a user with each TP and set of CDIs; the TP may access the CDI on behalf of the user if this is a "legal" operation

Clark-Wilson rules

- **E2** requires keeping track of triples (user, TP, {CDIs}) called "*allowed relations*", and therefore the identification and authentication of the users:
  - **E3** system must authenticate every user attempting a TP; note this is per TP request, not per login
- ensuring external consistency requires separation of duty:
  - **C3** assignment of TPs to users must meet the requirements of "separation of duty"
- integrity requires that an extensive audit trail (with "who did what") be kept:
  - **C4** all TPs must append to a log enough information to reconstruct the operation

Clark-Wilson rules

- when information enters the system, it cannot necessarily be trusted or constrained (i.e. can be a UDI):
  - **C5** any TP that takes an UDI as input may only perform valid transactions for all possible values of the UDI; the TP will either accept (convert to CDI) or reject the UDI
- finally, to prevent people from gaining access by changing qualifications of a TP:
  - **E4** only the certifier of a TP may change the list of entities associated with that TP

conclusions

conclusions

Figure 25: questions or comments ?