Policies and Models in Information Security (Part II)

Ioanna Maratsi - HT21

Integrity Policies

- *Integrity policies focus on integrity rather than confidentiality*
- *Most commercial and industrial firms are more concerned with accuracy than disclosure of information*

Integrity Policies

Principles of operation that are required to ensure data integrity:

- *Separation of duty*
- *Separation of function*
- *Auditing*

Biba integrity model (BIM)

- Another development from the 1970's
- Concerned with unauthorized modification of data
- Context: Data
  - Visible to users on multiple or all security levels
  - Should be modified in controlled ways and by authorized agents only
  - The elements of the BIM have the structure as BLP (subjects and objects)
  - Each subject and object is assigned an integrity level, such as I(S) and I(O), for subject S and object O respectively

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

BIM/2

- *Strict ordering of levels from the lowest to the highest, imposed by hierarchical classification*
- *The basic model can be augmented with a set of categories*
- *Access modes*
  - *Modify – to write and update information in an object*
  - *Observe - to read information in an object*
  - *Execute – to execute an object*
  - *Invoke – a communication between two subjects*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

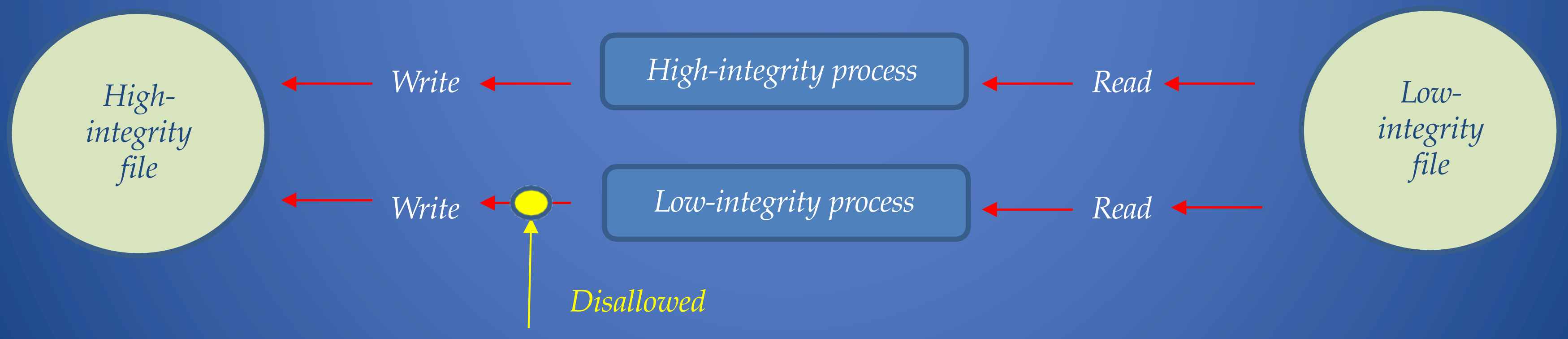
BIM/3

- *BIM modes Modify, Observe, Execute are analogous to the BLP access modes.*
- *An extension with alternative policies mapped on the model such as strict integrity policy, and the rules*
  - *Simple integrity: A subject can modify an object if the integrity level of the subject dominates the integrity level of the object I(S) >= I(O)*
  - *Integrity confinement: A subject can read an object only if the integrity level of a subject is dominated by the integrity level of an object I(S) =< I(O)*
  - *Invocation property: A subject can invoke another subject only if the integrity level of the first subject dominates the integrity level o/f the second subject I(S1) >= I(S2)*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

BIM/4

- *The Simple integrity and Integrity confinement rules are analogous to those of the BLP, but (1) deal with integrity, and (2) reverse the order.*



Contamination with Simple Integrity Controls

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

BIM/5

- Translation of the rules and the diagram
  - Simple integrity rule = the logical write-up restriction preventing contamination of high-integrity data
  - There is no problem when low-integrity process reads low-integrity file, however it should be prevented from contaminating a high-integrity file.
  - How?
  - By using the Simple integrity rule. Is this sufficient? No, since high-integrity process may copy low-integrity data in a high-integrity file.
  - It may happen due to (1) code error, and (2) Trojan horse.
  - Hence we need the Integrity confinement rule.

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Clark-Wilson Integrity Model (CWI)

- *Slightly more sophisticated and practical (late 1980's)*
- *Context: Changed from military to commercial*
- *The semantics comes from the two concepts relative to commercial security policies*
    - *Well-formed transactions – no arbitrary manipulation of data - constrained only to those that preserve the integrity of the data*
    - *Separation of duty among users – any person with a permission to create or certify well-formed transaction may not have the permission to execute it.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Clark-Wilson Integrity Model (CWI/2)

The data is said to be in a consistent state (or consistent) if it satisfies given properties.

- *Well-formed transactions*
- *Separation of duty (who examines and certifies the transactions/ who checks that they are performed correcttly?)*

For example…

Clark-Wilson Integrity Model (CWI/3)

Let D be the amount of money deposited today,

W the amount of money withdrawn today, YB the amount of money in all accounts at the end of yesterday and TB the amount of money in all accounts so far today.

The consistency property is:

$$D + YB - W = TB$$

Before and after each action, the consistency conditions must still hold!

CWI/4

- *So, we have integrity controls on data and transactions.*
- *Model structure*
  - *Constraint data items (CDIs) – subject to strict integrity controls*
  - *Unconstrained data items (UDIs) – unchecked data items*
  - *Integrity verification procedures (IVPs) - assurance that all CDIs conform to some application – specific model of integrity and consistency*
  - *Transformation procedures (TPs) – System transactions that change the state of the system from one consistent state to another*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

CWI/5

- *CWI – enforces integrity via certification and enforcement rules on TPs.*
- *Certification rules - security policy restrictions on IVPs and TPs*
- *Enforcement rules – system security mechanisms to attain the objectives of the certification rules.*
- *There are 5 certification rules and 4 enforcement rules.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

CWI model Certification Rules

- CR1 – All IVPs must ensure that all CDIs are in a valid state when IVPs run.
- CR2 –All TPs must be certified to be valid.
- CR3 - The list of relations in ER2 must be certified that they meet the separation of duty requirements.
- CR4 - All TPs must be certified – to write to an append-only CDI info on reconstructing the operation.
- CR5 – Any TP that takes UDI as an input value must be certified to perform only valid transformations.

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

CWI model Enforcement Rules

- *ER – The system must maintain a list of relations specified in rule C2.*
- *ER2 – A system must maintain a list of the form (UserID, TP1, (CDIa, CDIb, …)) which relates a user, a TP, and the data object that may be referenced by TP.*
- *ER3 – The system must authenticate the identity of each user with respect to a TP execution.*
- *ER4 – Only agents permitted to certify entities may change the list of such entities associated with the list of TPs, CDI and the list of users associated with a TP.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Comparison of the CWI and BIM

The contribution of CWI when compared to BIM:

- Certification rules: BIM has none & no mechanism/procedure is provided to verify trusted entities
- Trusted entity certification procedure BIM vs CWI

Hybrid Policies

Most organizations do not want to limit their security objectives to confidentiality OR integrity…

Instead they aim for some mixture of both.

Models for hybrid policies such as:

- *Chinese Wall Model (CWM)*
- *Clinical Information Systems Security Model*

Chinese Wall model (CWM)

- Commercial applications – possibility for a conflict of interest (CoI)
- Different approach towards confidentiality and integrity - using a Chinese wall to prevent CoI

• Indirect information flow:

• A and B who compete with each other have accounts in the same bank C.

• Analyst-A deals with A and C, and updates C portfolio with sensitive info about A

• Analyst-B deals with B and C, gains an access to information about A

CWM/2

- *Elements of the model*
  - *Subjects – active entities that may access protected objects (users, processes)*
  - *Information – organized in hierarchy with three levels*
    - *Objects – individual item of information – single entity/corporation*
    - *Dataset (DS) – all objects that relate to the corporation*
    - *Conflict of Interests (CoI) class: all datasets whose entities/corporations are in competition*
  - *Access rules – for read and write*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

CWM/3

- *Enforcing Chinese wall policy through two rules:*
  - *Simple security rule: A subject S can read on object O only if*
    - *O is in the same DS as an open object already accessed by S, OR*
    - *O belongs to a CoI from which S has not yet accessed any information*
  - *The simple security rule does not prevent an indirect flow of information behind possible CoI. We need another rule:*
  - **-property rule: A subject S can write an object O only if*
    - *S can read O according to the simple security rule, AND*
    - *All objects that S can read are in the same DS as O*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

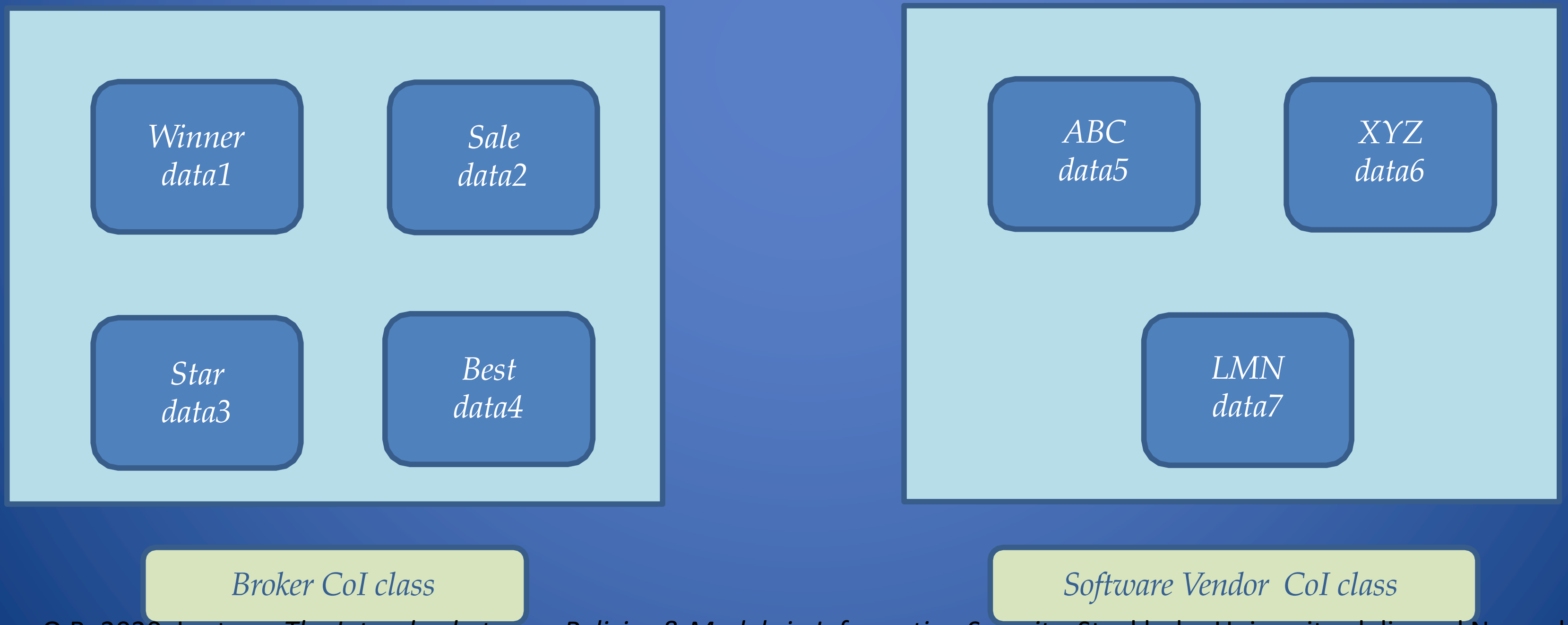
CWM/4

- *Simply*
  - *Either a subject cannot write at all (doing nothing), or*
  - *A subject can access (both read and write), but limited to a single dataset. –looking at DS that are not overlapping…*
- *The *-property rule is quite restrictive. In many cases the subject needs only read access.*
- *Relaxing the restriction – with the concept of sanitized data – data derived from the entity (corporation) but not sufficient to discover the identity of the entity.*
- *In this case, there is no need for the two CWM rules.*
- *In principle the model implements dynamically changing access rights.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

A Primer of the Chinese Wall Model

There are two CoI classes, Stock broker and Software Vendor, which have four CDs and three CDs respectively. The set of objects has seven elements.



Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Applications, problems and directions

- *Motivation – to protect flow of information that will cause CoI.*
- *Creating virtual walls based on MACs.*
- *Based on "unrealistic" assumption that data of an entity can be grouped into non-overlapping and distinct CoI classes.*
- *To deal with this problem there is a modification termed as Aggressive Chinese Wall Security Policy (ACWSP).*
- *In this case we replace the CoI class with the Generalized CoI class (CCIR).*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

In search of generality

- Harrison-Ruzo-Ullman (HRU) model
  - Defines authorization systems that state policies for
    - Changing access rights
    - Creation and deletion of subjects and objects
  - The model is built from
    - A set of subjects S
    - A set of objects O
    - A set of access rights R
    - An access matrix M = (M_{SO}) where s belongs S and o to O, and the entry M_{SO} is the subset of R which specifies the rights subject s has on an object o.

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Primitive operations in HRU model

- *Six primitive operations*
  - *Enter r in M_{SO}*
  - *Delete r from M_{SO}*
  - *Create subject s*
  - *Delete subject s*
  - *Create object o*
  - *Delete object o*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Primitive commands in HRU

- *A sort of a programming language*

```
C ($x_1$, $x_2$, …,$x_k$)
        if $r_1$ in $Ms_1,o_1$ and
        if $r_2$ in $Ms_2,o_2$ and
        …
        if $r_m$ in $M_{sm,om}$
        then
                        $op_1$
                        $op_2$
                        . . .
                        $op_n$
        end
```

Where s_i and o_i are take from $x_{1,}$ x_2,…,x_k.

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Leaking of rights

- *What is an effect of a command*
  - *An access matrix describes the state of the system*
  - *Recorded as a change to the access matrix*
  - *The model should campture security policies and the regulation of the allocation of rights.*
    - *Compliance with the policy is based on making sure that there is no way to grant undesirable access rights.*
  - *An access matrix M*
    - *Leaks the right r if there exists a command c that adds the right r into a position of the access matrix that previously did not contain r.*
    - *Is defined to be safe with respect to right r if no sequence of commands can transform M into a state that leaks r.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Safety properties

- *Three important theorems*
  - *<u>Theorem A</u>: Given an access matrix M and right r, verifying the safety of M with respect to r is undecidable.*
  - *<u>Theorem B</u>: Given a mono-operational authorization system, an access matrix M and right r, verifying the safety of M with respect to r is decidable.*
  - *<u>Theorem C</u>: The safety problem for arbitrary authorization systems is decidable if the number of subjects is finite.*
  - *Comments:*
    - *Mono-operational commands contain a single operation.*
    - *Even with two operations per command , the safety problem is undecidable.*
    - *Limiting the size of the authorization system may make the safety problem more tractable.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Discourse about generality and possibilities

- The solution to the safety problem cannot be solved in general.
  - Basically there is no universal or any kind of algorithm that we can use and prove safety/security
  - If we use complex models to base the design of a complex systems, the more we increase the complexity the further we are from the solution.
  - In a worst case we end up with undecidability or no solution in all cases (that is for all systems that we have designed or would like to design in the future).

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Discourse about generality and possibilities/2

- *How do we proceed?*
  - *Decrease complexity – limit, so make things more manageable – we do it time and again.*
  - *We might increase the coarseness of our model (make it more abstract, leave some parts out of it), however it becomes more feasible.*
  - *We also increase the efficacy of the parts that are doable.*
  - *We do not cover everything, which means we lose expressiveness, but at least we solve some parts of the problem.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Discourse about generality and possibilities/3

- *Compare with the soundness and completeness of propositional logic and predicate logic.*
- *We lose the ability to express the richness of our world, but we can still solve certain problems, if not all of them.*
- *Be pragmatic, design simple systems based on a simple models, and then slowly infuse some complexity to increase the domain and the relevance.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Conclusions

- *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 as trust can be guaranteed in some convincing way, such as through the use of formal systems and analysis.*
- *Trusted computing systems – we have sufficient hardware and software assurance measures to enable processing classified and sensitive information.*

Popov, O.B. 2020, Lecture: *The Interplay between Policies & Models in Information Security*, Stockholm University, delivered November 2020.

Thank you for your attention!