Welcome to

4. Integrity and Availability Policies

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

4-integrity-availability-policies.tex in the repo security-courses

Plan for today

Subjects

- Accuracy vs disclosure
- The Biba Model
- Clark-Wilson Integrity Model
- Trust models
- Deadlocks
- Availability and flooding attacks
- Protection against TCP Synfloods

Exercises

- Databases - discussion about Relational Database Management System RDBMS Model and NoSQL
- SYN flooding exercise

Reading Summary

Bishop chapter 6: Integrity Policies

Bishop chapter 7: Availability Policies

TCP Synfloods - an old yet current problem, and improving pf's response to it, Henning Brauer, BSDCan 2017

Accuracy vs disclosure

Lipner five commercial requirements:

- 1. Users will not write their own programs, but use existing production software.
- 2. Programmers develop and test applications on a nonproduction system, possibly using contrived data.
- 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 system logs

Available from

`https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1982/05/24/proceedings-5th-seminar-dod-computer-security-initiative/documents/1982-5th-seminar-proceedings.pdf`

Separation of duty ns function

> **Separation of duties** (SoD; also known as Segregation of Duties) is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

Quote from `https://en.wikipedia.org/wiki/Separation_of_duties`

> **Separation of function**. Developers do not develop new programs on production systems because of the potential threat to production data.

Computer Security, Matt Bishop, 2019

Danish: Funktionsadskillelse

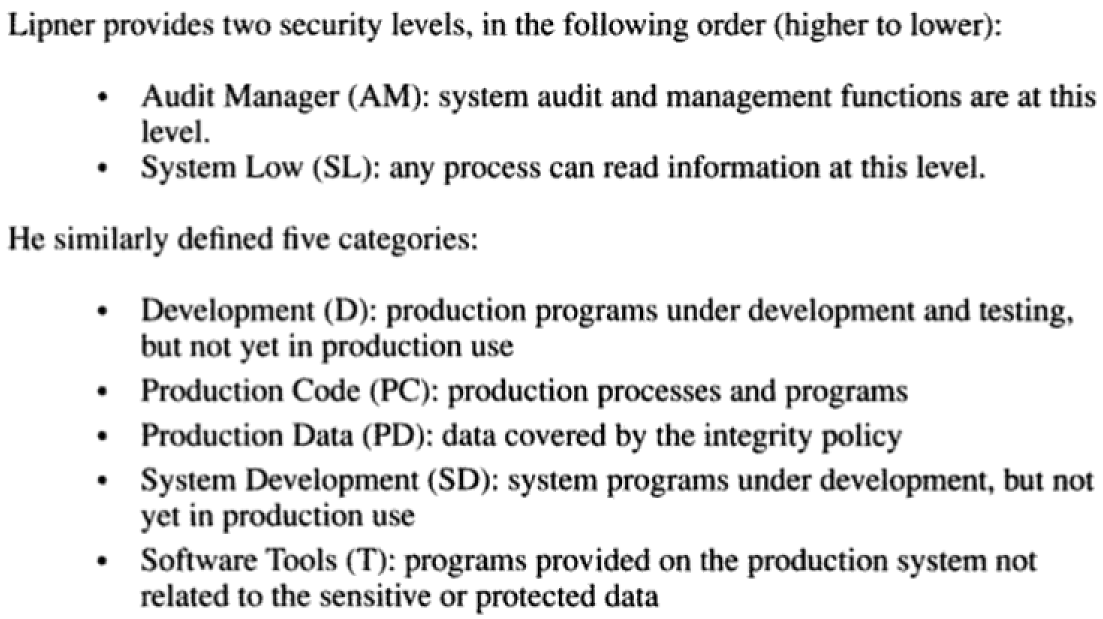
auditing

The Biba Model

Example page 178

FreeBSD

Lipners Integrity Matrix Model



Lipner provides two security levels, in the following order (higher to lower):

- Audit Manager (AM): system audit and management functions are at this level.
- System Low (SL): any process can read information at this level.

He similarly defined five categories:

- Development (D): production programs under development and testing, but not yet in production use
- Production Code (PC): production processes and programs
- Production Data (PD): data covered by the integrity policy
- System Development (SD): system programs under development, but not yet in production use
- Software Tools (T): programs provided on the production system not related to the sensitive or protected data

Non-Discretionary Controls for Commercial Applications, Steven B. Lipner, IEEE Symposium on Security and Privacy, and Fifth Seminar on the DoD Computer Security Initiative, 1982

Lipners Integrity Matrix Model

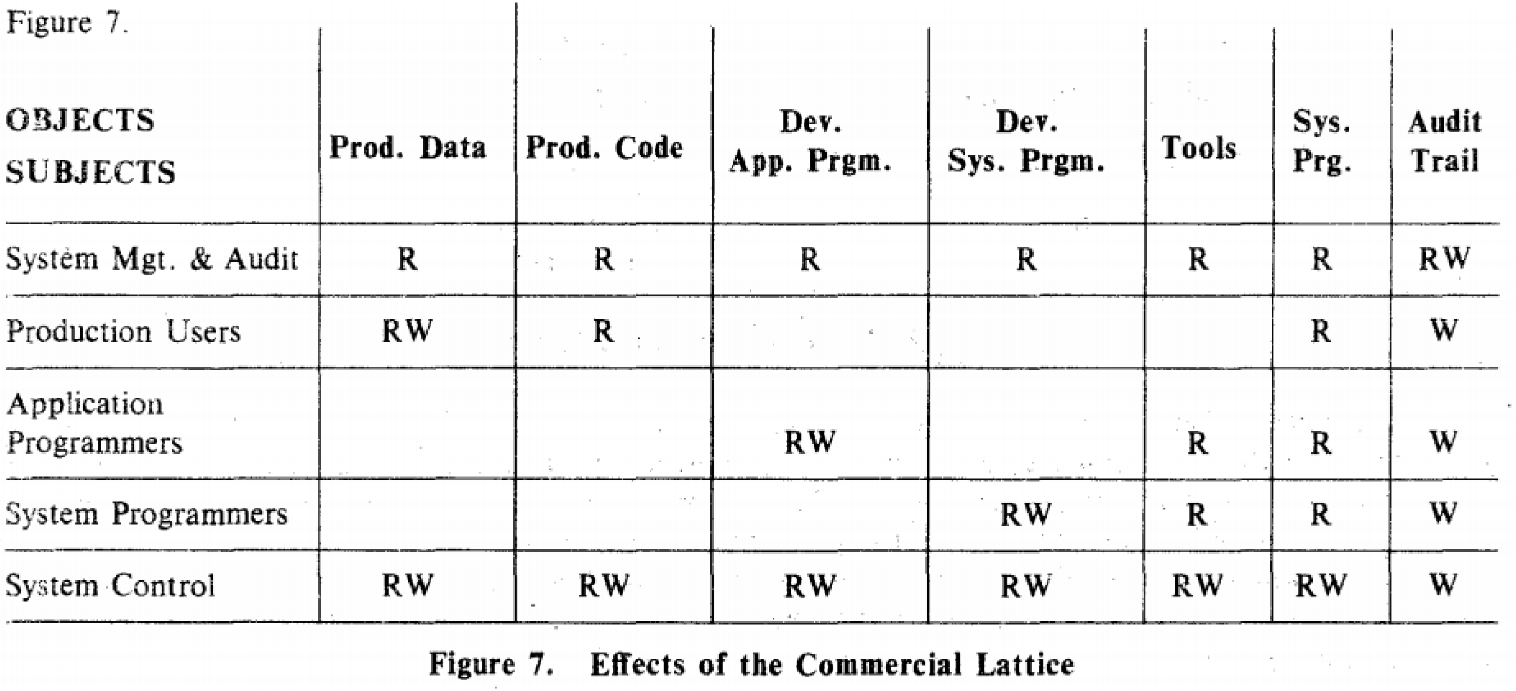


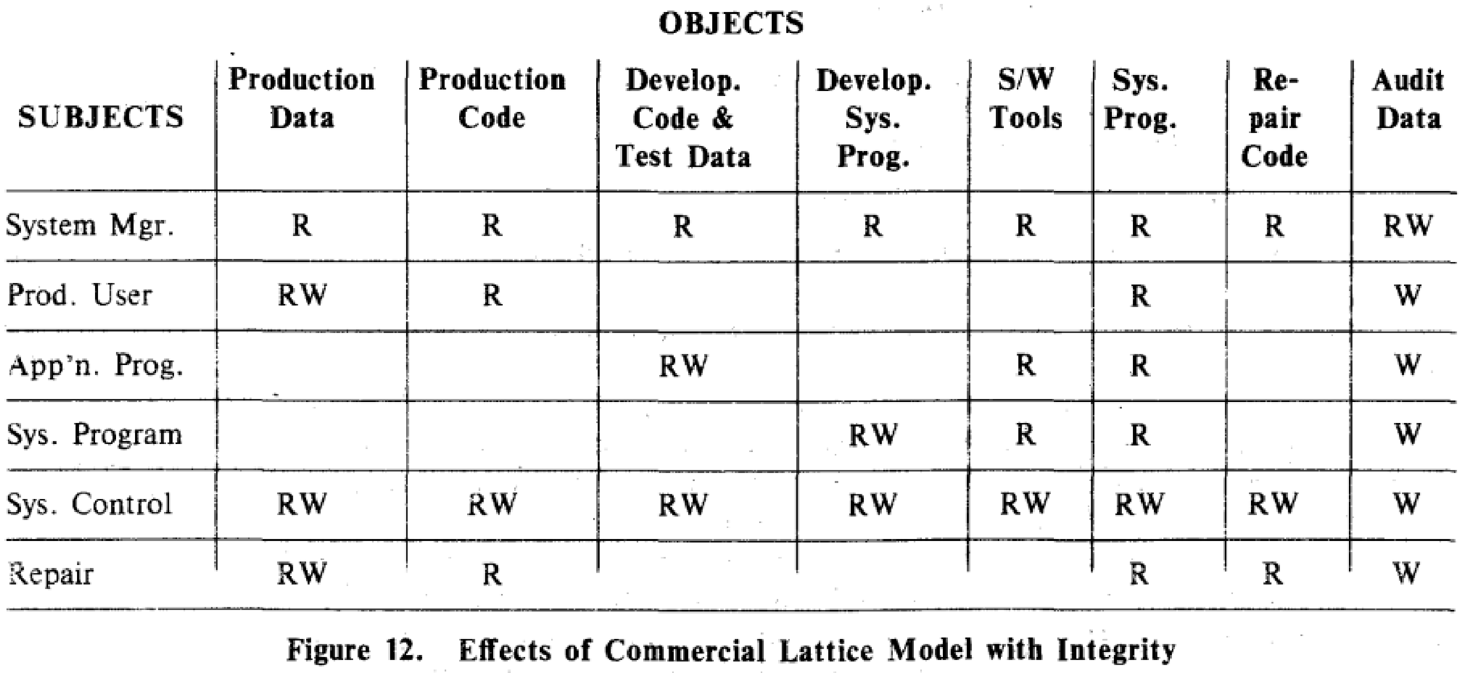
Figure 7.

OBJECTS SUBJECTS	Prod. Data	Prod. Code	Dev. App. Prgm.	Dev. Sys. Prgm.	Tools	Sys. Prg.	Audit Trail
System Mgt. & Audit	R	R	R	R	R	R	RW
Production Users	RW	R				R	W
Application Programmers			RW		R	R	W
System Programmers				RW	R	R	W
System Control	RW	RW	RW	RW	RW	RW	W

Figure 7. Effects of the Commercial Lattice

Non-Discretionary Controls for Commercial Applications, Steven B. Lipner, IEEE Symposium on Security and Privacy, and Fifth Seminar on the DoD Computer Security Initiative, 1982

Lipners Integrity Matrix Model



	OBJECTS							
SUBJECTS	Production Data	Production Code	Develop. Code & Test Data	Develop. Sys. Prog.	S/W Tools	Sys. Prog.	Re-pair Code	Audit Data
System Mgr.	R	R	R	R	R	R	R	RW
Prod. User	RW	R				R		W
App'n. Prog.			RW		R	R		W
Sys. Program				RW	R	R		W
Sys. Control	RW	RW	RW	RW	RW	RW	RW	W
Repair	RW	R				R	R	W

Figure 12. Effects of Commercial Lattice Model with Integrity

Non-Discretionary Controls for Commercial Applications, Steven B. Lipner, IEEE Symposium on Security and Privacy, and Fifth Seminar on the DoD Computer Security Initiative, 1982

One source of truth

Clark-Wilson Integrity Model

A **well-formed transaction** from one consistent state to another consistent state.

- Constrained Data Items: CDIs are the objects whose integrity is protected
- Unconstrained Data Items: UDIs are objects not covered by the integrity policy
- Transformation Procedures: TPs are the only procedures allowed to modify CDIs, or take arbitrary user input and create new CDIs. Designed to take the system from one valid state to another.
- Integrity Verification Procedures: IVPs are procedures meant to verify maintainance of integrity of CDIs.

A Comparison of Commercial and Military Computer Security Policies, David D. Clark and David R. Wilson, 1987

Clark-Wilson rules

Certification rule 1 —When an IVP is executed, it must ensure the CDIs are valid.

Certification rule 2 —For some associated set of CDIs, a TP must transform those CDIs from one valid state to another. Since we must make sure that these TPs are certified to operate on a particular CDI, we must have E1 and E2.

Enforcement rule 1 —System must maintain a list of certified relations and ensure only TPs certified to run on a CDI change that CDI.

Enforcement rule 2 —System must associate a user with each TP and set of CDIs. The TP may access the CDI on behalf of the user if it is "legal".

Enforcement rule 3 -The system must authenticate the identity of each user attempting to execute a TP. This requires keeping track of triples (user, TP, CDIs) called "allowed relations".

Certification rule 3 —Allowed relations must meet the requirements of "separation of duty". We need authentication to keep track of this.

Certification rule 4 —All TPs must append to a log enough information to reconstruct the operation. When information enters the system it need not be trusted or constrained (i.e. can be a UDI). We must deal with this appropriately.

Certification rule 5 —Any TP that takes a 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:

Enforcement rule 4 —Only the certifier of a TP may change the list of entities associated with that TP.

Clark-Wilson Integrity Model

> The model uses a three-part relationship of subject/program/object (where program is interchangeable with transaction) known as a triple or an access control triple. Within this relationship, subjects do not have direct access to objects. Objects can only be accessed through programs

A Comparison of Commercial and Military Computer Security Policies, David D. Clark and David R. Wilson, 1987

See also `https://en.wikipedia.org/wiki/Clark%E2%80%93Wilson_model`

Trust models

Availability Policies

Deadlocks

Relational Database Management Systems RDBMS

introduction

Database deadlocks

Exercise

Now lets do the exercise

Database Security

which is number **11** in the exercise PDF.

Fairness and starvation

Old operating systems vs pre-emptive multitasking.

Availability and Network flooding attacks

SYN flood

Exercise

Now lets do the exercise

SYN flooding 101

which is number **12** in the exercise PDF.

Protection against TCP Synfloods

TCP Synfloods - an old yet current problem, and improving pf's response to it Henning Brauer, BSDCan 2017

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools