Computer Security Tutorials

Computer Security COMPGA01

Nicolas T. Courtois, November 2011

Answers to be filled in directly with a pen, solutions are given in class. The question numbers are of the form X.Y where X corresponds to the numbering of pdf slides. Many questions are the same as in previous exam or homework.

Question 2.1.

Question	Answer
Explain what is a *security policy*.	
A *security mechanism* (in this context).	
What is a reference monitor?	
State the three main properties it should satisfy.	
Explain DAC and MAC. Which one is more vulnerable to malware?	
Explain briefly the Chinese wall model in terms of classes, information flows, transitive closure in directed graphs.	

Question 2.2.

Question	Answer
What is an order relation in mathematics? What are the R A T axioms?	
What is a POSET?	
What is the dual notion for LUB? Alternative names?	
Exact mathematical definition?	
In $< \mathbb{N}, \mid >$, what is the transitive closure of $\mid$?	
Given a set of classifications H with a total ordering $\leq_H$, and a lattice $C = P(Cat), \subseteq$ where Cat is any set of "categories", write a definition of the Bell-LaPadula product lattice.	

Question 2.3. Consider the set of confidentiality levels

$$L = \{PUB < OFF < SEC\},$$

and the set of categories

$$Cat = \{Production(P), HumanRessources(H), Finance(F)\}.$$

We consider four objects o_1, o_2, o_3, o_4 and two subjects s, t with the following clearance levels:

$$\begin{aligned}
\lambda(o_1) &= (PUB, \{P\}) \\
\lambda(o_2) &= (PUB, \{\}) \\
\lambda(o_3) &= (OFF, \{H, P\}) \\
\lambda(o_4) &= (SEC, \{P\}) \\
\lambda(s) &= (OFF, \{H, F, P\}) \\
\lambda(t) &= (SEC, \{P\})
\end{aligned}$$

Answer the following questions in the Bell LaPadula model:

Question	Answer
Count security classes in this classification lattice.	
The Bottom element $\perp=$	
The Top element $\top =$.	
LUB$(\lambda(o_1), \lambda(o_4)) =$	
which users can read both o_1 and o_4?	
GLB$(\lambda(o_1)), \lambda(o_3)) =$	
which users can write both o_1 and o_3	
LUB$(\lambda(s)), \lambda(t)) =$	
which object can be written by both s, t	
GLB$(\lambda(s)), \lambda(t)) =$	
which objects can be read by both s, t	
Which objects s can read.	
Which objects t can write?	

Question 2.4. Consider the set of integrity levels

$$L = \{UserSpace(US) < System(SH)\}.$$

Consider the following set of categories

$$Cat = \{SensitiveWorkFiles(S), PersonalData(P)\}.$$

Let Bob be a subject and and $\{do1, fi2, pr3\}$ a set of objects with the following classifications.

$$\begin{array}{rcl} \lambda(Bob) & = & (SH, \{S\}) \\ \lambda(do1) & = & (US, \{P\}) \\ \lambda(fi2) & = & (SH, \{S\}) \\ \lambda(pr3) & = & (US, \{S\}) \end{array}$$

Fill in the following table working all the way down for each of the 5 policies. Consider that the operations are executed in order, so that potential changes in security levels λ can affect further operations.
We recall that LWM = Low Water Mark policy. In the strict Biba and in the Ring policy current levels never change. In the Integrity Audit policy all operations are permitted and only changes in λ need to be recorded.
For each operation (working column by column) do explain whether the operation will be allowed (Y) or denied (N). Note any potential changes (if any) to the security classes: write a new value of $\lambda(x)$ each time it is changed. If it does not change, there is no need to write it.

policy ▷	Biba strict	LWM for Objects		LWM for Subjects		Integr. Audit	Ring
operation	Y/N	Y/N	λ change	Y/N	λ change	λ change	Y/N
read(do1)					$\lambda(Bob) =$	$\lambda() =$	
read(pr3)					$\lambda() =$	$\lambda() =$	
write(fi2)			$\lambda() =$			$\lambda() =$	
write(do1)			$\lambda(do1) =$			$\lambda() =$	
write(pr3)			$\lambda() =$			$\lambda() =$	
read(do1)					$\lambda() =$	$\lambda() =$	
write(fi2)			$\lambda() =$			$\lambda() =$	
write(do1)			$\lambda(do1) =$			$\lambda() =$	
write(pr3)			$\lambda() =$			$\lambda() =$	
read(pr3)					$\lambda(Bob) =$	$\lambda() =$	

Question 3.1. Here is a listing of a Unix directory.

Permissions	Owner	Group	Size	Last Update	File Name
`-rws-----x`	dave	gdev	1452306	Nov 03 21h11	gtool
`drwxrwxrwt`	dave	gdev	1452306	Nov 03 21h11	gdata
`-rwx--x--x`	alice	alice	214768	Nov 03 09h36	setup
`-rw-r-----`	alice	pcrack	12486	Dec 04 11h00	sourcg
`-rw-r--r--`	dave	pcrack	14257	Oct 02 18h44	config
`-rw--wxr--`	root	pcrack	176704	Nov 01 12h23	hosts

Suppose that user alice is a member of groups alice and pcrack. User dave is a member of groups dave, pcrack, and gdev. For each question specified in the following table, provide your responses.

Question	Answer
List the names of the files that alice can write.	
List the names of the files that dave can read.	
Suppose that alice executes program gtool. List the names of the files that the corresponding process can execute.	
Suppose that dave executes program setup. List the names of the files that the corresponding process can write.	
How do we distinguish directories? Explain x permission for directories.	
The permissions for gtool start with -rws. Explain what does ’s’ stand for?	
Explain what sticky bit is. when does it apply.	

Question 3.2.

Question	Answer
In Unix/Windows, can a process be more privileged than the user who calls it? Give one example.	
Can it be less privileged? One example?	
Explain what is *Real User Id* and *Effective User Id* in Unix systems.	
Explain very briefly how in Windows, a system knows if a user is allowed to access a specific file with (Discretionary) Access Control Lists (ACL's).	

Explain what a "closed" policy is. In Apache web servers, explain what happens when the *.htaccess* file contains the following 3 lines in order.
`Order Allow,Deny`
`Deny from all`
`Allow from cs.ucl.ac.uk`	

Question 5.1.

Question	Answer
*Which is bigger $H(X,Y)$ or $H(X)$? When equality is achieved?	
*Which is bigger $H(X,Y)$ or $H(X) + H(Y)$? When equality is achieved?	
For a discrete variable with n outcomes which is bigger $H(X)$ or $log_2(n)$? When equality is achieved?	
*Which is bigger $H(X\|Y)$ or 0? Equality?	
*Which is bigger $H(X\|Y)$ or $H(X,Y) - H(Y)$? When equality is achieved?	
*Which is bigger $H(X\|Y)$ or $H(X)$? When equality is achieved?	
Define Entropy of a password with distribution $p_1, \ldots, p_n$.	
In which case the entropy measures the strength of a password?	
Define Min-entropy of a password.	
In which case the Min-entropy measures the strength of a password?	

Question 5.2.

Question	Answer
What is ”spoofing” in the context of password security?	
What are the three factors? Why writing the password down defeats a 2-factor system without necessarily making it less secure? Solutions?	
Give two examples of self-defeating security recommendations regarding passwords.	
Can passwords be possibly stored encrypted by a deterministic block cipher algorithm with a fixed key?	
What is the encryption AND the storage is implemented in a secure hardware?	
How to use a hash function to store a password?	