THE UNIVERSITY OF BRITISH COLUMBIA

Miscellaneous

EECE 412

Session 20

Last Session Recap

Principles of Designing Secure Systems

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Privilege
7. Least Common Mechanism
8. Psychological Acceptability
9. Defense in depth
10. Question assumptions

Today Session Outline

1. Putting it all together: Case Study
   - guest lecture
2. Sample solution for controlling access to course online content
3. Results of Formative Feedback Survey II

Case Study

Guest Speaker Dave Tyson

- Manager of Information Technology Security for the City of Vancouver
- 22 years of work in IT and Physical Security Industry
- MBA with specialization in Digital Technology Management
- Certified Protection Professional (CPP)
- Certified Information Systems Security Professional (CISSP)
- Previously worked at IBM Global Services

THE UNIVERSITY OF BRITISH COLUMBIA

Sample Solution for Controlling Access to Course Online Content

Each Group

Develop configuration (i.e., label graph, and clearance and classification assignments) for access control mechanisms based on Bell-LaPadula model for the following application and policy

Application:

- 10 students: s_1 … s_{10}
- 3 instructors: i_1, i_2, i_3
- 5 courses: c_1, … c_5
  - $C_1 = \{i_1, \{s_1, s_2, s_3\}\}$
  - $C_2 = \{i_2, \{s_3, s_4, s_5\}\}$
  - $C_3 = \{i_3, \{s_5, s_6, s_7\}\}$
  - $C_4 = \{i_1, \{s_7, s_8, s_9\}\}$
  - $C_5 = \{\{i_2, i_3\}, \{s_8, s_9, s_{10}\}\}$

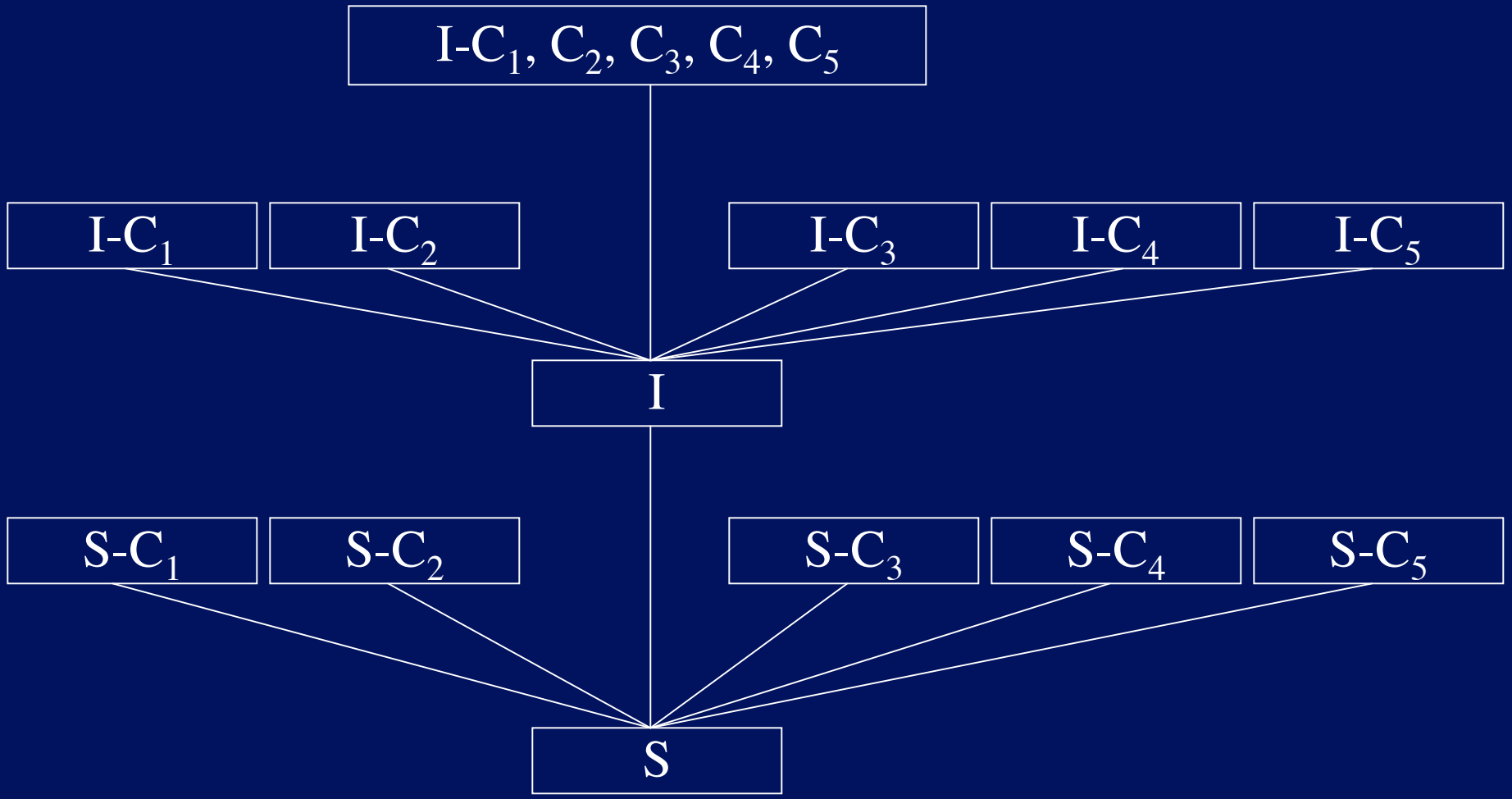
Policy:

1. Students can
   1. read course material and assignment instructions for the courses they are registered
   2. submit (i.e., write) their assignments for the registered courses
2. Instructors can
   1. read student submitted assignments for the courses they teach, and
   2. post (i.e., write) course material and assignment instructions for their courses

Solution

1. Security level Lattice
2. File classifications
3. User clearances
4. DAC matrix

Security level Lattice



File Classifications

Course material for course i == CM_i

Assignment Submission for course i == AS_i

	S	$S\text{-}C_1$	$S\text{-}C_2$	$S\text{-}C_3$	$S\text{-}C_4$	$S\text{-}C_5$	I	$I\text{-}C_1$	$I\text{-}C_2$	$I\text{-}C_3$	$I\text{-}C_4$	$I\text{-}C_5$	$I\text{-}C_1 \ldots C_5$
CM_1		√											
AS_1		√											
CM_2			√										
AS_2			√										
CM_3				√									
AS_3				√									
CM_4					√								
AS_4					√								
CM_5						√							
AS_5						√							

User Clearances

	S	S-C_1	S-C_2	S-C_3	S-C_4	S-C_5	I	I-C_1	I-C_2	I-C_3	I-C_4	I-C_5	I-C_1…C_5
i_1								√			√		
i2									√			√	
i3										√		√	
s1		√											
s2		√											
s_3		√	√										
s_4			√										
s_5			√	√									
s_6				√									
s_7				√	√								
s_8					√	√							
s_9					√	√							
s_{10}						√							

DAC Matrix

	CM_1	CM_2	CM_3	CM_4	CM_5	AS_1^1	AS_1^2	AS_1^3	AS_2^3	AS_2^4	AS_2^5	AS_3^5	AS_3^6	AS_3^7	AS_4^7	AS_4^8	AS_4^9
any	R	R	R	R	R												
i_1	O			O		R	R	R							R	R	R
i_2		O			O				R	R	R						
i_3			O		W							R	R	R			
s_1						O											
s_2							O										
s_3								O	O								
s_4										O							
s_5											O	O					
s_6													O				
s_7														O	O		
s_8																O	
s_9																	O
s_{10}																	

Assignment Submission for course i by student j == AS_i^j