 THE UNIVERSITY OF BRITISH COLUMBIA

Miscellaneous


EECE 412
Session 20

Copyright © 2004 Konstantin Beznosov

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

Copyright © 2004 Konstantin Beznosov

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


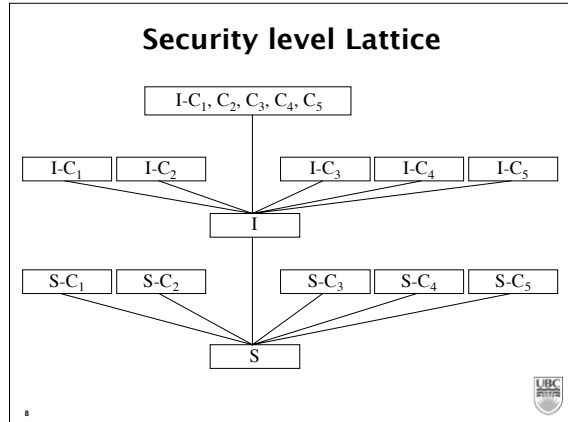
Policy:

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

File Classifications


Course material for course $i == CM_i$
 Assignment Submission for course $i == AS_i$

	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
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								√			√		
i ₂									√			√	
i ₃										√		√	
s ₁		√											
s ₂		√											
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 ₁ ⁴	AS ₁ ⁵	AS ₁ ⁶	AS ₁ ⁷	AS ₁ ⁸	AS ₁ ⁹
any	R	R	R	R	R									
i ₁	O		O			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														O

Assignment Submission for course i by student $j == AS_j$

