# 

# 

REQUIREMENTS ANALYSIS

Team 5

Guangchu Shi

Hongquan Yu

Ribe Ninan

Xiangfeng Wang

Yue Wang

Zeqian Huang

09/19/2017

**Table of Contents**

[**Software Quality Utility Tree**](#_v4dwm966ti80) **3**

[**Software Quality**](#_v4dwm966ti80) **Attributes and Scenarios 4**

[Usabilit](#_kgg5wklpwwqj)y 4

[Modifiability](#_utqmmb4mgn3g) 6

[Performance](#_kc6kcxxrqy2) 6

[Availability](#_w9fvkp48zncx) 7

[Security](#_rycj3ich0qr) 9

[Testability](#_5ful7ytxib4r) 9

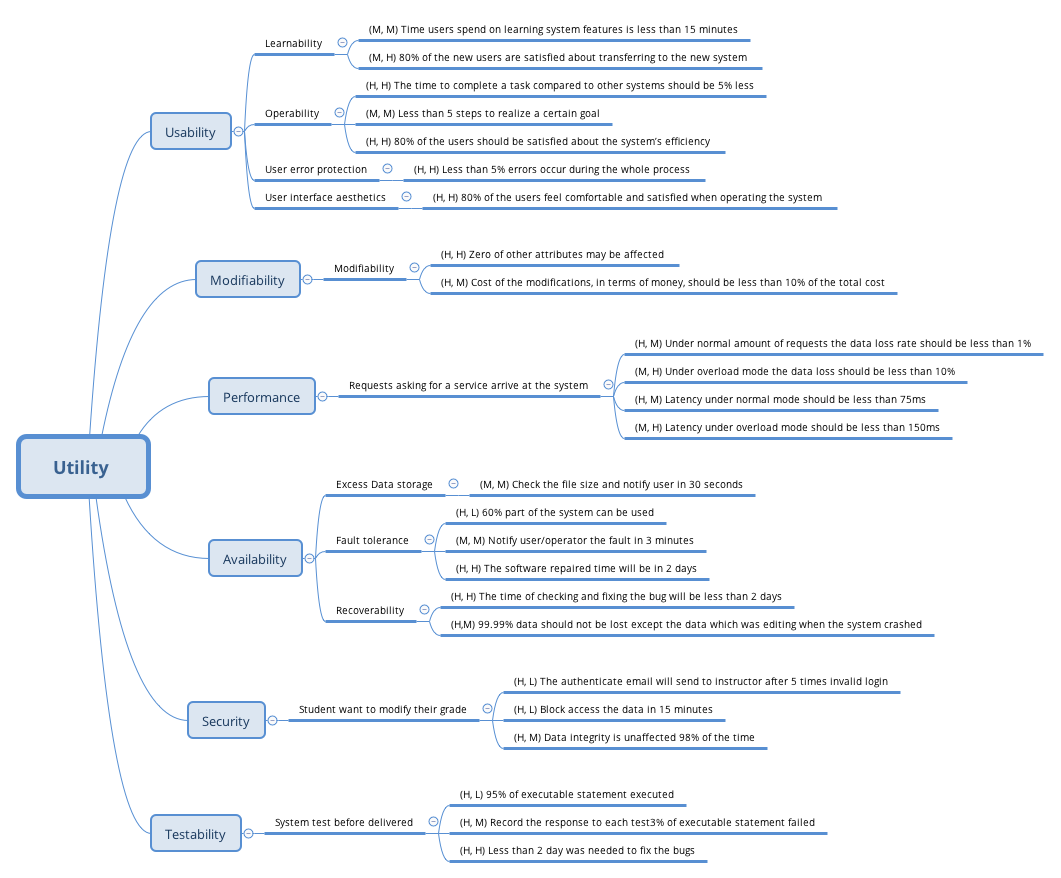
[**Security Requirements Abuse Case Model**](#_myfae5f67sfo) **11**

[Family of Abuse Case Diagram](#_4ccmgzhoyotj) 11

[Graphical Descriptions](#_3t4d5bwk1fwo) 12

[Abuse Use Case Description](#_w4ja4mvrp1ey) 14

# **Software Quality Utility Tree**



# 

# **Software Quality Attributes and Scenario**

## **Usability：**

* Learnability.
* Operability.
* User error protection.
* User interface aesthetics.

|  |  |
| --- | --- |
| Quality Attribute | Usability |
| Scenario | Learnability |
| Source | Students and instructors |
| Stimulus | Both students and instructors want to adapt to the system and learn system features without difficulties |
| Artifact | System |
| Environment | At runtime |
| Response | * Help topics are rich and sensitive to context * The user interface is similar to other online learning systems that users used before * In an unfamiliar context, the user interface is still easy to use |
| Response Measure | * Time users spend on learning system features is less than 15 minutes (M, M) * 80% of the new users are satisfied about transferring to the new system (M, H) |

|  |  |
| --- | --- |
| Quality Attribute | Usability |
| Scenario | Operability |
| Source | End users |
| Stimulus | Users want to use the system efficiently |
| Artifact | System |
| Environment | At runtime |
| Response | * Reuses already entered data and/or commands * Supports efficient navigation within a screen * Provides a comprehensive searching within the website * Allows multiple simultaneous activities |
| Response Measure | * The time to complete a task compared to other systems should be 5% less (H, H) * Less than 5 steps to realize a certain goal (M, M) * 80% of the users should be satisfied about the system’s efficiency (H, H) |

|  |  |
| --- | --- |
| Quality Attribute | Usability |
| Scenario | User error protection |
| Source | End users |
| Stimulus | Users want to minimize the impact of their errors |
| Artifact | System |
| Environment | At runtime |
| Response | * Be able to retrieve forgotten usernames and passwords * Be able to undo, cancel, or recover from system failures * Be able to roll back to the initial stage if unsuccessful transactions occur * Be able to recognize and correct user errors |
| Response Measure | * Less than 5% errors occur during the whole process (H, H) |

|  |  |
| --- | --- |
| Quality Attribute | Usability |
| Scenario | User interface aesthetics |
| Source | End users |
| Stimulus | Users want to use a beautifully designed website and feel comfortable navigating through it |
| Artifact | System |
| Environment | At runtime |
| Response | * Layout of the website should be concise and intuitive * The design should be consistent across all subsystems and sections * The system should enable users to work at their own pace, without distractions |
| Response Measure | * 80% of the users feel comfortable and satisfied when operating the system (H, H) |

## **Modifiability (M, L)：**

|  |  |
| --- | --- |
| Quality Attribute | Modifiability |
| Scenario | Some attributes of the system are to be modified/added/deleted |
| Source | Developers and system admins |
| Stimulus | Developers and admins wish to add/delete/modify/vary system functionalities and quality attributes |
| Artifact | System user interface; platform; environment |
| Environment | At design time; compile time; at build time; at run time |
| Response | * System should be able to locate the places that need to be modified * System should be able to allow developers to make the necessary changes, without affecting other functionalities * System should be able to deploy the modifications |
| Response Measure | * Cost of the modifications, in terms of money, should be less than 10% of the total cost (H, M) * Zero of other attributes may be affected (H, H) |

## **Performance (H, H)：**

|  |  |
| --- | --- |
| Quality Attribute | Performance |
| Scenario | A number of requests asking for a service arrive at the system |
| Source | Web requests |
| Stimulus | Web requests arrive at the system and ask for the response of a certain service |
| Artifact | System |
| Environment | Normal mode; overload mode; |
| Response | * System handles the requests without errors * System be able to protect itself against overwhelming requests |
| Response Measure | * Under normal amount of requests the data loss rate should be less than 1% (H, M) * Under overload mode the data loss should be less than 10% (M, H) * Latency under normal mode should be less than 75ms (H, M) * Latency under overload mode should be less than 150ms (M, H) |

## **Availability：**

* Excess Data storage
* Fault tolerance
* Recoverability

|  |  |
| --- | --- |
| Quality Attribute | Availability |
| Scenario | Excess Data storage |
| Source | Internal to the system |
| Stimulus | User wants to upload the files bigger than the data size limitation |
| Artifact | Persistent storage |
| Environment | Normal operation |
| Response | * Notify user the size limitation of the uploaded files * Continue to operate when use upload files under the limitation. |
| Response Measure | Check the file size and notify user in 30 seconds;(M, L) |

|  |  |
| --- | --- |
| Quality Attribute | Availability |
| Scenario | Fault tolerance |
| Source | Internal to the system |
| Stimulus | Some process fault in the hardware or software |
| Artifact | System’s processor |
| Environment | Degraded mode |
| Response | * Report it； * Notify user/operator; * Some source are temporarily unavailable; * Continue degraded mode until cause of the fault is found and fixed |
| Response Measure | * 60% part of the system can be used;(H,L) * Notify user/operator the fault in 3 minutes;(M,M) * The software repaired time will be in 2 days.(H,H) |

|  |  |
| --- | --- |
| Quality Attribute | Availability |
| Scenario | Recoverability |
| Source | External to the system or internal to the system |
| Stimulus | System crashed |
| Artifact | System‘s processor |
| Environment | Degraded mode |
| Response | * Report it; * Notify it to user/operator; * Operator check the system and fix the problem; * The data will be recovered; * Notify user the system can be used by email. |
| Response Measure | * The time of checking and fixing the bug will be less than 2 days;(H,H) * 99.99% data should not be lost except the data which was editing when the system crashed.(H,M) |

## **Security (H,M)**

|  |  |
| --- | --- |
| Quality Attribute | Security |
| Scenario | Student want to modify their grade. |
| Source | Hacker from inside the organization |
| Stimulus | Students attempt to modify grade data |
| Artifact | Grade data within system |
| Environment | Normal mode |
| Response | * Authenticates user； * blocks access to data and/or services； * records access/modifications or attempts to access/modify data by identity； * informs instructor |
| Response Measure | * The authenticate email will send to instructor after 5 times invalid login;(H,L) * Block access the data in 15 minutes.(H,L) * Data integrity is unaffected 98% of the time(H,M) |

## **Testability (H,L)**

|  |  |
| --- | --- |
| Quality Attribute | Testability |
| Scenario | System test before delivered |
| Source | System developer and end user |
| Stimulus | Execution of tests due to completion of code increment |
| Artifact | Portion of the system; Full system |
| Environment | Compile time; Integration time; Deployment time; Run time |
| Response | * Controlled to perform the desired tests * Record the response to each test * Capture cause of fault, record it and fit the bug * Monitor the every state of the system |
| Response Measure | * 95% of executable statement executed;(H,L) * 3% of executable statement failed;(H,M) * Less than 2 day was needed to fix the bugs(H,H) |

# 

# 

# 

# 

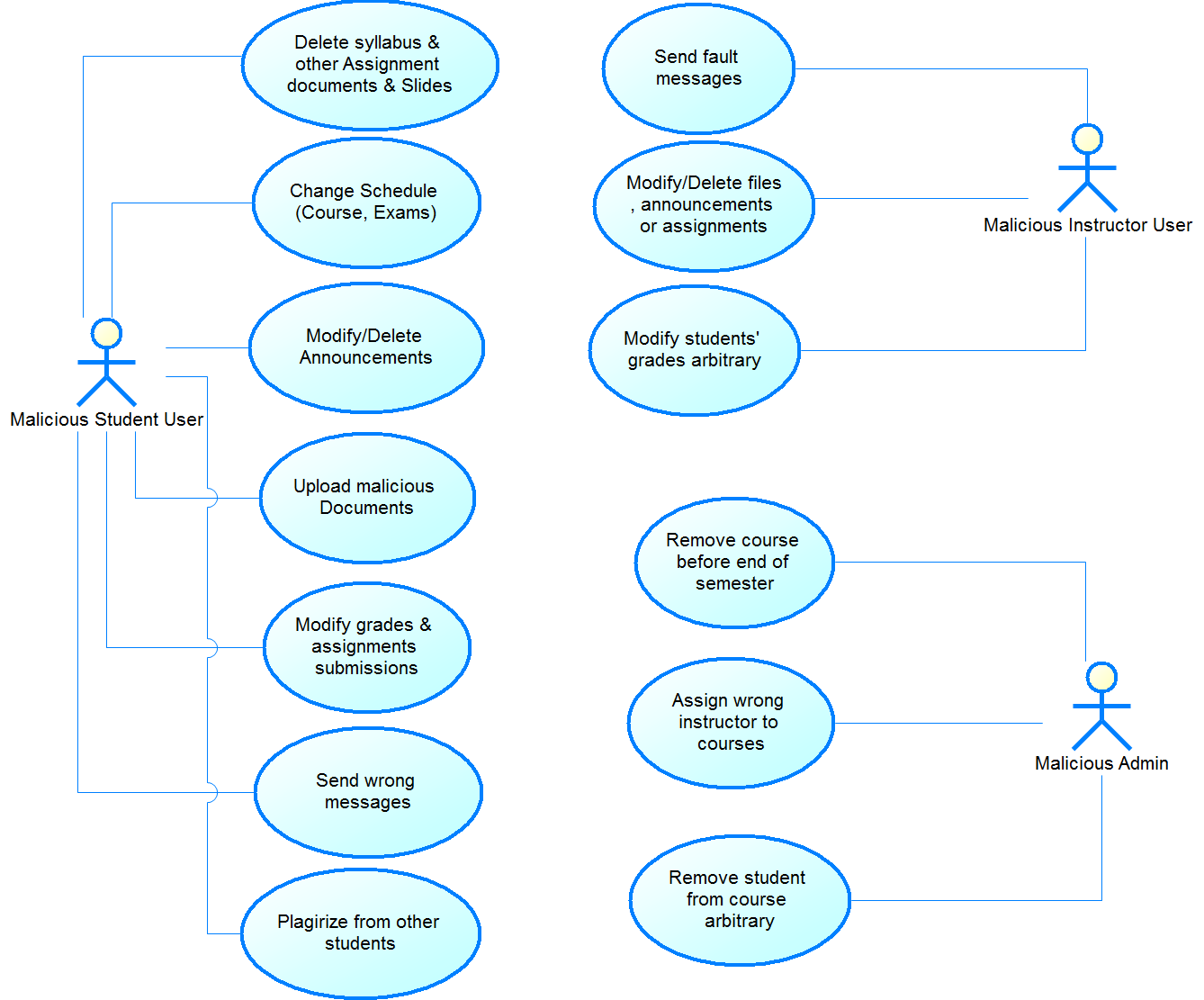
## 

## 

# 

# **Security Requirements Abuse Case Model**

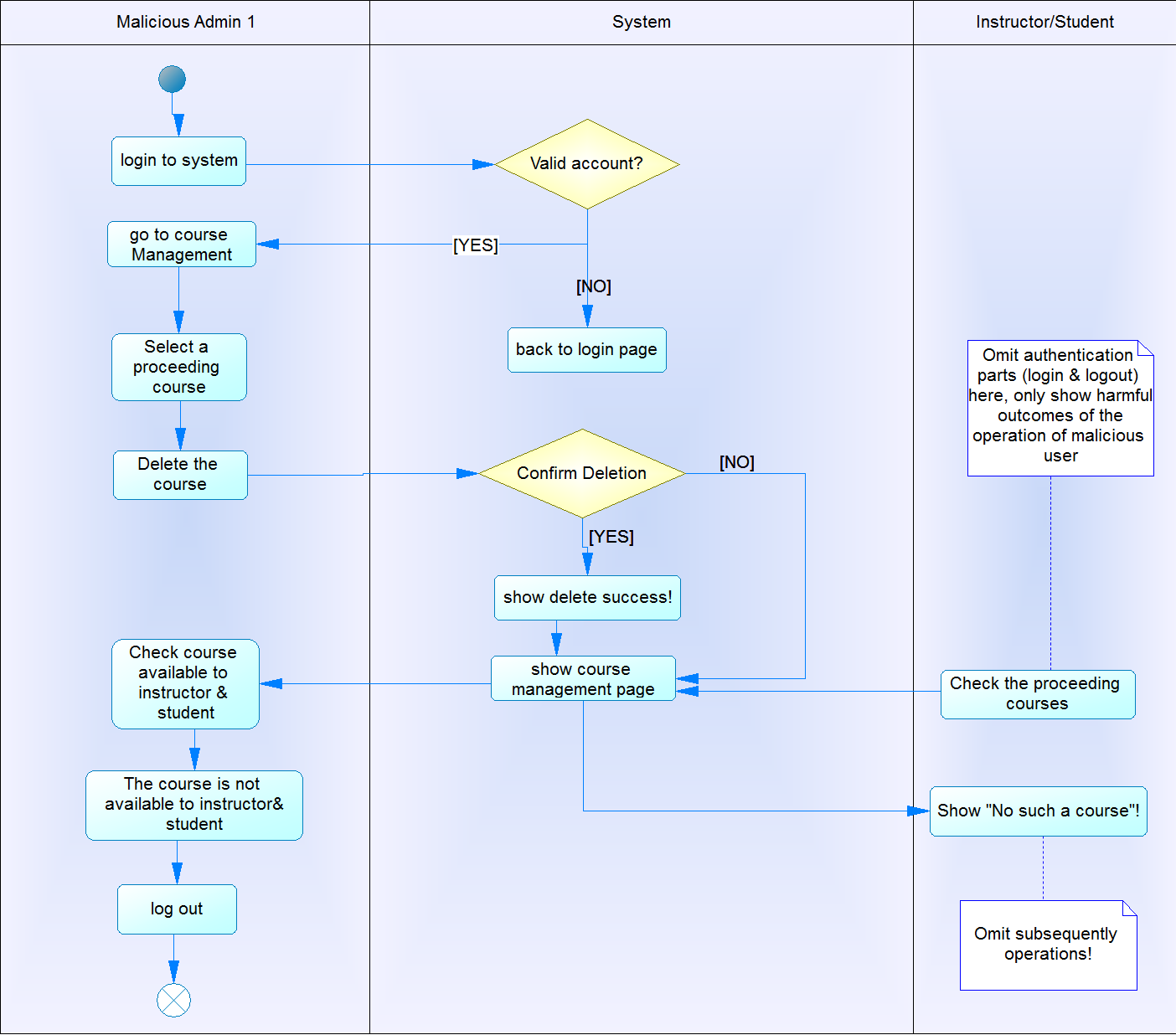
## **Family of Abuse Case Diagram**

****

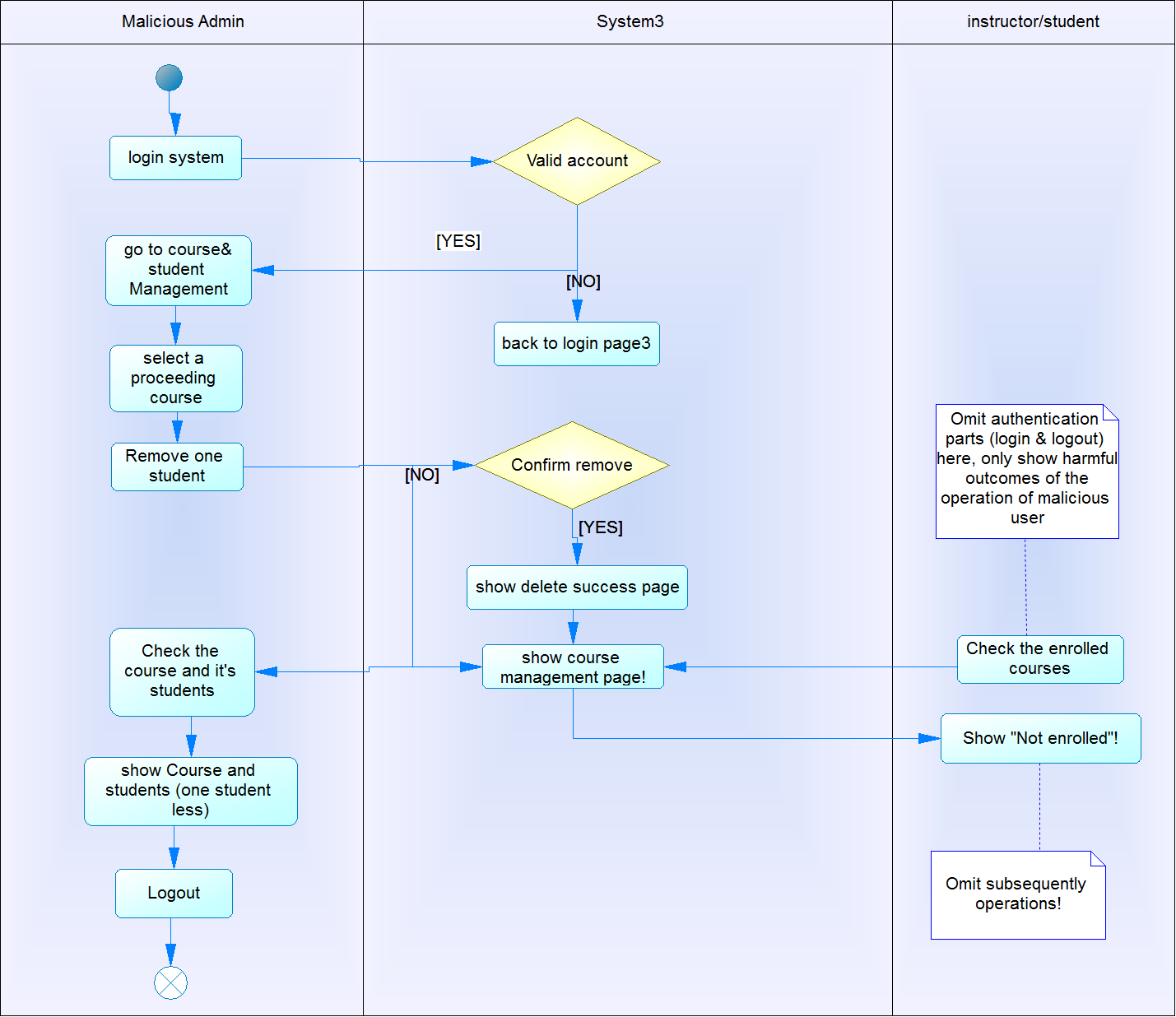
## 

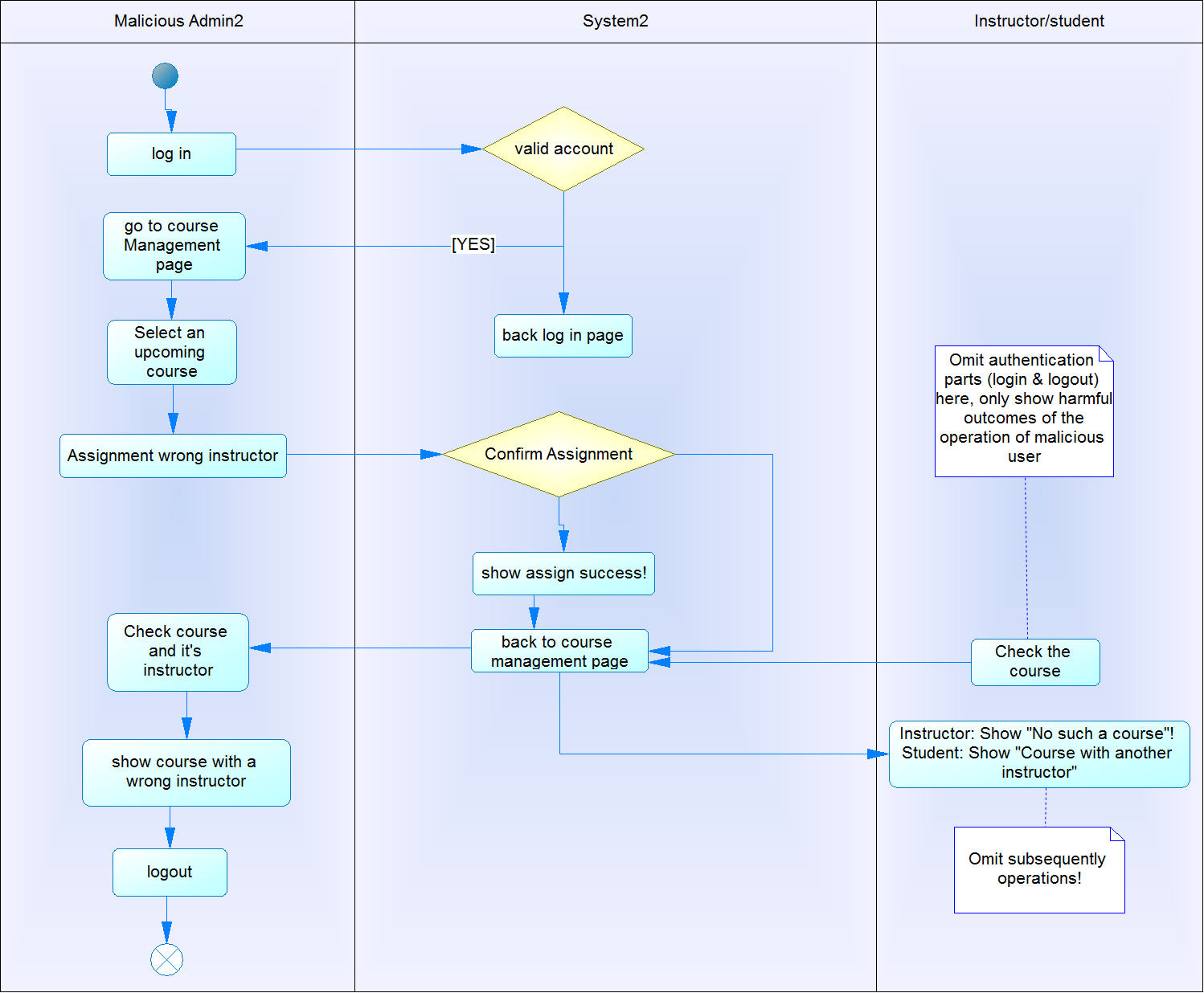
**Graphical Descriptions**

**1. Malicious admin remove a proceeding course:**

****

**2. Malicious admin remove student arbitrary:**

****

**3. Malicious admin assigns wrong instructor to a course**

## 

## 

## 

## 

## **Abuse Use Case Description**

|  |  |
| --- | --- |
| **Abuse Use Case Name** | malicious admin try to change the content and delete or create the information inside the system |
| **Actors** | Malicious admin |
| **Privileges** | Assign or instructor to certain course and assign the authority to certain instructor  Assign student to certain courses and assign the authority to certain student |
| **Abused privileges** | Remove the course before the semester ends  Assign wrong instructor to course  Remove the student from certain course |
| **Preconditions** | There exist correct class information and student instructor information in the system |
| **Postconditions** | **Success post\_conditions:**  malicious admin is able to change or delete or create the information online.  **Failure post condition(s):**  malicious admin can't get access to the information and make the abused actions. |
| **Trigger** | malicious admin try to login the system |
| **Basic flow** | • Malicious admin use attack tool try to log into the system  • System *authenticates* the login incident to check is admin is eligible to log in  • Malicious admin fails to log in and get access to the information inside the system |
| **Alternative flow** | • Malicious admin use attack tool 2 successfully logged in to the system(pass the authentic process)  • Malicious admin tries to do some operations on the course information, student account or instructor account  •System test try to figure out the whether this admin has been authorized.  •Malicious admin is not authorized to make any changes, so he/she can only browse the information in the system |
| **Exception flow** | **A**ttacker performs attack 3 using multiple attack tools, and successfully passed the authentic and authorized part. And he can make any change to the information inside the system. |
| **Harm** | Instructor and student cannot get access to the deleted course anymore  Instructor find himself not in a right course  The student who got enrolled into the system cannot access the system. |

|  |  |
| --- | --- |
| **Abuse Use Case Name** | Malicious students try to abuse the system |
| **Actors** | Malicious student |
| **Privileges** | Upload the documents  submit the assignment  send the message to other people in his class  take the quiz  download document |
| **Abused privileges** | Delete syllabus & other assignment document & slides  Change schedule(Course, Exam)  Modify/Delete announcements  Upload malicious Documents  Modify grades & assignment submissions  Send wrong messages  Plagiarize from other students |
| **Preconditions** | Student successfully gets enrolled into a class and has instructor and assignment and other documents instructor created inside the system |
| **Postconditions** | **Success post\_conditions:**  malicious student is able to change or delete or create the information online.  **Failure post condition(s):**  malicious admin can’t make any change out of their privileges. |
| **Trigger** | malicious student try to login the system |
| **Basic flow** | •Malicious student use attack tool1 try to log into the system  • System *authenticates* the login incident to check is admin is eligible to log in  • Malicious student fails to log in or get access to the information inside the system |
| **Alternative flow** | • Malicious student use attack tool 2 successfully logged in to the system(pass the authentic process)  • Malicious student tries to do some operations on the course content or send false message  • System test try to figure out the whether this student has been authorized by instructor or admin to make such actions.  • Malicious student is not authorized to make any such changes out of his privileges |
| **Exception flow** | Malicious student performs attack 3 using multiple attack tools, and successfully passed the authentic and authorized part. And he can make any change to the information inside the system like delete the course assignment or upload any documents. |
| **Harm** | • Other students and instructor can’t get access to the any kind of these content inside the course anymore.  • Send the wrong information to other student about the schedule which influence the student learning process.  • The important announcement delivers the wrong information to students or student can’t get aware of the certain announcement made by the instructors  • Messages sent to people1 turns out to be sent to people 2. Or wrong message which causes the communication between student and instructor.  • Student violates the academic honor integrity |

|  |  |
| --- | --- |
| **Abuse Use Case Name** | Malicious instructor try to abuse the system |
| **Actors** | Malicious Instructor |
| **Privileges** | Upload the slides/assignment/document  Create the group for students  Upload the quiz and make some authorization.  send announcement to his class students  Download the assignment submitted by the students  Release the grade and feedback for student’s assignment |
| **Abused privileges** | Send fault messages  modify/delete files, announcements or assignments  Modify students’ grades arbitrarily |
| **Preconditions** | Instructor has been assigned to certain class |
| **Postconditions** | **Success post\_conditions:**  malicious instructor is able to make abuse actions  **Failure post condition(s):**  malicious instructor can’t make any change out of their privileges. |
| **Trigger** | malicious instructors try to login the system |
| **Basic flow** | •Malicious instructors use attack tool1 try to log into the system  • System *authenticates* the login incident to check is instructor is eligible to log in  • Malicious instructor fails to log in or get access to the information inside the system |
| **Alternative flow** | • Malicious instructor uses attack tool 2 successfully logged in to the system(pass the authentic process)  • Malicious instructor tries to do some operations on the course content or send false message  • System test try to figure out the whether this instructor has been authorized by admin to make such actions.  • Malicious instructor is not authorized to make any such changes out of his privileges |
| **Exception flow** | Malicious instructor performs attack 3 using multiple attack tools, and successfully passed the authentic and authorized part. And he can make abuse action to the information inside the system. |
| **Harm** | •Student received the wrong information which influences the communication and problem solving.  •important file/announcement or assignment disappear or being changed which influences the instructors teaching plan and students feedback.  •the wrong grade for students does not reflect students performance and learning |