Collaborative Discussion 1: UML Flowchart

Units 1-3

Initial Post

- Select one of the coding weaknesses which have been identified by OWASP and create a flowchart of the steps which may have led to the weakness occurring. Which UML models might you use to present the design of your proposed software, and why are they the most appropriate choice(s)?
- In one of the TED Talks, Misha Glenny joked that “there are two types of companies in the world: “those that know they’ve been hacked and those that don’t” (September 13, 2011). But behind the humorous tone, a frightening reality is depicted: that of malevolent people who can take advantage of all security flaws and illegally use the personal data of anyone. We just have to look at all the data breaches of the 21st century: 3 billion yahoo accounts were hacked in 2013, and 700 million LinkedIn users and 533 million Facebook users faced the same fate in 2021 (Hill & Swinhoe, 16 July 2021).
  - Personal and sensitive data, therefore, require extra protection, especially since they also fall under international privacy laws and regulations such as the GDPR. The Open Web Application Security Project (OWASP), as a non-profitable foundation, aims to improve the security of software and has identified some software vulnerabilities. The coding weakness I have selected is ‘Cryptographic Failures’. Previously called Sensitive Data Exposure, it includes hacking of passwords, credit card numbers, health or personal information.
  - To represent the steps that may have led to the weakness occurring, I have thought of either the activity diagram or the state diagram. I’m a bit hesitant about using the state diagram, but I thought it would represent well the states of authentication, encryption, decryption or lack of it (but I’m not sure):

Initial Post (cont…)

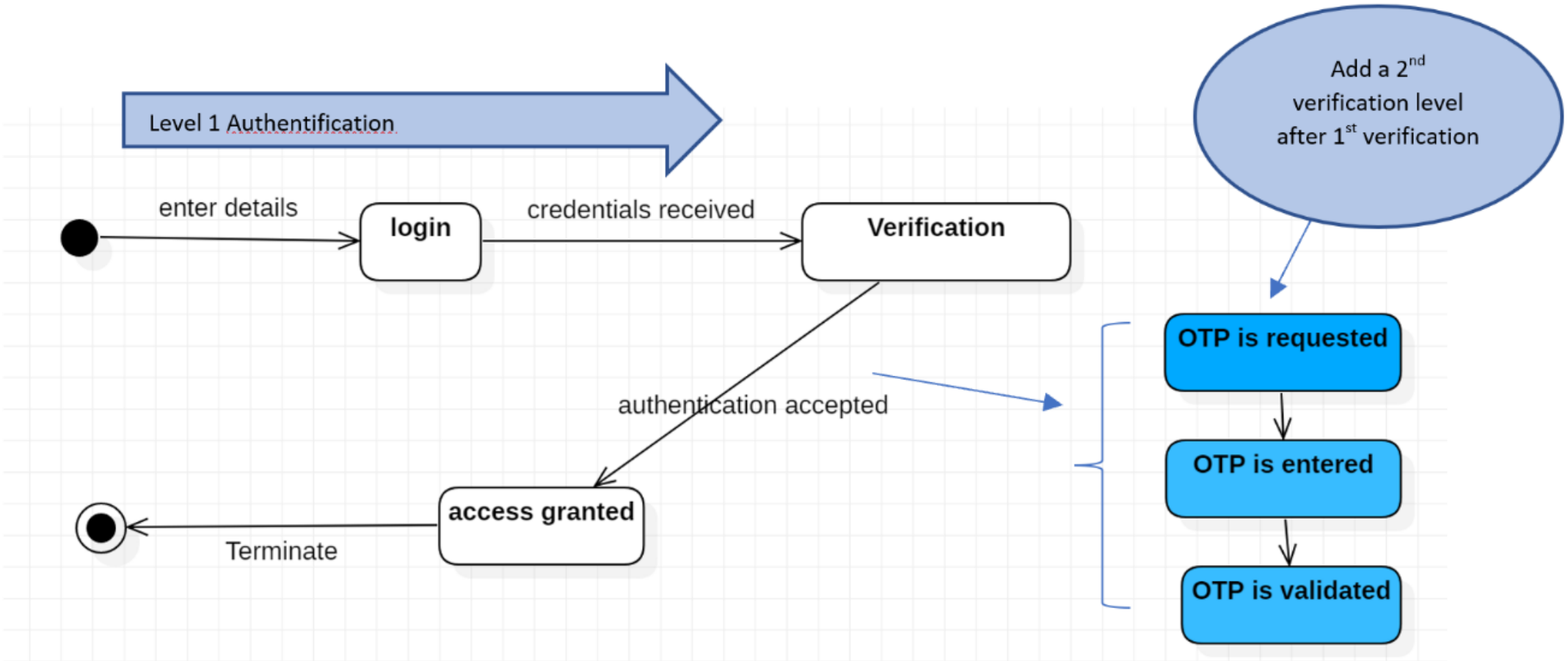
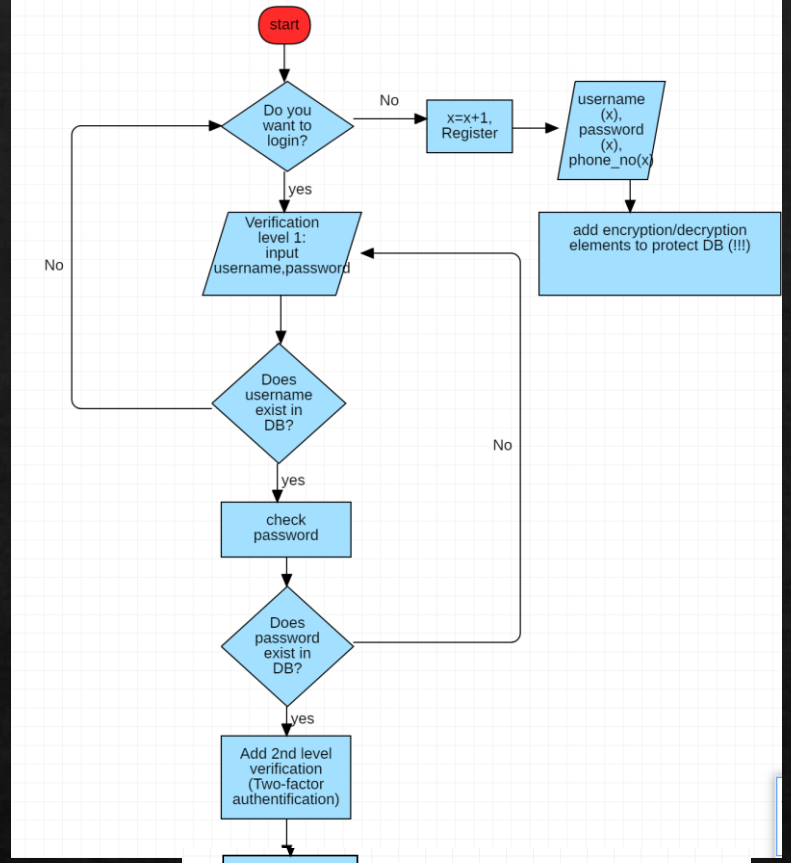
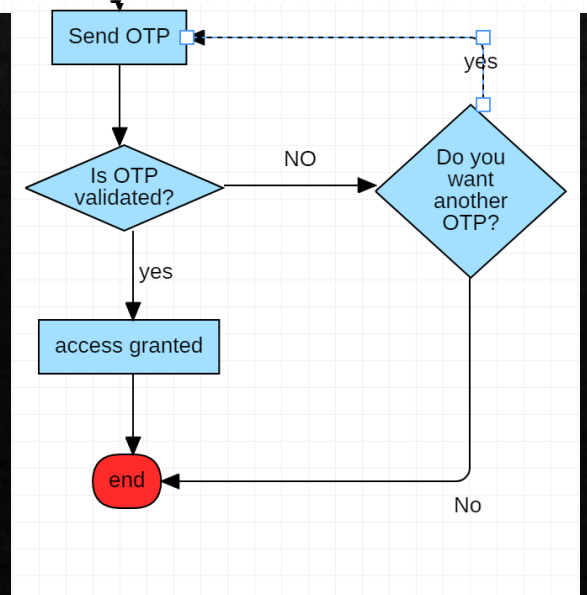


Figure 1: State Diagram with comments

Initial Post (cont…)

- A more detailed UML diagram for secure data transmission would be the activity diagram/flowchart.





References:

- Glenny, M. (September 13, 2011) “Hire the Hackers”, TED TALKS. Available from: https://www.ted.com/talks/misha_glenny_hire_the_hackers?language=en [Accessed 14 November 2021]
- Hill, M. & Swinhoe, D. (July 16, 2021). “The 15 biggest data breaches of the 21st century”, *CSO*, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
- OWASP. Available from: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ [Accessed 14 November 2021]

Tutor’s Comments

Hi Neelam,

Thank you for sharing this. In your model, you have captured the steps which should be taken to ensure that sensitive data exposure does not occur through the use of a OTP. What activities, on the other hand, may have led to the sensitive data exposure occurring? Perhaps the absence of a OTP to access a location where sensitive data should not have been stored?

In relation to the presentation of your model, I might have a check at the beginning: 'Do you want to register?'. After registration, the user can then be directed to: 'Do you want to login?'

Best wishes,

Cathryn

Summary Post

Summary of Coding Weaknesses (OWASP) chosen by classmates and Comments

Gennaro Coppola

Cross-site Request Forgery: "an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated". Clicking link sent via email or chat... (OWASP)

Solution to CSRF attacks: generate a token

Comments of tutor: Add i) another strategy: If the request does not pass input sanitisation, then the request might fail perhaps. ii) use swimlanes in the model to make it very distinct which system actor is responsible for the activity

Comment from Thien: Attack same as clickjacking - user clicks on a button or link on another page without their intention. Solution i)generate a single hard-to-guess random value /token as mentioned in post; ii) keep clear of cookies iii) adequately log out of all sites before visiting another. iv)use the browser's incognito mode.

Thien Liu

Access control (top 1 security risks) is a set of constraints on who (or what) can perform relevant actions or access resources that they have requested.

Tutor's Comments: add multiple decision points to authenticate a user to access a system.

Activity of "deny access by default", which is otherwise known as the 'Principle of Least Privilege'

Michael Botha

Security logging and monitoring failures is one of the top ten web application security risks (OWASP, 2021).

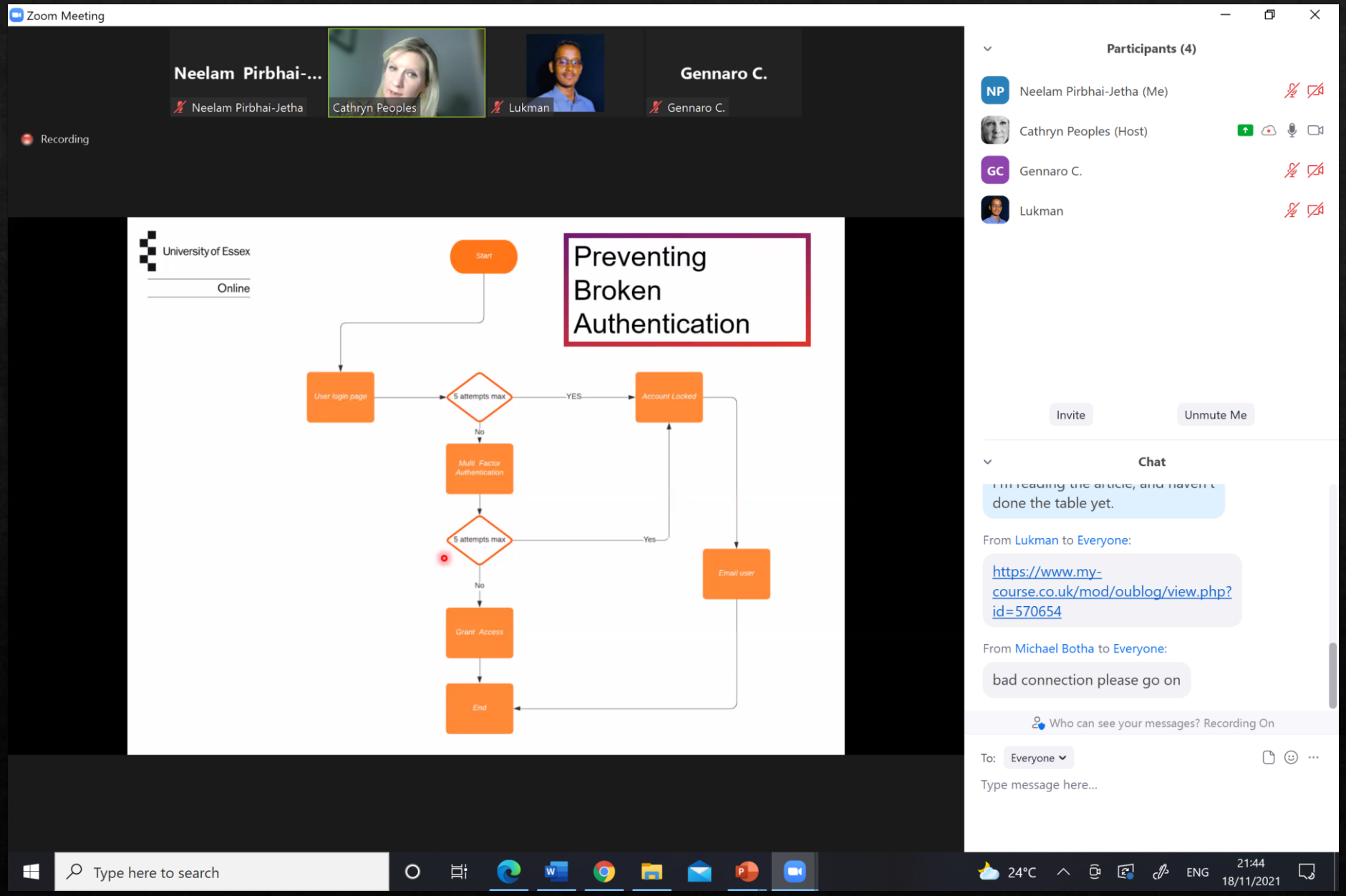
Tutor's Comments: Think of securing username and password attempt details, the location of where the login attempt is originating from, the frequency at which login attempts are being made and login attempts from a new device. These details might be retained within a 'threat log', in recognition of the fact that a variety of logs may be maintained for different objectives (e.g. information, warning, error).

Lukman Mohamed

According to OWASP, injection is an attacker's attempt to send data to an application in a way that will change the meaning of commands being sent to an interpreter. (OWSAP)

Solutions: i) Validate user input and consider the relevant properties like type, length, syntax... etc; ii)Thoroughly inspect API functions that are misused in a way that renders the system vulnerable; iii) Implement output encoding; iv)Protect sensitive data; v)Implement good authentication and session management

Examples of Tutor



Zoom Meeting

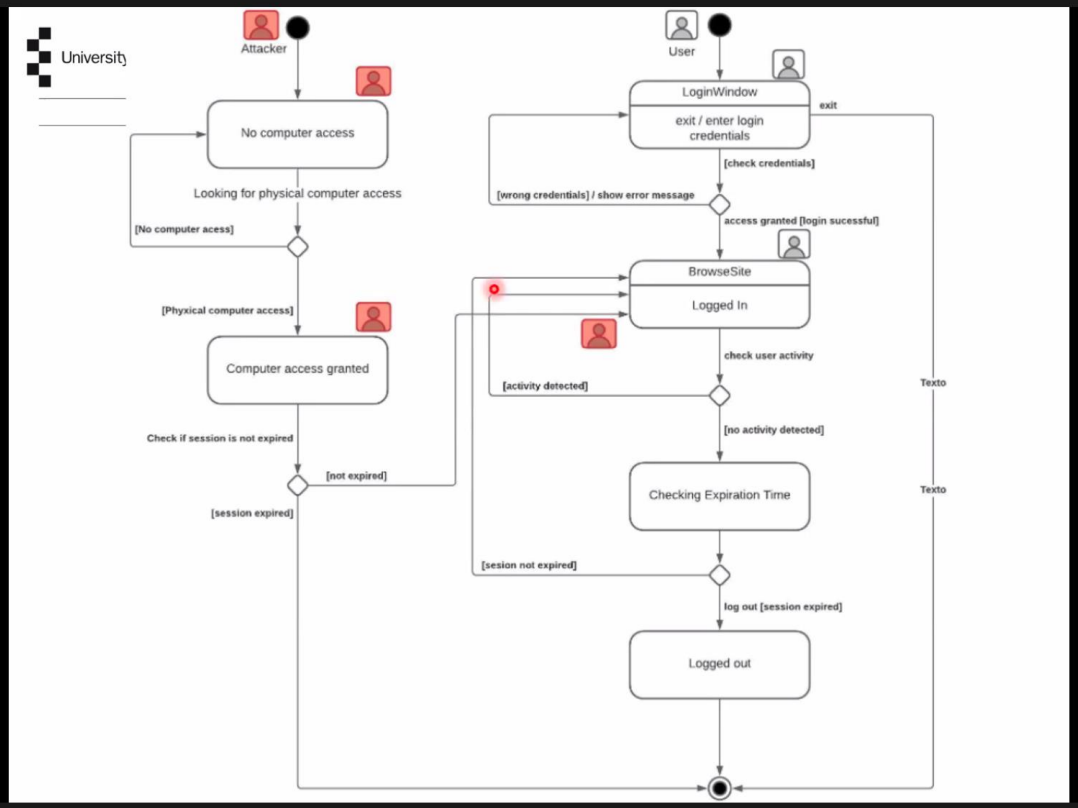
Neelam Pirbhai-...
Neelam Pirbhai-Jetha

Cathryn Peoples

Lukman

Gennaro C.
Gennaro C.

Recording



Participants (4)

NP Neelam Pirbhai-Jetha (Me)

Cathryn Peoples (Host)

GC Gennaro C.

Lukman

Invite

Unmute Me

Chat

done the table yet.

From Lukman to Everyone:

https://www.my-course.co.uk/mod/oublog/view.php?id=570654

From Michael Botha to Everyone:

bad connection please go on

Who can see your messages? Recording On

To: Everyone

Type message here...

Type here to search

24°C ENG 21:46 18/11/2021