
Default Question Block

Q1.

This information constitutes the "consent information" for the survey:

Dear Students,

We would like to invite you to participate in a survey. This survey is about the Cybersecurity concepts that were covered during the Project 4 on "Personal Web Server" in your course CS 3214. 5% of Project 4 grade will be assigned to this survey.

This survey is a part of Cybersecurity Education research study funded by the National Science Foundation at VT. Our goal is to assess the effectiveness of the Cybersecurity learning modules implemented in your course this semester and improve these learning modules based on your valuable feedback. The findings will also be published in journal and conference papers/posters for sharing our experiences to educators interested in Cybersecurity education.

The survey is confidential and we would very much appreciate your participation. Consent is implied with the submission of the survey. The survey includes 40 multiple choice questions and it will take a maximum of 15 minutes for completing the survey. Please note that the survey that is a part of the course assignment will be used for the research study. Thereby no additional time will be required on your part.

Important Note: Kindly note if you are a minor (under the age of 18), you are requested not to participate in this survey. For questions about your human subject protections, email The Virginia Tech Institutional Review Board at irb@vt.edu.

Thanks for your participation

Regards,

Vinod Lohani (vlohani@vt.edu)

Cybersecurity Education Project Team

- I consent to participate in the research study, in addition to taking this survey as part of Course CS3214
- I do not consent to participate in the research study. Please only use my survey as part of Course CS3214

Q2. For which course are you given this survey?

- ECE 3574
- CS 3214

Q3. From where are you taking the course?

- On-campus
- Online

Q4. What is your discipline?

- Computer Science
- Computer Engineering
- Electrical Engineering
- General Engineering
- CMDA
- Others

Q5. What is your academic level?

- freshman
- sophomore
- junior
- senior

Q6. What is your gender?

- Male
- Female
- Others

Q7. What is your ethnicity?

- White/Caucasian
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Hispanic or Latino
- Other

Q8. Did you take CS1114 in **Fall 2016 or Spring 2017 or Fall 2017**?

- Yes
- No

Q9. Did you take CS2114 in **Spring 2017 or Fall 2017**?

- Yes
- No

Q10. Did you take CS2506 in **Fall 2017**?

- Yes
- No

Q11. I can define the cybersecurity principle of data integrity

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q12. I can define the cybersecurity principle of data authenticity

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q13. I can define the cybersecurity principle of data availability

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q14. I can define the cybersecurity principle of resource integrity

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q15. I can define the cybersecurity principle of system integrity

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q16. I can define the cybersecurity principle of confidentiality

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q17. I can describe potential security threats to authenticity

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q18. I can understand the security threats to web applications

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q19. I can understand how to mitigate the security threats to web applications

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q20. I can understand the purpose and use of JavaScript Web Tokens to implement a stateless user authentication method for a web server.

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q21. Data integrity can be described as:

- The ability of a system to recover data from backup after it has been deleted.
- The ability of a system to ensure data can be accessed only by authorized users
- The ability of a system to determine whether data has been modified since its creation
- The ability of a system to ensure the absence of tampering by unauthorized parties

Q22. Data authenticity means:

- The ability of a system to ensure that data originates from a given source, i.e., has not been fabricated
- The ability of a system to validate users' passwords before granting access
- The ability of a system to ensure that data is modified only by authorized parties
- The ability of a system to ensure the accuracy and precision of the data

Q23.

Data availability can be described as:

- The ability of the system to encrypt/secure personal data
- The ability of a system to ensure that data originates from a given source, i.e., has not been fabricated
- The ability of the system to achieve a reasonable level of service even under a cyber attack
- The ability of a system to ensure the absence of tampering by unauthorized parties

Q24.

Resource integrity can be described as:

- The ability of the system to ensure accuracy and precision of its assets
- The ability of the system assets to validate client data
- The ability of the system to protect against the depletion of its assets (e.g. running out of memory or network bandwidth)
- The ability of the system to integrate all its assets for a shared purpose

Q25. System integrity can be described as:

- The ability of a system to detect and respond to attempts at intrusion
- The state of an information processing system where it performs its intended function unimpaired and is free from inadvertent, unauthorized or deliberate manipulation of the system.
- The absence of memory safety-related vulnerabilities because a type-safe language such as Java is being used
- The state of an networked system of computers wherein all traffic is being monitored

Q26. Confidentiality can be described as:

- Ensuring that personal information is deleted after an appropriate period of time has passed
- Ensuring that sensitive information is disclosed only to authorized users
- Ensuring that only the person whose personal information is kept can access it
- Ensuring that encryption is used at all times

Q27. JWT uses a hashing algorithm in its

- Header
- Payload
- Signature
- Header and Signature

Q28.

A user logs into Facebook. They provided their username and password. Facebook "does something" and the user is directed to their feed. "Does something" can be described as

- Facebook is authenticating and then authorizing the user
- Facebook is only authorizing the user
- Facebook is ensuring that the user remains anonymous
- Facebook does none of the above

Q29.

Which of the below is correct?

- Identity providers save users from having multiple passwords with third party web applications
- Identity providers do not share users' passwords with third party web clients
- Identity providers share users' data with third party web application
- All of the above are true with respect to identity providers

Q30.

Which of the following is not true of JWTs?

- They can be encrypted
- They can expire
- They are typically used for stateful authentication
- They ensure payload integrity

Q31.

User "A" logs into Evernote - a web-based note taking app. He is prompted with the message "Sign in with a Google account". Which of the below holds true?

- Evernote cannot access A's gmail password but can access some other data from A's gmail account with A's permission
- Evernote has access to A's gmail password but policies prevent Evernote from manipulating it
- Evernote can access A's gmail password with A's permission
- Evernote can access A's gmail password and manipulate it if need be

Q32. For questions 33 to 40, note that the word "coursework/course" refers to anything that you do in your course related to **cybersecurity**, including projects, activities (Lab/s), readings, etc.

Q33. The coursework held my attention

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q34. The coursework was beneficial to me

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q35. I enjoyed the instructional methods used in this course

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q36. I enjoyed completing the coursework

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q37. I will be able to use the knowledge I gained in this course

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Disagree
- Strongly disagree

Q38. Did you find the coursework related to cybersecurity **interesting**? If **yes**, why do you think so?
If **no**, why do you think so?

Q39. Did you find the coursework related to cybersecurity is **useful**? If **yes**, why do you think so? If **no**, why do you think so?

Q40. Please provide your comments/suggestions for the cybersecurity initiative for improvement

Powered by Qualtrics