Default Question Block

Q1.
This information constitutes the "consent information" for the survey:

Dear Students,

This survey is a part of a Cybersecurity Education project funded by the National Science Foundation at VT. Our goal is to assess the effectiveness of the cybersecurity learning modules that will be 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.

As a reminder, this survey is about the cybersecurity concepts that will be covered in class during project 6 (for ECE 2574) or Lab 11 and 12 (for CS 2114).

Although the survey is voluntary and confidential, we would very much appreciate your participation. Consent is implied with the submission of the survey. The decision to participate or not to participate will not affect your grade in this course. The survey includes 39 questions and it will take a maximum of 15 minutes for completing the survey.

Important Note: Kindly note if you are a minor (under the age of 18), you are requested not to participate in this survey.

Cybersecurity Education Project Team

Q2. For which course are you given this survey?

- ECE 2574
- CS 2114

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
- ◯ Other

Q8. Did you take CS1114 or ECE 1574 in **Fall 2016 or Spring 2017**?

- ◯ Yes
- ◯ No

Q9. I can define the cybersecurity principle of data integrity

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

Q10. I can define the cybersecurity principle of data authenticity

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

Q11. I can define the cybersecurity principle of data availability

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

Q12. I can define the cybersecurity principle of resource integrity

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

Q13. I can describe potential security threats to resources

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

Q14. I can identify characteristics of workloads that represent legitimate request streams

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

Q15. I can identify tell-tale characteristics in workloads stemming from malicious attackers

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

Q16. I can apply defense strategies to protect resources

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

Q17. Data integrity can be described as:

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

Q18. Data authenticity means:

- ◯ The ability of a system to ensure that data is modified only by authorized parties
- ◯ 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 the accuracy and precision of the data

Q19.

Data availability can be described as:

- ◯ The ability of the system to achieve a reasonable level of service even under a cyber attack
- ◯ 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 a system to ensure the absence of tampering by unauthorized parties

Q20.

Resource integrity can be described as:

- ◯ The ability of the system to integrate all its assets for a shared purpose
- ◯ 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 ensure accuracy and precision of its assets
- ◯ The ability of the system assets to validate client data

Q21.

Which of the following attacks is not primarily targeted at resource integrity?

- ◯ Spear phishing attacks in which an attacker tricks victims into revealing personal data such as passwords
- ◯ A Ping flood attack in which an attacker sends multiple ICMP echo request packets to a destination.
- ◯ A Distributed Denial-of-service (DDoS) attack in which a botnet of compromised machines attempts to overwhelm a server by sending many requests.
- ◯ A TCP Sync attack in which a rogue client attempts to overflow a server's TCP connection table

Q22. Which of the following attacks is not primarily targeted at resource integrity?

- ◯ A compromised computer issuing a large number of connection attempts from a single IP address
- ◯ A compromised computer making a requests that requires significant computing, or the sending of large amounts of data, by a server
- ◯ Distributed Denial-of-service (DDoS) attack where a group of compromised computers make coordinated requests that attempt to mimic legitimate users
- ◯ Spear phishing attacks in which an attacker attempts to get users to reveal personal data such as usernames or passwords

Q23.

Consider a medium-sized web cache designed for 100,000 users of which on average 100 users are online. Users interact with a web application that is behind the web cache. Under normal working conditions, what would the distribution of requests in the request stream seen by the cache look like?

- ◯ There are no common patterns in the distribution of requests for such caching systems.
- ◯ Single accesses from a relatively small number of clients whose composition shifts over time.
- ◯ Frequent accesses that result in misses in the web cache.
- ◯ Multiple, temporally local accesses by a relatively small number of clients whose composition shifts over time.

Q24. When considering a system that processes user requests sent across a network, what would be common characteristic of the request stream if the system is servicing legitimate users (under normal conditions)?

- ◯ Application-dependent access patterns that appear to be from moderate number of client groups and are consistent with an analysis of system traces
- ◯ A wide range of access patterns that cannot be clustered into client groups—instead the access patterns are distinct
- ◯ Single accesses from distinct IP addresses to wide range of system services, some of which are rarely used based on analysis of system traces
- ◯ Repeated authentication failures from a subset IP addresses

Q25.

Considering the same systems, which of the following could be characteristics of an ongoing denial-of-service attack?

- ◯ Numerous single requests for data items that have not been requested in a long time (such as requests for random URLs), resulting in cache misses.
- ◯ Numerous repeated requests for the same item from the same source.
- ◯ Repeated requests associated with authentication failures.
- ◯ All of the above

Q26.

Which of the following could be characteristics of a system that is under denial-of-service attack?

- ◯ Numerous repeated requests for the same data item from the same IP address or user/client
- ◯ Numerous single requests for data that is uncorrelated, or has not been accessed by the user in a long time
- ◯ Repeated requests associated with authentication failures
- ◯ All of the above

Q27.

Which following defense strategies **cannot** be used to lessen the impact of an attack on system resources?

- ◯ Blacklisting of client IP or network addresses.
- ◯ Improved load balancing/cache replacement policy for requests from different clients/users.
- ◯ Increasing the scrutiny with which the data contained in each request is sanitized
- ◯ Throttling of requests.

Q28. Which following defense strategies **cannot** be used to lessen the impact of an attack on system resources?

- ◯ Encrypting passwords of a client
- ◯ Blacklisting of IP addresses
- ◯ Improved load balancing of server requests from different clients/users
- ◯ Throttling of server requests

Q29. For questions 24 to 34, note that the word “coursework/course” refers to anything that you do in your course related to cybersecurity, including assignments, activities (Project or lab), readings, etc.

Q30. The coursework holds my attention

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

Q31. In general, the coursework is useful to me

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

Q32. The coursework is beneficial to me

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

Q33. The instructional methods used in this course holds my attention

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

Q34. I enjoy the instructional methods used in this course

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

Q35. The instructional methods engage me in the course

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

Q36. I enjoy completing the coursework

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

Q37. I find the coursework to be relevant to my future

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

Q38. The coursework is interesting to me

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

Q39. I will be able to use the knowledge I gained in this course

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

Q40. The knowledge I gained in this course is important for my future

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

Q41. Do you find the coursework related to cybersecurity interesting? If yes, why do you think so?If no, why do you think so?

Q42. Do you find the coursework related to cybersecurity is useful? If yes, why do you think so?If no, why do you think so?

Q43. Please provide your comments/suggestions for the cybersecurity initiative.