

## Systems, Networking, and Cybersecurity Ph.D. Qualifier Exam

Spring 2022

The following questions relate to the papers in the reading list on the Spring 2022 qualifier webpage (<https://people.cs.vt.edu/boji/qual/>). For full citations, please see that reading list. Before starting, read and understand the following guide provided by Virginia Tech: Avoiding Plagiarism: A Guide For Graduate Students at Virginia Tech ([https://graduateschool.vt.edu/content/dam/graduateschool\\_vt\\_edu/graduate-honor-system/avoiding-plagiarism-short-guide.pdf](https://graduateschool.vt.edu/content/dam/graduateschool_vt_edu/graduate-honor-system/avoiding-plagiarism-short-guide.pdf)). In your answers, you must avoid unattributed direct quotations and paraphrases and use proper documentation of all sources you use. This requires that you include a bibliography in your response. Failure to follow these guidelines represents a violation of Virginia Tech's Honor Code and will result in a score of 0.

1. The following questions relate to the paper “Quantifying Memory Underutilization in HPC Systems and Using it to Improve Performance via Architecture Support”.
  - a. What is the problem being solved in the paper?
  - b. What are some key insights in the paper?
  - c. What are some key causes of low memory utilization in HPC systems?
  - d. How does the paper exploit unused memory to improve memory performance?
  - e. What are some limitations of this work?
2. The following questions relate to the paper “Forget Failure: Exploiting SRAM Data Remanence for Low-overhead Intermittent Computation”.
  - a. What is the problem being solved in the paper?
  - b. What are some key insights in the paper?
  - c. How does the paper preserve reliability for intermittent computing?
  - d. How does the paper improve performance over conventional intermittent computing?
  - e. What are some limitations of this work?
3. The following questions relate to the paper “Quantifying Server Memory Frequency Margin and Using it to Improve Performance in HPC Systems”.
  - a. What is the problem being solved in the paper?
  - b. What are some key insights in the paper?
  - c. In servers today, what typically happens to applications when they encounter an uncorrectable memory error?
  - d. How does the paper preserve system-level reliability while operating memory faster than specification?
  - e. What are some limitations of this work?
4. The following questions relate to the paper “Is the Web Ready for OSCP Must-Staple?”.
  - a. Describe why the certificate revocation checking is needed.
  - b. List all revocation checking mechanisms.
  - c. Explain the security vulnerabilities for each revocation checking mechanism.
  - d. Explain why it is hard to deploy OSCP Must-Staple?

5. The following questions relate to the paper “A Longitudinal, End-to-End View of the DNSSEC Ecosystem”.
  - a. Describe why DNSSEC is necessary.
  - b. Explain why we need two different private-public key pairs, i.e., ZSK and KSK.
  - c. Describe the whole process to authenticate example.com’s A record.
  - d. (Other than the proposed methodology in the paper), describe potential methodologies to keep track of the DNSSEC deployment status on DNS “resolvers”.
  - e. Discuss the root causes of the low deployment of DNSSEC and its potential solutions.
6. The following questions relate to the paper “NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities”.
  - a. Summarize the attack methodology proposed in the paper.
  - b. Describe the root causes of the feasibility of this attack.
  - c. Discuss the potential methodologies allowing to attack “local” resolvers.
  - d. Describe the potential methodologies to amplify the proposed attack.
7. The following questions relate to the paper “ATP: In-network Aggregation for Multi-tenant Learning”.
  - a. Summarize this paper in terms of the motivation, main objective, challenges, key ideas, main results, and unique contributions.
  - b. What are the unique properties and limitations of programmable switches?
  - c. What are the key limitations of the baseline solutions (BytePS, SwitchML, Horovod, etc.)?
  - d. What are the limitations of ATP? Do you have any suggestions for further improvement?
  - e. Besides in-network computation/aggregation, what other applications of programmable switches would you suggest?
8. The following questions relate to the paper “New Directions in Automated Traffic Analysis”.
  - a. Summarize this paper in terms of the motivation, main objective, challenges, key ideas, main results, and unique contributions.
  - b. What are the standard data representation options for network traffic? What are their pros and cons?
  - c. What are the unique properties of the proposed nPrint? What are the pros and cons of nPrint? Do you have any suggestions for further improvement?
  - d. Do you think it is feasible if someone proposes to implement nPrint using programmable switches (discussed in the ATP paper)?
  - e. Besides the use cases discussed in the paper, what other applications of nPrint would you suggest?
9. The following questions relate to the paper “Exploring LoRa for Long-range Through-wall Sensing”.
  - a. Summarize this paper in terms of the motivation, main objective, challenges, key ideas, main results, and unique contributions.
  - b. What are the existing wireless sensing technologies? What are their limitations?
  - c. What are the unique properties of LoRa? What are the pros and cons of LoRa-based wireless sensing?

- d. What are the important factors that impact the sensing performance? How robust is LoRa sensing against these factors?
- e. Besides the use cases discussed in the paper (i.e., long-range through-wall respiration sensing and human tracking), what other applications of LoRa sensing would you suggest?