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

Spring 2023

The following questions relate to the papers in the reading list on the Spring 2023 qualifier webpage (https://people.cs.vt.edu/tijay/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). 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 "Is the Web Ready for OCSP Must-Staple?".
   - Describe why the certificate revocation checking is needed.
   - List all revocation checking mechanisms.
   - Explain the security vulnerabilities for each revocation checking mechanism.
   - Explain why it is hard to deploy OCSP Must-Staple?

2. The following questions relate to the paper "Under the Hood of DANE Mismanagement in SMTP".
   - Describe how DANE should work from the both perspective of a server and client.
   - Explain why DANE has not been deployed in the Web-PKI ecosystem.
   - Explain why classifying the thirty-party hosted server is challenging.
   - Explain why rollover in DANE is challenging.

3. The following questions relate to the paper "CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers
   - List all the revocation checking mechanisms for Web PKI and explain how they work
   - Explain the potential performance degradation when a web browser checks revocation
   - Discuss the challenges of using Bloomfilter and why it is applicable to CRLite
   - Discuss the potential challenges and limitation of CRLite when extending it to non-web PKI such as code-signing PKI

4. The following questions relate to the paper "SECFLOAT: Accurate Floating-Point meets Secure 2-Party Computation (Full Version)".
   - What is the secure computation that the paper is referring to?
   - What is the problem in secure computation that the paper is addressing?
   - What is the main methodology of the paper?
   - How does the paper improve performance and security over state of the art?
   - What are the limitations of this paper?

5. The following questions relate to the paper "Omnes pro uno: Practical Multi-Writer Encrypted Database".
   - What is the problem that this paper is trying to solve?
   - What are the main methodology and high-level idea of this paper?
   - How does the paper improve the performance and security over state of the art?
   - What is the security notion the proposed technique relies on and how does the proposed technique achieve security?
   - What are the limitations of this paper?

6. The following questions relate to the paper "S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing".
   - What is ORAM and its main security feature?
   - What is the problem in ORAM this paper is addressing?
   - What are the main methodology and high-level approach of this paper?
   - How does the proposed technique improve over state of the art?
   - What are the limitations of this paper?

7. The following questions relate to the paper “Quantifying Location Privacy”.
    - What is the problem being solved in the paper?
    - Explain why expected estimation error is a good metric to quantify location privacy.
    - Describe a scenario in which location privacy is a concern and applying a location privacy protection mechanism (you pick one) can help. Then describe how the location-privacy meter can be used to evaluate the effectiveness of the location privacy protection technique.
    - What are some limitations of this work?

8. The following questions relate to the paper “On the Security and Performance of Proof of Work Blockchains”.
    - What do you see as the main contribution of the paper?
    - What is selfish mining? Explain when and how selfish mining can allow an attacker to gain more rewards comparing to honest mining in a POW-blockchain.
    - What is double spending? Give an example that double spending can occur on PoW-blockchain.
    - What metric(s) are used to evaluate the security of blockchain instances in this paper?
    - What are the key findings about the impact of the block interval and the block size on the security of a blockchain?

9. The following questions relate to the paper “Practical Techniques for Searches on Encrypted Data”.
    - What is the problem being solved in the paper?
    - What are the key security properties that the proposed search techniques provide in this paper? Explain why those properties are important for such schemes.
    - Show how the final scheme supports search of a word W over the ciphertext. What information Alice must give to Bob? Show the steps that Bob takes to search for W in the ciphertext.
    - Do a complexity analysis of the search algorithm in the final scheme.