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

Spring 2014

Direct all your questions to Prof. Wenjing Lou at wjlou@vt.edu
Email your written answers to Prof. Wenjing Lou at wjlou@vt.edu
by midnight Monday, Feb 3, 2014
Use "Qualifier Answer" in the subject area.

Questions on the paper "Computer Viruses: Theory and Experiments"

1. Please list all the results on the infeasibility of viral defense that are described in the paper.

2. Among the above infeasibility results, please choose one and give a brief proof.

3. Can you think of a method that can be used to defend against virus spreading? Please discuss its effectiveness, e.g., would it be easily evaded by attackers?

Questions on the paper "Mimimorphism: A New Approach to Binary Code Obfuscation"

1. Can you think of four ways for obfuscating binary code (to evade signature based malware detection)?

2. Please describe step-by-step how a high-order mimic function works.

3. What are the advantages of the proposed high-order mimic function over the existing Huffman mimic function?

4. Can you think of a countermeasure to defeat the proposed mimicry attack?

Questions on the paper "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds"

1. Use your own words, please list all the security properties that a cloud customer desires in cloud computing.

2. Describe all the attack capabilities that the authors demonstrate in this paper that threaten the security of cloud computing. Please itemize your answer.

3. For achieving co-residency with the target victims,
   a. What are the two proposed strategies?
   b. How do these two strategies perform experimentally?

Questions on the paper "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core"

1. The authors claimed three main contributions of the paper. Please elaborate on one of the contributions and comment on this contribution with regard to what is lacking in the prior research and how it advances the state-of-the-art knowledge at the time of publishing.

2. In order to characterize the impact of malicious mobile phones on a cellular network core, the paper described an attack. Please answer the following questions regarding the designed attack:
   a. What resources and capability are necessary for an adversary to successfully launch such an attack?
   b. What is the intended damage/ consequences the attack is trying to achieve?
   c. The paper demonstrated that the impact of the attack can be amplified by adopting an attack strategy that exploits the cellular networking functionality. Describe the attack strategy.

3. Describe three possible mitigation techniques.

Questions on the paper "A Key-Management Scheme for Distributed Sensor Networks"

1. Explain the core idea of this paper. List the operational or resource limitations of the applications where this scheme is suitable to apply.

2. This paper proposed a random key-predistribution scheme for distributed sensor networks. As comparison, two straight forward key predistribution schemes are also presented: 1) A single mission key scheme and 2) Pair-wise secret key predistribution scheme, where every pair of sensors pre-share a unique secret key before deployment. Provide an analysis for these three schemes in terms of a) memory requirement, i.e. number of keys each sensor needs to carry; b) security, i.e. resilience to sensor node capture; and c) network connectivity. State any assumptions that are necessary for your analysis. Note that your focus is to demonstrate, by comparison, the pros and cons of the various key-distribution schemes.

3. The following two schemes are commonly used scalable key management schemes. Discuss why these two schemes are not suitable in distributed sensor networks.
   a. KDC-based secret key distribution scheme, where each sensor share a unique secret key with the KDC (Key Distribution Center); when sensor Alice wants to talk to sensor Bob, Alice contacts KDC for a key to be used with Bob.
   b. Public key based key distribution, where each sensor has its own public key signed by a centralized certification authority (CA). Each sensor carries its own public key certificate and the CA's public when deployed.

Questions on the paper "PARROT: A Practical Runtime for Deterministic, Stable, and Reliable Threads"

1. What is the core idea of this paper? Explain in a short (200 words) paragraph. Be sure that you focus on a single idea.

2. Enforcing stability reduces the schedulers flexibility and introduces (in the case of PARROT) additional constraints (round-robin scheduling in PARROT). Does enforcing stability always come at the price of reduced performance?

3. What is a serious drawback of COREDET in comparison with PARROT? Where causes this drawback in COREDET?

4 . Explain intuitively why the soft barrier results in the improved performance shown in Figure 4.

5. The PARROT schedule shown in Figure 4 is simpified. Considering only the producer and consumer 1 explain the detailed sequence of events that are omitted from Figure 4 by drawing and explaining a figure that more accurately shows the missing details.

6. Figure 7 shows the pthread_cond_wait wrapper. Show the code for the pthread_cond_signal operation that is not given.

7. What is relevance of model checkers (like DBUG) to concurrency? Explain how this is realized in PARROT.

Questions on the paper: "Everything You Always Wanted to Know About Synchronization but Were Afraid to Ask"

1. Which of the observations made in Section 1 are supported by the data in Table 2 and Table 3? Be specific.

2. Are there results in Table 4 that are surprising given the results in Table 2?

3. Explain the statement on page 41: "Not surprisingly, the CLH and the MCS locks are the most resilient to contention."

4. Given the variation in lock scalability (single vs. multiple sockets, low vs. high contention) describe an approach that would allow an application to perform well across different platforms and contention conditions. Consider the description of SSYNC given on page 34 of the paper.