1. Shared Themes

(a) Both Spanner and DTHREADS refer to the concept of a transaction yet these systems are radically
different in their design and goals. Explain the important aspects of the transaction concept.

(b) Creating a deterministic computation is a critical element of DTHREADS while Spanner has no
such concern. Explain this different view of the role of deterministic computation.

2. DTHREADS Questions

(a) Explain how DTHREADS achieves the goals of “greatly simplify record and replay for
multithreaded programs…and it would enable the execution of multiple replicas of multithreaded
applications.” (see the top of the right column on page 327)?

(b) What is meant by cache-line false sharing? (See Contributions page 327)

(c) What is meant by "printf debugging"? Explain why this is a concern in the context of this paper.
(see Contributions page 327)

(d) Explain the idea of copy-on-write and explain its significance in this paper.

(e) Describe a worst-case scenario where DTHREADS would perform poorly with respect to
 pthreads.

(f) Section 4.2.2, first paragraph says that a thread computes a diff from a twin (unmodified) page. Why
not use the existing page in the shared memory?

(g) In reference to Section 4.3.1, is it possible that threads can experience starvation under
DTHREADS when this would not happen with pthreads? Explain.

(h) If you run an application successfully under DTHREADS and then, for performance reasons, run
this application under pthreads what guarantees do you have about the pthreads execution?

3. Spanner Questions
(a) Explain the concept of a lease that is used in Spanner. What relevance does it have in ensuring fault-tolerance?

(b) Under what circumstances is a given replica both a participant leader and a coordinator leader?

(c) Section 4.1.1 describes the “disjointness invariant: for each Paxos group, each Paxos leader’s lease interval is disjoint from every other leader’s.” Explain why this invariant is needed.

(d) Section 4.1.2 says that “Transactional reads and writes … can be assigned timestamps at any time when all locks have been acquired, but before any locks have been released.” Explain why any time in this interval can be chosen.

(e) Assume that transaction T_1 and T_2 write to the same data and have both committed. It is known that the time at which T_1 acquired the lock on the data is earlier than the time at which T_2 acquired this lock. Extend as needed the notation in Section 4.1.2 to prove that the commit timestamp of T_1 is less than the commit timestamp of T_2. Be as detailed and precise in your answer as the authors.

(f) Spanner uses locking in contrast to “optimistic concurrency control” (bottom of left column on page 3). Using the facilities of TrueTime, outline how an optimistic concurrency control scheme could be implemented in Spanner.

4. BINDER Questions

For the paper “BINDER: An Extrusion-based Break-In Detector for Personal Computers”, please answer the following questions.

1) The key idea of the paper is to correlate network activities with user inputs in order to detect break-ins and suspicious network traffic. What is the main advantage of this approach compared to the signature scanning method (e.g., SNORT or Symantec anti-virus)?

2) What is the authors' assumption on the trustworthiness of the user? Can attacks caused by insider threats (e.g., data leak due to disgruntled employees) be prevented by BINDER?

3) Why the process information needs to be utilized in the detection?

4) Describe step-by-step the detection algorithm.

5. Onion Routing Questions

For the paper “A Peel of Onion”, please answer the following questions.

1) Onion routing provides routing anonymity. What are its advantages compared to virtual private network (VPN)?

2) What is the strongest adversary model (attackers' capabilities) that onion routing can defend against, that is, in the most advanced onion routing solution (i.e., Tor), what are attackers allowed to do?

3) What is hidden service? Describe how hidden service is realized by onion routing.

4) Alice would like to send Bob an anonymous letter with the help of 3 onion routers and onion routing technique (i.e., a message wrapped in layers of public-key encryption, one per each router on the path). The letter is confidential and only Bob can read it. However, Bob should not know the name or IP address of the sender (Alice). No eavesdropper or onion router can learn who the sender or receiver is. 
   I. Describe step-by-step how the message is encrypted, routed to next hop destination, and decrypted. Use notation to represent cryptographic keys, message, ciphertext, etc. Let IP_A, IP_B, and IP_C be the IP address of onion routers A, B, and C, respectively.
II. In order to fulfill the anonymity goal (namely, no eavesdropper or onion router learns who the sender or receiver is), what else do Alice, Bob, and onion routers all need to do in addition to transmitting the above message?

6. QUIRE Questions

For the paper “QUIRE: Lightweight Provenance for Smart Phone Operating Systems”, please answer the following questions.

1) The paper describes methods for tracking and authenticating IPC call chains for smart phone OS such as Android. Why is this security problem unique for smart phone operating systems in comparison to conventional Linux OS environments?
2) Evil apps may attempt to forge or tamper with the IPC call chain information in order to gain unauthorized access. How does QUIRE prevent these types of attacks?
3) The paper describes several applications of the proposed solution (in sections 1 and 4). Please describe
   I. another application scenario for using QUIRE,
   II. the security property gained by using QUIRE,
   III. draw the message flow in your scenario similar to Figure 4 on page 9.

7. Authenticated Syscall Questions

For the paper “System Call Monitoring Using Authenticated System Calls”, please answer the following questions.

1) How does the research problem in this paper fundamentally differ from the one studied in QUIRE?
2) Describe the attack model in this paper. In other words, what attacks (or problems) can be prevented by the proposed solution? Describe the security assumptions of the paper, i.e., the necessary conditions for the proposed solution to work securely.
3) Given a program $p$, describe in details step-by-step how system calls in $p$ can be authenticated. ($p$ was developed by developers who are not aware of the authenticated syscall environment which $p$ will be run in.)
4) You try to sell this technology to a company. The company's CTO is interested in adopting it within his company, but is concerned about its security, performance, and usability.
   I. What would be the CTO's top three concerns?
   II. How do you address these concerns with the help of experiment results in this paper?