**EMCS2020: Advanced Topics in Computer Security**

Post-Work Assignment: Cloud Security Concepts

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Based on what you learned in class and the recommended readings, please answer the following questions:

***Explain succinctly (about 200 words) and in your own words what are provable data possession and proof of replication and why they are relevant to a cloud storage deployment. Assume your reader is a CEO or Board member who does not have a cybersecurity background. (5 points)***

PDP and POR systems ( or schemas ) are frameworks that provide verifiable proof that data on a cloud system has been stored and/or replicated. In some cases, the client of the cloud provider wants to verify that the information has been stored and NOT replicated, the sake of privacy. Many of these schemes rely on cryptological hashing and Merkle trees to create tamper-proof verifications. All of them will require some type of challenge-response setup up so the client can be assured that the host is telling the truth about the contents and structure of the cloud server. This type of verification can be tricky and a user ( client ) can be easily fooled by the host’s ability to fabricate data structures on the fly to lie about the contents of a server. As a general rule when adding a file to the system serialization should be slow since it involves hashing the file and adding the hash to a large data structure which also must be rehashed, but the verification of the file should be sub-second fast since all the pieces already exist. A slow verification process is a red flag that the host is trying to build a data structure in the background to match the verification request.

***Explain succinctly (about 200 words) and in your own words which security risks stem from optimization methods commonly used in processor architecture and how an organization can mitigate such risks when planning a cloud computing deployment. Assume your reader is a CEO or Board member who does not have a cybersecurity background. (5 points)***

Cloud file storage systems like DropBox, for example, provide a way for users to store their files on the host system without having to worry about keeping the file on the user’s local file system. So, when the user changes computers, for example, they can just log in to the DropBox system and retrieve the file. In order to optimize the use of space, if more than one user happens to store the same file, cloud providers tend to optimize by only storing one copy of the file and user permissions to manage access. As a result, when a user adds this file to the host provider’s system there is no data transfer, as the host provider application notices that the file is identical to the one already on the server. This is a breach of privacy. Users can protect themselves by adding unique information to their files, thereby disrupting the ability of the host provider’s application to recognize the file as a file that is already stored on the server. Furthermore, the host provider application should find ways of obfuscating data transmission rates and sizes from users.

***Complete the sentence below by filling in the two first words. (1 point)***

**branch prediction** relies on the ability of the CPU to run code “speculatively” and throw away results if that code should not have been run in the first place.

***Is the following statement true or false? No justification is needed. (1 point)***

Migrating from an on-premises to a cloud solution solves or mitigates Spectre and/or Meltdown vulnerabilities? **False**

***Is the following statement true or false? No justification is needed. (1 point)***

Research has shown that sharing hardware resources can cause the unintentional leakage of secret information across tenant boundaries in cloud contexts. **True**

***Is the following statement true or false? No justification is needed. (1 point)***

A protected database search system deployed in the cloud increases data exposure to breaches by cryptographically isolating the roles of reading from, writing to, and administering the database. **True**

***Select the best completion of the sentence "A side-channel attack is ... " from the four options below. No justification is needed. (1 point)***

A. a turbulent river in France

B. a new villain group in the Marvel Universe

C. an attack against a cloud storage system that attempts to modify files in a stealthy manner, without changing the cryptographic hashes of the files

**D. an attack that exploits inadvertent leakage of information by a system via observation of properties such as the timing of operations, power consumption, and network traffic**

Note that this post-work assignment counts for half of the points for Module 10. The remaining half of the points will be assigned based on your participation in the in-class discussions.