Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

1. Identify three actors (user categories) in the system.
2. Identify three security and/or privacy threats against the system.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

1. Identify three actors (user categories) in the system.

   Canvas: Students, Teachers, Module Admin

   eBay: Sellers, Buyer, Admin

   Facebook: Friends, Non-friends, Facebook Moderators

2. Identify three security and/or privacy threats against the system.

   Personal details leak, friends list leak, student grades leak…

   Data tampering

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

3. For one (or more) of the threats describe the capabilities of an attacker.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

3. For one (or more) of the threats describe the capabilities of an attacker.

    a. Attacker is an inside person at eBay. It can change data on local HDD which is not authenticated.

    b. Attacker is one of the Canvas developers. It has embedded a back door in the system which forces Canvas to encrypted data with a known key.

    c. The attacker is a proxy server that is placed in-between the user and the server and it breaks the TLS connection.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

4. Propose a way to protect your data from your attacker by using encryption, authentication and/or integrity checks. Explain your choices.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

4. Propose a way to protect your data from your attacker by using encryption, authentication and/or integrity checks. Explain your choices.

   a. eBay: authenticate messages using a users key. Encrypt messages using end-to-end.

   b. Use CryptDB to protect the data against the malicious administrator.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

5. Identify one advantage and one disadvantages for your chosen method of protecting the data.

Cloud computing security

Consider a popular cloud based system (i.e., a well-known system that we also know about) that you are familiar with (e.g. Canvas, eBay, Facebook).

5. Identify one advantage and one disadvantages for your chosen method of protecting the data.

   a. Simple non-keyed MACs are not useful because they can be produced by the attacker. We need keyed MACs (HMACs or CMACs). This will allow a user to verify its own data, for multiple users will require key exchange which is difficult…

   b. CryptDB will hide database contents, but will eventually use the weakest encryption allowed which might not be sufficient. CryptDB is vulnerable to frequency analysis…