What TC Can and Can't Do

- Guarantee that EK is safe
  - Yes because it is stored in and used by hw only
  - No because it can be obtained if someone has physical access but this can be detected by user or remote system (tamper bit is set in TPM)
- Guarantee that no keys can be compromised
  - No, keys that go to OS and are used by sw can still be compromised
- Guarantee that applications cannot be changed or compromised
  - No, I can only detect compromise by comparing hashes of apps in hw

What TC Can and Can't Do

- Guarantee that no rootkits can reside on the system
  - No, but we can detect compromise by comparing hashes of OS files in hw
- Guarantee that applications cannot interfere with each other
  - Yes, due to OS separation
- Guarantee data safety on disk
  - Yes, we can encrypt data separately for each virtual system and we can encrypt the whole disk
  - No, because encryption happens in sw

Privacy