The downside of trusted computing

Technology, Information Technology

The downside of trusted computing College In spite of the many principles concerning the safety of trusted computing, the design has brought up some concerns over privacy and functionality. Practically, trusted computing utilizes cryptography to aid in enforcing a chosen behavior (" Weighing the pros and cons of the Trusted Computing Platform," n. d.). The major feature of trusted computing is to permit someone else to authenticate that only certified code runs on a system. Remember, trusted computing when used alone does not guard against attacks that abuse security susceptibilities set up by programming bugs.

The problem comes up with the main purpose of the chip. It is technically achievable with trusted computing, to protect the hardware for its possessor as well as to secure it against its holder. Other related issues comprise of the exploitation of validation of software remotely. In this case, the maker and not the client who possesses the computer system make a decision on what software would be permitted to run (" Weighing the pros and cons of the Trusted Computing Platform," n. d.). Another concern is that client action in these circumstances might be recorded in a proprietary database without the knowledge of the user. In this case, user privacy happens to be an issue as well as forming a security acquiescence conflict.

Designs that exist are essentially damaged since they expose the public to new dangers of anti-consumer as well as anti-competitive behavior. Although the hardware is employed as per published specifications, it can still be utilized in a manner that harms computer possessors. Second, makers of certain trusted computers as well as components may surreptitiously implement them wrongly (" Weighing the pros and cons of the Trusted

Computing Platform," n. d.).

Hardware enrichments may be one technique to develop computer safety (" Trusted Computing: Promise and Risk | Electronic Frontier Foundation," n. d.). Treating computer holders as enemies is not growth in computer security. The owner control, interoperability and competition as well as similar issues intrinsic to the NCSCB and TCG approach are very serious that we advocate against embracing these trusted computing technologies up to the time these issues have been tackled.

References

Weighing the pros and cons of the Trusted Computing Platform. n. d.. Retrieved from http://searchdatacenter. techtarget. com/tip/Weighing-the-pros-and-cons-of-the-Trusted-Computing-Platform

Trusted Computing: Promise and Risk | Electronic Frontier Foundation. n. d.. Retrieved from https://www. eff. org/wp/trusted-computing-promise-and-risk