

ABSTRACT

Secure Keyboard is created to prevent or guard against one of the modern crimes especially for keylogger attacks. The current prevention or countering solution for keylogger attack is already exist and it's called anti-keylogger, but this solution is not really effective to prevent all different types of keylogger because the evolving technique of keylogger starting from software, hardware and even into kernel level. This problem makes any normal input device that intentionally used for normal use such as password input or any critical user data become vulnerable and can be used for criminal activity.

This thesis contains about secure keyboard design and implementation using Teensy Development Board emulated as a computer keyboard. Data transfer between the emulated keyboard and the computer is encrypted using AES encryption algorithm. The result of this implementation then tested against security vulnerabilities and user performance while protecting both system from keylogger attacks.

The result of this research concludes that AES algorithm can be implemented on keyboard used to type as input in the system using microservice. During testing, keyboard command cannot be detected by keylogger but this came with the cost of reduced functionality of the keyboard such as inability to send more than one command at a time. The encryption system works well with decryption performance under 1 ms, typing delay under 100 ms and affalanche effect averaging around 50.03 %.

Keyword: *Encrypted Keyboard, Encryption, AES Encryption, Keylogger.*