A Multi-threading approach to Secure VERIFYPIN

Ibraheem Frieslaar
Barry Irwin

Abstract:
This research investigates the use of a multi-threaded framework as a software countermeasure mechanism to prevent attacks on the verifypin process in a pin-acceptance program. The implementation comprises of using various mathematical operations alongside a pin-acceptance program in a multi-threaded environment. These threads are inserted randomly on each execution of the program to create confusion for the attacker. Moreover, the research proposes a more improved version of the pin-acceptance program by segmenting the pro-gram. The conventional approach is to check each character one at a time. This research takes the verifying process and separates each character check into its individual thread. Furthermore, the order of each verified thread is randomised. This further assists in the obfuscation of the process where the system checks for a correct character. Finally, the research demonstrates it is able to be more secure than the conventional countermeasures of random time delays and insertion of dummy code.