In this research, I describe a semi-automatic, rapid keystroke injection USB device: The Rubber Ducky. This project demonstrates the amount of damage possible – though limited to a Windows virtual machine – by sending commands at up to 1000 words per minute [1]. Of concern is, unlike other USB delivery methods [2], the Ducky circumnavigates traditional antivirus software and other securities by appearing to the computer as a keyboard typing. Damage implications carry to medical devices [3] and voting machines [4], with their typically easily accessible, fully functional, and input-accepting USB ports.

A successful attack is measured primarily by amount of content affected (passwords, banking information), but may include how stealthily it was carried out (hidden command execution, shorter times) and how much evidence was removed (registry artifact deletion). As shown in this project, regardless of whether by social engineering, the morbid curiosity of users, or an attacker having mere seconds undisturbed with the computer – by allowing the Ducky to run, the game is lost. Trade secrets are forfeit; files, held ransom. The attacker may even install a backdoor and carry on undetected – for years – as an Advance Persistent Threat [5].