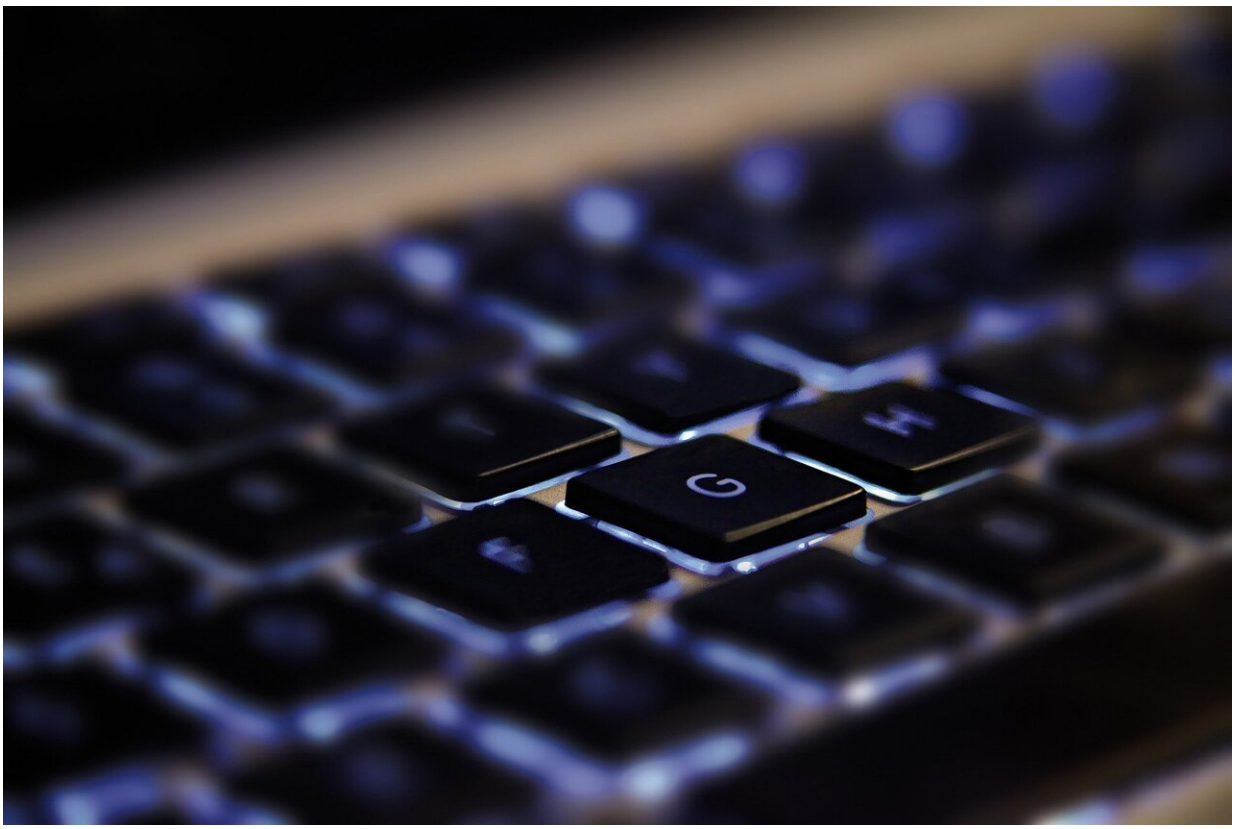
New computer attack mimics user's keystroke characteristics and evades detection

June 6 2019



Credit: CC0 Public Domain

Ben-Gurion University of the Negev (BGU) cyber security researchers have developed a new attack called Malboard. Malboard evades several

detection products that are intended to continuously verify the user's identity based on personalized keystroke characteristics.

The new paper, "Malboard: A Novel User Keystroke Impersonation Attack and Trusted Detection Framework Based on Side-Channel Analysis," published in the *Computer and Security* journal, reveals a sophisticated attack in which a compromised USB keyboard automatically generates and sends malicious keystrokes that mimic the attacked user's behavioral characteristics.

Keystrokes generated maliciously do not typically match human typing and can easily be detected. Using artificial intelligence, however, the Malboard attack autonomously generates commands in the user's style, injects the keystrokes as malicious software into the keyboard and evades detection. The keyboards used in the research were products by Microsoft, Lenovo and Dell.

"In the study, 30 people performed three different keystroke tests against three existing detection mechanisms including KeyTrac, TypingDNA and DuckHunt. Our attack evaded detection in 83 percent to 100 percent of the cases," says Dr. Nir Nissim, head of the David and Janet Polak Family Malware Lab at Cyber@BGU, and a member of the BGU Department of Industrial Engineering and Management. "Malboard was effective in two scenarios: by a remote attacker using wireless communication to communicate, and by an inside attacker or employee who physically operates and uses Malboard."

New Detection Modules Proposed

Both the attack and detection mechanisms were developed as part of the master's thesis of Nitzan Farhi, a BGU student and member of the USBEAT project at BGU's Malware Lab.

"Our proposed detection modules are trusted and secured, based on information that can be measured from side-channel resources, in addition to data transmission," Farhi says. "These include (1) the keyboard's power consumption; (2) the keystrokes' sound; and (3) the user's behavior associated with his or her ability to respond to typographical errors."

Dr. Nissim adds, "Each of the proposed detection modules is capable of detecting the Malboard attack in 100 percent of the cases, with no misses and no false positives. Using them together as an ensemble detection framework will assure that an organization is immune to the Malboard attack as well as other keystroke attacks."

The researchers propose using this detection framework for every keyboard when it is initially purchased and daily at the outset, since sophisticated malicious keyboards can delay their malicious activity for a later time period. Many new attacks can detect the presence of security mechanisms and thus manage to evade or disable them.

The BGU researchers plan to expand work on other popular USB devices, including computer mouse user movements, clicks and duration of use. They also plan to enhance the typo insertion detection module and combine it with other existing keystroke dynamic mechanisms for user authentication since this behavior is difficult to replicate.

More information: Nitzan Farhi et al, Malboard: A novel user keystroke impersonation attack and trusted detection framework based on side-channel analysis, *Computers & Security* (2019). DOI: 10.1016/j.cose.2019.05.008

Provided by American Associates, Ben-Gurion University of the Negev