# Password managers vulnerable to insider hacking

August 15 2018


Credit: George Hodan/Public Domain

A new study shows that communication channels between different parts and pieces of computer software are prone to security breaches. Anyone with access to a shared computer – co-workers, family members, or guests – can attack or involuntarily subject it to security breaches.

Researchers from Aalto University and the University of Helsinki have

found over ten computer security-critical applications that are vulnerable to insider attacks. Most of the vulnerabilities were found in password managers used by millions of people to store their login credentials. Several other applications were found to be similarly susceptible to attacks and breaches across the Windows, macOS and Linux operating systems.

Computer software often starts multiple processes to perform different tasks. For example, a password manager typically has two parts: a password vault and an extension to an internet browser, which both run as separate processes on the same computer.

To exchange data, these processes use a mechanism called inter-process communication (IPC), which remains within the confines of the computer and does not send information to an outside network. For this reason, IPC has traditionally been considered secure. However, the software needs to protect its internal communication from other processes running on the same computer. Otherwise, malicious processes started by other users could access the data in the IPC communication channel.

"Many security-critical applications, including several password managers, do not properly protect the IPC channel. This means that other users' processes running on a shared computer may access the communication channel and potentially steal users' credentials," explains Thanh Bui, a doctoral candidate at Aalto University.

While PCs are often thought to be personal, it is not uncommon that several people have access to the same machine. Large companies typically have a centralized identity and access management system that allows employees to log into any company computer. In these scenarios, it is possible for anyone in the company to launch attacks. An attacker can also log in to the computer as a guest or connect remotely, if these

features are enabled.

"The number of vulnerable applications shows that software developers often overlook the security problems related to inter-process communication. Developers may not understand the security properties of different IPC methods, or they place too much trust in software and applications that run locally. Both explanations are worrisome," says Markku Antikainen, a post-doctoral researcher at the University of Helsinki.

Following responsible disclosure, the researchers have reported the detected vulnerabilities to the respective vendors, which have taken steps to prevent the attacks. The research was done partly in co-operation with F-Secure, a Finnish cyber-security company.

**More information:** Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer: www.usenix.org/conference/usen … y18/presentation/bui

Provided by Aalto University