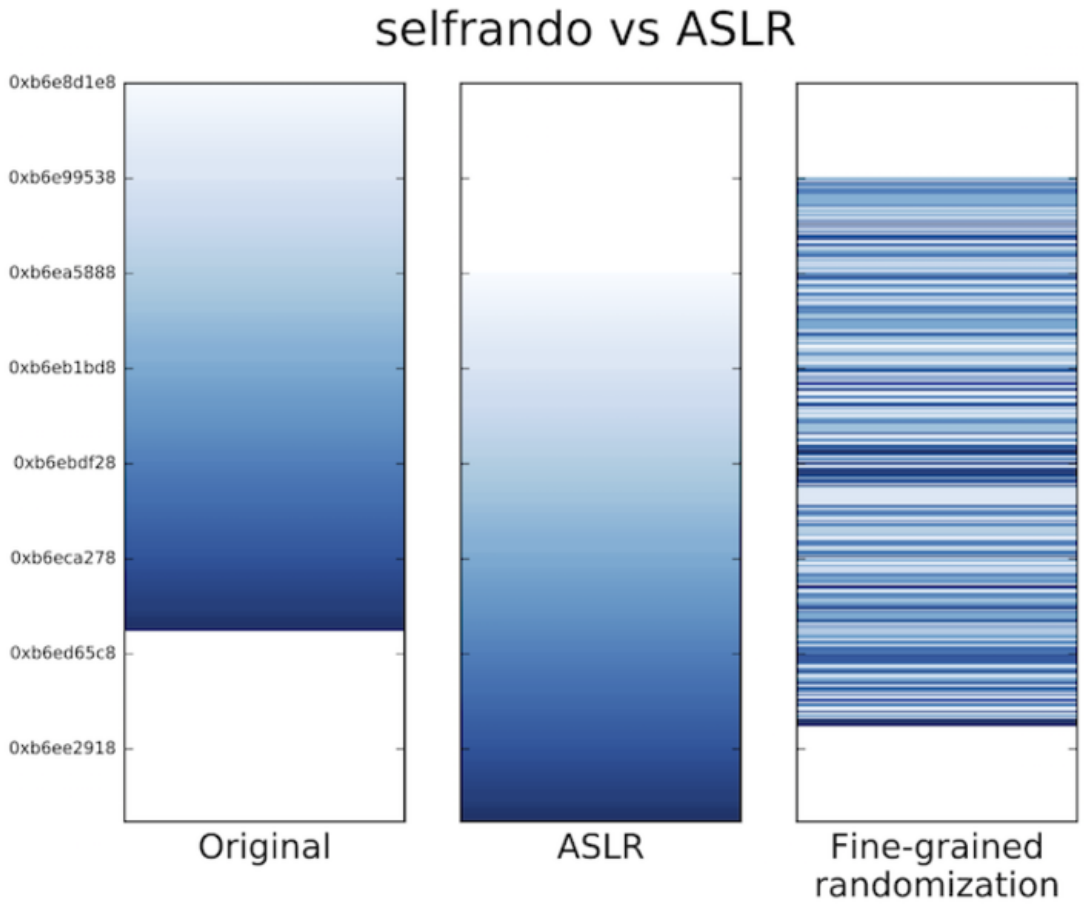
Software engineers create new defense to protect Tor users

June 24 2016



Common ASLR moves the whole code of the application as a single block to a different region of memory. Selfrando randomly rearranges the code in a fine-grained fashion every time the application is launched. Credit: Technische Universitat Darmstadt

Researchers from TU Darmstadt developed successfully in collaboration with the University of California Irvine a new protection for Tor users. "Selfrando" strengthens the Tor Browser against attempts to hack and de-anonymize Tor users.

CYSEC researchers Tommaso Frassetto, Christopher Liebchen and Ahmad-Reza Sadeghi have collaborated with Immunant, Inc., University of California Irvine, and the Tor Project to integrate new software security research into the hardened version of the Tor Browser. Their defense, called "selfrando," strengthens the Tor Browser against attempts to hack and de-anonymize Tor users.

Tor users, such as activists, journalists, and whistleblowers, use the Tor Browser to preserve their anonymity online. Obviously the Tor Browser is an enticing target for hackers, including nation-states, attempting to de-anonymize and track Tor users. In the hardened Tor Browser series, the Tor Project is testing new defenses to proactively protect Tor users from attacks on their browser.

Randomizing the internals of the software

The most powerful attacks against browsers such as the Tor Browser aim to remotely exploit a victim using state-of-the-art techniques known as "code reuse". Essentially, an attacker pieces together bits of the target program into malware that controls the victim's computer meaning that the attacker does not need to inject code to the victim's machine at first place.

Selfrando defends modern software against this class of exploits by randomizing the internals of the software. Without knowing these randomized details, an attacker has a much harder time constructing a reliable (code-reuse) attack.

Selfrando significantly increases security without sacrificing performance or compatibility. It does not require changes to software build tools or processes and adds less than 1% performance overhead. In practice, selfrando is completely unnoticeable to users while significantly increasing security.

More information: Advance copy of the research paper is available online: people.torproject.org/~gk/misc … ando-Tor-Browser.pdf

Selfrando is available for use in other open-source projects at GitHub: github.com/immunant/selfrando

Provided by Technische Universitat Darmstadt