

With Boxmate malicious programs have no place left to hide

9 March 2016



Konrad Jamrozik, Andreas Zeller and Philipp von Styp-Rekowsky are protecting smartphones and more. With Boxmate malicious programs have no place left to hide. Credit: Oliver Dietze

No matter how well-tested our software may be, hackers keep on finding vulnerabilities to exploit or control systems at will. "The attackers are always one step ahead," says Andreas Zeller, professor of computer science at Saarland University and researcher at the Center for IT Security, Privacy and Accountability (CISPA). "The core problem of existing security systems is that the attack needs to have been observed at least once to be able to recognize it the next time - and then, you have to update everything again and again." This threat is particularly prominent in the upcoming "Internet of Things", where hundreds and thousands of devices can become potential targets.

A new approach called "Boxmate" is now set to prevent other programs from surreptitiously changing their behavior, as this would be part of or a result of a hidden attack, or a backdoor exploit. Developed by Zeller together with graduate students Konrad Jamrozik and Philipp von Styp-Rekowsky, Boxmate systematically generates

program inputs in order to investigate the program's regular behavior. "During this automatic testing, we log which critical data - say locations or contacts - and which critical resources - microphone or Internet access - the program is accessing to perform these tasks," Zeller explains, "and the test generator ensures that all visible features actually are exercised."

During production, the program then gets placed into a "sandbox," an automated watchdog which oversees the operation of the program in question - and which raises an alarm whenever some data is being accessed that was not already accessed during testing. If the program is compromised or exhibits previously unseen malicious behavior, the sandbox will catch and prevent the attack.

The nicest feature of Boxmate, says Zeller, "is that malicious programs no longer have a place to hide." Indeed, if a program wants to use certain kinds of data later on, it will already have to access it while being tested by Boxmate - and thereby expose what it is doing. "Any hidden functionality will be disabled by the sandbox," says Zeller, "and this will make it hard for attackers".

But wouldn't the sandbox also raise alarms during normal usage? "Our test generator explores behavior so well that during regular usage, we normally have no alarms at all," says Zeller, who has already tested Boxmate on more than a hundred different apps with his team. Modern mobile systems request authorizations for every access to sensitive data like the camera, contacts, and the microphone. "With Boxmate, we already know from testing that these are being used, and how," says Zeller.

The current implementation of Boxmate protects apps on Android smartphones. However, the concept can equally be applied on the desktop, servers, or embedded systems, and it requires no changes to existing programs. Zeller has already

applied for a worldwide patent for the technology underlying Boxmate, so licensing is already possible. To permanently establish Boxmate as a comprehensive security tool for industry and commerce, Zeller's research group has now joined forces with industry partner Backes SRT. This Saarland University spin-off has developed, for instance, the "SRT AppGuard" app, a security [program](#) available as a free app and already downloaded more than one million times. "Boxify," the extended, commercial version of AppGuard, works together with Boxmate and will also be presented at Cebit.

Zeller financed the research on Boxmate with funds from an ERC Advanced Grant. He had received the highest award of the ERC in 2011, with his proposal for "SPECMATE - Specification Mining and Testing".

Computer scientists from the Center for IT Security, Privacy and Accountability (CISPA) at Saarland University will present their method for the first time at the Cebit computer fair in Hannover between March 14 and 18 (Hall 6, Stand D 28).

More information: www.boxmate.org/

Provided by Saarland University

APA citation: With Boxmate malicious programs have no place left to hide (2016, March 9) retrieved 25 January 2021 from <https://phys.org/news/2016-03-boxmate-malicious-left.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.