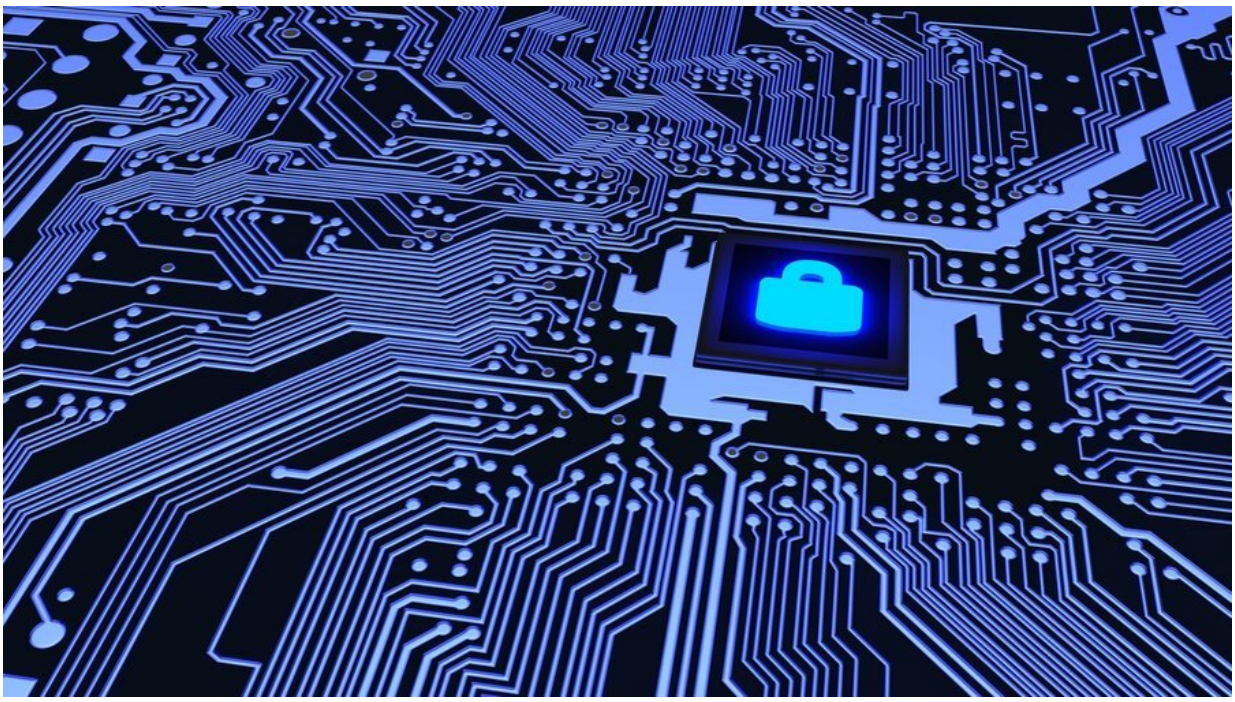
New technology allows software components to be isolated from each other with little computation

September 4 2019



Combining a hardware feature processors from the semiconductor firm of Intel with a software method, researchers at the Max Planck Institute for Software Systems in Kaiserslautern and Saarbrücken have come up with a new technology called ERIM to isolate software components from each other. In this way, for example, credit card data or passwords can be protected from hackers when they processed by online services. Credit: 123RF

Safeguarding passwords, credit card numbers or cryptographic keys in computer programs will require less computational work in the future. Researchers at the Max Planck Institute for Software Systems in Kaiserslautern and Saarbrücken have come up with a new technology called ERIM to isolate software components from each other. This allows sensitive data to be protected from hackers when the data is processed by online services, for example. The new method has three to five times less computational overhead than the previous best isolation technology, making it more practical for online services to use the technology. This was reason enough for USENIX, a US-American computing systems association, and Facebook to award their 2019 Internet Defense Prize to the researchers.

Computer programs are like a fortress. Just as a fortress is protected by thick walls, moats and iron gates, firewalls and other security technologies prevent cyber criminals from maliciously exploiting software apps. And just as one poorly guarded gate or a supposedly secret escape tunnel may allow besiegers to capture a castle, all hackers need is a small security gap to gain access to all components of a software. In the worst case, they can then get their hands on the data that grants them access to user accounts or even allow them to make credit card payments. For example, the Heartbleed bug in the widely used OpenSSL encryption software made user names and passwords of various online services and programs vulnerable to hackers.

Software components should be isolated like fortresses

In order to prevent such fatal attacks, software developers can proceed in a similar way to the master builders of cleverly devised fortresses. They can isolate various software components from each other, just as several walls barr direct access to the heart of a fortress to any assailants who

manage to overcome the outer ramparts.

But obviously, the better the protection, the more work this involves: castles need more construction materials and guards, and for a software this means more computing time. In fact, current isolation techniques for computer programs require up to 30 percent more CPU power, and a correspondingly higher number of servers have to run by online services, which also increases infrastructure costs proportionally. "A number of services don't believe that this increased cost is justified and thus use no isolation techniques," says Deepak Garg, a leading scientist at the Max Planck Institute for Software Systems. "Our isolation technology uses only five percent more computing time, making it very attractive for companies." So it comes as no surprise that the researchers have been awarded the 100,000 US dollar 2019 Internet Defense Prize, with which USENIX and Facebook honor outstanding developments in the field of Internet security.

Memory can be divided up with relatively little effort

A team headed by Deepak Garg and Peter Druschel, Director at the Max Planck Institute for Software Systems, ingeniously combined a hardware feature recently introduced in processors produced by the semiconductor firm Intel with a software-technique to build this isolation technology.-. The new hardware feature is known as Memory Protection Keys, or MPK for short, amongst experts.

However, MPK alone cannot reliably isolate components as it is still open to attack from resourceful hackers. The Max Planck researchers use this method together with another technique called instruction rewriting. "A software's code can be rewritten in such a way that an attacker is no longer able to get around the 'walls' between software components," says Peter Druschel. "However, this does not alter the code's actual purpose." These two methods can be used together to

divide the memory of a software app with relatively little computational work and then isolate these parts from each other. Other isolation technologies access the operating system's kernel for this purpose, which entails a greater computational effort. "Software developers are in a permanent race against time and cyber criminals," says Peter Druschel. "But data protection still has to be practical. This sometimes calls for systematic but unconventional approaches, like the one we pursued with ERIM."

Provided by Max Planck Society

Citation: New technology allows software components to be isolated from each other with little computation (2019, September 4) retrieved 17 April 2024 from https://techxplore.com/news/2019-09-technology-software-components-isolated.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.