Platform would protect smartphones from cyber criminals

March 6 2014

Criminals don't have to pick your pocket to get what they want out of your mobile. But a certifiably secure operating platform is being developed by Swedish researchers so that consumers can be confident that their mobile data is safe.

Market analysts expect the next decade to see a significant expansion in the numbers of connected devices and machines.

But increased connectivity also presents an opportunity for criminals. Mads Dam, an expert in computer security at Stockholm's KTH Royal Institute of Technology, says that devices and modules will be exposed to increasingly sophisticated attacks by cyber criminals.

"People are going to place even higher value on products with verifiable security claims," says Dam, who is Professor of Teleinformatics at KTH's School of Computer Science and Communication.

While compact in size, mobile phones pose a huge security challenge, Dam says. "Android, for example, has more than 10 million lines of code and is executing on a computing platform with one billion transistors.

"So it's not surprising that securing this kind of system is difficult," Dam says. "The good news is that an end-to-end security guarantee is within reach."

Dam and his colleagues aim to publish a certifiably secure, trusted execution platform for operating systems. The idea is to outwit malware and other attacks on a device with a layer of software called a "hypervisor", which is designed to secure the interaction between the operating system (OS) and the hardware.

"If the operating system asks for the camera to be turned on, the hypervisor can step in and verify whether that is really what the user wants," he says. "Or if the operating system wants to access a piece of memory that normally should be regarded as secure, it could step in and allow, or disallow, the request."

In fact, Dam says, a hypervisor-based solution could completely isolate different apps from each other, to create truly tamper-proof applications, for instance for banking or communication.

Such a platform could be made much smaller than the OS itself, he says. "We're talking about a factor of 1,000 to 10,000, which is sufficient to create mathematical models that can analyse the security of interaction between the OS and the hardware so well that we can formally guarantee the security of an operating system like Linux."

And it's not just mobile users that will benefit. In addition to mobile communications networks, the platform would be applicable in a wide range of areas including control systems for manufacturing plants, power stations, utilities and infrastructure. Other uses would be in vehicles, avionics and medical systems, cloud application platforms and also for devices in the internet of things.

The project partners, which include the Swedish Institute of Computer Science (SICS), propose publishing key components of the hypervisor as open source, in order to increase trust and allow de facto industry standardization of the security platform.

Dam says it will require more than a secure execution platform to secure devices from end-to-end, that is, from the user interface through the software stack, down to bits of silicon and back. Hardware and application platforms will have to be validated too. But the KTH team has made great progress during the last decade on tracing security from the application and user interface to the execution platform and back, he says, and the hypervisor will be a vital tool to achieve this.

"Soon we will be able to engage industry and organisations with serious security concerns, like banks, public organisations, defence and providers, and develop this space."

Provided by KTH Royal Institute of Technology