1 Project Description

Mobile Security has become a more and more important issue in recent years as the progress of communication technologies goes faster and the number of smartphone users increases sharply; as a result of these tremendous changes, all smartphones, just like computers in the past, have become preferred targets of attacks. These attacks, exploiting weaknesses related to smartphones, come not only from means of communication like SMS and Wi-Fi networks, but also from software vulnerabilities of both web browsers and operating systems. Operating systems are usually believed to be secure to the user-space applications we use everyday, but they also suffer from security defects just like user-space applications.

In the operating system security area, we now already have some research results coming out as to enforce strong security policies on both user application code and operating system kernel code. Secure Virtual Architecture (SVA) is one of them. SVA [3] is a compiler-based virtual machine placed between software and hardware layers that can be used to protect both the operating system kernel and applications from attacks like memory safety attacks [2] and control flow attacks [1]. However, SVA has just been implemented on Intel x86/x64 platforms. When it comes to ARM, which is the major architecture used for mobile devices running iOS and Android, it is just a blank space. To apply those security policies for hardware-software interaction layer on the ARM platform, we propose porting SVA from Intel
x86 to ARM and conducting security analyses. Our research will also investigate the performance overhead when using SVA on ARM to improve OS security.

2 Intellectual Merit

This research will explore the possibilities of putting SVA in a RISC environment to provide security and will verify the presumed foundation on which future security solutions for both application and operating system can be built. Continued exploration will give researchers insight into further improvements in both SVA and ARM designs.

3 Broader Impacts

The result of this research can be used in reducing security threats and protecting applications from compromised OS kernel when employing mobile devices. Regarding the fact that ARM devices are prevailing all around the globe, this research will definitely help build a better and more secure world. It will also relieve the designers and developers of mobile operating systems and applications from security bug obsession.

4 Research Plan

- Before everything gets started, we must have a sound grasp of how SVA works on x86 and other supported platforms and learn every detail of key points of SVA. We must also well understand the instruction set of ARM, based on which we can describe ARM by SVA hardware abstraction and the porting can be conducted.

- Develop the virtual machine that translates virtual instructions [4] into native ARM instructions.

- Perform security and performance analyses, along with bug fixes and improvements.

This is how the project will be going.
References


