MIST: Systematic Analysis of Microarchitectural Information Leakage on Mobile Platforms

WPI

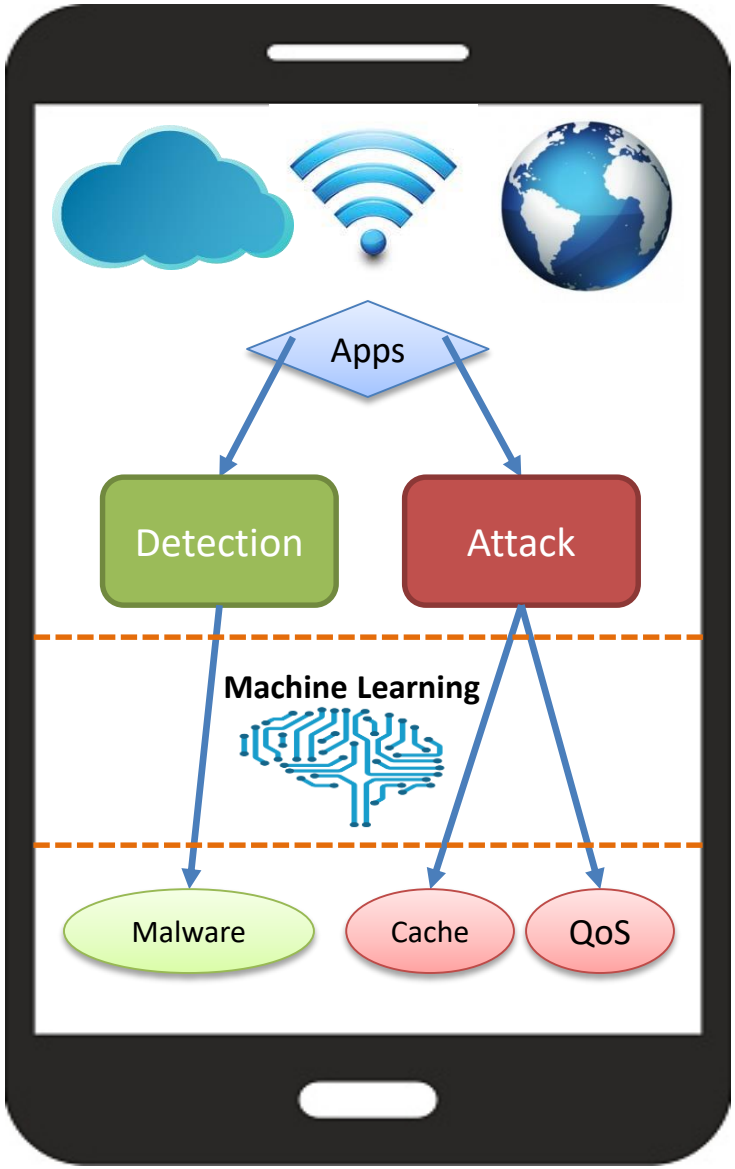
Challenge:

- Huge variety of processors, hardware architectures, system capabilities, Oss,
- Heavy performance and power optimizations for mobile CPUs and Oss,
- Lack of high precision CPU timers such as RDTSC, that are available in x86 systems,
- Lack of detailed documentation and restricted access to the hardware.

Solution:

Systematic Analysis of Microarchitectural Information Leakage on Mobile Platforms by:

- Exposing the vulnerability of mobile platforms via carefully crafted experiments,
- Establishing limits on the information that can be gleamed from such leakage,
- Developing techniques for the detection of leakage exploiting code,
- Detecting attacks in the wild by scanning apps on major app stores,
- Investigating countermeasures to prevent or minimize leakage.



Scientific Impact:

- Explore the interaction between sandboxing techniques, the underlying hardware, and attacks.
- Investigate side-channel leakage sources on mobile systems and the severity of the sandboxing violation.
- Systematically quantify the threat from microarchitectural attacks on real-world mobile platforms.
- Detection of microarchitectural attacks on mobile systems, using machine learning techniques.

Broader Impact:

- Will help secure personal information stored on mobile platforms.
- Improve mobile malware scanners to be able to detect microarchitectural attacks.
- Train the next generation security engineers and scientists.
- Raise awareness and develop solutions for side-channel leakage on mobile platforms.

CNS 1618837: MIST

Berk Sunar (sunar@wpi.edu)
Thomas Eisenbarth (teisenbarth@wpi.edu)
Vernam Lab at Worcester Polytechnic Institute