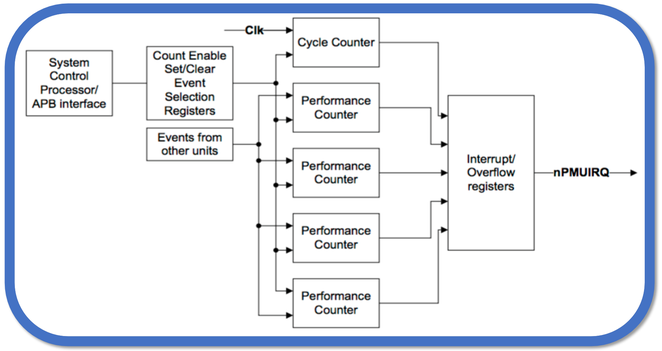
Automated Detection of Hacks

(Online Detection of Code Reuse Attacks)

Yifan Lu and Christopher Hansen

In order for hackers and viruses to compromise a modern computer system, they must first redirect control flow with a "code reuse attack." We created a classifier that can detect when this attack happens, allowing us to alert the system before the attacker gains complete control.

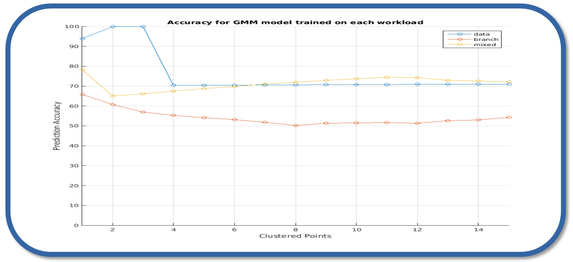


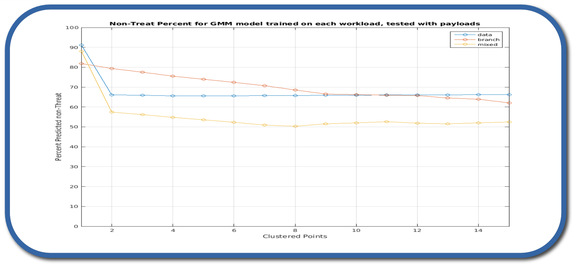
Data Collection

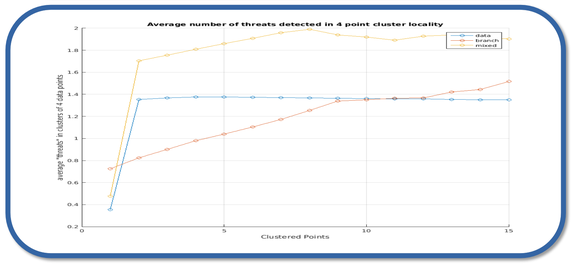
We used the built-in ARM performance monitors (shown to the left) to count architectural events to be used as features. We created a Linux driver that runs on a separate core and queries the monitors of the target core. We also created a workload simulation platform as well as an attack payload generator to train our classifier. The graphs on the bottom shows the event counts on the target core running our simulation without and with an attack.

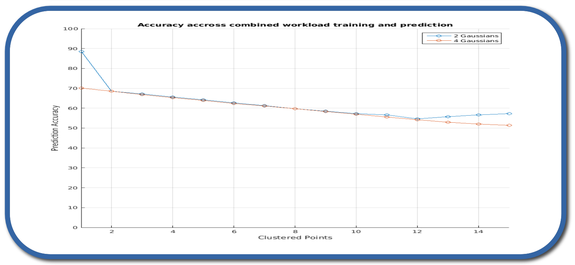
Machine Learning

ML attempts were made first with SVM and the with GMM. GMM was chosen as the primary approach due to its advantages of being fully unsupervised, training faster, not to mention showing better results.

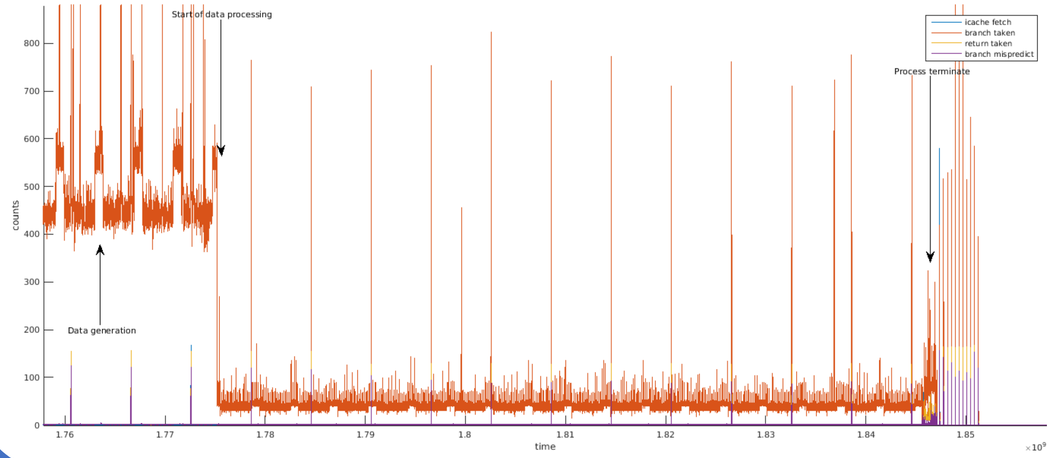








Normal Code Execution



Exploit Triggered in Execution