Network Intrusion Detection in Embedded/IoT devices

Motivation

Networks of sensors and cyber-physical systems are often targets for attacks. It is thus desirable to deploy Network Intrusion Detection Systems in order to monitor the traffic and detect attacks, either at the edge nodes of the network, or at the base station.

Although there are many available tools that can inspect network traffic and detect malicious signatures at high rates, their performance and scalability on embedded devices is not well studied. Providing security countermeasures for such devices is often challenging, due to the severe computation and energy constrains on these platforms. On the other hand, modern IoT hardware offers new features that have not been explored before (e.g. programmable, energy efficient GPUs).

This thesis will address the question of how standard malicious signature detection algorithms perform on these devices and provide new algorithms that make better use of the available hardware resources.

Challenge

This master thesis targets the development pattern matching algorithms that detect malicious signatures on ODROID devices. ODROIDs offer a set of interesting hardware features that introduce new tradeoffs for pattern matching, in terms of processing throughput and energy efficiency. Of particular interest is the graphic co-processor, that can be used to offload general purpose computing tasks (GPGPU) using OpenCL. The challenge is how to design algorithms that make efficient use of both the GPU and the CPU of those embedded devices, to provide faster processing at lower energy cost.

You can conduct this thesis individually or as team of two students. We will adapt the content accordingly. For details and further questions please contact us. Just come over for a coffee and discuss this thesis with us...