Sample Submissions

Sample #1

Session Title
Designing Intelligent Systems using Resource Constrained Edge Devices

Abstract
Traditional embedded software engineers often think that machine learning and intelligent systems are outside the realm of microcontroller based systems and therefore outside their realm of expertise. Advances in microcontroller technology have made designing intelligent systems using these resource constrained devices a reality. In this session, we will examine the tools and capabilities that are available to microcontroller designers to start using machine learning and adding a new level of intelligence to their devices. Developers will walk away understanding that machine learning and AI is not just for big data and the cloud.

Session Detail for Reviewers
We will start with a basic overview of machine learning and what is required to implement learning algorithms such as DSP, hardware floating point accelerators, etc. We will then examine the software libraries and capabilities that are available within the arm ecosystem to create machine learning capabilities. Since we are looking at resource constrained devices such as Cortex-M processors, we'll examine architectures and requirements for training in the cloud and deploying that training onto the resource constrained device. Finally, we will look at several examples and provide guidance on how developers can go further. We will look at examples on how machine learning can be used to monitor system behavior, watch for security threats, detect failing sensors and other potential applications.

This talk will take the viewpoint from a traditional embedded software engineer that now has the ability to use machine learning in their embedded system. I'm going to walk them through the high level machine learning concept, then give them the tools to start thinking how they can start deploying this new technology.

Key Takeaways
- Machine learning can be deployed on Cortex-M processors
- the tools and techniques needed to use Machine learning on a Cortex-M
- Ideas and design patterns that can be used on microcontroller based devices
- Potential applications for edge nodes that can utilize Machine learning

Sample #2

Session Title
IoT and silicon security: dissecting a real-life IoT attack

Abstract
Billions of IoT devices are expected to densely populate our cities, homes, offices and factories. Many of use cases will involve value data and physical proximity – ripe for silicon attacks. IoT attack mitigation has been broadly focused around software counter-measures, however the barrier for physical attacks is increasingly being lowered and silicon security urgently needs protecting. If IoT designers fail to protect all relevant attack vectors, significant data is at risk.

In this talk we will analyze a real-life attack, reviewing the flaws, providing a systematic

approach to security and demonstrating how you can now mitigate against silicon vulnerabilities.

Session Detail for Reviewers

Key Takeaways

1. The outlines of a systematic approach to define the security needs of IoT devices

2. The need to include silicon vulnerabilities in the addressed attack surface even for (relatively cheap) IoT devices

3. Techniques to mitigate different silicon vulnerabilities