**Progress in Mobile Payment Security**

In recent years there has been an enormous progress in mobile app security and secure mobile payment processing due to the ever evolving technology by semiconductor suppliers and their software partners. The process is still evolving, though, and has not been an easy journey.

According to Sy Choudhury, Senior Direct Product Management at Qualcomm Technologies, “Mobile payments is driving so much of the technologies in security today … Hollywood, with its content protection, used to drive security requirements. But now it’s transactions and finance. Banks and traditional credit card processing companies, as well as the new ‘wallets’, are really pushing the security features of our silicon as well as the embedded software.”

The mobile app security of mobile payments is supported by an ecosystem of key players, some of which are well-known while others lesser-known. These include banks, wireless communication carriers, Credit card processors, E-Wallets and other informal payment modes like AliPay, WeChatPay.

Trustonic is providing Trusted Execution Environment (TEE) in about 800 million mobile devices, and Qualcomm believes that this is only the beginning for TEE. According to Choudhury, biometrics data, that includes retina scanning and fingerprints, has encouraged mobile payments to spread in all parts of the world. According to him, three things are considered when designing semiconductor and chipset technology for secure mobile payments on smartphones. Firstly, how to provide mobile app security to the payment app? Secondly, how do you authenticate the user securely? And thirdly, how do you validate the device for its authenticity, and that it is not compromised?

The year 2013 came as a turning point for mobile payment security by enabling host card emulation. With this, banks could put the secure element in the cloud with their own server and communicate with the customers remotely on their phones.

Many of these semiconductor technologies will roll out this year and will be tested to check if they can withstand the highly expert network of hackers. Though no technology can fully counter attacks, yet for the one that needs to progress, it has to increase the breach time for hackers to say the least, and at the same time decrease the value of what they achieve once they succeed in their breaching efforts.