**Mobile Banking Trending as Mobile App Security Strengthens**

According to a report ‘Mobile Banking 2016’ by ING International Survey, use of mobile banking will continue to increase all across Europe with an increasing rate of 16% in the year 2017. The survey shows that mobile banking increased from 41% in 2015 to 47% in 2016. Similarly, according to the Federal Reserve, 67% of millennials in USA, who are the next generation of bank customers, are now using mobile banking. This changing landscape is making it critical for financial institutions to turn their focus towards a strong mobile banking strategy, in order to provide a reliable and efficient banking experience and build customer loyalty.

The Federal Reserve, however, also pointed out that people are hesitant to use mobile banking apps and 73% have concerns regarding the mobile app security. Hence, while the percentage of mobile banking apps continues to rise, banks need to consider mobile app security testing when developing apps to meet these security concerns of their customers.

OWASP has highlighted 10 most common mobile security vulnerabilities to help us understand the security of banking apps during development and mobile app security testing. These top 10 vulnerabilities in their order of importance are; lack of binary protections (19%), insecure data storage (17%), insufficient transport layer protection (16%), unintended data leakage (13%), weak server side controls (6%), poor authorization and authentication (6%), client side injection (4%), broken cryptography (3%), improper session handling (2%) and security decision via untrusted inputs (1%).

Other than the recommendations provided by OWASP, banks need to consider many other key factors to maximize their mobile app security. It all starts with a secure SDLC which protects the app from compromises by defending it in real time. A secure SDLC starts with planning and assessing high-level risks, defining security requirements, and developing a security policy. It then goes on to design, build and test the app by conducing security architecture review, threat modelling, app integrity protection design and mobile app security testing. The app is finally deployed and regular penetration tests and vulnerability assessments are carried out to detect timely vulnerabilities and fix them.

Benefits of mobile banking apps far exceed the risks, yet the risks come with higher impact. It is therefore, critical for banking sector to equip themselves with maximum protection and take help from experienced security professionals.