Segurança em dispositivos de Pagamento Móveis

José Lucio C. Azevedo, Ausberto S. Castro Vera

Com o avanço tecnológico da computação móvel, tornou-se possível várias inovações em métodos já consolidadas no nosso dia a dia, um exemplo é o pagamento. O pagamento móvel tornou-se uma tendência geral no mundo e constitui uma parcela cada vez mais substancial dos pagamentos. Com ele, os pagadores podem realizar um pagamento a qualquer momento e em qualquer lugar. Porém, também traz muitos problemas de segurança consigo, que podem causar grandes perdas, golpes, etc. Nesse contexto, o projeto explica os métodos de segurança utilizados em dispositivos de pagamento online, com o objetivo de informar e mostrar sua importância. As metodologias utilizadas foram pesquisas bibliográficas, o ambiente para teste e desenvolvimento de APIs Postman e a proxy Charles. Há vários métodos e padrões para a segurança do pagamento móvel. Bons exemplos são, a tokenização que protege as informações confidenciais do usuário e reduz a probabilidade de transações fraudulentas, é dividida em tokenização centralizada e distribuída. A segurança de ligação ao PAN (número da conta principal do cartão do banco) que consiste no protocolo de confiança de terceiros e no protocolo anti-vazamento do PAN. A autenticação de pagamento segura que dividimos em pagamento remoto (PIN e identificação biométrica) e pagamento TOTP (One-time Password). Além de padrões que são utilizados na segurança em geral, como a utilização do protocolo HTTPS que faz uso de TLS/SSL para criptografar os dados transmitidos. O trabalho se limita a muita teoria e um parcela mínima de prática e não cita todas as práticas de segurança para o pagamento móvel. O próximo passo é a implementação no Android Studio e o aprofundamento em métodos de segurança não citados, para garantir que nenhum dos aspectos fundamentais da segurança computacional seja quebrado.