Authentication: Choosing a Method That Fits

Miguel Almeida

Independent Security Consultant, Portugal
miguelalmeida@miguelalmeida.pt

Through the last five years, we, in the security field, have been witnessing an increase in the number of attacks to (web) application user's credentials, and the refinement and sophistication these attacks have been gaining. There are currently several methods and mechanisms to increase the strength of the authentication process for web applications. To improve the user authentication process, but also to improve the transaction authentication. As an example, one can think of adding one-time password tokens, or digital certificates, EMV cards, or even SMS one-time codes. However, none of these methods comes for free, nor do they provide perfect security. Also, one must consider usability penalties, mobility constraints, and, of course, the direct costs of the gadgets. Moreover, there's evidence that not all kinds of attacks can be stopped by even the most sophisticated of these methods. So, where do we stand? What should we choose? What kind of gadgets should we use for our business critical app, how much will they increase the costs and reduce the risk, and, last but not least, what kind of attacks we'll be unable to stop anyway? This presentation will focus on ways to figure out how to evaluate the pros and cons of adding these improvements, given the current threats.