Jeremy Hellmer
SE-4930
Article Review 3
January 25, 2012

The Case for Mobile Two-Factor Authentication

While secure authentication is not a new creation, the process of building secure authentication cannot simply be transferred from desktop to mobile devices due to some key differences in the devices. These differences stem from variances in how the devices are used. Two major security vulnerabilities present with mobile devices are device loss and phishing. Because it is more common to lose a mobile device, the situation of a malicious person gaining possession of the device is all too real. The best way to combat this is with the use of disk encryption, protecting the device and its contents even after physical access is gained. Phishing is a big problem with mobile phones because there is no browser, making the web look just as other local applications. This makes it easy for malicious attackers to trick users into typing their authentication information into the wrong location.

Authentication involves two entities: a prover and a verifier. The prover is showing that they are who they say they are by providing authentication information that the verifier will use to verify the identity. In addition to identifying the two ends of communication, the communication messages themselves must be authenticated. It needs to be checked that the message source and destination are correct and that the message was properly sent and not replayed or modified in mid-transaction.

Two-factor authentication requires two distinct identifying proofs. These can include something you have, know, or are. However, something you are such as a fingerprint is not secure because you leave fingerprints on everything you touch so they can be easily copied. In addition, your fingerprint cannot change so if they are copied it is copied for life. Therefore, two-factor authentication should use something you have and something you know.

Offline authentication involves activities such as unlocking the phone. This is automatically two-factor authentication because it requires both the unlock code and physical access to the phone. The code being something you know and the phone being something you have. Online authentication cannot be verified on the device. Therefore, an online server must confirm the identity of the user. Although both provide security benefits, users find it annoying to enter an offline code to unlock the phone followed by an online password. Therefore, offline authentication is often the only authentication being used regularly.

With mobile devices, passwords to online sites can be bypassed. By retrieving codes sent to mobile devices or using QR codes to log into web pages in a browser, two-factor authentication is achieved without passwords or persistent cookies. This is because the user receives the code on the phone which is something they have, the second factor.

Article Information

DeFigueiredo, D.; , "The Case for Mobile Two-Factor Authentication," *Security & Privacy, IEEE* , vol.9, no.5, pp.81-85, Sept.-Oct. 2011

doi: 10.1109/MSP.2011.144

URL: http://ezproxy.msoe.edu:2100/stamp/stamp.jsp?tp=&arnumber=6029364&isnumber=6029351