ABSTRACT
TOWARDS USABLE END-USER AUTHENTICATION

Mohammad Tanviruzzaman
Marquette University, 2014

Authentication is the process of validating the identity of an entity, e.g., a person, a machine, etc.; the entity usually provides a proof of identity in order to be authenticated. When the entity - to be authenticated - is a human, the authentication process is called end-user authentication. Making an end-user authentication usable entails making it easy for a human to obtain, manage, and input the proof of identity in a secure manner.

In machine-to-machine authentication, both ends have comparable memory and computational power to securely carry out the authentication process using cryptographic primitives and protocols. On the contrary, as a human has limited memory and computational power, in end-user authentication, cryptography is of little use. Although password based end-user authentication has many well-known security and usability problems, it is the de facto standard. Almost half a century of research effort has produced a multitude of end-user authentication methods more sophisticated than passwords; yet, none has come close to replacing passwords.

In this dissertation, taking advantage of the built-in sensing capability of smartphones, we propose an end-user authentication framework for smartphones - called ePet - which does not require any active participation from the user most of the times; thus the proposed framework is highly usable. Using data collected from subjects, we validate a part of the authentication framework for the Android platform. For web authentication, in this dissertation we propose a novel password creation interface, which helps a user remember a newly created password with more confidence - by allowing her to perform various memory tasks built upon her new password. Cognitive and muscle memory help the user remember and efficiently input a password. From a within-subject study we show that cognitive memory is sufficient for passwords; muscle memory mostly facilitate the input process and thus the memory tasks have been designed to help cement the cognitive memory of a newly created password. This dissertation concludes with the validation of the increased usability of the proposed interface through a between-subjects study.