Emerging technology space: User Interfaces

REMOTELY DETECTING LIVE PRESENCE OF A SERVER AND A MOBILE DEVICE AND ENABLING TRUSTED IN-BAND COMMUNICATIONS BETWEEN THEM ACROSS A POTENTIALLY NON-TRUSTED CLIENT INTERFACE

David W. Kravitz,
TrustCentral

ABSTRACT

This talk proposes the use of a mobile application that is set up with per- service provider templates and keys that are pairwise unique to the service provider and the user's mobile device, so as to enable secured unidirectional/bidirectional operations. These operations include entity authentication for remote detection of live presence, as well as authenticated and/or encrypted communications. The protocol is based on tunneling of communications between a mobile device and a server through a user-owned or public-access host computer running a potentially untrusted browser. Communications from the host computer's display inbound to the mobile device can be based on 2D barcodes or other optically scannable encodings, while outbound communications from the mobile device display can be addressed using robustly generated/derived short strings that are user-entered into the host computer. The protocol thwarts effective manipulation or forging of online transactions, detects adversarial intervention, increases confidentiality of sensitive transactional data, increases assurance regarding knowledge by the user of the outcomes of pending transactions prior to commitment, and increases assurance regarding session initiation and termination/logout. The protocol enables a more secure replacement for mechanisms that present the user with a relatively static image and/or phrase each time the user initiates login, in that remote workaround requires a successful per-session Man-in-the-Middle attack involving the legitimate server. There is also detection of Man-in-the-Browser active attacks, and of past misappropriation of keying material associated with the user's mobile device. Other than setup and possible refresh of shared secret values or keys, this method does not require the mobile device to be online or connected in any sense.