Preventing Authentication Systems From Keylogging Attack

Sodiya, A. S.[1], Folorunso, O.[2] Komolafe , P. B.[3] and Ogunderu, O. P.[4]

Department Of Computer Science University Of Agriculture,
P. M. B. 2240, Abeokuta, Nigeria. [1,2,3,4]

sinaronke@yahoo.co.uk[1], folorunsolusegun@yahoo.com[2], komopius@yahoo.com[3]
omoniyiogunderu@yahoo.com[4]

ABSTRACT

In this work, a countermeasure scheme known as the "Fool the Keylogger Model (FKM)" was developed for preventing keylogging attacks on Password Authentication Systems. In the FKM, an algorithm called Secured Keystroke Authenticated Password Against Keylogger (SKAPAK algorithm) was developed for dissuading attackers, The model divides the process of user authentication into 3 domains; the User, the Fooled, and the Authentication Domain. The User Domain provides environment for formulation of counterfeit-password. The counterfeit-password is a product of mixture of password characters and random alphanumeric characters or noise characters. This counterfeit-password is then used by the user a non-normal authentication data to login. The Fooled Domain creates an interface for the implementation of SKAPAK algorithm. The algorithm intelligently extracts password token from the counterfeit-password after which it has scaled beyond the visibility scope of the Keylogger. The algorithm then makes a valid authentication request using the normal authentication request data. The final verification and acknowledgement of user's credentials takes place in the Authentication Domain. The results of data analyzed for this research showed over 99.5% concealment of password from Keylogger and over 95% usability and acceptability of the model. The result revealed a complete elimination of shoulder surfing threats, which simply means spying a user login session and showed that the proposed scheme provides adequate protection against keylogging attack.

KEY WORDS

Computer Security, Password, User Authentication, Keylogging Attacks.