Forensic Implication of a Cyber-Enabled Fraud Taking Advantage of an Offline Adversary-in-the-Middle (AiTM) Attack

Publisher: IEEE

D.O. Lawal; D.W. Gresty; D.E. Gan; T.C. Durojaiye

Abstract:

Many computer users utilise the High-Definition Multimedia Interface (HDMI) for connecting external displays as this interface is common on modern computers. This work investigates the feasibility of performing an offline adversary-in-the-middle attack with a portable programmable device such as the Screen Crab which leverages the HDMI interface to covertly capture information being sent to the external display. This work also addresses the possibility of such attacks being carried out as the reconnaissance phase of a wider attack or being carried out as a standalone attack for data exfiltration, data theft, or espionage. Among the operational observations of the Screen Crab, while it was exfiltrating data, include its property of being storage and process efficient. In addition, there were no indicators on the external display (e.g., quality drop, lag/latency) to suggest to the target user that any form of tampering had been done to their machine. This paper also shows how it might be difficult for forensic analysts to detect the use of this device which poses a risk of the target user (victim) being falsely accused or wrongly prosecuted for divulging sensitive or classified information in this kind of situation.

Published in: 2023 46th MIPRO ICT and Electronics Convention (MIPRO)

Date of Conference: 22-26 May 2023

Date Added to IEEE *Xplore*: 29 June 2023

I