Have You Been Framed and Can You Prove It?

Publisher: IEEE

D.O. Lawal; D.W. Gresty; D.E. Gan; L. Hewitt

Abstract:

This work addresses the potential for a frameup attack through the use of a programmable USB e.g., a ‘Rubber Ducky’ to plant false evidence on someone else's computer. The aim is to determine who performed these actions, the human or the Rubber Ducky. Experiments were undertaken where a human interacted with a computer and a Rubber Ducky performed the same actions using identical computers, with identical baseline configurations, to detect differences in the artifacts left behind in each case. Forensics images generated from each experiment were analysed using forensics tools. Our findings pose the question can a programmable USB device be used to masquerade as a human, and can the forensic analyst or legal counsel make informed decisions about the provenance of any artifacts identified, as the expert may not be able to differentiate between the actions of the human user or the programmable USB, which could lead to a miscarriage of justice. This work alerts investigators and experts to the potential presence of a programmable USB device, and presents some artifacts that show that a programmable USB could have carried out these actions, which might prevent an innocent individual being wrongfully convicted of a crime they did not commit.

Published in: 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)

Date of Conference: 27 September 2021 - 01 October 2021

Date Added to IEEE *Xplore*: 15 November 2021

ISBN Information:

Electronic ISSN: 2623-8764