Evaluating the Impact of Juice Filming Charging Attack in Practical Environments

Nowadays, smartphones are widely adopted in people's daily lives. With the increasing capability, phone charging has become a basic requirement and a large number of public charging facilities are under construction for this purpose. However, public charging stations may open a hole for cyber-criminals to launch various attacks, especially charging attacks, to steal phone user’s private information. Juice filming charging (JFC) attack is one such threat, which can refer users’ sensitive information from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the whole charging period. Due to the potential damage of JFC attacks, there is a need to investigate its influence in practical scenarios. Motivated by this, in this work, we firstly conduct a large user survey with over 2500 participants about their awareness and attitude towards charging attacks. We then for the first time investigate the impact of JFC attack under three practical scenarios. Our work aims to complement the state-of-the-art and stimulate more research in this area.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Advanced Digital Sciences Center, Singapore, Singapore, Institute for Infocomm Research, University of Luxembourg, University of Aizu
Contributors: Meng, W., Lee, W., Liu, Z., Su, C., Li, Y.
Pages: 327-338
Publication date: 2018

Host publication information
Title of host publication: Information Security and Cryptology
Publisher: Springer
ISBN (Print): 9783319785554
Keywords: Computer Science, Systems and Data Security, Data Encryption, Artificial Intelligence (incl. Robotics), Smartphone privacy, Android and iOS, Video recording, Charging station, Juice filming charging attack, Practical evaluation
DOIs: 10.1007/978-3-319-78556-1_18
Source: FindIt
Source-ID: 2397567477
Research output: Research - peer-review ▶ Article in proceedings – Annual report year: 2018