Paper Title: Drones’ Cryptanalysis: Smashing Cryptography with a Flicker

Venue: S&P 2019

Link: <https://www.computer.org/csdl/proceedings-article/sp/2019/666000a832/19skg3hM8Qo>

Abstract: The paper tries to the answer the research question of how can we tell whether a passing drone is being used by its operator for a legitimate or illegitimate purpose? Thus  a new method is presented that can detect whether a specific POI (point of interest) is being video streamed by a drone. It is shown that applying a periodic physical stimulus on a target/victim being video streamed by a drone causes a watermark to be added to the encrypted video traffic that is sent from the drone to its operator and that this watermark can be detected using interception.

Contribution: It presents a simple idea as the solution to a relatively complex problem in the field. It implements that idea using known techniques but applying them in new contexts through novel methods.

Evidence: As an evidence, It shows a PoC video and also presents necessary scripts in the appendix section to perform the shown interception.

Impact: The method used in the paper makes vulnerable all the drone manufacturers using WiFi for FPV Transmissions. It also presents some countermeasures, the most effective of which is eliminating video compression completely.

Citations: 4

Paper Title: Demystifying Hidden Privacy Settings in Mobile Apps

Venue: S&P 2019

Link:<https://www.computer.org/csdl/proceedings-article/sp/2019/666000a850/19skg3Y4ne0>

Abstract: The paper tries to evaluate the landscape of the privacy settings in Mobile Apps. These settings, however, are often hard to locate and hard to understand by the users, even in popular apps, such as Facebook. More seriously, they are often set to share user data by default, exposing her privacy without proper consent. This paper, reports the first systematic study on the problem, which is made possible through an in-depth analysis of user perception of the privacy settings. More specifically, two user studies are conducted(involving nearly one thousand users) to understand privacy settings from the user’s perspective, and identify these hard-to-find settings.Then 14 features are selected that uniquely characterize such hidden privacy settings and utilize a novel technique called semantics-based UI tracing to extract them from a given app.

Contribution: The paper provides the first systematic study of the landscape of privacy settings in mobile apps and it also provides suggestions for landscape to develop apps with a more privacy-focused design.

Evidence: It shows a tool called Hound that can recover privacy settings and identify problematic ones with an accuracy 93.54%. Also a few helpful suggestions are also provided to developers for future design.

Impact: It was observed that the problem of hidden privacy settings becomes more serious from the year 2017 to 2018, possibly due to the fundamental causes of privacy settings’ problematic designs.

Citations: 1

Paper Title: is your vote overheard? A new scaleable side-channel attack against paper voting.

Venue: Euro S&P 2019

Link:<https://www.researchgate.net/publication/333894647_Is_Your_Vote_Overheard_A_New_Scalable_Side-Channel_Attack_Against_Paper_Voting>

Abstract: The paper presents a novel side-channel attack against the physical environment of traditional paper-based elections. More precisely, the paper presents a device based on an Arduino development board and cheap electret microphones, capable of triangulating the locations of marks made on wooden tables with high precision. This will allow breaching privacy of ballot sheet designs that rely on the voter marking her choice(s)between a potentially high number of candidates printed on one large sheet. The attack is further complemented with a study on various aspects of deployment of facial recognition. This gives rise to the setup where the attacker installs cameras in the polling stations, aiming at automated detection of people leaving the voting booths. Combining the two approaches, a completely automated attack against the privacy of paper-based voting can be executed.

Contribution: The major contribution is the side-channel attack presented in the form of the Arduino platform and countermeasures to protect against the aforementioned attack.

Evidence: The average accuracy of detecting the correct 4×5 cm cell on the board reached over 90% in the best setup. The cost of the device is also relatively low at 20-30$ per device.

Impact: Assuming that the attacker will be able to deploy several installations of the devices, this gives rise to a privacy breach of much larger extent than at homes in case of remote Internet voting (at least for a mid-level attacker,unable of creating and distributing custom malware).

Citations: 1