DATX11-23-25

Security risk analysis of a vehicle or IOT device

Background:

Software impregnates more and more of our lives. From being something restricted to usage on expensive devices larger than a room, software now can run on devices cheaper than 1 krona and permeates society.

Nowadays, software based devices are involved in many areas, like the mixing of fuel and air in a car, keeping the electrical grid running or the allowing remote access and control of IoT devices like light bulbs, baby monitors, security cameras or fridges.

As software based devices become more prevalent and more features are added to them so do the risk arising from any bugs the software may contain.

For example, modern vehicles usually include complex infotainment systems which have access to health data produced by the vehicle's control systems. Similarly these vehicles delegate more and more control functionality (like brakes or steering) to software controlled devices. This could be fatal as an attacker could abuse a flaw in the complex infotainment system to gain control of the vehicle.

Other similar abuses of vulnerabilities in software can be seen on baby monitors being exploited to harass others or the DoS attacks performed by the Mirai network.

Project description:

This project will be made in six steps.

During the first week, students will research about ethics and full and responsible disclosure to ensure that they handle any finding arising from the project correctly.

As a second step, students will gather broader knowledge on the field of IT security and in particular in penetration testing with the objective of learning about the current testing techniques and tools used in the field. The objective of this step is for the students to have a good ground knowledge to be able to execute tests and to be able to explain the implications of any exploits they find.

On the third step, a testing target will be agreed upon (we aim at allowing the students to test the security of a modern vehicle but since this will depend on the vehicle manufacturer's willingness, we may have to fall back to instead testing the security of a commercially available IoT device). In this step we will also sign any legal agreements needed to be able to perform the tests (the car manufacturer will likely require signing an NDA to avoid disclosure of specific findings).

Once the testing target is decided, students will focus their research on the specifics of how to analyze the security for the specific product. This will involve learning about any communication protocols involved, how risks affect similar products and how such products are made and programmed.

The fifth step will be the actual testing of the targeted product for security vulnerabilities using the acquired knowledge.

Finally, on the sixth step the students will report any findings to the manufacturers of the product and write a report showing the knowledge they have acquired.

IMPORTANT: Notice that it is still unclear whether this project will be able to test a vehicle or a IoT product bought by the team using their budget. This will be unclear until at least January. Nevertheless the project will involve doing a security audit of a software based device.

Suggested reading (and watching) material:
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/
https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Target group: D, DV, IT, E and Z

Special prerequisites: Prior knowledge on programming, electronics, computer security basics (EDA263 can be taken along this project) and embedded systems are all strongly recommended.

Note to the organization team: I can only take one group for this thesis. If more than six students are interested in this specific project maybe we can get them to write a short motivation letter and choose the 6 most motivated ones.

Proposal author: Francisco Blas Izquierdo Riera