https://www.online.muni.cz/en/science/9906-it-experts-discover-a-vulnerability-in-chips

IT experts from Muni discover a vulnerability in chips

Science

14 November 2017

Martina Fojtů, eng Jana Doleželová

Foto: Martin Kopáček / CC-BY

Research group leader Petr Švenda from Faculty of Informatics Masaryk University.

The faulty chips are used in the ID cards of some countries. While the Czech Republic is not affected, Estonia, Spain, and Slovakia use them in their ID cards and are now addressing this problem.

IT experts from Masaryk University have discovered a vulnerability in a very sensitive subject. While examining chips used as a protection measure in highly sensitive equipment and documents, they discovered that the products from one specific company fall far short of the promised level of security.

The members of the Centre for Research on Cryptography and Security discovered the fault by chance when examining the cryptographic keys generated by a large number of various chip libraries to study their properties. “And this is how we found the problem in the method used to generate keys in chips produced by Infineon Technologies, a German company. By using the public part of the code, it is possible to obtain the secret part much faster than should be possible,” explains the research group leader Petr Švenda from Faculty of Informatics.

The experts found the fault in the chips produced by one of the three largest global producers of these devices, and following the usual practice in the field, they first contacted the producer so that the company could remove the fault. However, the situation was further complicated by the fact that the fault first appeared at least ten years ago and runs throughout the entire product series.

“It is present in a software library that generates keys and that the company uses in many of its products. This is because they have this specific library certified and obtaining certification is expensive,” says Švenda to explain why the impact is so huge. As they agreed with the company, the experts only published their findings after a delay of several months along with a tool for detecting the fault.

The faulty chips are also used in the ID cards of some countries. While the Czech Republic is not affected, as Czech cards use chips from a different producer, Estonia, Spain, and Slovakia all use the faulty chips in their ID cards and are now addressing this problem. The fault was removed from the producer’s new products and technology companies have already released the necessary software updates.

However, some things still need to be resolved. According to the Czech News Agency, Slovakia decided to publish new advanced electronic signatures for ID card chips as a result of the fault. In the first phase, the new version will be available upon request to those users who have already used their signatures. In the coming weeks, authorities are planning to remotely upload the safer version to users who have not yet used their electronic signatures.