Dr. S.P. Picek (TUD), DISTANT

English scientific summary

Today, embedded devices such as banking/transportation cards, car keys, and mobile phones use cryptographic techniques to protect personal information and communication. Such devices are increasingly becoming the targets of attacks trying to capture the underlying secret information, e.g., cryptographic keys. Attacks not targeting the cryptographic algorithm but its implementation are especially devastating and the best-known examples are so-called side-channel and fault injection attacks. Such attacks, often jointly coined as physical (implementation) attacks, are difficult to preclude and if the key (or other data) is recovered the device is useless.

To mitigate such attacks, security evaluators use the same techniques as attackers and look for possible weaknesses in order to "fix" them before deployment. Unfortunately, the attackers' resourcefulness on the one hand and usually a short amount of time the security evaluators have (and human errors factor) on the other hand, makes this not a fair race.

Consequently, researchers are looking into possible ways of making security evaluations more reliable and faster. To that end, machine learning techniques showed to be a viable candidate although the challenge is far from solved. Our project aims at the development of automatic frameworks able to assess various potential side-channel and fault injection threats coming from diverse sources. Such systems will enable security evaluators, and above all companies producing chips for security applications, an option to find the potential weaknesses early and to assess the trade-off between making the product more secure versus making the product more implementation-friendly. To this end, we plan to use machine learning techniques coupled with novel techniques not explored before for side-channel and fault analysis. In addition, we will design new techniques specially tailored to improve the performance of this evaluation process. Our research fills the gap between what is known in academia on physical attacks and what is needed in the industry to prevent such attacks. In the end, once our frameworks become operational, they could be also a useful tool for mitigating other types of threats like ransomware or rootkits.

English public summary

Small devices like transportation and bank cards are typical targets for adversaries looking into creative ways to break them, often using various side channels. This proposal will consider machine learning algorithms in order to assess the strengths of such adversaries and to protect our devices and data.

Dutch public summary

Chipkaarten zoals transport- of bankkaarten zijn gewilde doelwitten voor aanvallers die hiervoor vaak gebruik maken van zijkanalen. Dit voorstel zal de kracht van zulke aanvallers in schatten met behulp van machine learning algoritmen teneinde deze toestellen, en onze data in het algemeen, te beschermen met de gepaste tegenmaatregelen.