A better poker face for computers

Spectacular security loopholes discovered in modern processors are setting new challenges for scientists: Computer Science Professor Heiko Mantel and his team are studying the danger of difficult to detect attacks via so-called side channels and possible countermeasures.

Photography: Katrin Binner

Alexandra Weber, Dr. Damien Marion and Professor Heiko Mantel (from left to right) are performing a side-channel analysis.

By Ann-Kathrin Braun

"A bad poker face can also be viewed as a side channel", says Professor Heiko Mantel to explain his research on "side channels". In a game of cards, your facial expressions and your body behaviour might reveal to other players a lot about the quality of your cards. Similarly, side-channel attacks in IT-systems leak secret information via channels that were not meant to be used for such communication.

The security of confidential data does not only depend on security mechanisms such as cryptography or access controls. It also depends on restricting the flow of information, meaning where and how information is propagated when running a program. Information-flow control does not exclude access to confidential information, but rather limits how it can be used. Heiko Mantel has been investigating the theme of information-flow security since being a doctoral candidate and on his path to becoming a professor in Computer Science. This theme was the main focus of the Priority Programme "Reliably Secure Software Systems" that he headed, and that was funded by the German Research Foundation (DFG). His work in the CROSSING Collaborative Research Centre at TU Darmstadt builds on this prior work.

The complexity of IT systems has increased considerably over time due to rapid advances in technology. "A major achievement of Computer Science is the ability to think about systems using abstractions. Differentiating between layers of abstraction makes the conceptual complexity of such systems tractable", says Mantel. Thinking in terms of such layers is essential for most applications – after all, software developers, for example, cannot be expected to take all details of the hardware and operating system into account when they are programming. However, thinking only within abstraction layers creates "an open door for side channels". The betrayal of secrets does not have to take place within a single system layer: "Side channels do not obey the rules of abstraction", emphasises the computer scientist.

In a poker game, you can exploit the side channel "facial expression", that is, the bad poker face of other players. In Computer Science, side channels can be established based on other more technical characteristics, such as the emanation of heat, processing time, electromagnetic waves, sounds, or power consumption. The research in Mantel's group focuses on side-channel attacks that do not require any physical access and, hence, are particularly dangerous. To identify them, the scientists in the CROSSING Collaborative Research Centre pursue multiple approaches.

> *"The question is not only whether a system is secure or not, but rather how secure is it?"*

Firstly, they employ formal methods: This allows one to understand and analyse a program's behaviour based on precise, mathematical models. Describing models in natural language would not be sufficiently precise for obtaining reliable, unambiguous analysis results. After all, a security guarantee should not be interpretable in different ways.

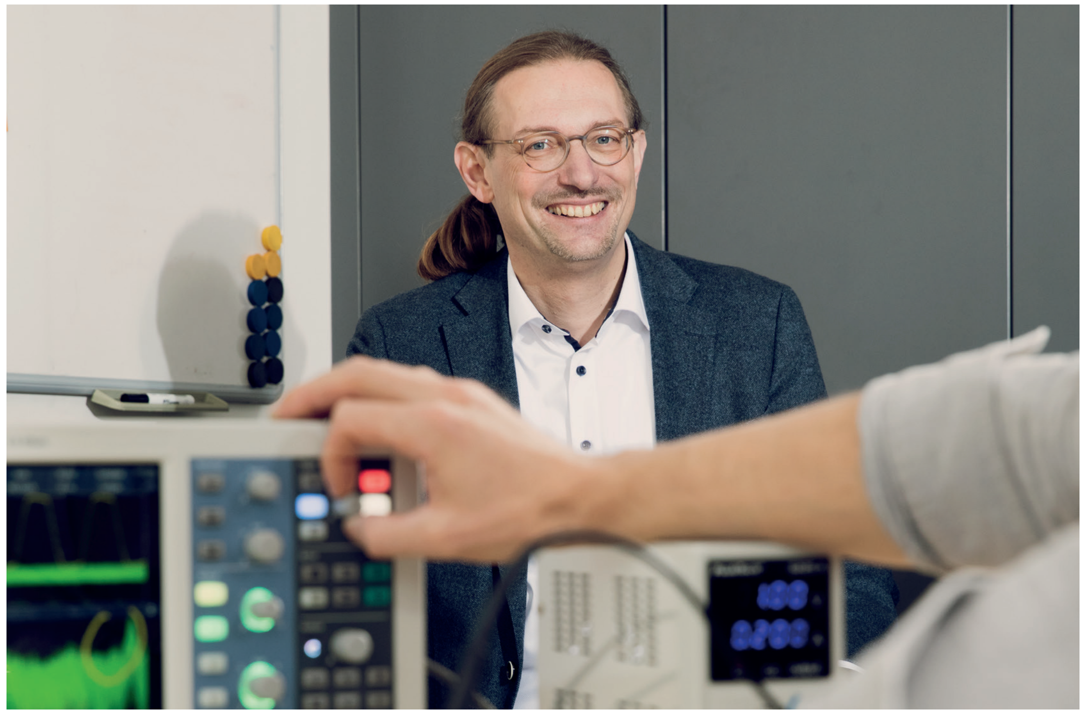
Following this approach, the objective is to determine upper bounds on how much secret information might be betrayed to others. The doctoral candidate Alexandra Weber is working on this subject at Mantel's chair. "I can determine how much of a secret might be leaked in a worst case scenario.", says the young scientist. "I find it very motivating that my research allows me to provide such precise and reliable security guarantees." For instance, if a cryptographic key consists of 256 bits, the formal approach can be used to calculate how many bits might be leaked to an attacker via a side channel at most. "In the process, the mathematical model defines where information is permitted to flow, what the secrets are, and what the attacker is able to "see"", according to Weber. The aim of the research in CROSSING is to create tools for analysing software with respect to side channels automatically.

It was already possible to semi-automatically identify such loopholes in a very successful interdisciplinary cooperation between the research group headed by Professor Mantel and the team "q-TESLA". q-TESLA is a post-quantum signature scheme developed in the CROSSING Collaborative Research Centre that was submitted to the world's first standardisation process in this area. In the implementation of the previous version, the teams were able to identify a cache side channel in the function that generates the signature. By eliminating this weakness, they improved the security of the signature scheme, which could also increase the opportunities in the standardisation process.

In the CROSSING Collaborative Research Centre, a second approach is pursued for evaluating the risks posed by side channels. The researchers take the perspective of an attacker to identify potential side channels experimentally. Hereby, they determine the amount of information about a secret that an attacker can find out at least by a feasible attack. The result indicates how high the danger of such attacks is at least. "The attack-oriented approach allows us to find a so-called lower bound", says Mantel. If the upper and lower bounds lie close together, this confirms the accuracy of the bounds. The security of a system is thus not evaluated absolutely – i.e. not only in terms of "insecure" and "secure" – but rather in more fine-grained degrees of security. This makes it possible to give security guarantees, even for systems that are not fully secure, and to compare the security of such systems. "The question is not only whether a system is secure or not, but a much better question is how secure is a system?", summarises Mantel.

Heiko Mantel views side channels as a promising field for scientific research that is becoming increasingly important in practice: "Spectre and Meltdown constitute two prominent examples of side-channel attacks that were reported widely in the press." Side-channel attacks are very difficult to detect forensically, which is one reason why the Computer Science Professor believes that further research will be beneficial. After you have lost enough money in a poker game, you will realise that something is not going well, and you will try something different or simply stop playing. However, "you do not receive this sort of helpful feedback in the case of side-channel attacks", according to Mantel. "Secrets are revealed but without anybody noticing. And when it does become obvious that somebody knows the secret, it is almost impossible to draw sensible conclusions in retrospect about when, where and how this information was revealed." And this is why the researchers in Darmstadt are continuing to work on giving computers a better poker face.

The author is an online journalist and member of the CYSEC Profile Area.



Photography: Katrin Binner

The power consumption of hardware components can be measured using an oscilloscope, and this information can be used for side-channel attacks.

CROSSING

More than 65 scientists from cryptography, quantum physics, system security and software engineering work together in the CROSSING Collaborative Research Centre at TU Darmstadt and carry out both basic and applied research. The aim is to develop security solutions that will enable the development of secure and trustworthy IT systems even in the future. CROSSING has been funded by the German Research Foundation since 2014.

Information

Computer Science
Prof. Dr.-Ing. Heiko Mantel
Phone: +49(0)6151/16–25252
Email: mantel@cs.tu-darmstadt.de
http://www.mais.informatik.tu-darmstadt.de