Master Thesis:

A Smart Attack using the Frequency Covert Channel

Context

Today’s Laptops, Servers and mobile devices (smartphones, tablets, …) leverage multi-processor systems on chip (MPSoCs) that put several components (cores, caches, accelerators, …) onto the same piece of silicon. These devices are often used for sensitive applications (bank, health, …) as well as non-sensitive applications (games).

While various sandboxing and segregation techniques exist to ensure the security of sensitive applications and information, the applications still share the physical silicon of the MPSoC. We are studying how attackers could leverage this physical property to leak information from an infected authorized application to an unauthorized one, which is otherwise isolated at the software and architecture level. In particular, we are trying to demonstrate how applications can communicate using covert channels established through the measurement of the operating frequency of the cores. Our goal is to develop smart source (src) and sink (snk) applications, which are capable to explore the frequency covert channel by themselves and establish a working data transmission.

Tasks

The student will extend our work on the evaluation of covert channels which are established through the operation frequency of the cores. The main tasks to complete the thesis will be:

• Get to know the existing measurement framework (Matlab, C, C++, Java, UNIX Shell Scripts)
• Develop smart sink and source apps which can adapt to different running environments.
• Build a case study to evaluate the channels achievable maximum capacity and the robustness.
• Run the case study on the target devices.

Requirements / Skills

• Basic Knowledge in ...

  – C / C++ / Java development (Android Apps)
  – Data Analysis (MATLAB, Python or similar)
  – UNIX Shell or similar System Programming (Script Languages)
  – Signal Processing, Classification and Deep Learning

  • Curiosity and interest in security and in systems research

Interested? Please have a look at http://www.tec.ethz.ch/research.html and contact us for more details!

• Philipp Miedl: philipp.miedl@tik.ee.ethz.ch, ETZ G76
• Matthias Meyer: matthias.meyer@tik.ee.ethz.ch, ETZ G81