

# Program

- 9:00 Reception**
- 9:15 What's hot & what's happened**  
We share the topics and trends in side channel testing that were relevant in the past year. What results were publicly reported and what are the new practical attacks to take into account?
- 10:00 Far-field measurements on crypto chips**  
For exploits at slightly larger distance a far-field attack via a side channel can offer a nice attack path. This session explains one such use case.
- 10:30 Coffee Sessions**  
Please take some time to visit a demo while enjoying your brew of choice on one of the following set ups:
- Automating your side-channel setup
  - Creative setup building for embedded chips
  - Taking far-field measurements on shielded crypto chip
  - WBC in practice
- 11:15 Invited speaker – Europe: Mathias Wagner, NXP**  
Template Analysis has been growing in relevance and Mathias Wagner presents a novel approach that takes this technique to the next level.
- 12:15 Lunch**
- 13:30 Build it yourself!**  
You are offered a challenge, build it fast! .
- 14:00 Fault injection on ARM**  
We present a fault injection weakness in the ARM instruction set. This weakness can be used to achieve runtime control on ARM-based embedded systems using fault injection.
- 14:45 Coffee Sessions**  
Please take some time to visit a demo while enjoying your brew of choice on one of the following new products:
- Automation with Inspector
  - Creative setup building for embedded chips
  - Taking far-field measurements on shielded crypto chip
  - WBC in practice
- 15:30 Inspector software releases**  
Get a quick overview of the most significant changes and features that we've released, as well as the topics we are currently working on. Questions and feedback encouraged!
- 16:00 How to pick the right laser sources?**  
With so many laser sources available nowadays, it is difficult to decide which one to use for what with the limited time you have available. We share how we approach this problem in practice. Aspects covered are laser technology (laser cutter, single/multimode diode, DPSS), wavelengths and silicon / memory characteristics.
- 17:00 Closing**
- 19:00 Dinner**
- 9:00 Reception**
- 9:15 Metrics for Side-channel Analysis in practice**  
In practice, it is very difficult to determine how good your side-channel setup is. We will present different metrics that can be useful to evaluate and compare your measurement setups, such as SNR, RDM, and MIA.
- 9:45 Tips & Tricks**  
Our customer support team receives many questions. We share a selection of answers to make your life easier.
- 10:30 Coffee Sessions**  
Please take some time to visit a demo while enjoying your brew of choice on one of the following new products:
- Automation with Inspector
  - Creative setup building for embedded chips
  - Taking far-field measurements on shielded crypto chip
  - WBC in practice
- 11:15 Research @ Riscure**  
In this session you learn about the research we have conducted in the side channel space. Besides our own research we will also share the results of many internships at Riscure.
- 12:00 Lunch**
- 13:30 Playing with ill-formed applets**  
The session introduces novel attacks on secured containers which allow an attacker to retrieve keys and PINs of other applets on a Java Card.
- 14:15 Where is key enumeration heading?**  
Over the past years, we have worked intensively with key enumeration. We would like to present what we have found in practice thus far, and offer our vision on the future of this technique in the field.
- 14:45 Coffee Sessions**  
Please take some time to visit a demo while enjoying your brew of choice on one of the following new products:
- Automation with Inspector
  - Creative setup building for embedded chips
  - Taking far-field measurements on shielded crypto chip
  - WBC in practice
- 15:30 How to perform side channel testing on USB smart cards**  
We demonstrate how to build a setup using a USB smartcard (ISO 7816-12) and how to attack it. The takeaway is how to go about building a non-conventional/non-standard setup.
- 16:00 EMA probes and their different use cases**  
With so many different affordable probes available, the choices become harder to make. Different approaches have their pros and cons, and in this session we share these approaches to enable you to choose the best approach for your use cases .
- 16:45 Recap**  
We have presented a lot of information during this User Workshop, and we may have gotten some new insights when discussing topics with the attendees. Before closing, we will present a short overview of what we've presented, seen and heard during the past two days.
- 17:15 Winner announcement physical smart card challenge**
- 17:30 Closing**