**Add to your Google Calendar**

---

**D1**

**Wednesday**

**September 2nd**

<table>
<thead>
<tr>
<th>When (GMT+2)</th>
<th>Keynote + r2wars + workshop</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:00-17:10</td>
<td>Pancake</td>
<td>Opening presentation by radare2 author!</td>
</tr>
<tr>
<td>17:10-17:40</td>
<td>r2wars For N00bs</td>
<td>This talk is related to the r2wars tournament which is always being held during r2con. It serves as an introduction for people that aren't yet familiar with r2wars, but may also be interesting for people that have already participated in previous tournament editions.</td>
</tr>
<tr>
<td></td>
<td>Captain Banana</td>
<td>There are many strategies to win and the goal of this talk is to make you familiar with some of the main strategies. Also, you will learn about several tricks which may be helpful to optimize your bots &amp; how to participate in the tournament.</td>
</tr>
<tr>
<td>17:40-18:40</td>
<td>Skuater</td>
<td>r2wars is a game similar to Core Wars, which has been around for several years. There's a shared memory space of 1KB that's mapped as RWX. Both participants submit bots that get instantiated in this memory space at random locations. These bots can be developed in x86, x64, ARM and M68K. After the battle starts, the goal is to cause the opponent's bot to crash. This can be accomplished by corrupting the instruction pointer of the opponent. Another option is to cause invalid reads/writes that also result in crashes.</td>
</tr>
<tr>
<td></td>
<td>Mobile Reverse Engineering with R2frida</td>
<td>Attendees will learn about: - Unveiling crypto on Automotive challenges - Bypass jailbreak protections - SSL pinning - Anti-debugging - Frida detections using Frida itself</td>
</tr>
</tbody>
</table>

To avoid the prerequisites of Mac/iOS devices, the hands-on will be Android focused. Walkthroughs & demonstrations of iOS will be featured.
<table>
<thead>
<tr>
<th>Time (GMT+2)</th>
<th>Talks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17:00-18:00</td>
<td>r2wars</td>
<td><a href="https://t.me/joinchat/AnoeOVDr7--s_89_DFhyrw">Skuater</a></td>
</tr>
</tbody>
</table>
| 18:00-18:30 | Semi-Interactive Simplification of Hardened Android Malware | Modern malware analysis has also progressed to a very mature stage with the advent of maintained symbolic execution frameworks, binary instrumentation, and automated analysis environments. In this talk, the speaker will:  
- Showcase a few common obfuscation techniques.  
- Present semi-automated methods to simplify a hardened Android codebase.  
  The speaker will present a modular deobfuscation script used to realign a distorted APK and annotate an execution run. |
| 18:30-19:00 | Softening r2 Signatures | Go is everywhere these days (because Go is awesome).  
It is now common to find Go binaries compiled to ELF, Edge computing devices, and web assembly applications. In this talk, we will highlight differences between C and Go binaries, using radare2.  
With the help of Go, we will identify what makes Go binaries unique, and recommend approaches to reverse Go applications. The proposed approach will help anyone interested in RE Go binaries conduct a faster and more effective analysis of Go apps. |
| 19:00-19:30 | Radare2 & Gophers - Analysis of Go Binaries with Radare2 | Go is everywhere these days (because Go is awesome).  
It is now common to find Go binaries compiled to ELF, Edge computing devices, and web assembly applications. In this talk, we will highlight differences between C and Go binaries, using radare2.  
With the help of Go, we will identify what makes Go binaries unique, and recommend approaches to reverse Go applications. The proposed approach will help anyone interested in RE Go binaries conduct a faster and more effective analysis of Go apps. |
| 19:30-20:00 | Break | |
| 20:00-20:30 | ESLSolve: A Symbolic Execution Engine using ESL | ESLSolve is a new framework that uses r2’s ESL IR with s2 (and potentially other SMT backends) to symbolically execute code.  
This talk will cover:  
- Quick explanation of ESL tailored to ESLSolve topics (if necessary)  
- The challenges of ESL based symex and how they were overcome  
- Examples of how ESLSolve can be used to solve RE and security problems  
- Demo of ESLSolve and its API. |
| 20:30-21:00 | Introduction to reverse engineering deeply embedded devices | Embedded devices are found in a surprising amount of everyday things.  
From household devices to light bulbs and routers, everything contains at least one micro controller running software that realizes the device’s functionality. Often, this software is only provided in binary form without any documentation (about internal workings) or API.  
In this talk, we give an introduction to the analysis of deeply embedded systems, a class of embedded devices that has only limited resource availability.  
First, we acquire an overview of ways to obtain the device firmware.  
Afterwards, we demonstrate how to use Cutter to reverse engineer an unknown device firmware. In particular, we have a look at function identification, peripheral interactions & code understanding via static analysis.  
The talk concludes by giving an outlook of dynamic analysis capabilities for deeply embedded systems. |
| 21:00-22:00 | XVILKA presents - talks by 2020 GSoC students | This year’s students in the Google Summer of Code program will speak about their work on radare2.  
https://summerofcode.withgoogle.com/organizations/4946212249141248 |
<table>
<thead>
<tr>
<th>Time</th>
<th>Session/Presenter/Affiliation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:30-17:00</td>
<td>Adrian Hendrich, r2wars + talks + workshop</td>
<td>Okay, so you don't like shellcode too? Shellcode is often spotted to execute a malformed code in a way that can trigger the injection or further exploitation process, or other operations, mostly used in offensive ways.</td>
</tr>
</tbody>
</table>
| 17:00-18:00  | Sylvain Pelissier, Security expert, researching Cryptography & embedded devices.                | r2wars Session: Join the tournament here [link]. Many analyses of binaries or memory dumps contain cryptographic material. This talk will present crypto-related commands in r2wars and how they can speed up or resolve some practical uses. The talk will cover:
- Yara integration into r2wars
- Some commands to search AES keys, public key or certificates in memory dumps or during debugging sessions.
- The features presented will be compared with existing solutions. |
| 18:00-18:30  | Sylvain Pelissier, Security expert, researching Cryptography & embedded devices.                | In radare2, it means cryptography: In this session, Sylvain will present crypto-related commands in r2wars and how they can speed up or resolve some practical uses. The talk will cover:
- Yara integration into radare2
- Some commands to search AES keys, public key or certificates in memory dumps or during debugging sessions.
- The features presented will be compared with existing solutions. |
| 19:00-20:00  | Tim Blazytko, Reverse engineer & former security researcher at the Ruhr-Universität Bochum, Senior Security Engineer at emproof GmbH | [2 hour workshop] Semi-automatic Code Deobfuscation: In modern businesses, code obfuscation has become a vital tool to protect, for example, intellectual property against competitors. In the second part, we use symbolic execution & SMT solvers to break these techniques in an automated manner. |
| 21:00-21:30  | Sylvain Pelissier, Security expert, researching Cryptography & embedded devices.                | ESL, side-channel simulation: During the talk, we will present how we instrumented ESL's ESL to simulate the effects of fault attacks on embedded firmware. The firmware is instrumented using r2pipe and thus the fault models & the scope of the attack are completely scriptable. |
| 21:30-22:00  | Jan Srenssen, Mobile security engineer with iOS development background. Specialised in RASP solutions, automation and low-level mobile internals. | A security review of 1,300 AppStore applications: Session: 1,300 Security research. I will show that it doesn’t take to be an expert to use Frida & Frida to easily detect app hardenings. I will give a walk-through of the current usage of RASP techniques in the mobile industry. |
When (GMT+2) | r2wars + talks + closing + post-r2CON live chiptune party! | Description
--- | --- | ---
17:00-18:00 | Pancake + Skuater | Join the tournament here: https://t.me/joinchat/AnoeOVDr7--s_89_DFhyrw
18:00-18:45 | From hardware to zero-day | **Pietro Oliva**
Security researcher with a degree in IT security from Università di Milano. Experience in pentesting, red teaming & security/vulnerability research.
This talk will explore the risks associated with them by sharing a personal research performed on a closed security camera. This talk will retrace all the steps that have been performed to go from hardware analysis & flash dumping, to zero-day discovery & exploitation.

19:00-19:30 | Symbolic Execution in rader2 | **Chase Kanipe**
This talk is on using the new “Modality” rader2 plugin to perform symbolic execution. The tool is built on top of angr, and provides a faster alternative to using angr than writing scripts. This integration has numerous advantages, including easy switching between concrete & symbolic execution, useful visualizations of the angr backend, as well as a suite of features for vulnerability detection & exploit generation.

19:30-20:00 | Keys to Homebrew | **Anonymous**
An american who has been living in r2land since 2014.
Relatively quick walkthrough to exploiting and running custom code on a smart key, starting with zero knowledge about the system, ending of course with playing DOOM on the embedded device, showing hardware hacking, and how to reverse.

20:00-20:45 | Where is my Ransom? | **Kevin Gomez**
I'm an incident responder with a strong focus on malware analysis. PhD student.
My interests are forensics, malware analysis and reverse engineering.
My goal is to collect the newest samples of specific ransomware gangs and understand the different actors.
At the beginning of this project, I started to analyse samples from different reports by hand. This task was very time consuming.
I was not able to gain new insights after analysing a few samples for a specific group. The collected IOCs and TTPs were already know. So I was not able to generate benefit for anyone.

21:00-21:45 | Codename: flip.re | **Lars Haukli**
At the age of 12, I was falsely accused of infecting my neighbor's PC with a virus. I had no idea how a virus worked, and I had nothing to do with it. All I wanted was to play a video game.
We will present an sandboxed plugin to turn r2 into a hypervisor-level debugger to analyse malware on Windows. The plugin is conceptually similar to the zdbg plugin presented at r2con 2017 by the same author, but it is written from scratch in Rust.
The project aims to form one of the basic building blocks on which we will build a new commercial malware analysis product.
We seek to empower the open source community, contribute to the radare2 project and release the plugin as open source.

21:45-22:00 | Closing Pancake | **Live Chiptune**
40boy + Neuroflip + 2dig3 + Alex Wiklund + Klirre
Live chiptune music generated with Game Boyz and Amiga, with love from the artists that made possible the r2CON 2019 chiptune live party in Barcelona!