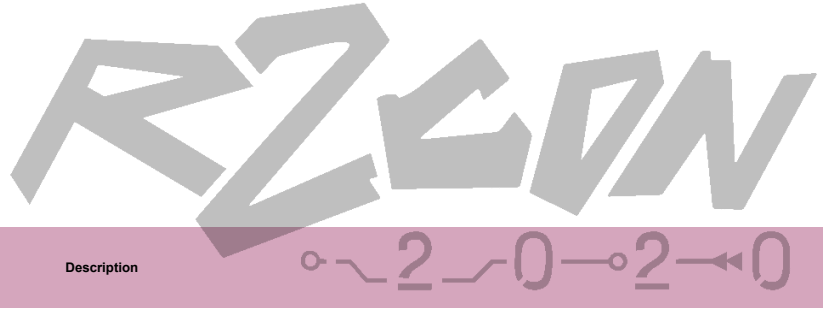
v0.3.1

[Add to your Google Calendar]

D1

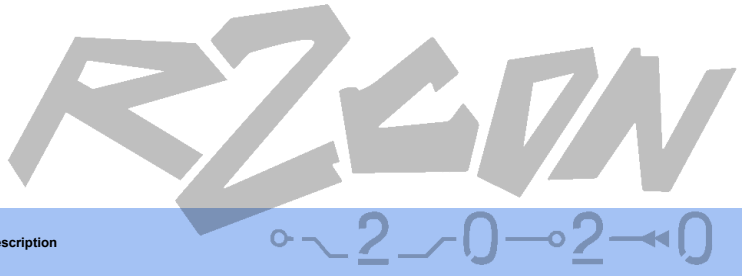
Wednesday
September 2nd



When (GMT+2)	keynote + r2wars + workshop	Description
17:00-17:10	**Keynote** **Pancake** Author of radare (2006) and the complete rewrite radare 2 (2009). Security engineer @NowSecure.	Opening **presentation** by **radare2 author!**
17:10-17:40	**r2wars For N00bs** **Captain Banana** Banana loving haxxor.	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. 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** & **how to participate in the tournament**.
17:40-18:40	**r2wars** **Skuater**	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 MIPS ASM. After the battle starts, the **goal is to cause the opposing bot to crash**. This **can be accomplished** by **corrupting the instruction pointer of the opponent**. Another option is to **cause invalid read/writes** that also result in crashes. **Join the tournament here** https://t.me/joinchat/AnoeOVDr7--s_89_DFhyrw
18:40-22:40	**[4 hour workshop]** **Mobile Reverse Engineering with R2frida** **Eduardo Novella (@enovella_),** Mobile Security Researcher @ NowSecure. **Alex Soler (@as0ler)**, Chapter lead Security Engineer @ AttackIQ. **Grant Douglas (@Hexploitable)**, Mobile Security Researcher @ NowSecure.	**Combining dynamic & static analysis** is the key to quickly solving many challenges when performing binary analysis. We will walk you through **how to use r2frida**, an **IO plugin to use Frida in r2land**, **to analyze Android and iOS mobile apps**. Attendees will learn about: - **Unraveling crypto on Automotive challenges** - **bypass jailbreak** protections - **SSL pinning** - **anti-debugging** - **Frida detections** using Frida itself To avoid the pre-requisites of Macs/iOS devices, the **hands-on** will be **Android focused**. **Walkthroughs & demonstrations** of **iOS** will be featured.

D2

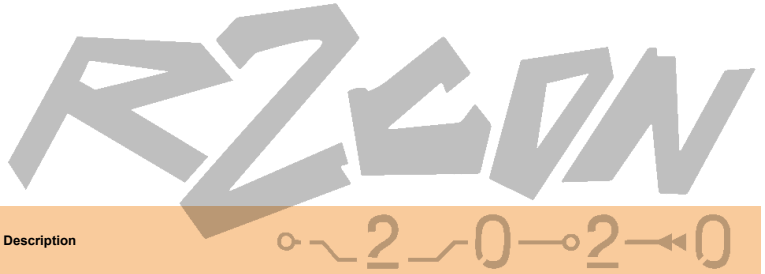
Thursday
September 3rd



When (GMT+2)	r2wars + talks	Description
17:00-18:00	**r2wars** **Skuater**	**Join the tournament here https://t.me/joinchat/AnoeOVDr7--s_89_DFhyrw**
18:00-18:30	**Semi-Interactive Simplification of Hardened Android Malware** **Abdullah Joseph** Abdullah Joseph is the mobile security team lead of Adjust. His team works on researching current and future mobile ad fraud schemes and developing appropriate countermeasures.	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** **Dennis Goodlett** Professional Magician turned penetration tester after college. I enjoy making computers do things. **Barton Rhodes** Engineer focused on building secure and reliable machine learning systems for malware classification	Exact matches on **r2 signatures save a lot of time** -- so shouldn't a near match still save some time? This talk is about **using signatures**, even when they're less than perfect.
19:00-19:30	**Radare2 & Gophers - Analysis of Go Binaries with Radare2** **hex0punk -** Application Security Engineer at Trail of Bits. He has published research on artificial intelligence technologies.	Go is everywhere these days (because Go is awesome). It is now common to find Go binaries embedded in IoT, 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 r2, we will **identify what makes Go binaries unique**, and **recommend approaches to reverse Go app**lications. 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	**ESILSolve: A Symbolic Execution Engine using ESIL** **Austin Emmitt** Mobile Security Researcher at Nowsecure.	**ESILSolve** is a **new framework** that uses **r2's ESIL IR with z3** (and potentially other SMT backends) to **symbolically execute code**. This talk will cover - Quick explanation of ESIL tailored to ESILSolve topics (if necessary) - The challenges of **ESIL based symex** and how they were overcome - **Examples** of how ESILSolve can be used to **solve RE and security problems** - How ESILSolve can help **improve concrete ESIL emulation** - **Demo** of **ESILSolve** and its **API**
20:30-21:00	**Introduction to reverse engineering deeply embedded devices** **Benjamin Kollenda** PhD (binary analysis and RE) at the Chair for Systems Security in Bochum. I am a co-founder at emproof, working on securing 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** in the **analysis of deeply embedded systems**, a class of embedded devices that has only limited resources available. Instead of running well-documented operating systems (e.g. Linux), deeply embedded systems execute bare-metal software or tiny real-time operating systems. First, we acquire an **overview of ways to obtain** the device **firmware**. Afterward, 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**. We conclude our talk by giving an outlook of dynamic analysis capabilities for deeply embedded systems.
21:00-23:00	**GSoC talks** **Xvilka** radare2 GSoC mentor	This year's **students** in the **Google Summer of Code program** will **speak about their work on radare2.** **https://summerofcode.withgoogle.com/organizations/4946212249141248**

D3

Friday
September 4th



When (GMT+2)	r2wars + talks + workshop	Description
16:30-17:00	**Okay, so you don't like shellcode too?** **Adrian Hendrick** https://en.wikipedia.org/wiki/MalwareMustDie Working helping cyber attack victims at LAC Cyber Emergency Center https://www.lac.co.jp/english/service/incident/cyber119.html	**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**. In this presentation I will describe how I used **radare2 handling malicious shellcode** cases I dealt in multiple operating systems & architectures. Beforehand I will present **several basics & category of shellcode** in simple and practical ways. The talk can help other **analysts or r2 RE beginners recognizing types of shellcode & handling them** in their work on their **blue-team**'s fi In the end of presentation the case(s) in **dissection of a complex obfuscated shellcode** will be presented.
17:00-18:00	**r2wars** **Skuater**	Join the tournament here https://t.me/joinchat/AnoeOVDr7--s_89_DFhyrw
18:00-18:30	**In radare2, /c means cryptography** **Sylvain Pelissier** Security expert, researching Cryptography & embedded devices.	Many analysis of binaries or memory dumps contain cryptographic material. This talk will present **crypto-related commands in radare2** and how they **can speed up** or **resolve** some **practical uses cases**. The talk will cover: - **Yara integration into radare2** - **recent rules** added - **commands to search AES keys, public key** or **cert**ificates **in memory dumps or during debugging sessions**. The features presented will be compared with existing solutions.
18:30-19:00	**30' BREAK**	
19:00-21:00	**[2 hour workshop]** **Semi-automatic Code Deobfuscation** **Tim Blazytko** Reverse engineer & former security researcher at the Ruhr-Universität Bochum. Senior Security Engineer at emproof GmbH.	In modern businesses code obfuscation has become a vital tool to protect, for example, intellectual property against competitors. In general, it impedes analysis by making the to-be-protected program more complex. In this **workshop**, we focus on a small set of **common code obfuscation techniques** (e.g. **opaque predicates** or **Mixed Boolean-Arithmetic**). After **understanding** their **core concepts**, we **analyze** them on the **binary level**. In the second part, we use **symbolic execution & SMT solvers** to **break** these **techniques** in an **automated manner**. The **workshop** is **suitable** for everyone who has **experience** in **reverse engineering** of **x86 code** and **wants to deepen knowledge** in **advanced program analysis or code obfuscation techniques**.
21:00-21:30	**ESIL side-channel simulation** **Sylvain Pelissier** Security expert, researching Cryptography & embedded devices. **Nicolas Oberli** Security researcher for Kudelski Security in Switzerland. Research focus on embedded devices and communication protocols. Developer of Hydrabus hardware hacking tool & part of BlackAlps sec conf committee. **Karim Sudki**	Side-channel attacks on embedded devices is sometimes hard to pull off, even with full knowledge about firmware. There are ways to evaluate the effectiveness of such attacks by RE the running software, but this heavily depends on the reverser's knowledge of the underlying CPU architecture. During this talk, we will present **how we instrumented r2's ESIL to simulate the effects of fault attacks on embedded firmwares**. The **firmware** is **instrumented using r2pipe** and thus the **fault models** & the **scope of** the **attack are** completely **scriptable**. Since the **faults are applied at** the **firmware level**, there is **no need** of the source code **to run simulations** over real case scenario. We'll **present various fault models used** and their **effect on an example firmware**, allowing to **recover** an **encryption key using differential fault analysis**.
21:30-22:00	**A security review of 1,300 AppStore applications** **Jan Seredynski** Mobile security engineer with iOS development background. Specialised in RASP solutions, automation and low-level mobile internals.	Runtime Application Self Protection gains momentum as we store more and more valuable data on our smartphones. Banking apps, crypto wallets, 2FAors and more are vulnerable to malware originating from malicious apps in the AppStore, websites or even messages on popular communicators. I will describe **how I automated AppStore crawling & queued apps for static & dynamic analysis to search for RASP protections**. I will show that **it doesn't take to be an expert** to use **Radare2 & Frida to easily detect app hardenings**. I will also share some **insight on** the **current usage of RASP techniques in** the **mobile industry**.

D4

Saturday
September 5th

When (GMT+2)	r2wars + talks +closing + post-r2CON live chiptune party!	Description
17:00-18:00	**r2wars** **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.	IoT devices are changing the world in both good and bad ways. It is exciting and fascinating to see how technology keeps improving our lives, but it is also worth considering the security impact and the vulnerabilities being introduced in our lives by such connected devices. This talk will **explore** the **risks associated** with them by sharing a personal research performed on a **cloud 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 radare2** **Chase Kanipe**	This talk is on using using the **new "Modality" radare2 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 r2 for reversing.
20:00-20:45	**Where is my Ransom?** **Hunting for Ransomware Gangs using r2 and Yara** **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. How am I able to collect new samples for specific groups? I decided to hunt using Yara and I used VirusTotal and Hybrid Analysis to perform my hunts. In my talk, I will explain: - the **goal of Yara and its capabilities**. - the **syntax & best practice**s. - how I created **Yara rules using Cutter**. - I will illustrate this for two rules: **The maze & clop ransomware**. - In addition, I will explain what I learned during the journey.
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 **io/debug plugin to turn r2 into a hypervisor-level debugger**, to **analyze malware on Windows**. The **plugin is conceptually similar** to the **zdbg plugin (unreleased) presented at r2con 2017** by the same author, **but** 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**. The talk will discuss the **design & implementation** of an **advanced r2 plugin in Rust**, and will showcase **practical use cases** of the plugin to **analyze malware**. We also want to discuss **how the r2 community can get involved** as we work towards an early alpha version of our malware analysis product. This will be a follow-up talk to my 2017 talk on zdbg, which I was unfortunately not able to release. The flip project builds on my previous experience, but is a brand new project started from scratch, undertaken by an **early stage cybersecurity startup** that I **recently founded**.
21:45-22:00	**Closing Pancake**	
22:00-23:00	**Live Chiptune** **4Dboy & Neuroflip**	**Live chiptune music generated with Game Boys and Amiga**, with love **from the artists** that made possible the **r2CON 2019 chiptune live party** in Barcelona!