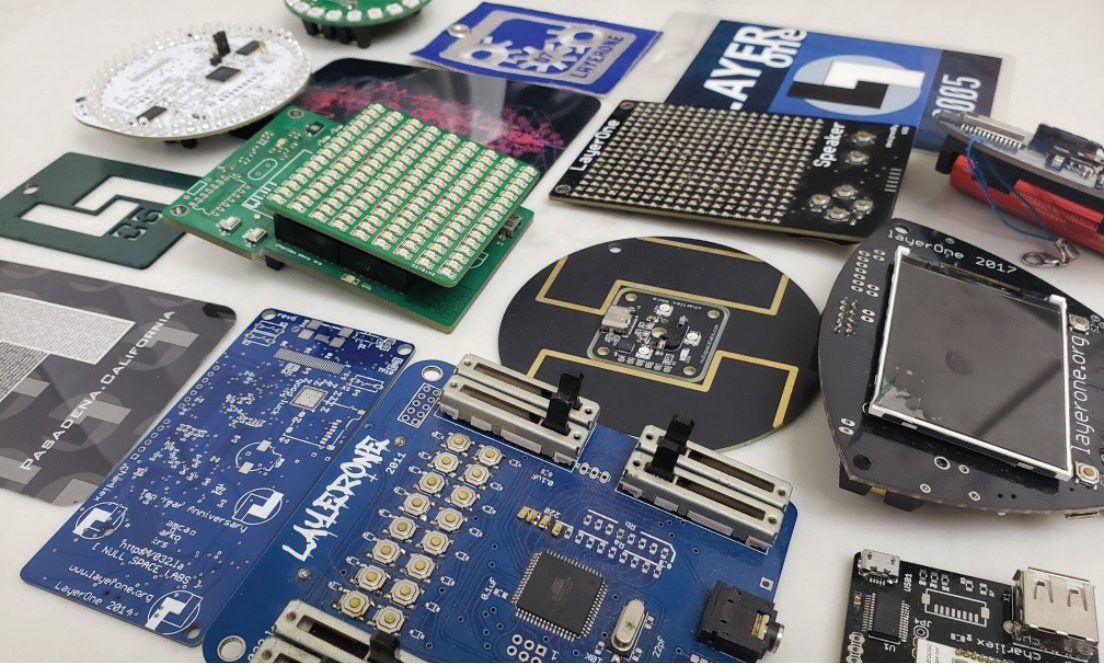
LayerOne 2024

Pasadena, California

May 25-26



20 Years of LayerOne

Twenty years ago I went to a hacker conference in Los Angeles called LayerOne. It was awesome. I met a lot of like minded folks who were interested in doing cool things, learning, and constantly improving their skill sets. They helped me figure out what parts of tech and security really interested me and motivated me to keep growing. One of them, a LayerOne organizer by the name of M, even bought me my very first lockpicking set on THE INTERNET. I was a degenerate young hacker who didn't trust credit cards so I needed his help. Yeah. That kind of hacker. With that lockpicking set I went on to give my first talk at a conference at LayerOne 2005 and from there the rest is history. I hope that this year's conference helps you find what you're passionate about in a friendly, hands-on environment. The many villages, contests, and events that make up LayerOne are described in this booklet, but feel free to ask staff for some help if you're not sure what to do or where to go. LayerOne is all about getting involved so get out there, have fun, learn, and help others do the same!

- datagram

Badge Info:

When asked about this year's badge, the badge team said "You spin me right round, baby, right round (with a hall effect sensor)". This year's badge is once again graciously designed by M, charlieX, and KRS of Null Space Labs who work tirelessly year round so that they change their mind at the last minute and rush to finish the badge a few days before con. Check out the display tables near registration to see an awesome collection of badges designed for LayerOne over the years! Want to mod your badge and make it better and badder? Hack on your badge in the Hardware Hacking Village throughout con!

Events & Spaces

Chillout Room

The Chillout Room is a special area of the conference where attendees can unwind by lounging on a couch or playing some games with friends. On hand are a wide variety of gaming consoles, board games, card games, and maybe even a pinball machine or two. Sponsored by the LA hackerspace, Null Space Labs, there will be volunteers on hand to help you get set up, recommend games you might like, and generally assist with the process of chilling out.

The Chillout Room is open on Saturday & Sunday from 10:00 to 18:00.

HAM Testing

Are you lonely? Need someone to talk to? Do discussions about volts, amps, watts, ohms, and high voltage excite you? Are you a social outcast without a hope of ever finding companionship? If you answered yes to all of these questions, you are probably already a ham. If you answered no to any of them, you probably aren't a ham - but we can fix that!

Come ruin your social life the right way by taking the amateur radio exams at LayerOne! If you're looking to upgrade (read: become even more uncool and/or lose your significant other) we can handle that for any amateur radio license class, too!

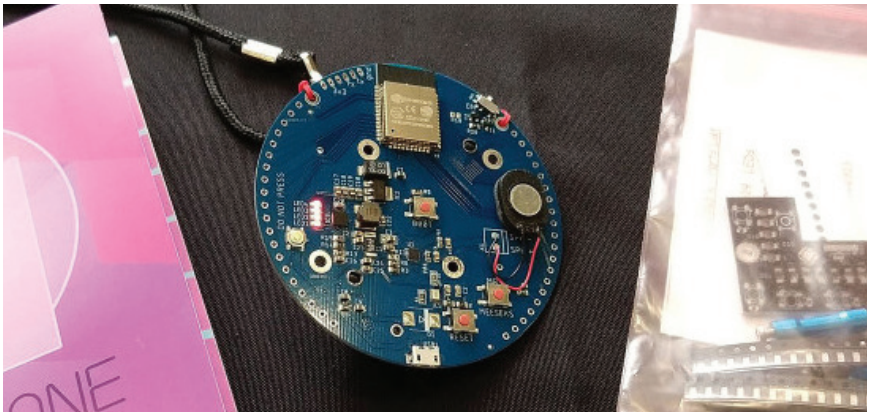
Sign up at examreg.emergencycomm.org - testing takes place on Saturday, May 25, 2024 at 18:00 Pacific time in the Lockpicking Village

Lockpicking Village

The Lockpicking Village is a special area of the conference where attendees can learn about locks, lockpicking, and physical security. Visitors can practice picking locks in a hands-on setting and learn about many of the locks that are used to secure their homes and businesses. Visitors are encouraged to bring any locks that they want to learn more about, either how to open them, disassemble them, or just learn what features they might have.

The lockpicking village is fun for all ages and all skill levels. If you've never picked a lock before this is the place to learn how! The Lockpicking Village is open from 10:00 – 17:00 Saturday and Sunday.

Events & Spaces



Hardware Hacking Village

The Hardware Hacking Village is a special area of the conference where attendees can learn about hardware hacking and the basic concepts of electrical engineering, including surface-mount soldering and circuit design. Sponsored by the LA hackerspace, Null Space Labs, there will be volunteers on hand demonstrating how to assemble this year's badge and a number of other electronics projects. This year's badges (both attendee and speaker) will be electronic, but you have to assemble them in the hardware hacking village!

At LayerOne we want you to get down and dirty with hardware hacking. Learn how to solder and use the plethora of equipment available! The Hardware Hacking Village has top of the line Metcal soldering irons, ovens, hotplates, solder dispenser syringes with automatic solder paste feeders, thru hole, scopes, meters, power supplies, and more! The Hardware Hacking Village is also the perfect place to plan, assemble, and fix your HeboCon Robot Battle entry!

The Hardware Hacking Village is open from 10:00 – 18:00 Saturday and Sunday.

Events & Spaces

RaiseMe Career Village

Whether you are currently outside the information security field and looking for your first role, or an established member of the InfoSec industry and want to kick up your career a notch, weâ€™re here to lend a helping hand. Our volunteer consultants provide Resume Review, Mock Interviews, Job Hunting Assistance, and Career Check-ups. We also help companies looking for talent by connecting our participants with their hiring managers and staffing professionals.

The vision for RaiseMe is to make career dreams come true. We serve the entire community — from newcomers to principal engineering talent, from tiny startups to well-established public corporations. Is there a role in security you wish you had but have no idea where to start to make that dream come true? If you want to make a career change, we want to help!

The RaiseMe Career Village is open 10:00 – 17:00 on both Saturday and Sunday.

Saturday Night Dinner & Casino Night

“This year’s Saturday Night Party is a Casino Night! Come enjoy the banquet feast, then roll with the best of them! Banquet starts at 7:30 PM on Saturday in the International Ballroom.

Sunday Night Party @ NSL

Our good friends at the Null Space Labs Hackerspace in Burbank, CA host the official LayerOne afterparty! Come join us for shenanigans, barbeque, and more! The afterparty starts at 6:30 PM on Sunday, May 26, 2024. Null Space Labs is located at 2522 N Ontario St, Burbank, CA 91504. See https://032.la/#contact for a map and additional info about the hackerspace.

Contests

Demo Party

The LayerOne Demo Party is back again for another year of awesome demos! Demos are a combination of programming challenge, artwork, and music. You're given specific hardware with any number of restrictions – code size, available memory, processor speed. Your goal is to output audio and video that pushes the limits of what is considered possible with such limited hardware.

Demo Party starts at 6 PM on Saturday in the Hardware Hacking Village

Hebocon (Robot Battles)

Hebocon is a Robotic Battle for those on an extreme budget. Originating in Japan, it pits poorly constructed robots, modified electric toys and last-minute creations against one another in a Sumo-style arena.

You play by building a robot. A really terrible robot. You can either build your robot and bring it to the conference, or build it on-site in our renowned Hardware Hacking Village. There should be plenty of electronics rework equipment in the HHV, but feel free to bring some extras to guarantee that you have tools to work with or share with others. See the LayerOne website for full contest rules and restrictions for robot construction and operation; sign up to compete in the HHV!

Soldering Olympics

Come test your soldering skills from beginner to advanced by completing several levels of increasingly difficult and wonderful soldering challenges. This contest is graciously hosted by Pendula Labs!

The Soldering Olympics is located in the Hardware Hacking Village!

Contests

Capture the Flag

Capture the Flag is back! This year's contest is graciously hosted by Qualcomm. The game will use a Jeopardy style board with challenges. This contest is for both beginners and experienced CTFers. Challenges will span many domains including web hacking, system hacking, forensics, reverse engineering, crypto, and more! Registration is open to all, no qualifications necessary.

AI CTF

New for 2024! Come to the AI Village Popup on Saturday, May 25, from 13:00 – 17:00 to learn about ML and AI security. There will be demos that will showcase different aspects of these systems, how they work, and when they fail. No registration/qualification necessary, the AI CTF happens in the Hardware Hacking Village.

Tamper Evident Contest

Do you have extensive knowledge of defeats for tamper-evident devices? Or maybe you've heard about the tamper contests and would like to try your hand at it? We have just the challenge for you: King of the Seal! Come one, come all – play against your friends!

To enter, you must open and close (unseal/reseal) a tamper evident device without visible, tactile, or olfactory evidence that you did so.

There will be multiple seals available for your purview including mechanical and adhesive seals. Old favorites and new challenges will be present for you to play with. This is an excellent way for you to practice tampering seals you have never seen and beating those that have frustrated you for years.

The LayerOne Tamper-Evident Contest runs from 10:00 Saturday to 14:00 Sunday!

Talks

The Silver Bullet Ecosystem and You!

A historical account of how the Silver Bullet ecosystem evolved, and how to find the versions of it that are likely pwning you during this talk. Don't know what the Silver Bullet ecosystem is? You should come to this talk!

vyrus is a grumpy young man with an even grumpier old soul who yells at clouds. The things he yells at the aforementioned clouds about include but are not limited to: threat intelligence, genetic – self proliferating – environmentally encrypted malware tradecraft, adversary engagement, and all things "cyber" automation.

Evil ELFs and Dishonest DWARFs

This talk will detail several practical examples of frustrating reverse engineering using crafted symbols and DWARF debug information. To do this, we'll dive into the internals of reverse engineering tools such as IDA Pro, Ghidra, and radare2 and discuss the various ways that ELFs store symbols. Topics include:altering automated program analysis using forged symbols; breaking debuggers using crafted DWARF bytecode; altering program flow based on the status of symbols on a binary

Jack Baker is a professional nuisance with too many IDA licenses

Python for Security Orchestration Automation and Response

Evolution took millions of years to produce flying snakes that glide from the tops of trees, but to make a snake SOAR you only need Python on your computer. Focusing on using Python for Security Orchestration Automation and Response (SOAR), Merlin will talk about the what, why, and how Python can be used to implement SOAR processes. SOAR platforms of the commercial and open source variety will be compared and contrasted based on their Python integrations. Even if your organization does not yet have a centralized SOAR platform, Merlin will explain how you can engage in a local-first SOAR process using just Python to get and show value to your organization.

Merlin is a wizard who provides magical solutions in Engineering for Security, Software, Systems, Networking, and occasionally Hardware.

Talks

Reverse Engineering Satellite Communications

This aerospace cybersecurity themed talk will cover the fundamental concepts and tools required for reverse engineering satellite communications. Participants will be guided through a step-by-step process, covering the essentials of demodulating, decoding, and organizing data transmitted via satellite downlinks. From extracting weather imagery from remote sensing NOAA satellites to intercepting telemetry and communication data from amateur radio satellites, the presentation will demonstrate the practical application of tools like GNURadio and Wireshark alongside covering cybersecurity topics such as packet dissection, decoding, and more.

Angelina Tsuboi (G4LXY) is a software developer and an aerospace cybersecurity instructor focusing on satellite systems. With over a decade of programming and development experience in addition to being a scientific researcher for NASA, she has been involved in numerous aeronautical and space-focused security initiatives for a wide range of applications ranging from drones, aircraft, and satellites. Driven by her passion for teaching, Angelina finds joy in simplifying complex subjects such as aerospace, cybersecurity, and programming to empower her students, Angelina focuses on ensuring that her students can readily apply the acquired skills to their professional and personal endeavors. Angelina is also the founder of Stellaryx Labs, a consultation, education, and development services company at the nexus of software, security, and aerospace. To learn more about her work, visit her website: angelinatsuboi.com

Kubernetes Security - What not to do

Kubernetes automates the deployment, scaling, and management of containerized applications. The complexity of handling all these aspects makes it a challenge to properly configure all the aspects securely. This talk will discuss security models in Kubernetes and how to correctly implement them with an eye towards anti-patterns that can lead to security issues.

Daryll Strauss has been a technologist in the top facilities in Hollywood for the last 30 years. His software has helped to create hundreds of feature films and television series. He has been credited for his work in two academy award winning films. He has contributed to Linux and open source projects since 1995. He is currently consulting for Movie Labs to implement a zero trust security architecture for content production.

Talks

Everything wrong with "AI" Security

Have you ever wondered what attacks on "AI" systems look like in the wild, what real adversaries care about (hint: it's not prompt injection), and why security researchers love MLOps software? In this talk we will discuss the standard ML development cycle and how to effectively attack each stage with both real world examples and overhyped "attacks". We will also cover a comprehensive analysis of exploits and vulnerability classifications and discuss strategies for mitigating supply chain risks, paving the way for a more secure and resilient "AI" ecosystem.

Sanjana Sarda (meap) currently leads Offensive Security efforts at an autonomous robot startup after focusing on security and privacy for ML systems at Stanford. Her research has previously been featured in Forbes and Vice's Motherboard and she has given talks at DEFCON, BSides, and Bumble (no comment).

Beginner Microcontroller Education: Teach Ethical Hacking on a Budget

Join Kody Kinzie for a talk on using microcontrollers for ethical hacking education! From his personal journey in hardware hacking to innovative teaching methods, Kody covers key challenges in microcontroller instruction, the transformative role of WebSerial and user-friendly languages like CircuitPython, and introduces the Nugget – a beginner-friendly microcontroller. Discover practical insights into the trade-offs of selecting and using devices like the ESP8266, Pi Pico, and ESP32s2 for educational purposes. The session concludes with real-world applications from hackerspaces and educational programs, offering a valuable perspective into the usefulness of low-cost microcontrollers for both hackers and educators.

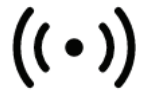
Kody Kinzie is a security researcher who specializes in open-source intelligence and Wi-Fi security. I teach cybersecurity to beginners on two popular YouTube channels called Hak5 and Null Byte, as well as organizing cybersecurity training and outreach events. I'm currently the host of the Hacking with Friends show on the SecurityFWD YouTube channel. I also enjoy putting together workshops on cybersecurity, computer science, and electrical engineering.

Talks

Automating DNS-01 The Less Lazy Way (with acme-DNS)

The ACME protocol used by Let's Encrypt and other Certificate Authorities is used for domain ownership validation and distributing zero-cost TLS certificates. While the HTTP-01 Challenge can be the easiest to deploy, the DNS-01 Challenge can be used to procure a certificate for non-HTTP services, internal services, or services requiring a wildcard certificate. However, automating the DNS-01 challenge requires a compatible DNS hosting service with an API, and may require storing your password or API credentials in cleartext on every server that you automate. The acme-dns project provides an alternate way to automate the DNS-01 challenge with any DNS hosting service, on a per-domain basis, while eliminating the need for administrative API credentials. It's extremely useful for Homelab users, but may also have a place in corporate environments without public-facing services.

Davie wasn't so much born as assembled in the Cisco factory. After a rogue network engineer gave him life, Davie set about finding his purpose in the real world. Traversing from subnet to subnet, he is always looking for new ways that he can bring his networks together, both IRL and on the net. His hobbies include building crazy live disks, ferret racing, and hanging out in trashcans.



Introduction to RF Demodulation

Over the last couple of years, I've been learning about and experimenting with how to take energy out of the air and convert it back into the original bitstream (the 1's and 0's; the data). This talk is a collection of that knowledge and walks through the signal identification and demodulation process, specifically for OOK in automotive key fobs. If this sounds interesting, you only need to bring your curiosity, no prior knowledge in the world of wireless data transmission. The first portion of this talk is brief primer in RF theory. This will be followed by a discussion of the hardware required to start doing this yourself and some practical demos against modern Chrysler and Honda key fobs going from pressing a button to seeing 1's and 0's on a screen. The last phase of this talk is a discussion of the current state of automotive security and interesting future areas of research where this learned knowledge can be applied.

Nate Singer is an experienced security engineer currently working primarily on cloud and web security for a large US-based silicon-valley tech company. He is interested in a variety of areas of technology, but has most recently been interested in cloud computing security and the integration of Large Language Models (LLMs). A recent core focus has been the secure usability of LLMs in vulnerability research and broader applications. At a much lower level, he continues to do some reversing and binary exploitation work, and if you find him at the conference feel free to ask about the 8-bit 16B computer he is building on breadboards.

Talks

Demystifying Static Analysis for Security Research

Program analysis, the examination of computer code to understand its behavior, is essential in developing Static Application Security Testing (SAST) tools that identify security vulnerabilities without executing the code. Static analysis tools are incredibly useful in application security. However, the typical program analysis literature is blurred with complex mathematical notations and formulas, intimidating even seasoned programmers. Moreover, much of the knowledge about building tools for examining code is buried in academic jargon. Yet, practical program analysis can be straightforward and accessible. You don't need a PhD to start developing tools that leverage program analysis techniques for uncovering vulnerabilities, modeling systems, and automating threat modeling and attack enumeration by analyzing source code. This talk aims to demystify the art of static analysis. We will talk about modern tools like Semgrep and CodeQL, and will learn how static analysis tools go with a special focus on Go. By the end of this session you will learn about modern static analysis tools like Semgrep and CodeQL and how you can use them for discovering new vulnerabilities. You'll have a clearer understanding of how static analysis tools function so you can better evaluate SAST tools You'll learn about various static analysis techniques, including Abstract Syntax Tree parsing, control flow analysis, and taint analysis. We'll explore how static analysis extends beyond finding bugs to automating threat modeling and attack surface enumeration, illustrating many of the concepts mentioned above. Join us to navigate the world of static analysis and empower your hacking skills!

Alex Useche is a security senior staff security engineer at FullStory. He has worked at companies like Trail of Bits, where he was the director of application security, and has written code for companies like Disney and Dell. Alex specializes in static analysis, application security, and Go.

Talks

LLM Prompt Engineering: A Toolkit for Hackers and other Geeks

Are you harnessing the full potential of Large Language Models (LLMs) in your cybersecurity strategies? Embark on a journey to explore the capabilities and inner workings of today's leading LLMs, including ChatGPT, BERT, and others. Discover how precise prompts can help you streamline tasks like drafting security policies, searching for information about CVEs, scripting in Python, and more. By perfecting your prompt engineering skills, you can enhance your ability to command AI, turning complex queries into clear, actionable insights. Are you ready to unlock the full potential of LLMs?

Corvus (aka Bronwen Aker) (M.S. Cybersecurity, GSEC, GCIH, GCFE) likes to describe herself as a "constantly evolving geek." She has worked with computers since elementary school when she was introduced to FORTRAN programming using bubble cards. These days, Bronwen works for Black Hills Information Security (BHIS) as a technical editor, AI researcher, and general plate-spinner, reading and editing pentest reports, giving webinars, writing blogs, and doing various other things here and there.

My Pal Rebeus

Come with us as we adventure into the forest as we tame the three-headed beast to request, forge, harvest, and roast our way to elevated privileges. First there was kekeo. now there's Rubeus. My new best friend. Rubeus is a toolkit developed to facilitate Kerberos interaction (and exploitation). In this talk, I'll be covering the various attacks Rubeus has implemented, from requesting, extracting, harvesting, and forging tickets to abusing delegation and kerberoasting. If there's time, we might even be able to cover detections!

cesi0: As a 15 year veteran of the security industry, I've lead forensic investigations, red team exercises, and currently hunt for threats for a managed detection provider. However, you can find me happiest while painting minis, in my garden, or bouldering.

Sponsors

Adaptable Connectivity

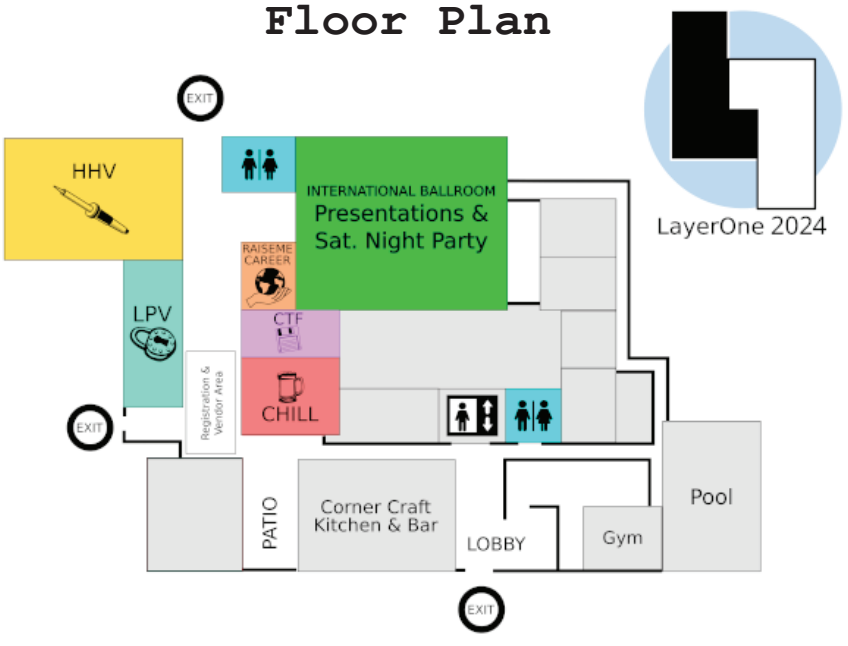
20 YEARS • LAYERONE

OWASP® Los Angeles

Eric DeSantis

ericdesantis.myportfolio.com

Floor Plan



Notes

Saturday, May 25

09:00 Registration opens & breakfast in San Gabriel Ballroom

09:45 Opening Remarks
- Capture the Flag begins.
- Tamper-Evident Contest and Soldering Olympics Begin.
- All Villages Open.

10:00 vyrus - The Silver Bullet Ecosystem & You!

11:00 Jack Baker - Evil ELFs and Dishonest DWARFs

12:00 Lunch Break

13:00 Merlin Corey – Python for Security Automation & Response
- AI CTF Begins

14:00 Angela Tsuboi (G4LXY) – Reverse Engineering Satellite Communications

15:00 Daryll Strauss - Kubernetes Security - What not to do

16:00 Sanjara Sarda (meap) - Everything Wrong with "AI" Security

18:00 Demo Party in the Hardware Hacking Village
HAM Testing in the Lockpicking Village

19:30 Banquet Dinner in the Main Speaking Room (International Ballroom)

Sunday, May 26

09:00 Registration opens & breakfast in San Gabriel Ballroom!

09:45 Opening remarks
All Villages Open.

10:00 Kodie Kinzie - Beginner Microcontroller Education: Teach Ethical Hacking on a Budget

11:00 Davie - Automating DNS-01 the Less Lazy Way (with acme-dns)
- Hebocon Robot Battles start in HHV

12:00 Lunch Break

13:00 Nate Singer - Introducing RF Demodulation

14:00 Alex Useche - Demystifying Static Analysis for Security Research
- Soldering Olympics Finals Begin

15:00 Bronwen Aker (Corvus) - LLM Prompt Engineering: A Toolkit for Hackers and Other Geeks

16:00 cesi0 - My Pal Rebeus

16:30 All contests end (even if they don't want to)

17:00 Closing remarks & contest winners

18:00 Afterparty at Null Space Labs