
LayerOne
May 24-25 2025

INTRODUCTION

Welcome to another great year of LayerOne! This year we have an awesome selection of talks, villages, contests, and events for you to participate in.This year's theme is GLITCH! We've glitched our shirts, our badges, and even some of the contests. The rest of the conference should be glitch free, however - if you experience any problems feel free to find someone in a staff shirt and let us know how we can help!

I'm particularly excited about this year's badge, which is a fully featured hardware glitching and fault injection tool! It also blinks, of course. This is one of our most ambitious badges, so show M and charlieX some love in the Hardware Hacking Village!

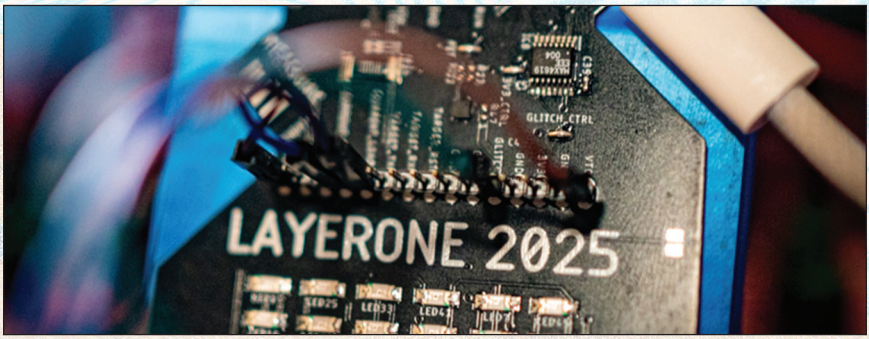
LayerOne is put together by a relatively small group of volunteers who work throughout the year to create fun stuff for you to enjoy. Show them some love! We know this year is a tough one on many fronts, so we appreciate you taking the time out of your busy schedules to join us.

Is it your first time at the conference? Awesome! 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

BADGES

The L1 Badge is more than just a conference keepsake, it's a fully functional fault injection platform designed for hands-on exploration of hardware security. Built around precision timing, crowbar glitching, and power path manipulation, this badge lets you experiment with voltage glitch attacks, glitch detection, and microcontroller fault tolerance. Whether you're a seasoned red teamer or new to embedded security, the L1 Badge provides a compact, hackable testbed for fault injection research, right from your lanyard.



CONTESTS + EVENTS

For more information about any of these events, contests, and villages, visit layerone.org/events

Capture the Flag

Competitive hacking and penetration testing event that runs throughout LayerOne. No sign-ups or qualifications – play, learn, and WIN!

The Intercept

The Intercept is a hardware Capture the Flag (CTF) event focused on testing your skills in hardware hacking, anti-tamper technologies, programming, and more!

Tamper Evident King of the Hill

Test your tampering skills in a contest against other attendees. Impress the judges to win and claim your crown as king of the hill.

Hebocon Robot Battles

Crush your opponents. Hopefully. Build the best worst robot you can in this tour de force robot battle!

Demo Party

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.

Ham Testing

Take your amateur Ham radio license tests at LayerOne!

VILLAGES

Lockpicking Village

10:00-17:00 Saturday and Sunday
The lockpicking village an area of the conference where attendees can learn about locks and how to open them. There will be mini-lectures and hands-on workshops throughout the weekend on various topics related to lockpicking, safecracking, and locksmithing.

Hardware Hacking Village

10:00-18:00 Saturday and Sunday
The Hardware Hacking village is where conference attendees can learn about electronics, soldering, and circuit design. Classes will be held throughout the weekend to teach you how to assemble the electronic L1 badge, get better at surface mount soldering, and how to design your own PCBs.

Chillout Room

A place to relax, chat, and socialize.

RaiseMe Career Village

10:00-17:00 Saturday and Sunday
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!

PARTIES

Saturday Night

This year's Saturday Night Party is a Game Night! Come enjoy the banquet feast, then roll with the best of them while enjoying the finest in both co-op and competitive board games. Feel free to bring your favorite board or card games to share with others! Banquet, fun, and games start at 7:30 PM on Saturday in the International Ballroom.

Sunday Night

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 25, 2025. 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.

TALKS

We'll Do It Live: Experiments in Self-Modifying Code – b0t

In the 1990s-2010, code self-modification was considered a must-have feature for malware to evade anti-virus products. After finding many much easier ways to evade anti-virus, the need for this fairly complex feature died out.

As with all things computer related, we have come full circle to relying on self-modification as a great way to avoid detection. We'll cover an example of a custom metamorphic code mutation engine. We will also explore additional limits of what is possible with code self-modification. We will answer the question of how feasible it might be to write code that can learn how to achieve a goal.

b0t *is a virtual machine enthusiast and helped create and run a free, public malware archive called VX-Underground from its inception. b0t also produced a hacking magazine called VX-Underground Black Mass. He has 7 years of professional security research experience.*

Keeping Things Local: Making Your Own Private LLM – Bronwen "Corvus" Aker

Ever wanted your own private version of ChatGPT? LLMs offer powerful capabilities, but not everyone is comfortable sending their data over the internet to Microsoft, OpenAI, or Anthropic. Fortunately, open-source tools make it possible to set up and customize a local, secure LLM on your own terms. From installation to customization, this talk will guide you through the process step by step, with demos to illustrate each stage. Itâ€™s time to build your own mini-Jarvis and start getting things done, efficiently, securely, and privately.

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 the dark ages when she was introduced to FORTRAN and bubble cards. These days, Bronwen works for Black Hills Information Security (BHIS) as a member of the Continuous Pen Testing team (ANTISOC), an AI researcher, and technical editor. When not working, she spends time playing with her dogs, LLMs, and studying data science.*

Revenge of the $ol $tealer$ - ce$i0

You just joined the Discord of your favorite influencer and you got a private message from them! It's your lucky day — they send over a link to receive a free airdrop of crypto tokens, just link your wallet. You click the url, follow the instructions, and just like that, your crypto wallet is drained. You've just been targeted by an impersonator and the link they sent is to a crypto drainer. We'll be going over some common tactics used by threat actors as well as deep diving into few samples of malware actively deployed. As a treat, we'll even dive into the op-sec failures of a particular actor and how I was able to track down their location.

Threat Hunter. Incident Responder. Security Engineer. All around degen. All of these titles fit **cesi0** *as a 15 year veteran of the security industry. cesi0 has performed forensics, malware reverse-engineering, threat detection, red teaming, and responded to all sorts of incidents. Returning to LayerOne for his 11th year, cesi0 brings extensive experience in all things relating to threat hunting and analysis.*

Covert Regional Communication with Meshtastic – Daryll Strauss

Meshtastic uses inexpensive LORA radios to create ad hoc mesh messaging networks that don't require centralized organizations or companies to operate. This makes them ideal for regional communications, and when configured properly, provides secure anonymous communications. Whether you want to chat with friends, share data among devices in the region, or want to perform highly covert communication in a group, this talk will give you all the information you need.

This presentation will discuss the fundamentals of LORA radio and mesh networking, the capabilities of Meshtastic, the hardware choices for running Meshtastic, how to configure Meshtastic for secure communications, an examination of additional threats to covert communication and what configuration options/techniques can be used to mitigate them.

I've been a technologist in Media and Entertainment for the last 30 years building visual effects studios and technology. My most recent work is focused on zero trust security architectures.

WINE for Video Game Hackers — Jack Baker

WINE, the Windows compatibility layer for Linux, has had a significant upsurge in the past few years, particularly amongst PC gamers. This has created a unique landscape for video game hackers, much of which isn't well understood by most developers. In this talk, we'll explore WINE internals and how both hackers and defenders can take advantage of them.

Topics include Windows/Linux operating system internals, anti-debugging tricks, and general video game hacking.

Jack *is a hobby video game hacker turned professional reverse engineer. In his day job, he's the game security lead of an indie studio.*

Introduction to Fault Injection - Joe Rozner

Fault injection has long been one of the primary methods for bypassing security controls and gaining code execution on secure chips. In recent years the cost of tooling, available information, and examples of attacks have exploded making it much more approachable. We'll explore the basics of fault injection, how it's used, available tooling, look at some real world examples, and provide resources to learn and gain more hands on experience.

After years leading the offensive security program at Yahoo **Joe** *co-founded Based Security where he can continue to yell about how terrible we are at identity and access control and maybe do something about it. Shout out to red team gang.*

Reverse Engineering Toys into Robots — Josh "savant" Brashars

I reverse engineered a life-sized animatronic Yoda holiday decoration and jammed in microcontrollers, sketchy SBCs, hoverboard parts, and more than a few zip ties.

Whether you're reverse engineering a piece of electronics, or breaking into the transportation network for a municipality, the processes is the same. This talk will walk through my workflow of identifying the goal (make a robot) and working backwards to a functional attack plan. I will demonstrate Robo YoYo's karaoke mode, utilizing voice cloning + deep fake tech, YoYo's agentic chatbot personality and not-at-all tiresome speech structure, YoYo's scratch built autonomous sled, enabling him to rove and dance (Automotive/Smart vehicle security), reverse engineering the control systems to drive the animatronics, OSINT techniques for datasheets, and hunting for non-destructive entry.

Former Red Team @ Apple, Amazon, Salesforce, Yahoo! Paranoids, Rivian Automotive, and more. Lifetime @dc949.

Microarchitectural Side Channel Attacks — m0zy

Processors are optimized for speed, efficiency, and parallelism — but these same design choices have introduced subtle and powerful security risks. Microarchitectural side channel attacks exploit the invisible behaviors of silicon: leaking sensitive data not through software flaws, but through the way hardware internally manages caching, speculation, prediction, and resource sharing. This talk will explore the current state of microarchitectural attacks and how they bypass traditional security boundaries. If you're interested in breaking systems at a layer most people ignore — or want to think like an attacker operating below the OS — this talk is for you.

m0zy *is a Principal Security Researcher with over a decade of experience in embedded systems and low-level software security. She specializes in building and breaking autonomous vehicles, cyber-physical systems, and IoT devices, bringing expertise in reverse engineering, vulnerability research, and exploit development.*

Boo Boo Runs Wild: Guerilla Open-Source Manufacturing - machinist

Last year, a bear broke into my kitchen window when my whole family was home. Luckily and without incident, she spooked and ran off before meaningful damage was done. I suppose this explains the industrial-grade electric fences some neighbors have in front of their doors. However, I've lived in the local mountains for many years, and this strikes me as unusual bear behavior. No bear arms in my kitchen, please!

Considering this problem deeply, I realized there are some CAD designs on the intertubes that could be useful in this regard. Using the dual magic of computers and caf-

TALKS

feine, we'll play with FreeCAD to manifest these designs into reality with a RepRap. I will explain some nuances of the processes regarding Geometric Dimensioning & Tolerancing, measurement, polymer choice, and slicer setup.

Using this toolchain, you too can make an infinite variety of custom hardware widgets to improve your life, whether it's organizing the spice rack or keeping the bears away.

You may remember me from previous LayerOne talks such as "3D printing our way to Skynet" and "Swords to Plowshares". I tend to talk about Computer-Aided-Design, and my background is a lifetime of hardware. I currently work with hardware that goes to space.

Securing AI Systems - Sam Bowne

Everyone is deploying chatbots and many other AI systems now, but few understand the security risks they cause. To understand the risks, you need to understand how AI systems operate–especially Large Language Models. These systems are not actually intelligent, but perform intelligence simulation, giving the appearance of knowledge without actually understanding anything they are saying. When you see how words are encoded, embedded, and transformed, you'll understand what LLMs are doing and why they hallucinate.

Several attacks and defenses are demonstrated, including prompt injection, evasion, poisoning, and deep neural rejection. This talk also covers security guidelines from OWASP, NIST, and the UK Government.

A CTF game is introduced so you can practice setting up AI systems, attacking, and defending them yourself. The game, with other materials including tutorials, slides, and videos will be available at samsclass.info after the talk for anyone to use.

Sam Bowne *has been teaching computer networking and security classes at City College San Francisco since 2000. He has given talks and hands-on trainings at DEF CON, DEF CON China, Black Hat USA, HOPE, BSidesSF, BSidesLV, RSA, and many other conferences and colleges. He founded Infosec Decoded, Inc., and does corporate training and consulting for several Fortune 100 companies, on topics including Incident Response and Secure Coding.*

Quantum Conundrums: Conquering Quomputing Challenges – Vincent Benzoni

Quantum computing poses a fundamental challenge to modern cryptography, but the reality of its impact is often misunderstood or exaggerated. This talk provides a clear, technically grounded overview of how quantum algorithms like Shor's and Grover's threaten widely used encryption schemes, including RSA, ECC, and certain symmetric ciphers. We'll review the current state of quantum hardware, assess realistic threat timelines, and evaluate which cryptographic systems are at risk—and which are not.

I'm **Vincent Benzoni***—aka Guillotine—Lead Cybersecurity Engineer at Hoag Hospital. Before I broke into cybersecurity, I spent years wiring up superconducting circuits trying to elaborate a quantum simulator aka the dumb brother of quantum computer for my PhD in Quantum Physics (proof I suffered https://theses.hal.science/tel-03611001). Now I build AI-powered detection systems, bend Microsoft Logic Apps almost to my will, and try automate everything that moves.*

Amped up for (Learning) Radio - wasabi

Forget high-powered transmissions—this talk is all about low-power radio (ISM) and making RF learning fun! We'll dive into interactive examples, including number stations and custom-built transmitters using the ever-reliable CC1101. Along the way, we'll share successes and challenges in getting students excited about radio, exploring what works (and what doesn't) when introducing RF concepts. Best of all, we'll have live demos to showcase just how accessible and exciting radio can be. Whether you're an educator, a hobbyist, or just RF-curious, this session is for you!

Wasabi *is a tinkerer of many things, security researcher, sometimes cloud engineer.*

SPONSORS

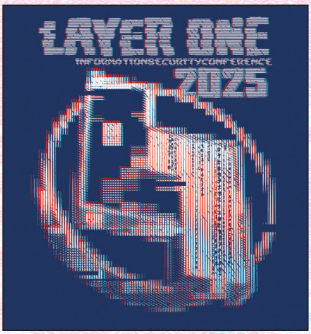
AdaptConn – adaptconn.com

OWASP
owasp.org/www-chapter-los-angeles

Information Systems Security Association
Los Angeles Chapter – issala.org

Eric DeSantis Illustrations
ericdesantis.myportfolio.com

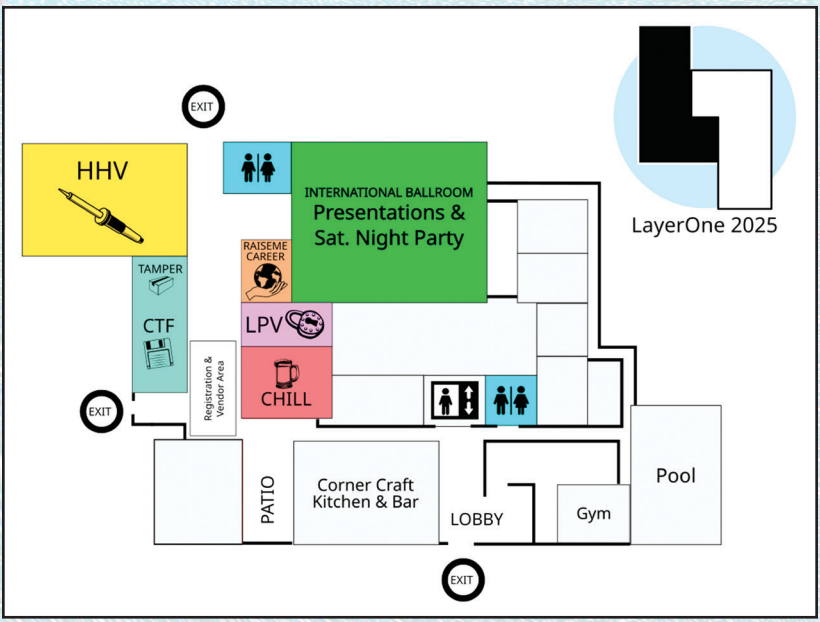
Adaptable Connectivity



OWASP® Los Angeles

Los Angeles Chapter ISSA
Information Systems Security Association

FLOORPLAN



SCHEDULE

Saturday – May 24

09:00 Registration opens & breakfast in San Gabriel Ballroom

09:45 Opening Remarks
Capture the Flag begins.
Tamper-Evident Contest begins.
The Intercept begins.
All Villages Open.

10:00 Joe Rozner – Introduction to Fault Injection

11:00 m0zy – Microarchitectural Side Channel Attacks

12:00 Lunch Break

13:00 Bronwen "Corvus" Aker – Making Your Own Private LLM
Hardware Hacking Village: Mehmet Sencan –
Self-Destructing Hardware Attacks (lightning talk)

14:00 Jack Baker – WINE for Video Game Hackers

15:00 Vincent Benzoni – Quantum Conundrums:
Conquering Quomputing Challenges

16:00 Daryll Strauss – Covert Regional Communication with Meshtastic

18:00 Demo Party in the Hardware Hacking Village
Amateur Radio License Testing in the Lockpicking Village

19:30 Banquet Dinner in the International Ballroom

Sunday – May 25

09:00 Registration opens & breakfast in San Gabriel Ballroom

09:45 Opening remarks
All Villages Open.

10:00 wasabi – Amped up for (Learning) Radio

11:00 Josh "savant" Brashars – Reverse Engineering Toys into Robots
Hebocon Robot Battles begins in Hardware Hacking Village

12:00 Lunch Break

13:00 Sam Bowne – Securing AI Systems

14:00 b0t – We'll Do It Live: Experiments in Self-Modifying Code

15:00 cesi0 – Revenge of the Sol Stealers

16:00 machinist – Boo Boo Runs Wild: Guerilla
Open-Source Manufacturing

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