LAYER ONE 2019

Pasadena California
May 24 - 26

Welcome to the sixteenth annual LayerOne Security Conference!

LayerOne is known for its hands-on approach to hacking and socializing. I hope to see you working hard in all the villages, participating in the contests, and making new friends! Just trying to relax? There's a Chillout Room to rest and play some games in between talks and contests. Don't learn by watching - learn by doing!

We're always interested in having new, exciting events at con. New for 2019 is the RaiseMe Career Village, an area dedicated to improving your resume and interview skills; a variety of new contests: The Intercept (Hardware CTF), Coffee Wars, Threat Hunting with Splunk CTF, and a WiFi mini-CTF. Please let me know what you think about these events and if you'd like to see more of them in future years!

CharlieX and MMCA of Null Space Labs have an insane badge design for this year. I say that every year, but this year is really gorgeous! There's a description of capabilities later in this program, so head there if you want to be wowed with what you can do with your badge. You're interested in hacking your badge, right? I thought so. Head over to the Hardware Hacking Village and build something that will wow us!

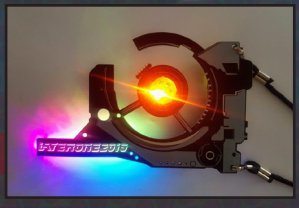
LayerOne is brought to you by three dozen extremely hard working volunteers, all of our fabulous sponsors, and YOU, our awesome attendees. So get out there: learn, do, and help others do the same!

- datagram

Badges

This year's badge is a Voight-Kampff machine, a very advanced form of lie detector that measures contractions of the iris muscle and the presence of invisible airborne particles emitted from the body. The VK is used primarily to determine if a suspect is truly human by measuring the degree of his empathic response through carefully worded questions and statements. Will you pass the test?

Features:
* Attiny2313A Processor
* LED Dome with 6 red LEDs
* 14 RGB LEDs
* Rechargeable 18650 Battery



Get your full facial recognition on with the extension kit that adds an ESP32 module, the OV2640 Camera, USB-C, and support for adding other components: MPU6050 (Accelerometer), BME280 (Humidity/Pressure Sensor), and an analog microphone. The extension kit is accompanied by a mobile application that interacts with the badge. Kits for the extended badge components are available for purchase in the Hardware Hacking Village! As always, top of the line soldering equipment is available in the HHV to build and hack your badge.

Head to https://www.layerone.org/badge for more details, software, and other info!

Villages

All villages are open from 10:00 - 18:00 Saturday and Sunday.

Lockpicking

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!

Hardware Hacking

The Hardware Hacking Village will be 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. 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!

Internet of Things (IoT)

The Internet of Things (IoT) Village is a special area of the conference where attendees can learn about the security of IoT and embedded devices through hands-on interaction with them. Sponsored by the LA hackerspace, Null Space Labs, security researchers and experts will be available to help you learn about IoT and embedded device security, walk through both hardware and software design of these devices, and demonstrate attacks against these devices. Attendees are encouraged to get their hands dirty taking these devices apart to learn what makes them tick. This year's focus is biomedical device security!

Chillout

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.

RaiseMe Career Village

New for 2019! 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, we'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.

Contests and Events

Capture the Flag

Capture the Flag is back! This year's contest is graciously hosted by the folks over at 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, and crypto.Participate now at http://layerone.ctf.land! Hang out in the Hacking Village to work with and heckle other CTFers!

Hebocon Robot Battles

Build 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. Visit the Hardware Hacking Village for full contest rules and restrictions for robot construction and operation. The Hebocon Battle Royale starts at 11:00 on Sunday 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! This year's contest is a King of the Hill format that runs all weekend long in the Lockpicking Village. Go visit the Lockpicking Village for full contest details and information on how to get started!

The Intercept (Hardware CTF)

New for 2019! The Intercept is a hardware Capture the Flag (CTF) event focused on testing your skills in hardware hacking, anti-tamper technologies, programming, and more! Your team plays a nation-state intelligence agency who intercepts a package. Your job is to reverse engineer and tamper with the device within to extract valuable data, implant backdoors, and attack other devices at the conference. What could go wrong? Maximum team size 5. Registration will be ON SITE, first-come first-served in the IoT Village.

Threat Hunting with Splunk CTF

New for 2019! Competitors will be searching for network attacks in data from a multi-server corporate-style network using a Splunk server, and they will also be deploying their own cloud servers, sending attacks, and detecting them. All challenges are freely available and will remain so after the event. This event will use BOSS OF THE SOC data published by Splunk, Google Cloud, Suricata, Drupal, and Metasploit. The Threat Hunting CTF takes place on Sunday, May 26th, 2019 at 14:00 in the Lockpicking Village! This event is graciously hosted by Sam Bowne! 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 DEFCON, HOPE, B-Sides SF, B-Sides LV, BayThreat, LayerOne, Toorcon, and many other schools and conferences.

WiFi CTF - Catch the Chicken Man

New for 2019! The Chicken Man Game is a low-cost WPA2 password cracking game designed by computer science students Kody Kinzie and Brandon Paiz at Pasadena City College to be a safe, reactive target for teaching Wi-Fi security.
The Chicken Man runs Saturday and Sunday, May 25-26, 2019 and can be found in the Hardware Hacking Village. The Chicken Man is graciously hosted by Pasadena City College's Leadership in Technology (@LITpcc) group!

Coffee Wars

Do you have a favorite coffee? Put it to the test and have it blindly judged by a panel of LayerOne attendees! Bring your favorite coffee in ground or bean form, and we'll put it in a bracket against other contestants. All coffee will be brewed in the pour-over method and served black. Coffee Wars takes place in the Hardware Hacking Village on Saturday, May 25, 2019 at 13:00. Come join us for an after-lunch coffee!

Contests and Events

Hebocon Robot Battles

Build 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. Visit the Hardware Hacking Village for full contest rules and restrictions for robot construction and operation. The Hebocon Battle Royale starts at 11:00 on Sunday in the Hardware Hacking Village!

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! Ham testing (including license upgrades) begins at 6:00 PM on Saturday in the Lockpicking Village. Bring $14 (cash only) and two forms of ID (one should be a government issued photo ID, such as a driver's license).

Demo Party

Creating a "demo" is a challenge that requires you to be fluent in programming, optimization, 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. At the same time, you're wowing your audience with an impressive and entertaining demo! This year's Demo Board runs a PIC24FJ256DA206 chip with the following specs: 16Mhz, 16-bit; 96Mhz GFX Core (CLUT, Fonts); 96K SRAM; 256K FLASH.
Brought to you by Arko of Null Space Labs, the LayerOne Demo Party begins on Saturday at 18:00 in the Hardware Hacking Village.

Saturday Night Party

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 live jazz and blues music. Feel free to bring your favorite board or card games to share with others! Banquet, Games, and live music starts at 8:00 PM on Saturday in the International Ballroom.

Sunday Night After Party

Our good friends at the 23b Shop Hackerspace in Fullerton, CA host the official LayerOne afterparty! Come join us for shenanigans, barbeque, and more! The afterparty starts at 6:30 PM on Sunday, May 28, 2017. The 23b Shop is located at 418 E Commonwealth Ave, Fullerton, CA 92832.

Speaker Bios

Amber Welch - Until she's accepted for a Mars mission, Amber's goal is to advance data protection and personal information privacy as a Privacy Technical Lead for Schellman & Company. Amber been assessing corporate privacy compliance programs for the past year and prior to that, managed security and privacy governance for a suite of SaaS products. She has previously worked in companies creating ERP, CRM, event planning, and biologics manufacturing software.

Chloe Messdaghi is a Security Researcher Advocate/PMM @Bugcrowd. Since entering cybersecurity space, she sees security as a humanitarian issue. Data breaches don't just impact companies, but governments, environments, and people. Her previous and current humanitarian passion has led her to become passionate about cybersecurity. Chloe has advised as a UN Volunteer and served as a board member for several humanitarian organizations. Chloe is also the head of WIST organization, a mentor and advocate for inclusion in tech, and founded a nonprofit called Drop Labels.

Chris Schafer started in infosec 7 years ago playing CCDC. Since then, he's worked extensively with logging, SIEMs, automation, and malware. His greatest professional goal is automating himself out of a job.

Christina Lekati is a Social Engineering expert and ethical human hacker. With a background in Psychology, she learned the mechanisms of behavior, motivation, decision making, as well as manipulation and deceit. She became particularly interested in human dynamics and passionate about social engineering. Her writings on social engineering strategies earned her a distinction during her master studies. She is currently working with Cyber Risk GmbH, a provider of cyber security training programs, as a social engineering expert and trainer.

Fotis (@ithilgore) Chantzis is a principal information security engineer at Mayo Clinic, where he manages and conducts technical vulnerability assessments on medical devices and clinical support systems. He has been a contributor to the Nmap project since 2009, when he wrote the Ncrack network authentication cracking tool, which he still maintains, and has published a video course on "Mastering Nmap". His research on network security includes exploiting the TCP Persist Timer (published on Phrack #66) and inventing a new stealthy port scanning technique by abusing the popular XMPP. His most recent research focus has been on medical device & IoT security.

Funsized is an EE by day, and... still an EE at night. He enjoys building robots and cooking. Sometimes these hobbies are combined in terrifying and delicious ways.

Geoffrey Janjua is the founder of Exumbra Operations Group is a former US DoD civilian with 12+ years of operational field experience conducting offensive computer operations. He is currently conducting full-scope penetration testing, vulnerability research and exploit development of high-value products for a Fortune 500 company, has identified multiple zero-days, and holds many security related industry certifications to include OSCP, GPEN, CEPT, CPT, ECSA, CEH, and CRT.

IrishMASMS (@IrishMASMS) is an old school hacker, fighting the good fight in Computer Network Defense (CND)/blue team efforts for over 19 years. Panel member at HOPE 5, presenter at a couple of Notacon's,

Speaker Bios

LayerOne, Toorcon, Bsides, and some other conferences that are hard to remember or may lean on the more professional side. Having progressed through the ranks to hiring manager and director level, he has experienced the pain from both sides of the hiring process and desires to improve the situation for the InfoSec community.

Jason spent nearly 15 years as an intelligence officer: designed, executing, and managing offensive cyber and technical operations all over the world. He left the government in 2017 and is working to deprogram as quickly as possible, and is helped in this endeavor by coffee and red wine. He is currently the Vice President for Advanced Security Concepts at eSentire.

Justin Bui (@slyd0g) is an Operator at SpecterOps and has experience performing penetration tests, red team engagements and web application assessments. He is passionate about all things security and helping organizations improve their security posture. Justin enjoys writing code, developing offensive tools and blogging security stuff at https://medium.com/@slyd0g
machinist is the Dr. Dolittle of robots.

Ravin Kumar is an engineer and data expert. He's deployed machine learning models in production and writes production-grade software.
Marcus has been working in information security over 12 years and currently hacks at Somerset Recon. He actively host and participates in capture the flag hacking competitions and enjoys reverse engineering, exploit development, lock picking, SCADA security, embedded device hacking, web hacking and mobile application hacking.

Brett (Security Panda) is a Breaker of Web Applications, Leader of a DefCon Group, Maker of Tasty Food, and Owner of a Majestic Beard. He has over 17 years of experience in IT and Security, specializing in Web Application Pentesting, PCI practices, vulnerability scanning, and management.

Tigran (th3CyF0x) Terpandjian is presently an Incident Handler. He has been fascinated with languages, cultures, social psychology, military tactics and history since childhood. Despite a degree in international relations, he stumbled across Cyber Security and decided to pull the trigger and tumble down the security rabbit hole. Along the way, he was beset by the beasts of Compliance (FedRAMP) but found his banner under Red Teaming. Tigran enjoys applying red teaming concepts to conduct threat hunting and is passionate about emulating an adversary. He also loves playing tennis and is an avid practitioner of Krav Maga.

Vyrus (@vyrus001) has been associated with a variety of subjectively nefarious entities and or projects that include but are not limited to, OCTF, Thotcon, BsidesLV, HOPE, BlackHat, BalcCon, LayerOne, ShmooCon, Ceaser's Challange, You Shot The Sharif, BerlinSides, Bsides Knoxville, and ToorCamp. While almost the entirety of his skillet is still hidden from public disclosure, he has been implicated, though never charged, in over a dozen other confidence schemes and frauds.

wasabi: Perpetual researcher, tinkerer of electronics, builder of competitions, and experimenter of IoT.
bluescreenofwin: Senior windows system administrator, maker of beer, and enthusiast Windows hacker. Beer, binary, Battlestar Galactica.

Talks

The SEArt of War: The Chimaera Threat Model - Christina Lekati & Tigran Terpandjian

In recent years, "red teaming" has become a market buzzword often prompting corporate excitement and weaving an image of "pentesting" in a red cape. This is unacceptable. In the talk we will discuss how "red teaming" is not limited to the digital arena alone but includes physical and social vectors that should be considered for an effective operation. We will expand on Dr. Mark Mateski's concepts by applying both of them respectively to analyzing the character Grand Admiral Thrawn from the Star Wars universe and the way he successfully does his threat profiling and fusion of intelligence from a diverse number of sources. The parallelism with Grand Admiral Thrawn is considered to be an entertaining yet representative example of applying critical thinking in gathering and analyzing intelligence and conducting threat profiling. Examples from the real world will be provided throughout the presentation as well, showcasing how the elements discussed in the CHIMAERA model have significantly contributed in past cases. Lastly, participants will have the option to participate in a "debrief". Participants will be provided with certain threat actors and they will be given a few minutes to research and to think critically to figure out why those threat actors do what they do, not in terms of the TTPs but in terms of their motivations, rationale, etc.

Tracking and Blocking Malware Distribution with Automation- Chris Schafer

This talk will conduct an analysis of one of the most effective Malware Distribution Networks being used today, form inferences on their distribution methods based on the behavior, and determine how to automatically block those distribution methods (preventing distribution of the malware samples). This process includes automatic collection of the malware being distributed, identifying additional downloaders, and analyses (both static & dynamic) of the stage 1 payloads and stage 2 malware samples.

Network Exploitation of IoT Ecosystems - Fotios "Fotis" Chantzis

Internet of Things (IoT) ecosystems are comprised of a large variety of connected devices that are rife with "smart" features and textbook vulnerabilities. IoT devices are usually embedded with low-energy and low processing capabilities, deprioritizing security robustness as a result. In this talk we are going to present techniques and attacks on network protocols and insecure implementations commonly found in IoT ecosystems. We are going to explore how penetration testers can abuse zeroconf networking protocols like UPnP, mDNS, WS-Discovery and others to conduct a variety of. Other IoT security angles will be explored as well: from the default insecurity of video streaming protocols like RTP, heavily used by networked cameras, to the growing usage of IPv6 and what that entails in terms of the security posture of the IoT world.

Chip Decapping on a Budget - Funsized

Introduction to IC decapping including why it's interesting, standard methods used in industry and how to do it at home without asphyxiation or explosions. Presentation will conclude with photos of decapped ICs.

Let's Talk About WAF (Bypass) Baby - Security Panda

All modern Web Application Firewall are able to intercept (and even block) most common attacks from the web. However, what happens when an attacker uses HTTP2 to send attack traffic to a web application or service? In this talk we will cover basic attacks against web applications and services using HTTP2 to bypass WAFs and Proxys. Attendees will gain knowledge of how to bypass WAF and Proxies using the HTTP2 Protocol, and steps they can take to protect themselves against these kinds of attacks.

How to Fix the Diversity Gap in Cybersecurity - Chloe Messdaghi

Women make up just 11 percent and minorities are slightly less than 12 percent of the cybersecurity workforce. I've connected with persons who are underrepresented in the field, and many after spending years in cybersecurity are

Talks

leaving the field. From their shared experiences as well as my own, it is clear that the cybersecurity space needs to get real about the lack of diversity in the space. In this talk we will discuss our brains and how we label and prejudge, hear experiences of underrepresented people in the space, what can be done to fill the gap, and how to increase and retain the number of qualified candidates in cybersecurity.

Data Access Rights Exploits under New Privacy Laws - Amber Welch
New privacy laws such as the GDPR and CCPA have been great advances for personal data rights, although the ability to request access to all the personal information a company has on an individual has created new attack vectors for OSINT. This talk will discuss the personal data access options required in different regions, how most companies respond to data access requests, and the most effective exploits for privacy vulnerabilities. We'll explore the psychology driving corporate responses to requests and ways these emotions can be exploited. Best practices for identifying data subjects, minimizing the data released, and legally denying abusive requests will be covered. Key sections of the laws you need to know for exploits and defense will be highlighted.

Competing for the Future: Building and Automation InfoSec Competitions - Wasabi
Ever wonder what it takes to build an InfoSec? This talk will cover the Western Regional Cyber Defense Competition and the efforts we have put into building a more realistic and challenge competition through custom tooling, infrastructure, and applications that we have been building into our competitions. Some of the things we will be covering include using modern tools such as Ansible in combination with our agent "Mr. Smith" which can allow for a highly scalable competition, and how to build and deploy usable ICS systems quickly for competitions.

Hashes to Ashes: Life & Times of Clandestine Infrastructure - Jason Kichen
Exploits and implants get all the press, but infrastructure is the bedrock for APT actor operations. It's the first thing created, the last thing destroyed, and the costliest to have caught, exposed, or otherwise burned. Clandestine operations infrastructure possesses an extreme complexity, and this talk aims to describe and explore that complexity in detail. By examining the complexity of APT actor operations from the perspective of their infrastructure, including highlighting the complexity involved alongside a real-world example, this talk help network defenders improve their understanding of the threat landscape and perhaps give ideas for red teamers as well.

Tales from the Lockpicking Village - Marcus Richerson
This talk will cover a variety of techniques utilized to defeat locks and physical security mechanisms, stories about lock picking villages and provide tips and tricks for hosting a successful lockpicking village.

Swords to Plowshares: Repurposing the Ghost Gunner - Machinist & Ravin Kumar
In this talk machinist and Ravin look under the hood of the Defense Distributed Ghost Gunner, a very capable desktop-sized CNC mill designed specifically for creating firearms. The overbuilt hardware of the Ghost Gunner lends itself to being a versatile, generalized tool. With some clever code and implementation, this machine is transformed into a more useful, and less legally-sketchy CNC mill.

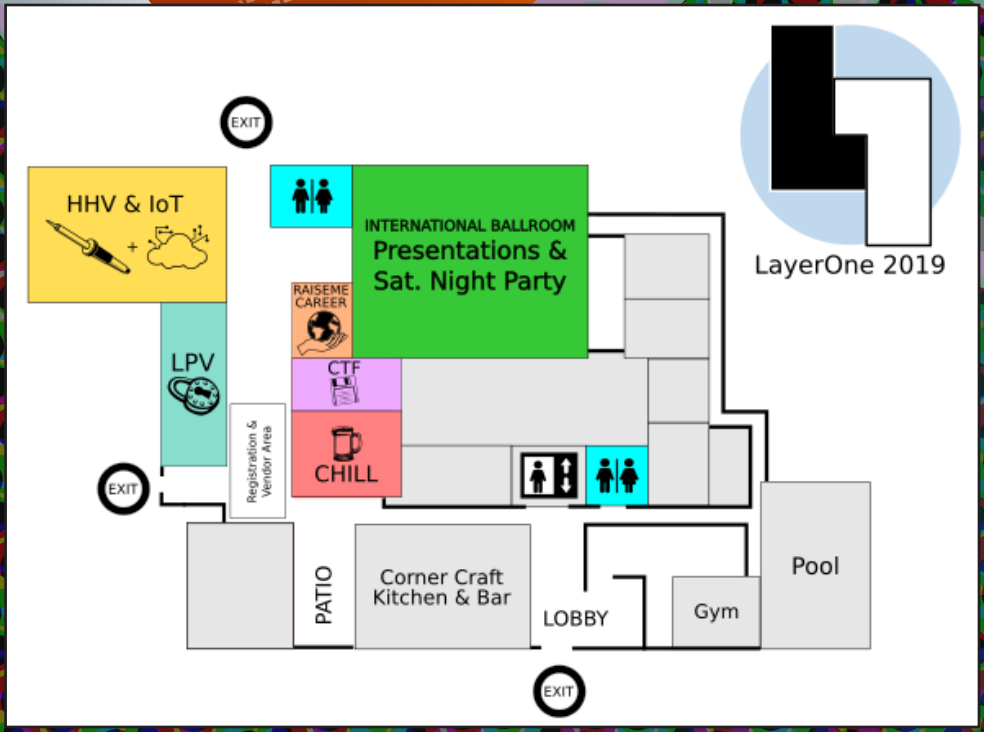
Digital Forensics is not just for incident response anymore - IrishMASMS
When leveraging digital forensics, there are opportunities to let the data tell the story beyond our incident response efforts. Let the story provide insight on the risks your organization face, provide insight on how to mitigate, and provide the evidence to take the actions needed. What sort of organizations and what sorts of use cases are there; and what real world examples have organizations been able to leverage digital forensics to identify and manage their risks?

InfoSec Industry Panel Q&A

The InfoSec Industry Panel is a live Q&A session where audience members can ask questions to a panel of information security professionals with many years of experience between them. Audience members will have the opportunity to ask security professionals open questions on their careers, the security industry, and anything in between! This year's panel is focused on red teaming, penetration testing, exploit development, and other offense-related industry positions.

The panel will be made up of infosec industry experts Geoffrey Janjua, Fotis Chantzis, Justin Bui, and Vyrus.

The InfoSec Career Panel takes place on Saturday, May 25, 2019 at 3:00 PM in the Lockpicking Village.



Schedule

Saturday

09:00 - Registration opens & Continental breakfast!

09:45 Opening remarks

10:00 - Christina Lekat & Tigran Terpandjian - The SEArt of War: The chimera Threat Model
- Tamper-Evident King of the Hill begins.
- Capture the Flag begins.
- All Villages Open.

11:00 - Chris Schafer - Tracking and blocking malware distribution with automation

12:00 -Lunch Break
-Lockpicking Village: Intro to Lockpicking

13:00 - Fotis Chantiz - Network Exploitation of IoT Ecosystems
- Coffee Wars in the Hardware Hacking Village

14:00 - Funsized - Chip Decapping on a Budget

15:00 - Security Panda - Let's Talk about WAF (Bypass) Baby
- Lockpicking Village: Intro to Lockpicking
- InfoSec Career Panel begins.

16:00 - Chloe Messdaghi - How to Fix the Diversity Gap in Cybersecurity

17:00 - Demo Party begins in Chillout Room.

18:00 - HAM Testing begins in Lockpicking Village.

20:00 Saturday Night Dinner & Party

Sunday

09:00 - Registration opens & Continental breakfast!

10:00 - Amber Welch - Data Access Rights Exploits under New Privacy Laws

11:00 - Wasabi - Competing for the Future - Building and Automation InfoSec Competitions
- Hebocon Robot Battle Royale begins in Hardware Hacking Village

12:00 Lunch Break
- Lockpicking Village: Intro to Lockpicking

13:00 - Jasen Kirchen - Hashes to Ashes: Clandestine Infrastructure

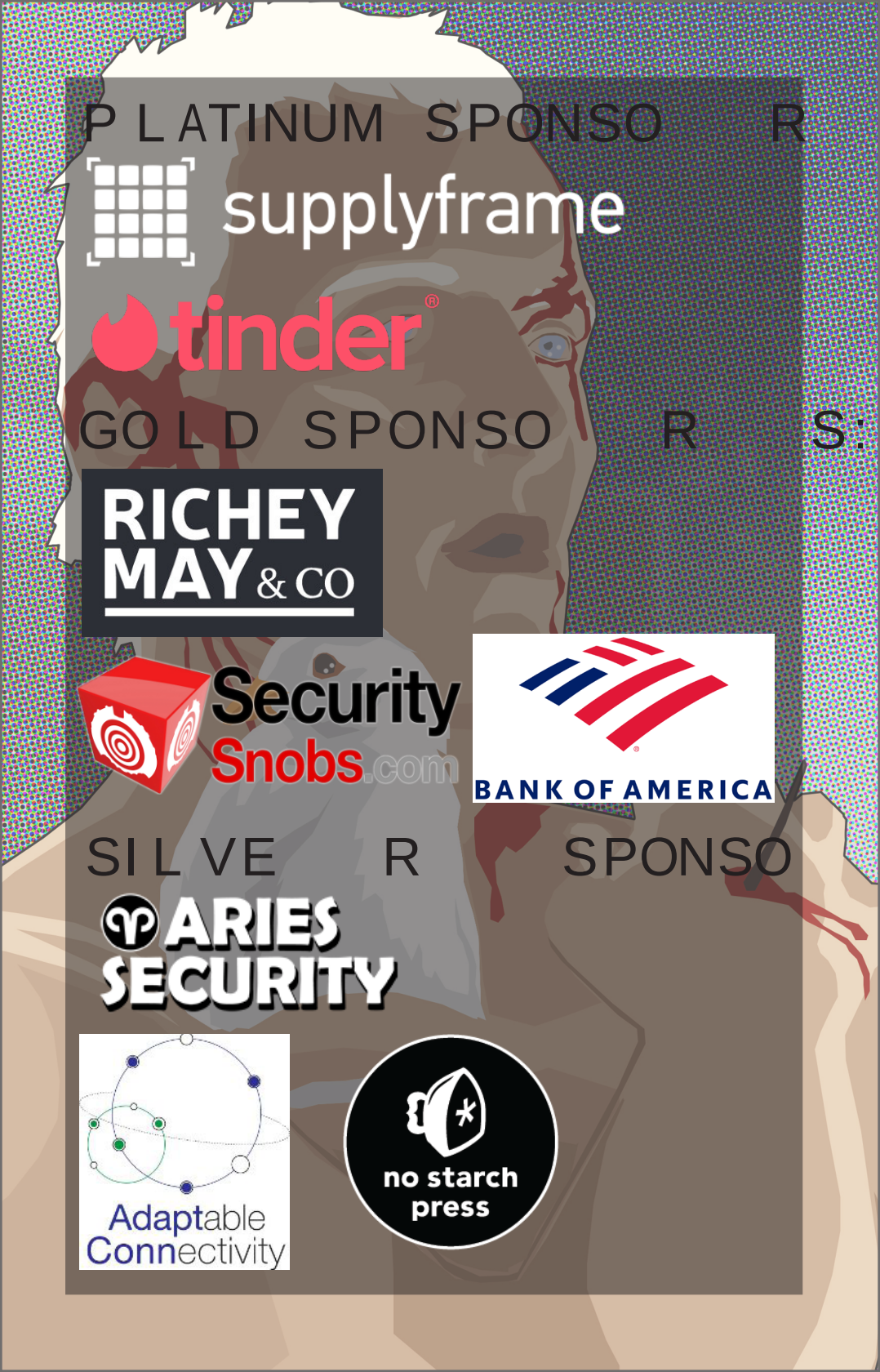
14:00 - Marcus Richerson - Tales from the lockpicking village
- Lockpicking Village: Threat Hunting CTF

15:00 - Machinist & Ravin Kumar - Swords to Ploughshares: Repurposing the Ghost Gunner

16:00 - IrishMASMS - Digital Forensics is not just for incident response anymore
- Tamper-Evident King of the Hill ends.
- Capture the Flag ends.

17:00 Closing ceremonies

18:00 - After Party at the 23b Shop


PLATINUM SPONSOR
supplyframe
tinder
GOLD SPONSORS:
RICHEY MAY & CO
Security Snobs.com
BANK OF AMERICA
SILVER SPONSOR
ARIES SECURITY
Adaptable Connectivity
no starch press