THE LOST POLICYMAKER'S GUIDE TO

Hacker Summer Camp

POLICY PASSPORT

2019 LAS VEGAS, NEVADA, USA

DEFCON / BSIDES / BLACKHAT

TIPS, RESOURCES, MAPS

LOSTPOLICYMAKER.ORG
#LOSTPOLICYMAKER
@LOSTPOLICYMAKER

I AM A HACKER, ENTER MY WORLD...

lostpolicymaker.org
#lostpolicymaker
@lostpolicymaker

(The Hacker Manifesto, see page 29.)

Table of Contents

Table of Contents 3
Quick Reference 4
About the Authors 8
Highlights 10

Getting Started

The Conferences 18
Black Hat 19
August 3-6, 2019 TRAININGS
August 7-8, 2019 BRIEFINGS

BSides Las Vegas 20
August 6-7, 2019

DEF CON 21
August 8-11, 2019

Hacker Culture and History 23

Planning and Information 32
Health and Safety 35

Itineraries 38
DEF CON Villages 41
Side Events & Parties 45
Quick Look Checklists 48

Quick Reference

CAVEAT LECTOR

For those who prefer the BLUF (bottom line up front) model, we created a quick reference guide to help you get the main points necessary for a productive, and painless, hacker summer camp experience. Unless you prefer trial by fire (which we highly recommend against), we figured it best to equip you with some tools if you decide to read nothing else in this guide.

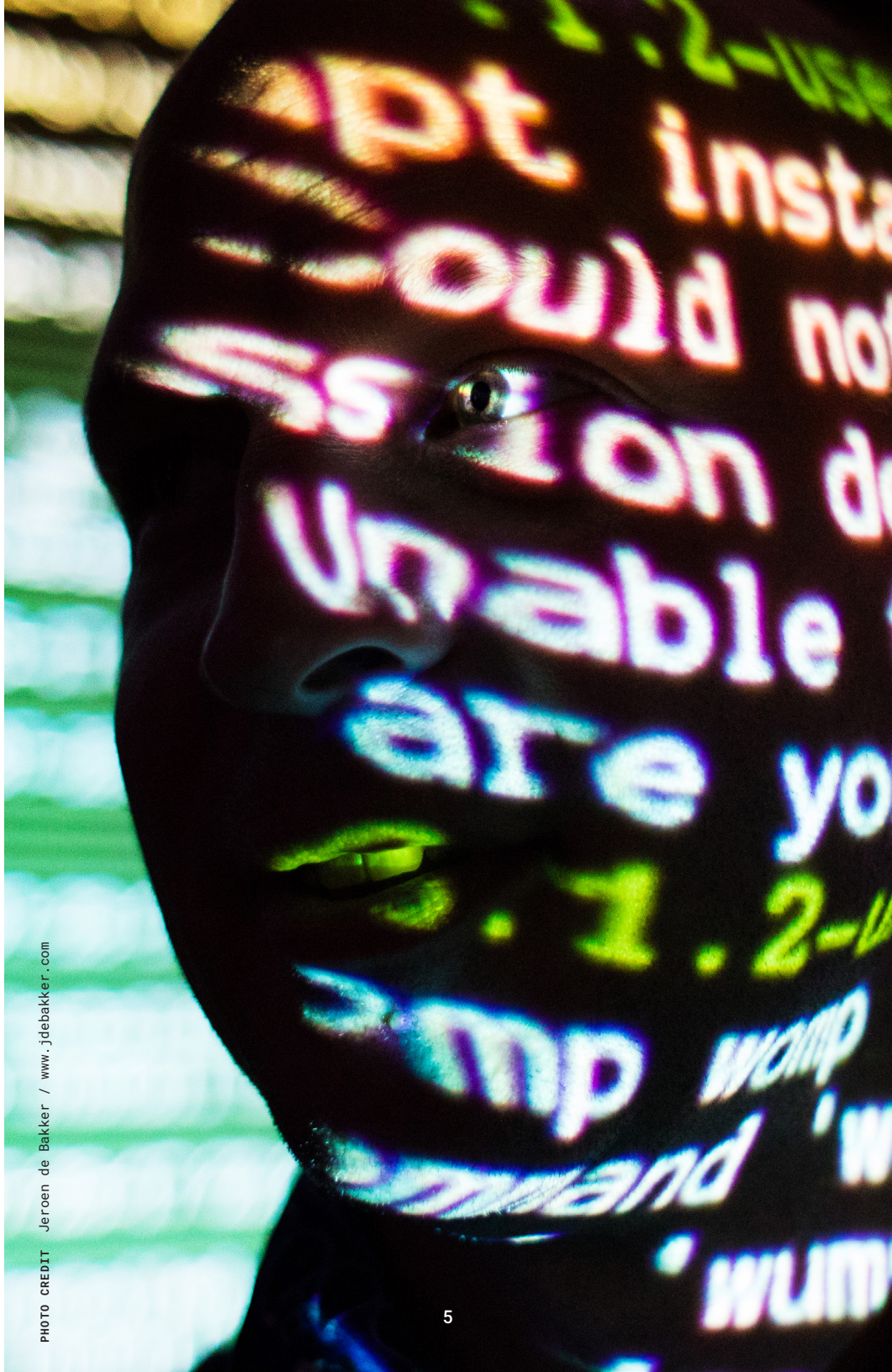
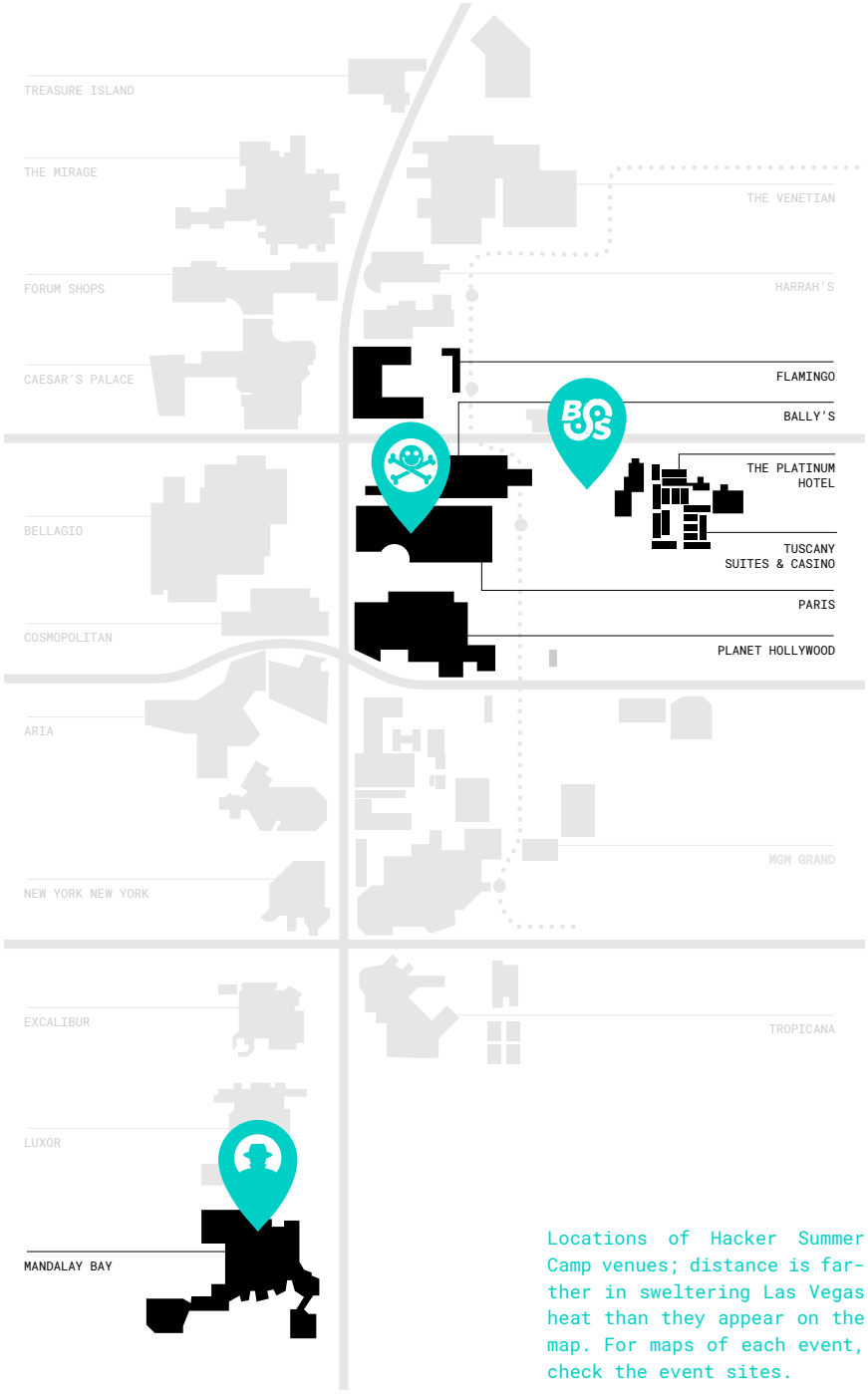


PHOTO CREDIT Jeroen de Bakker / www.jdebakker.com



Locations of Hacker Summer Camp venues; distance is farther in sweltering Las Vegas heat than they appear on the map. For maps of each event, check the event sites.

Important Dates + Locations

Las Vegas is in the Pacific Time Zone. The weather in August averages from 75-105ºF (25-40ºC) with 1 day of rain. The terrain is flat desert, with little shade.

BSides Las Vegas
August 6-7, 2019
Tuscany and Platinum Hotels

BlackHat USA
August 3-6, 2019 TRAININGS
August 7-8, 2019 BRIEFINGS
Mandalay Bay Hotel

DEF CON XXVII
August 8-11, 2019
Paris, Bally's, Planet Hollywood, and Flamingo Hotels

Before You Go

> Update all your technology
> Buy and test a new, clean phone, with new accounts (optional)
> Register for conference secure wifi
> Prepare to stand and walk a lot (bring comfy shoes)
> Rest up for a few days before
> Earmark some talks, villages, and events
> Schedule time to eat and sleep
> Bookmark defconparties.com
> Download the Hacker Tracker app (Android, iOS)
> Pack: ear plugs, sunscreen, shorts, sunglasses
> Check out some Hacker Films (see p. 27)
> Join and participate in the DEF CON Forums[1]

[1] https://forum.defcon.org/

About the Authors

Who we are, why you should trust us. The authors come from diverse backgrounds and perspectives. Authors are selected from among the many individuals who bridge the gap between the hacker and public policy communities. In addition to the authors, many others contributed to drafting this document and we greatly appreciate their efforts!

Heather Blanchard

@poplifegirl / #defconpolicy

Heather works on global innovation and ecosystem strategy and outreach for the wireless industry in San Francisco. She is the co-founder of CrisisCommons, a digital humanitarian community and served the U.S. Department of Homeland Security from 2003–2010, including as Business Liaison Director of Technology and Telecommunications for the Private Sector Office and external advisor to the DHS Silicon Valley Office. Since leaving government in 2010, Heather has volunteered as a Press Goon for DEF CON.

Allan Friedman

@allanfriedman

Allan Friedman is Director of Cybersecurity at National Telecommunications and Information Administration in the US Department of Commerce. Prior to joining the Federal Government, Friedman spent over 15 years as a noted InfoSec and tech policy scholar at Harvard's Computer Science Department, the Brookings Institution and George Washington University's Engineering School. He is the co-author of the popular text 'Cybersecurity and Cyberwar: What Everyone Needs to Know,' has a degree in computer science from Swarthmore College and a PhD in public policy from Harvard University, and is quite friendly for a failed professor-turned-technocrat.

Ayan Islam

@ayanmislam

Ayan enjoys leveraging her multi-disciplinary skill set (legal, policy, and stakeholder engagement) to solve problems and advance causes that improve public safety. She is a member of I Am The Cavalry (IATC) and the Cybersecurity and Emerging Technologies Working Group for the Women of Color Advancing Peace and Security (WCAPS). On the IATC scale[2], Ayan is a Puzzler and Protector.

Andrea Little Limbago

@limbagoa

Andrea is the Chief Social Scientist at Virtru. She has taught conflict studies in academia, was a technical lead in the Department of Defense, and most recently has worked at several startups integrating social science methods for analyses on attacker trends, human-computer interaction, digital authoritarianism, and security culture. Andrea earned a PhD in Political Science from the University of Colorado at Boulder and a BA from Bowdoin College.

Whitney Merrill

@wbm312

Whitney is a privacy and information security attorney and technologist. Previously, she served in government as an attorney at the Federal Trade Commission, where she worked on a variety of consumer protection matters including data security, privacy and deceptive marketing and advertising. She was also a member of the NSF's CyberCorps. She also runs the Crypto & Privacy Village, which appears at DEF CON and BSidesSF.

Beau Woods EDITOR + COORDINATING AUTHOR

@beauwoods @iamthecavalry

Beau wears a lot of hats, all white. He has hacked medical devices, won Best Mustache at Movember London, evaded Mafiosi near Moscow. Beau is also a leader with I Am The Cavalry, an Atlantic Council Fellow, DEF CON Goon, Village organizer, BSidesLV staff, has a BS in Psychology from Georgia Tech, and lives in DC.

lostpolicymaker.org
#lostpolicymaker

[2] https://iatc.me/motivations

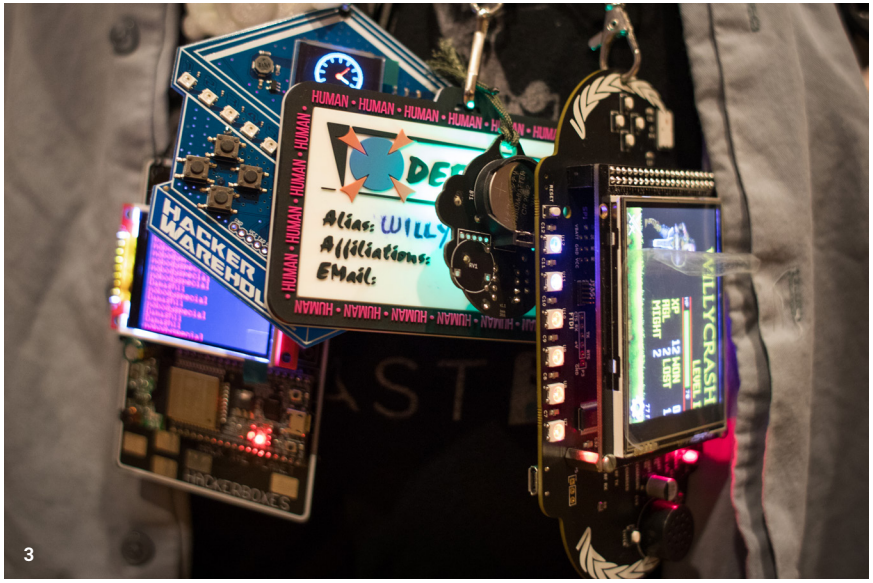
Highlights

PHOTO CREDITS @astcell / @MrB0t

1 LINE CON / With tens-of-thousands of people at the events, long lines are virtually guaranteed. These are some of the best places to meet people and strike up a conversation and a friendship. **2 VENDOR AREA /** Vendors at each event are very different! **3 BADGES /** Badges and bling make for cool decorations and some can serve as status symbols. The #badgelife trend sees electronics manufacturers, puzzle designers, and hobbyists turning out pieces of art for participants to enjoy.

PHOTO CREDITS @astcell

PHOTO CREDITS Jeroen de Bakker / @astcell



3

4

5

4 CONTESTS / Hackers learn and compete in puzzles, games, and challenges that put their skills and knowledge to the test. The Capture the Flag (CTF) competition at BSides Las Vegas has dozens of competitors and teams. Light-hearted contests like the Tinfoil Hat Contest engage creative spirit, regardless of technical capabilities. **5 VILLAGES /** These self-contained, subject-specific spaces within the DEF CON event host a variety of contests, talks, and other content. There are often long lines to participate.

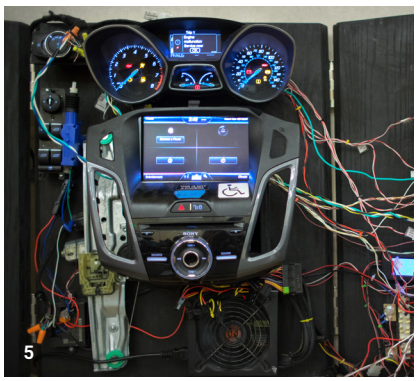

5

PHOTO CREDITS Jeroen de Bakker / @MrB0t

PHOTO CREDIT Jeroen de Bakker / www.jdebakker.com

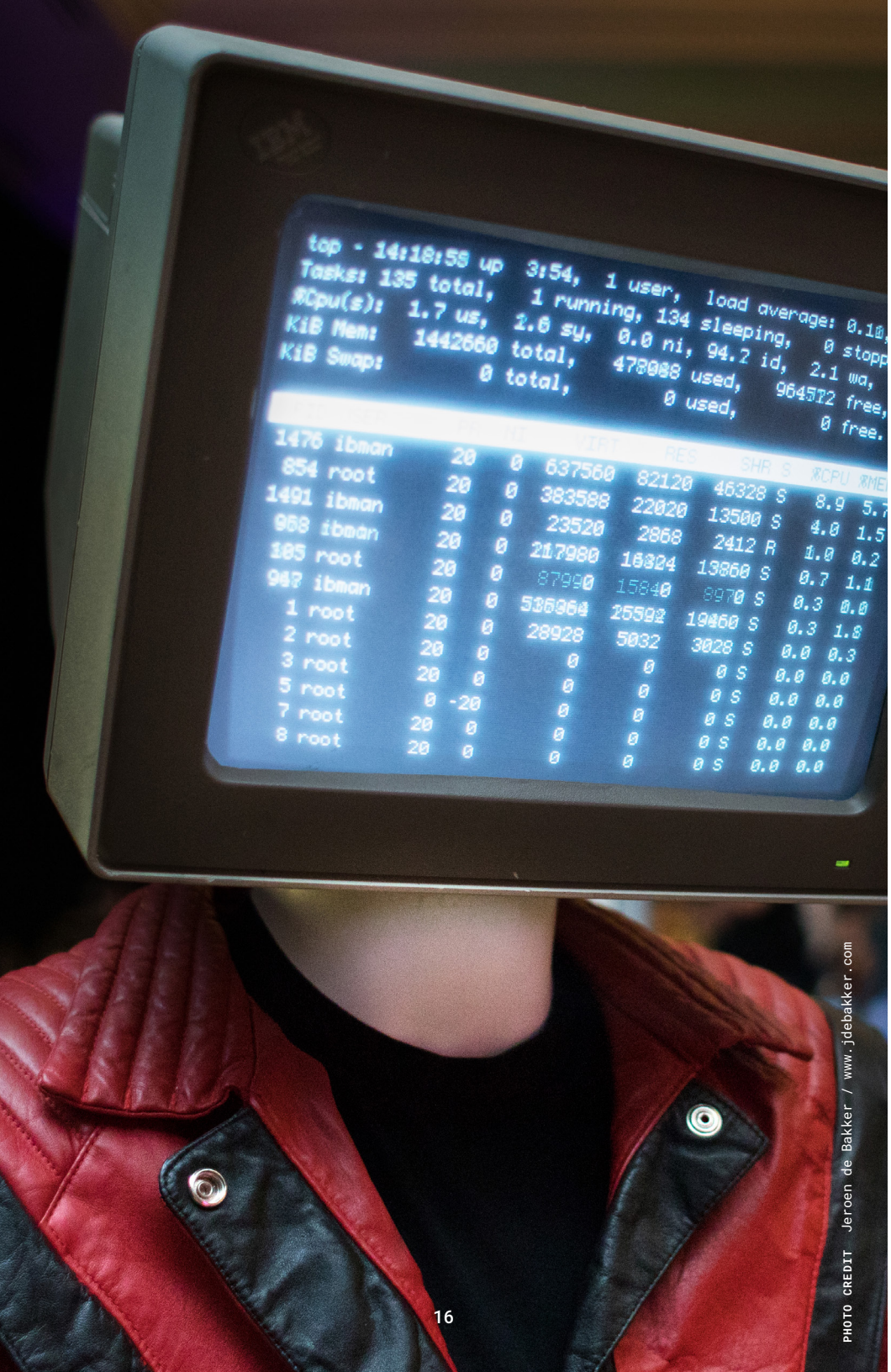


PHOTO CREDIT Jeroen de Bakker / www.jdebakker.com

6 GOONS / DEF CON and BSides Las Vegas bring their own security staff-volunteers from among the participants. Look for people in a red shirt who look like they know what they're doing, if you're lost or need some kind of help.

PHOTO CREDITS Jeroen de Bakker / @astcell

Getting Started

THE CONFERENCES

The colloquial term “Hacker Summer Camp” refers to three Las Vegas conferences with very different personalities and demographics. DEF CON, the oldest of the three, draws the largest crowd, largely from the hacker (or security researcher) community. Black Hat is the most like a typical convention, with a large vendor hall and high cost. BSides Las Vegas, the most recent, is a non-profit organization put on by the community, for the community. These events typically take place the first full week in August, and the following weekend.

Black Hat

AT A GLANCE ///////

DATES	August 3-6, 2019 Trainings August 7-8, 2019 Briefings and Business Hall
WEBSITE	https://blackhat.com/us-19/
LOCATION	Mandalay Bay Convention Center
QUALITY	Professional information security event, with training and a convention floor

The Black Hat conference was founded in 1997 by the organizers of DEF CON, for a business audience. This event features talks about security issues and approaches that impact enterprises and corporations. Black Hat is much more expensive than the other two events, and draws from a different crowd. However, many Black Hat attendees also attend DEF CON, as the two always run back-to-back. Black Hat draws nearly 20,000 attendees, for trainings and presentations, as well as a large vendor floor. Of the three events, this one feels the most like a traditional conference or convention. Black Hat has grown from a single annual conference in Las Vegas and are held annually in the United States, Europe and Asia.

BSides Las Vegas

AT A GLANCE ///////

DATES	August 6-7, 2019
WEBSITE	www.bsideslv.org
LOCATION	Tuscany Hotel and Casino
	Platinum Hotel and Spa
QUALITY	Community-run non-profit, with friendly hackers

BSides Las Vegas is the original, and one of the largest Security BSides events in the world. Since its founding in 2009, BSides Las Vegas has grown year-over-year, and is currently viewed as the perfect middle ground for conference goers transitioning between Black Hat and DEFCON.

The annual two-day event started as an 'un-conference' supporting talks previously rejected by Black Hat, and has since grown to one of the must attend events of the summer. BSides Las Vegas is a source of education, communication, and collaboration. The technical and academic presentations are given in the spirit of peer review and for the dissemination of knowledge among all specialties.

DEF CON

AT A GLANCE ///////

DATES	August 8-11, 2019
WEBSITE	www.defcon.org
LOCATION	Paris Convention Center
	Bally's Convention Center
	Flamingo Convention Center
	Planet Hollywood Convention Center
QUALITY	World's largest hacker conference
	Known for its edginess and diverse sub-cultures

Started in 1992 by the Dark Tangent, DEF CON is the world's longest running and largest underground hacking conference. The talks at the first event resemble what you might hear today: Talks from lawyers and law enforcement, gender and social issues in technology, technical explainers, and warnings about issues that would manifest in the future. DEF CON remains an open space for intellectual exploration, open to all those who want to participate.

New this year at DEF CON Policy is a guided experience for government officials, public policy members and staff to explore and get the most out of DEF CON 27. Activities and support includes: advance registration, daily policy pocket guide schedule, invitations to DEF CON policy roundtables, 1:1 guided tours and meetings with DEF CON communities, villages and speakers.

POLICY PASSPORT ///////

DEF CON 27 Policy Registration[3]

HASHTAG #defconpolicy

CONTACT Heather Blanchard
policy@defcon.org
@poplifegirl

Now in its 27th year, DEF CON draws 25,000-30,000 people and is usually held the first full weekend in August, is unlike typical conventions or trade shows.

> The DEF CON "Villages" are self-contained spaces dedicated to single issues, such as privacy, social engineering, lockpicking, voting machines, and vehicles—that tend toward highly interactive demonstrations and hands-on hacking.

> The vendor hall is more akin to a techno-bazaar than a trade show floor, with storefronts selling tools or knowledge, civil society groups engaging directly with their stakeholders, and universities recruiting students.

> DEF CON is perhaps the only conference that drafts its own all-volunteer security staff from among its attendees, called the Goons, who always wear red shirts for easy identification.

> Conference admission is cash-only, and comes with a custom designed badge, unique each year.

> The art and effort that have gone into the official badges have spawned a cultural trend called #badgelife[4], where dozens of unofficial electronic badges and digital ecosystems have sprung up. Badgelife describes the grueling experience of creating a piece of hardware from concept to completion in 8-10 months.

[3] http://bit.ly/DEFCONPolicy
[4] https://hackaday.com/2018/08/14/all-the-badges-of-def-con-26-vol-1/

Hacker Culture & History

One defining characteristic of hacker culture is that it tends to defy concise description. The dark, sinister, anti-social teenage boy prominent in stock photos and mainstream portrayals is an unfair, and inaccurate, depiction of the broader hacker culture that persists today. Instead, **the hacker culture has roots in creativity, breaking and fixing things, and welcoming individuals regardless of their demographics**. This is the predominant culture today; one which continues to evolve just as technology, business, and society adapt to a digital world.

Over twenty years ago, the L0pht testified[5] before the U.S. Senate Committee on Government Affairs and presented one of the first public warnings about the dual-use nature of the internet, largely using their online monikers rather than real names. Later that same year, a different group mobilized volunteers to digitally occupy (what we now call a Distributed Denial of Service or DDOS) high profile military websites as an act of civil disobedience, using their real names. These two groups of hackers represented the curiosity, drive, and public concern that permeates hacker culture but is often overshadowed by modern stereotypes—yet each was very different in their ideologies, approaches, and ends.

[5] https://www.youtube.com/watch?v=VVJldn_MmMY

HACKER MOTIVATIONS

Security researchers have diverse motivations for investigating security flaws in software and systems. As companies, policymakers, lawyers, and others interact with the security research community, understanding this truth can unlock more fruitful engagement. I Am The Cavalry[6] has been using a simple and useful framework to discuss the drivers of security researcher behavior. While this list isn't comprehensive, and while most of us fit at least two of these categories, this framing can catalyze a dialog that allows a fuller appreciation of why we do what we do, and that is the value of the framework.

PROTECT
make the world a safer place. These researchers are drawn to problems where they feel they can make a difference.

PUZZLE
tinker out of curiosity. This type of researcher is typically a hobbyist and is driven to understand how things work.

PRESTIGE
seek pride and notability. These researchers often want to be the best, or very well known for their work.

PROFIT
to earn money. These researchers trade on their skills as a primary or secondary income.

PROTEST/PATRIOTISM
ideological and principled. These researchers, whether patriots or protestors, strongly support or oppose causes.

(From I Am The Cavalry, used with permission)

[6] https://iatc.me/motivations

The term 'hacker' does not have any universally agreed upon definitions within the hacking community, while the debate remains ongoing[7] in the public as to whether hackers are inherently good or bad. Modern usage of the word hacker first emerged[8] in the mid-20th century, among M.I.T. train enthusiasts. The benign connotation emphasized finding creative means to solve technology problems and stretch beyond the realm of known capabilities. Within a decade, more malicious applications began to dominate, associating hacking with illegal activity. Despite the benign roots, the media and popular culture have embraced the malicious description, even to the point where a hack and cyber attack are used interchangeably in many popular outlets.

For many, today's hacking culture has roots in the 1980s as personal computers began to appear in households. Movies such as War Games[9] and Sneakers[10] reflected the emergence of these techno-wizards and placed them immediately within national security or criminal settings. However, the reality for most was quite different.

The personal computer and the early days of the internet provided many of today's hacker legends a venue to connect and network without geographical boundaries or the constraints of societal expectations. It may be difficult to believe in today's social media-driven world, but anonymity was a defining feature of early hacker culture. Personal handles – such as The Dark Tangent[11], who organizes the DEF CON conference – allowed hackers the freedom to shape perceptions and gain anonymity.

While there certainly are those who match the stereotypes, they are arguably the exception. Hacking culture has roots in an egalitarian counter-culture with a broader distrust of authority and a rejection of assimilating to society's expectations. But there is also an underlying

[7] https://www.csoonline.com/article/3245751/hackers-are-good-not-bad.html
[8] https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack
[9] https://www.imdb.com/title/tt0086567/
[10] https://www.imdb.com/title/tt0105435/
[11] https://www.defcon.org/html/links/dtangent.html

appreciation of excellence, inquisitiveness, and problem solving that is frequently mistaken for disobedience. In A Declaration of the Independence of Cyberspace[12], John Perry Barlow explains, "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity." This utopian vision of the Internet remains a defining, aspirational feature of hacker culture which has permeated into global advocacy groups fighting for internet freedom.

The hacking community tends to prefer the technical nuances of the latest technologies or novel ways to exploit a vulnerability as opposed to reaching out to mainstream audiences. Because of this, it may seem intimidating for outsiders to feel accepted. However, do not mistake the insular and often tight-knit nature of the hacking culture as a distrust of all outsiders. Instead, **hackers tend to be friendly and welcoming, especially when asked to talk about the latest technologies or their research projects.**

Language is an essential component of any culture, and hacking culture is no different. The hacking community has its own set of esoteric terms and abbreviations on par with those in the policy world. The hacking culture itself historically has been divided into black hats (malicious hackers), white hats (ethical hackers), and grey hats (occasionally violates laws but does not have malicious intent). The vast majority of hackers consider themselves firmly in the white hat category.

As part of the professionalization of the security industry, this rainbow of colors has extended into workplace roles, with the rise of blue team (defenders), red team (authorized hackers aimed at testing and compromising to help inform defenses), and now purple teams (combine daily security defenses with insights from red team activity). More than simply reflecting the growth of the industry along

[12] https://www.eff.org/cyberspace-independence

HACKER MOVIES

"Hackers may fascinate and terrify us, but they might be the immune system of our digital society. While dependence on connected technology has grown faster than our ability to secure it, friendly hackers improve public safety, public policy, and save lives—through security research. Yet media portrayals of hackers lack authenticity and fidelity, focused on harmful behavior and motivations, instead of diverse narratives in the real hacker community. Hacking is a superpower: for good or for ill. Better media role models will create the hacker heroes we need."

So began a panel at SXSW 2019 with hackers and media figures. We asked hackers what their favorite hacker movies were and why.

"War Games. It features similar technology and techniques from when I was getting started in computers, and has some really accurate characters. Plus, the hero goes from Puzzler to Protector when he realizes the stakes of the game." @BEAUWOODS

"'The Martian' because it shows a hacker as a problem solver. If there would have been practical jokes in the movie it would have been a perfect showcase for the meaning of the word 'hacker'." @ihackforfun

"Unpopular opinion: Hackers.Sure it gets all the hacking wrong, but it nails a lot of what the defcon community is like & about. I'll never know if it's art imitating life or life imitating art, but there is no question it is still a strong influence on the hacker community." @MisterGlass

"Superman 3, of course! Richard Pryor as a computer who uses his hacking skills to round pennies into his bank account AND synthesize fake Kryptonite to try to kill Superman. What's not to love?" @PatChadwick78

the entire offense/defense spectrum, these terms also signify a maturation of the industry and the demand for a diverse range of skill sets.

Hacking culture also has extreme disdain for many buzzwords, which usually tends to be those used in traditional marketing campaigns and is often prominently displayed in buzzword bingo cards. “Cyber” used as a noun or prefix will usually provoke the harshest responses, while other terms such as rock star, evangelist, or thought leader are equally considered words non grata.

Each conference at Hacker Summer Camp has its own unique character, but casual attire is common across all three. Other than a suit, almost anything goes. Don’t be surprised to see hair that is every color of the rainbow, men in kilts, light up clothing and jewelry, or even an occasional furry. If a t-shirt and shorts or jeans is not quite your scene, feel free to add a casual jacket to assimilate for the week. But if you have been waiting for the perfect time to pull out any retro attire or techno-nerd shirts, this is the week to do it. And feel free to grab a free t-shirt from the security vendors or support the conference and buy one from the merch booth. You can learn a bit more about hacker fancy dress culture at VanitySec[13].

Cultural shifts in the hacker community are, in part, driven by the increasing professionalization of the industry as hackers link up with experts from other disciplines, such as data scientists, devops engineers, and (yes!) policymakers. Many respected members of the hacking community increasingly advocate for reaching across the various disciplinary boundaries. For those new to these interactions, they will likely encounter hackers who seek to engage and educate. Crossing the trust boundary is essential, but once past it, it is hard not to get enveloped within the community.

This trust factor deserves additional depth. When hackers discover

[13] https://vanitysec.com/2017/09/01/what-to-wear-when-you-dont-know-what-to-wear/

HACKER ETHOS

Not everyone at Hacker Summer Camp are hackers, and not all hackers are at these events. Hackers tend to be playful, creative, individualistic, and candid. These characteristics have led them to develop advanced capabilities, in a space where norms and rules are fluid. This combination of personalities, skills, and environment can give rise to new emergent behaviors. Yet nearly every hacker takes to heart the great Stan Lee line, “with great power comes great responsibility.”

Early online arenas for discourse were entirely text-based, meaning participants lacked social cues such as status, education, age, gender, and ethnicity. When early hackers met in real life, they were often surprised by the misconceptions they harbored about physical characteristics of their counterparts. Because of this, common biases were dampened in hacker culture. Hackers tend to follow ideas, rather than the individuals behind them.

These sentiments are reflected powerfully in a brief essay, “The Conscience of a Hacker”[14] (also known as The Hacker Manifesto), published in the magazine *phrack*, on January 8, 1986, by a hacker going by the name The Mentor. Select passages follow.

> “This is our world now... the world of the electron and the switch, the beauty of the baud.”
>
> “We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.”
>
> “Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.”

[14] http://phrack.org/issues/7/3.html

HARD TRADEOFFS IN SECURITY RESEARCH

What would you do if you knew of an issue you believe could cause harm to millions? You know that adversaries will inevitably discover the same issue and use it for their own ends. Yet, when you report it to the software or device maker—the ones who created the flaw and who can fix it—they dismiss or threaten you. Would you be silent to shield your family from a legal battle, your would you go public and equip potential victims to protect themselves? Hackers live this dilemma on a daily basis.

Coordinated Vulnerability Disclosure is the act of reporting, in good faith, security issues which could cause harm. This is a complex and nuanced issue, going back decades. We will spare the history lesson and instead just leave it at this: there are hard tradeoffs among all stakeholders in deciding whether, how, and when to disclose a potential security flaw. I Am The Cavalry's[15] Position on Disclosure[16] that captures these tradeoffs and provides guidance. A brief excerpt below.

> *All systems fail. There is no system without flaw. Flaws with the potential to inflict harm make products – and the people that rely on them – vulnerable to accidents and adversaries. Researchers seek to find these vulnerabilities so we can fix them and improve safety.*
>
> *Unknown flaws represent potential harm. Finding and revealing them makes both adversaries and defenders aware. During the time between finding and fixing the vulnerability there may be a temporary adversary advantage. Defenders can address both the vulnerability itself and the practice that led to the flaw, giving them a permanent advantage.*

[15] https://iatc.me
[16] https://iatc.me/disclosure

vulnerabilities or other security concerns they face the uncertainty about whether it will be well-received, dismissed, or penalized—either financially or in the media with reputational damage. This contributes to the additional stress and burnout that are prevalent within the industry, as hackers often are put in a situation where they know an issue could harm millions, but the authorities or an organization may dismiss them. Adversaries will inevitably rediscover these same issues and use them for their own ends. Whether or not to go public is a dilemma many hackers frequently encounter.

Hacking culture will continue to evolve, and with that, will be the natural tension that emerges from change. However, the cultural evolution remains consistent with the founding roots of the community. Curiosity, freedom, creativity, and inclusion remain the aspirational features that drive hacking culture. This was epitomized last year as the L0pht returned[17] to DC to reiterate their previous warnings and offer new insights about growing concerns about the security and openness of the internet.

By and large, the hacking culture remains committed to supporting these aspirational goals and helping others seeking to learn and engage. Ask questions. Engage. Be open to new thinking. You'll discover how friendly and welcoming the hacking culture can be.

[17] https://the-parallax.com/2018/05/24/l0pht-hackers-return-dire-warnings/

Planning & Information

MONEY AND FINANCES

While Las Vegas casinos would love to extend you a line of credit, the hacker conferences that take place there don't always accept credit cards. Many of the independent vendors that sell swag (souvenirs like clothing), electronic badges, and tools, find it troublesome to deal with credit cards. Often the network is unreliable, the paperwork burden is too high, and many attendees refuse to use cards when at Hacker Summer Camp. Casino ATMs may be the world's most monitored cash points, and are official ones are generally safe, though they may be down in the immediate area of the conferences, victims of their own insecurity or network problems. Avoid ATMs that look unusual or temporary.

WHAT TO WEAR

Las Vegas casinos and conference speaking areas can get frigid, despite the hellish weather outside, even at night. A light, packable jacket—or yes, a hoodie—can help regulate the temperature swings. Many attendees rarely leave the relative comfort of hotels and taxis, though if you do, wear sunscreen to avoid quickly getting burned. And whatever you do, bring comfortable shoes for walking and standing!

The three conferences have varying ranges of dress. At the most corporate of these, Black Hat, dress will range from suit and tie, to shorts and t-shirts. The smallest and most friendly event, BSides Las Vegas, is very relaxed and you can fit in wearing anything short of business formal. DEF CON has the widest variety of dress—from fully casual to mascot costumes you might see at a theme park. Both men and women can keep it pretty casual if they want to play it safe: jeans or slacks and a t-shirt or polo will fit in at any of the events.

SECURING TECHNOLOGY

The technology environment at Hacker Summer Camp has been described as "the world's most hostile network," for good reason. There are hundreds or thousands of active attacks on the open conference networks at any given time. However, they are also some of the world's most surveilled networks, with dozens or hundreds of individuals and groups looking to discover attacks. Still, mobile carrier networks are likely to be more reliable and more secure. Fake base station attacks are less likely than in years past, as some conference staff routinely hunt these devices and get rid of them. A reputable VPN (installed and set up before you travel), in use at all times, further reduces risk of interception, eavesdropping, and tampering.

Mobile and tablet devices running the latest versions of iOS and Android, and fully updated, are some of the most secure commercial technology platforms ever. Security flaws (and attacks that exploit them) that are made public tend to be fixed quickly, and unknown attacks tend to be expensive to execute. So it's unlikely that adversaries would use these expensive attacks at Hacker Summer Camp, especially when everyone has their guard up. Sophisticated adversaries are more likely to target individuals in other settings.

Cautious attendees bring new, clean phones and create new accounts that they will discard after the conferences are over. Others bring their primary phones, backing them up, wiping them, and setting them up as new, with the minimum necessary applications and accounts. It's usually more of a hassle than a benefit to get a new number. And keep in mind that hotel safes aren't really safe (ask the Lockpicking Village to tell you why).

It takes a lot to remember all of this and practice good OPSEC (Operational Security). It's why some attendees decide to leave all their tech at home.

COMMON MISCONCEPTIONS

MYTH: Hacker Summer Camp is for criminals.
TRUTH: The vast majority of hackers are no more criminal than your neighbors or coworkers.

MYTH: I'll get hacked if I go to Hacker Summer Camp.
TRUTH: While the networks are indeed hostile, you're unlikely to have any technology hacked if it's up to date. And just being there doesn't tend to raise your threat profile.

MYTH: Government employees aren't welcome at Hacker Summer Camp.
TRUTH: It might surprise you to know that many of the people who make the conferences happen have some current or former government affiliation, including military, law enforcement, or local or state agencies.

Health & Safety

If you (or someone around you) needs help, **grab a Goon**. Goons are volunteer conference security staff (at DEF CON and BSides Las Vegas), there to make sure the events go well and to take care of health and safety issues. You can spot them by their red badges and red shirts, often with a backpack strolling the halls. Of course as a part of their duty they're tasked with keeping the hallways and doors clear, getting hotel staff and others around quickly, and maintaining a semblance of order. If they seem rude or brusk, keep in mind they've probably been on their feet for 6-8 hours, doing the grunt work so their friends can have fun without them. It's a thankless—and unpaid—task, though they will usually accept a hug or a hi-5 as a tip.

To be clear, despite the roots in inclusiveness, the hacking culture has experienced numerous high-profile incidents of harassment and discrimination. The community has stepped up to make events are safe for all who want to attend, which has given rise to codes of conduct and other mechanisms to help ensure the safety of all, especially those in underrepresented groups.

You're expected to get at least 3 hours of sleep, 2 meals, and 1 shower—every day. This is known as the 3-2-1 rule for Hacker Summer Camp. There's a note of humor here, yet also sound advice for several of the attendees who burn the candle at both ends. Between the social events, the puzzles and challenges, talks, Villages, contests, and other chaos, it's easy to see why some people consistently break this rule.

Las Vegas is HOT and dry; August is usually the hottest and driest time of year. As you could guess from the 3-2-1 rule, most attendees have their fair share of beer—and coffee—throughout the day. If you're driving or have a car, stock your hotel room with water and carry a couple of bottles at all times—one to drink and one to share. And no matter what your map tells you, walking outside to the next hotel over is NOT as close as it seems—stay indoors and take taxis or ride shares.

Hacker Summer Camp can get overwhelming. The heat, the stimulation, the crowds, and the chaos can get the better of anyone. One of the secrets to survival is to be able to sneak off to a quiet place to just relax a little bit. DEF CON streams talks to the conference hotel rooms, Bsides Las Vegas streams to the web, so you can watch the event from afar if you still feel like you're missing out.

DEF CON has established an anonymous 20-hour per day (8am-4am) hotline for reporting issues or getting help. Call their trained volunteers at +1 (725) 222-0934.

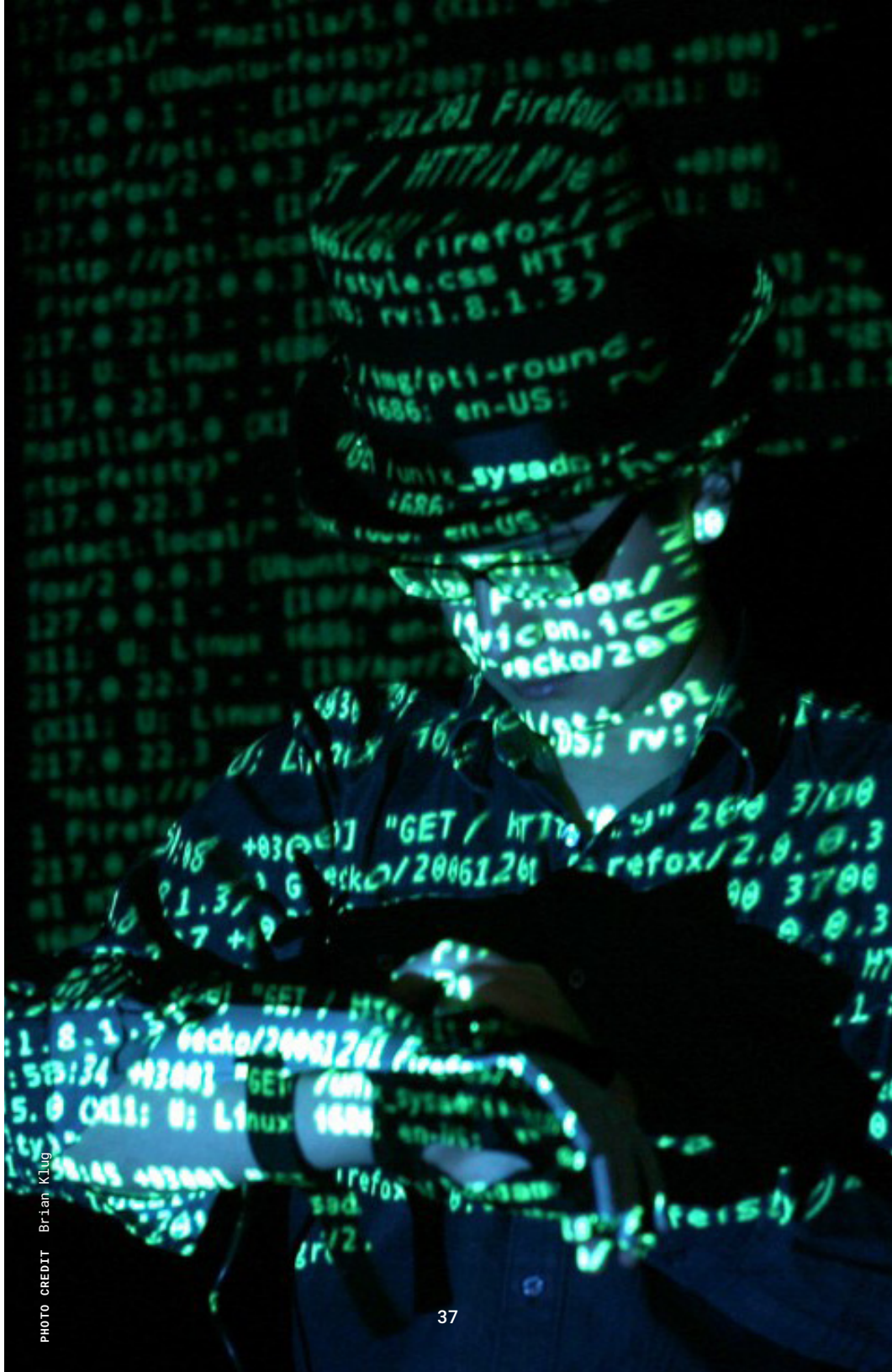


PHOTO CREDIT Brian Klug

Itineraries

Here we present some common and suggested routes through Hacker Summer Camp. A mix of conferences, talks, villages, contests, and events that we think will appeal to different people.

This is a sneak preview! More details to be published at **https://lostpolicymaker.org** soon!

THE "ALL-IN"

A grueling 7-day schedule. BSidesLV, BlackHat, and DEF CON—all-you-can-eat Vegas buffet style—including parties and a mandatory 3-2-1 rule.

THE "CRYPTO MEANS CRYPTOGRAPHY"

Mostly talks and villages about cryptography, encryption, privacy, law enforcement, civil liberties, and other relevant topics. Crypto & Privacy Village.

THE "SAFETY CRITICAL MASS"

Where bits and bytes meet flesh and blood: Talks and villages dealing with the impact of cybersecurity on human life and public safety. Villages include Biohacking, ICS, Car Hacking, Aviation, and Hack the Sea, as well as the I Am The Cavalry and Public Ground tracks at BSidesLV.

THE "CULTURAL TOURIST"

Load your schedule up with contests, villages, events, and parties. High interactivity with the locals. No talks before noon. Bonus points for getting a mohawk or showing up in a Furry costume.

THE "HACKING 101"

DEF CON 101 track, Lockpick Village, BsidesLV, Crypto & Privacy Village, main conference parties, and more!

THE "SUN TZU"

Because it can't be a serious "cyber" discussion if someone doesn't mention The Art of War. This tour centers on adversary actions/reactions, states and non-states, norms, deterrence, and other topics the DEF CON crowd doesn't usually pay attention to (but increasingly do).

THE “CHALLENGE”

DEF CON has a number of contests and challenges[18]. Some of these are highly technical (Capture the Flag, SOHOplessly Broken), some are non-technical (Beard and Moustache Contest, Tinfoil Hat), and some serve a positive role for society (OSINT CTF for Missing Persons). The Lonely Policymaker should not feel left out! Here are a handful of challenges to help you explore and learn.

FOR INSTANCE,

> GET A SELFIE WITH A VILLAGE ORGANIZER, A SPEAKER, A GOON, AND SOMEONE IN A COSTUME

> PICK A LOCK (at Lockpick Village)

> LEARN TO REVERSE CANBUS (at Car Hacking Village)

> DO A DEF CON SCAVENGER HUNT ITEM (in Contests and Events area)

> GET A MOHAWK (OR FAUXHAWK) AT MOHAWK CON (in Contests and Events area)

> CRACK WEAK WIFI (at Packet Hacking Village)

> PLAY A GAME ON A BADGE

> TAKE A SELFIE WITH AN UBER BADGE

> BREAK A CIPHER (at Crypto & Privacy Village, or in Contests and Events area)

> REMOVE A TAMPER EVIDENT SEAL (at Tamper Evident Village)

> SOLDER SOMETHING FOR THE FIRST TIME (at Hardware Hacking Village)

ORGANIZED TOURS

DEF CON is offering dedicated tours for members of the public policy community. Contact the DEF CON Policy Registration desk for more information, at policy@defcon.org!

[18] https://forum.defcon.org/node/227572

DEF CON Villages

DEF CON will host 31 self-contained subject matter areas, called Villages, in 2019. Several of these are noteworthy for government and the public policy community.

Aviation Village[19] @aviationvillage

Members of the security research community invite aviation industry leaders to work together toward safe, reliable, and trustworthy air travel.

> “The Aviation Village welcomes those who seek to improve aviation security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.”

AI Village[20] @aivillage_dc

From fundamental research to public policy positions, the AI Village seeks to build connections between the AI and security research communities.

> “We aspire to quell mounting discomfort and democratize the knowledge needed to capitalize on AI’s prodigious potential.”

Biohacking Village[21] @dc_bhv

Featuring talks, as well as hands on labs for biohacking and medical

[19] http://aviationvillage.org/
[20] https://aivillage.org/
[21] https://www.villageb.io/

device security research, the Biohacking Village seeks to create a safe space for individuals across the traditional and non-traditional healthcare communities to come together, leveraging the best technology has to offer, in the service of public health and wellness.

> "The Biohacking Village celebrates global health ingenuity arising from maker communities with the dynamic perspective of emerging biology, technology, and human-enhancement."

Car Hacking Village[22] `@carhackvillage`
Security researchers work together with the automotive industry to improve the security—and safety—of modern vehicles.

> "Leveraging the vast amount of experience the security research community brings to the Village may increase the safety and security of vehicles on the road today and for generations to come."

Crypto and Privacy Village[23] `@cryptovillage`
Bringing awareness and education about cryptography and privacy issues, with discussions from the latest technical techniques to public policy discussions.

> "At the Crypto & Privacy Village you can learn how to secure your own systems while also picking up some tips and tricks on how to break classical and modern encryption."

[22] https://www.carhackingvillage.com/
[23] https://cryptovillage.org/

Ethics Village[24] `@ethicsvillage`
Studies the unique ethics posed by the emerging field of information security and hacking, drawing on medicine, law, and philosophy.

> "The DEFCON Ethics Village, is an ethics conference focused on fostering a discussion about ethics in the security domain."

ICS Village[25] `@ICS_Village`
Equips industry and policymakers to better defend industrial equipment through experiential awareness, education, and training.

> "The ICS Village equips industry and policymakers to better defend industrial equipment through experiential awareness, education, and training."

Hack the Sea Discussions and hands on learning about maritime security and the trillions of dollars of global commerce it supports.

> "Hack The Sea, [is] a three day mini-conference organized to challenge the infosec community to apply their skills, red and blue, to protect our maritime critical infrastructure and human lives at sea."

[24] http://ethicsvillage.org/
[25] https://www.icsvillage.com/

Lockpick Village[26] `@toool`
One of the most hands-on experiences at DEF CON and offers a key insight into why security is a nuanced topic. Participants to learn to defeat the most prevalent physical security protections, often picking their first lock in under five minutes.

> "By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property."

R00tz Asylum[27] `@r00tzasylum`
A safe space for kids (and their parents) to learn about white hat hacking and staying safe online, with hands on activities available to kids to take the honor code.

> "r00tz Asylum is open to anyone who is curious and open to learning new things, like encryption, information security, hardware engineering and more."

Vote Hacking Village `@votingvillagedc`
Exploration of election security from technical and public policy perspectives.

> "The Voting Village ... will highlight the various aspects of election cybersecurity, including the technical components that make up our election infrastructure ranging from hardware, to software to databases."

[26] https://toool.us/
[27] http://r00tz.org/

Side Events & Parties

Attending Hacker Summer Camp doesn't just mean attending talks, there are tons of "side" events, mini-conferences, and parties that happen throughout the week. Every year there are a wide variety of events outside of the conference that are worth checking out. Here are a few!

SIDE EVENTS

NARWHAL

Narwhal[28] @narwhalbe is an event that runs parallel to BlackHat and DEF CON, focused primarily on aspects of information security not covered at the three major events, such as law, policy, and academia. Now in its fourth year, and will be held at the Flamingo hotel, August 7-10, 2019.

QUEERCON

Queercon[29] @queercon, a non-profit with thousands of members, is the largest LGBT+ Security group in the world. Now in its 16th year, the three-day event features talks and parties, taking place at the Alexis Park hotel, August 8-11, 2019.

LAWYER MEETUP aka the DEF CON Bar Association

It may surprise you, but some lawyers are also hackers (and vice-versa) and have been attending DEF CON for a long time. Attending lawyers practice in varying capacities: private practice, public non-profits, government, and solo-practitioners. Each year the lawyers organize to catch up, talk shop, and network. All lawyers or legal professionals are welcome to join! This event will take place on Friday, August 9, 18:00-20:00 at Napoleon's Bar in Paris.

DIANA INITIATIVE

The Diana Initiative[30] @dianainitiative founded in 2015, focuses on increasing representation of women and non-binary people in the information security community. It provides scholarships for those groups to attend DEF CON, and hosts an event nearby at the Westin hotel, with two speaking tracks, villages, workshops, and a capture the flag, August 8-11, 2019.

[28] https://narwhal.be/
[29] https://www.queercon.org
[30] https://www.dianainitiative.org/about/

DEF CON SHOOT

Many DEF CON attendees with military and law enforcement backgrounds may enjoy DEF CON Shoot[31], the long-running pop-up shooting range that takes place on August 7, 2019.

FRIENDS OF BILL W.

Meetings occur throughout DEF CON. Time and location are usually announced via the DEF CON twitter account @defcon. Meetings at 12:00 and 17:00 Thursday-Saturday, and 12:00 Sunday, located in Santa Monica 4 at Planet Hollywood.

DEAF CON

DEAF CON[32] @_deafcon_ is a non-profit organization that encourages deaf and hard of hearing individuals within the information security and hacker communities to attend conferences. They have been facilitating communication and providing a platform for networking with others, since 2011.

PARTIES

Hackers like to party and so there are tons of ways to enjoy yourself throughout the week of Hacker Summer Camp. Check out defconparties.com and @defconparties for more.

[31] https://deviating.net/firearms/defcon_shoot/
[32] https://www.deafconinc.org/mission

Quick Look Checklists

OPSEC

(Operational Security—learn more in Securing Technology, on page 33.)

> **PAPER AND PLASTIC.** Though many conference vendors accept credit cards, several (including badge sales) are cash only. Casinos have the world's most surveilled ATMs, so they're a pretty safe bet these days - though avoid any that look temporary.

> **SECURE CONNECTIVITY.** Mobile carrier networks are by far the most trustworthy, followed by secure conference wireless. Use a trustworthy VPN, and consider turning off WiFi/Bluetooth (if not the device) when not in use.

> **AVOID LAPTOPS; FAVOR PHONES/TABLETS.** Laptops - even those configured by experts - tend to be less securable than a fully updated phone or tablet made in the last 1-2 years.

> **DATA SECURITY.** Avoid connecting to work systems while in or near the conference areas, and treat anything with USB (including fans, power adapters, etc.) like candy - don't take it from strangers or pick it up off the floor.

> **BURNER PHONE OPTIONAL.** Bring a clean phone (or wipe your primary) set up as new, with minimal apps and accounts, and your primary number. Operating systems and apps older than the latest versions are a high risk in this environment.

> **DRESS FOR THE EVENT.** The events are laid back and so are the dress codes. you'll blend in and better endure the high heat and time on your feet by dressing simply and comfortably.

> **HOTEL ROOM (IN)SECURITY.** Ask your hotel about any room search policies and ask at check in how to verify staff that conduct these searches. Avoid leaving valuables or technology in your rooms - safes are not safe (see the Lockpick Villages for more).

> **PHOTO COURTESY.** Privacy is important to the hacker community. No wide shots. If you do want to take a photo, ask the people in the area first.

> **CONFERENCE SAFETY AND SECURITY.** If you have any questions about physical safety or security, find one of the red-shirted Goons. They are there to help.

> **HEALTHY DOSE OF PARANOIA.** If something looks suspicious, it probably is. Be cautious and skeptical, while exploring and finding what you'll enjoy about the conferences. Too much paranoia can be debilitating (trust us).

TALK LIKE A LOCAL (AND PHRASES TO AVOID)

> "Cyber" is a four-letter word in many hacker circles. Instead, try IT security, information security, infosec, or just security.

> Acronyms and common terms may have different meanings than in the public policy sphere. Policy, for instance, is what Human Resources directors or firewall engineers write. When in doubt, ask about a particular phrase, term, or acronym!

> Self-deprecation and humility are seen as respectful in the hacker community, whereas terms like "rock star," "thought leader," or any sort of chest puffing are generally looked down on.

> The hacker community appreciates curiosity. It's ok if you don't know how something works or what it is. Just ask! People love to talk about their passions and expertise.

> Phrases like "I'm from the government, and I'm here to help," are understood to be tongue-in-cheek, and will likely draw a laugh.

> You're likely to hear that "DEF CON is cancelled." It has been for the past 27 years, but people keep showing up!

> "MAKE A HOLE," is how the Goons, DEF CON's security team, ensures speakers, the differently abled, and important deliveries get through the halls when they're packed.

> The **Motherboard glossary**[13] is a great resource for terms from hackers' perspective, while the **DHS NICCS glossary**[14] is more cyber policy focused.

[13] https://www.vice.com/en_us/article/mg79v4/hacking-glossary
[14] https://niccs.us-cert.gov/about-niccs/glossary

THE LOST POLICYMAKER'S GUIDE TO

Hacker Summer Camp

How to talk like a local	PAGE 49
How to protect your tech	PAGE 33
What is a goon	PAGES 17 & 35
What is the hacker ethos	PAGE 29
What motivates hackers	PAGE 24
Where do I even get started	PAGE 18

PRODUCED AND SUPPORTED BY

WILLIAM + FLORA Hewlett Foundation

The William and Flora Hewlett Foundation is a nonpartisan, private charitable foundation that advances ideas and supports institutions to promote a better world. Our Cyber Initiative provides funding for the development of a cyber policy field that offers thoughtful, multidisciplinary solutions to complex cyber challenges for the benefit of societies around the world. **Hewlett.org**

I Am The Cavalry

I Am The Cavalry is a global grassroots initiative, focused on cybersecurity issues that intersect with public safety and human life—where bits and bytes meet flesh and blood. We provide pro bono, independent security expertise to help policymakers, manufacturers, regulators, and others better respond to cyber safety challenges and risks. **iamthecavalry.org** **@iamthecavalry**

lostpolicymaker.org / #lostpolicymaker / @lostpolicymaker