POLICY@ DEF CON

Interested in the cutting edge of hacking technology and its policy implications? Interested in talking with policy folks wanting an honest assessment of what is possible?

Hackers are early users and abusers of technology, and that technology is now critical to modern life. As governments make policy decisions about technology, hackers, researchers and academics need to be part of that conversation before the decisions are made, and not after policies are implemented.

These talks will take place in the Policy track in Summit Ballroom 224-227 at Caesars Forum.

FRIDAY

	Roundtable	Collaboratorium
12:00	Hacking law is for hackers - how recent changes to CFAA, DMCA, and global policies affect security research Harley Geiger, Leonard Bailey	Emerging Cyber Policy Topics TBA
14:00	Defense Through a TAC (Technical Advisory Committee) The Dark Tangent, Members of the TAC	Meet the Feds: ONCD Edition Staff from the Office of the National Cyber Director
16:00	Moving Regulation Upstream - An Increasing focus on the Role of Digital Service Providers Jen Ellis	Emerging Cyber Policy Topics TBA
19:00	Meet the Feds: CISA Edition (Lounge) CISA Staff	Fireside Policy Chats TBA
20:00	Meet the Feds: DHS Edition (Lounge) DHS Staff	
20:30		Fireside Policy Chats TBA

SATURDAY

	Roundtable	Collaboratorium
10:00	Imagining a cyber policy crisis: Storytelling and Simulation for real-world risks Safa Shahwan Edwards	Hacking Operational Collaboration David Forscey
12:00	Addressing the gap in assessing (or measuring) the harm of cyberattacks Adrien Ogee	Hacking Aviation Policy Timothy Weston, Meg King, Pete Cooper, Ayan Islam, Ken Munro
14:00	Return-Oriented Policy Making for Open Source and Software Security Trey Herr	Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet Neal Pollard, Jason Healey
16:00	Emerging Cyber Policy Topics TBA	International Government Action Against Ransomware Jen Ellis
19:00	Do No Harm (Lounge) Christian "quaddi" Dameff MD, Jeff "r3plicant" Tully MD, Jessica Wilkerson, Alissa Knight, Seeyew Mo	Fireside Policy Chats TBA
20:30		Fireside Policy Chats TBA

SUNDAY

	Roundtable	Collaboratorium
10:00	Better Policies for Better Lives: Cybersecurity Basics Peter Stevens	Improving International Vulnerability Disclosure: Why the US and Allies Have to Get Serious Stewart Scott
12:00	Protect Our Pentest Tools! Perks and Hurdles in Distributing Red Team Tools Sarah Powazek	Offensive Cyber Industry Roundtable Winnona DeSombre
14:00	Emerging Cyber Policy Topics TBA	Emerging Cyber Policy Topics TBA

FRIDAY

	Track 1	Track 2	Track 3	Track 4
10:00	Panel - "So It's your first DEF CON" - How to get the most out of DEF CON, What NOT to do. DEF CON Goons	Panel - DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world? DEF CON Policy Dept	Old Malware, New tools: Ghidra and Commodore 64, why understanding old malicious software still matters Cesare Pizzi	Computer Hacks in the Russia-Ukraine War Kenneth Geers
10:30				OopsSec -The bad, the worst and the ugly of APT's operations security Tomer Bar
11:00	Welcome to DEF CON & The Making of the DEF CON Badge The Dark Tangent, Michael and Katie Whiteley (Mkfactor)		The PACMAN Attack: Breaking PAC on the Apple M1 with Hardware Attacks Joseph Ravichandran	
11:30		DEF CON Policy Dept - Special Edition Policy Talk Chris Inglis		Running Rootkits Like A Nation-State Hacker Omri Misgav
12:00	Glitched on Earth by humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal Lennert Wouters		Avoiding Memory Scanners: Customizing Malware to Evade YARA, PE-sieve, and More Kyle Avery	One Bootloader to Load Them All Mickey Shkatov, Jesse Michael
12:30		Global Challenges, Global Approaches in Cyber Policy Gaurav Keerthi et al		
13:00	Emoji Shellcoding: 🪄,🐌, and 😎 Hadrien Barral, Georges-Axel Jaloyan		Backdooring Pickles: A decade only made things worse ColdwaterQ	You're Muted Rooted Patrick Wardle
13:30		A Policy Fireside Chat with Jay Healey Jason Healey et al	Weaponizing Windows Syscalls as Modern, 32-bit Shellcode Tarek Abdelmotaleb, Dr. Bramwell Brizendine	
14:00	Space Jam: Exploring Radio Frequency Attacks in Outer Space James Pavur		Process injection: breaking all macOS security layers with a single vulnerability Thijs Alkemade	Phreaking 2.0 - Abusing Microsoft Teams Direct Routing Moritz Abrell
14:30		Leak The Planet: Veritatem cognoscere non pereat mundus Emma Best, Xan North		Trace me if you can: Bypassing Linux Syscall Tracing Rex Guo, Junyuan Zeng
15:00	Exploring the hidden attack surface of OEM IoT devices: pwning thousands of routers with a vulnerability in Realtek's SDK for eCos OS. Octavio Gianatiempo, Octavio Galland		LSASS Shtinkering: Abusing Windows Error Reporting to Dump LSASS Asaf Gilboa, Ron Ben-Yitzhak	
15:30		How Russia is trying to block Tor Roger Dingledine		Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling James Kettle
16:00	Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE) Gal Zror		Wireless Keystroke Injection (WKI) via Bluetooth Low Energy (BLE) Jose Pico, Fernando Perera	
16:30		DEF CON Policy Dept - Special Edition Policy Talk DEF CON Policy Dept		A dead man's full-yet-responsible-disclosure system Yolan Romailler
17:00	Hunting Bugs in The Tropics Daniel Jensen		Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS Orange Tsai	
17:30		Walk This Way: What Run D.M.C. and Aerosmith Can Teach Us About the Future of Cybersecurity Jen Easterly, The Dark Tangent		Deanonymization of TOR HTTP hidden services Ionut Cernica
18:00	Killer Hertz Chris Rock		Pulling Passwords out of Configuration Manager: Practical Attacks against Microsoft's Endpoint Management Software Christopher Panayi	Tear Down this Zywall: Breaking Open Zyxel Encrypted Firmware Jay Lagorio
18:30		Dragon Tails: Supply-side Security and International Vulnerability Disclosure Law Stewart Scott, Trey Herr		
20:00				Hacker Jeopardy, followed by Whose Slide is it Anyway?

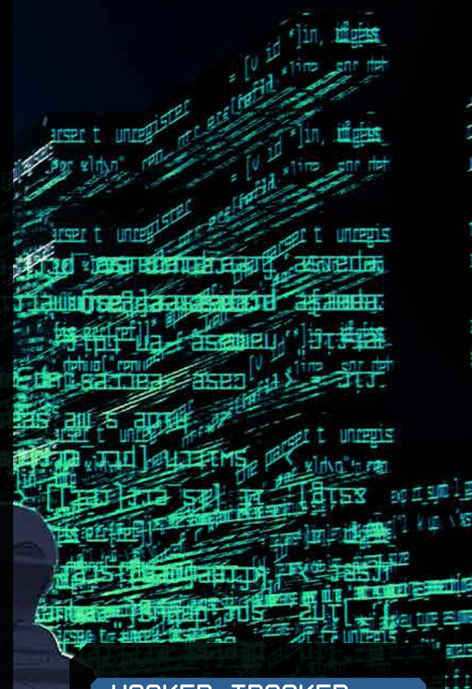
SATURDAY

	Track 1	Track 2	Track 3	Track 4
10:00	Brazil Redux: Short Circuiting Tech-Enabled Dystopia with The Right to Repair Paul Roberts, Joe Grand, Corynne McSherry, Louis Rossmann, Kyle Wiens	TBA	Scaling the Security Researcher to Eliminate OSS Vulnerabilities Once and For All Jonathan Leitschuh	Literal Self-Pwning: Why Patients - and Their Advocates - Should Be Encouraged to Hack, Improve, and Mod Med Tech Cory Doctorow, Christian "quaddi" Dameff MD, Jeff "r3plicant" Tully MD
11:00		My First Hack Was in 1958 (Then A Career in Rock'n'Roll Taught Me About Security) Winn Schwartau	No-Code Malware: Windows 11 At Your Service Michael Bargury	How To Get MUMPS Thirty Years Later (or, Hacking The Government via FOIA'd Code) Zachary Minneker
11:30	Reversing the Original Xbox Live Protocols Tristan Miller			
12:00		Tracking Military Ghost Helicopters over our Nation's Capital Andrew Logan	All Roads leads to GKE's Host : 4+ Ways to Escape Billy Jheng, Muhammad Alifa Ramdhan	The Evil PLC Attack: Weaponizing PLCs Sharon Brizinov
12:30	The Hitchhacker's Guide to iPhone Lightning & JTAG hacking stacksmashing	UFOs, Alien Life, and the Least Untruthful Things I Can Say. Richard Thieme		Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit. Jimmy Wylie
13:00	Chromebook Breakout: Escaping Jail, with your friends, using a Pico Ducky Jimi Allee		Exploring Ancient Ruins to Find Modern Bugs: Discovering a 0-Day in an MS-RPC Service Ben Barnea, Ophir Harpaz	
13:30		HACK THE HEMISPHERE! How we (legally) broadcasted hacker content to all of North America using an end-of-life geostationary satellite, and how you can set up your own broadcast too! Karl Koscher, Andrew Green		Do Not Trust the ASA, Trojans! Jacob Baines
14:00	OpenCola. The AntiSocial Network John Midgley, Oxblood Ruffin		The COW (Container On Windows) Who Escaped the Silo Eran Segal	
14:30		Digging into Xiaomi's TEE to get to Chinese money Slava Makkaveev		Doing the Impossible: How I Found Mainframe Buffer Overflows Jake Labelle
15:00	Deja Vu: Uncovering Stolen Algorithms in Commercial Products Patrick Wardle, Tom McGuire	The Big Rick: How I Rickrolled My High School District and Got Away With It Minh Duong	You Have One New Appointment - Hacking Proprietary iCalendar Properties Eugene Lim	
15:30	Automotive Ethernet Fuzzing: From purchasing ECU to SOME/IP fuzzing Jonghyuk Song, Soohwan Oh, Woongjo choi	Tor: Darknet Opsec By a Veteran Darknet Vendor & the Hackers Mentality Sam Bent		Perimeter Breached! Hacking an Access Control System Sam Quinn, Steve Povolny
16:00	Trailer Shouting: Talking PLC4TRUCKS Remotely with an SDR Ben Gardiner, Chris Poore		Low Code High Risk: Enterprise Domination via Low Code Abuse Michael Bargury	
16:30		Why did you lose the last PS5 restock to a bot Top-performing app-hackers business modules, architecture, and techniques Arik		Defeating Moving Elements in High Security Keys Bill Graydon
17:00	Hacking The Farm: Breaking Badly Into Agricultural Devices. Sick Codes		Internal Server Error: Exploiting Inter-Process Communication with new desynchronization primitives Martin Doyhenard	Black-Box Assessment of Smart Cards Daniel Crowley
17:30		Crossing the KASM--a webapp pentest story Samuel Erb, Justin Gardner		
18:00			The CSRF Resurrections! Starring the Unholy Trinity: Service Worker of PWA, SameSite of HTTP Cookie, and Fetch Dongsung Kim	Digital Skeleton Keys - We've got a bone to pick with offline Access Control Systems Miana E Windall, Micsen
18:30				
20:00		War Stories		Hacker Jeopardy, followed by Whose Slide is it Anyway?

SUNDAY

	Track 1	Track 2	Track 3	Track 4
11:00	Exploitation in the era of formal verification: a peek at a new frontier with AdaCore/SPARK Adam 'pi3' Zabrocki, Alex Tereshkin	emulation-driven reverse-engineering for finding vulns atlas	Save The Environment (Variable): Hijacking Legitimate Applications with a Minimal Footprint Wietze Beukema	STrace - A DTrace on windows reimplementation. Stephen Eckels
12:00	The Call is Coming From Inside The Cluster: Mistakes that Lead to Whole Cluster Pwnership Dagan Henderson, Will Kline	Taking a Dump In The Cloud Melvin Langvik, Flangvik	PreAuth ACE Chains on an MDM: KACE SMA Jeffrey Hofmann	Defaults - the faults. Bypassing android permissions from all protection levels Nikita Kurtin
13:00	Less SmartScreen More Caffeine - ClickOnce (Ab)Use for Trusted Code Execution Steven Flores, Nick Powers	DEF CON Policy Dept - Special Edition Policy Talk DEF CON Policy Dept	ElectroVolt: Pwning popular desktop apps while uncovering new attack surface on Electron Aaditya Purani, Max Garrett	The Journey From an Isolated Container to Cluster Admin in Service Fabric Aviv Sasson
14:00			Contest Closing Ceremonies & Awards Grifter	Solana JIT: Lessons from fuzzing a smart-contract compiler Thomas Roth
15:30	DEF CON Closing Ceremonies & Awards The Dark Tangent			

D3FCON POCKET GUIDE



HACKER TRACKER

Download the official DEF CON app! It contains all of the happenings of DEF CON. It is easy to use and updated as things change during the conference. It contains all of the maps and schedules so you can plan your best DEF CON experience.

Download on the App Store

android

CAESARS FORUM

HEART OF HOUSE

ICS VILLAGE

VOTING MACHINE VILLAGE

IOT VILLAGE

RETAIL VILLAGE

ALLIANCE ROOM

TRACK 4
HACKER JEOPARDY
WSIIA

INFO

ALLIANCE-ACADEMY PRE-FUNCTION 5

PACKET HACKING VILLAGE

ACADEMY BALLROOM

TRACK 3
MOVIE NIGHT

ALLIANCE PRE-FUNCTION 6

ACADEMY PRE-FUNCTION 7

REST-ROOMS

KITCHEN

MERCH

POLICY

INFO

DISPATCH
LOST & FOUND

AI VILLAGE

MISINFORMATION VILLAGE

PASSWORD VILLAGE

QUANTUM VILLAGE

REST-ROOMS

HEART OF HOUSE

UNITY BOARDROOM

DISHROOM/ STORAGE

HEART OF HOUSE

SUMMIT BALLROOM
10,000 SQ. FT.

CONTESTS

CTF

DEMO LABS

BCCC

ENTRANCE

PANTRY/ STORAGE

LOCKPICKING VILLAGE

TAMPER EVIDENT VILLAGE

PHYSICAL SECURITY VILLAGE

TEACHER'S LOUNGE

GREEN ROOM

SPEK OPS

SUMMIT PRE-FUNCTION 4

DEMO LABS

INFO

SUMMIT-FORUM PRE-FUNCTION 3

HEART OF HOUSE

HACKER KARAOKE/ CHESS

VENDORS

CAR HACKING VILLAGE

CHILLOUT

REST-ROOMS

ENTRANCE

PANTRY/ STORAGE

PANTRY/ STORAGE

HEART OF HOUSE

TRACK 1
FORUM BALLROOM

TRACK 2

AEROSPACE VILLAGE

FORUM PRE-FUNCTION 2

INFO

ENTRANCE

STORAGE

REG

FORUM PRE-FUNCTION 1

REST-ROOMS

ENTRANCE

ESCALATORS TO SKY BRIDGE (HARRAH'S, LINQ, MONORAIL)

ENTRANCE

FLAMINGO

EXECUTIVE CONFERENCE CENTER

LOWER LEVEL

VALLEY FIRE

DATA DUPE VILLAGE

LAKE MEAD II

VALLEY VI FIRE I

LAKE MEAD I

BRYCE

ZION

Escalator/ Stairs

HARDWARE HACKING VILLAGE

VI

VIII

INFO BOOTH

I

II

SOLDERING SKILLS VILLAGE

RED ROCK

CRYPTO & PRIVACY VILLAGE

Vista

ADVERSARY VILLAGE

SUNSET BALLROOM

Scenic

CLOUD VILLAGE

APPSEC VILLAGE

Twilight

BIC VILLAGE

Banquet Kitchen

Elevators

INFO BOOTH

CHILL

II

I

LAUGHLIN

BIO HACKING VILLAGE

III

CORPORATE CONVENTION CENTER

Third floor

ROOFTOP CHILLOUT

Garden View

INFO BOOTH

Elevators

HAM VILLAGE

VIRGINIA CITY

GIRLS HACK

Sahara

Eldorado Foyer

CHILLOUT

MEMORIAL ROOM

RED TEAM VILLAGE

Savoy Foyer

Elevators

Banquet Kitchen

RADIO FREQUENCY VILLAGE

BLUE TEAM VILLAGE

SAVOY

LINQ

Third Floor

SKYTALKS

Up 2nd Escalators in the BLOQ (5th Floor)

Connection A

Connection B

ROGUES VILLAGE

Evolution

INFO BOOTH

Social Square

Showroom

Social

SOCIAL ENGINEERING COMMUNITY

RECON VILLAGE

B

C

CHILLOUT