

1000 - There's no place like 127.0.0.1 - Achieving reliable DNS rebinding in modern browsers

Thursday at 10:00 in 101 Track

45 minutes | Demo, Tool, Exploit

Luke Young*Senior Information Security Engineer, LinkedIn*

Most people lock their doors at night, however if you walk into someone's home you likely won't find every piece of furniture bolted to the floor as well. We trust that if someone is inside our home they are supposed to be there. Unfortunately many developers treat local networks just the same, assuming all internal HTTP traffic is trusted, however this is not always the case. They incorrectly assume that their services will be protected by the same-origin policy in browsers, rather than implementing proper authentication mechanisms. By abusing this implicit trust we can gain access to confidential data and internal services which are not intended to be publicly accessible.

I will demonstrate that this is a poor security control and can be trivially bypassed via an older technique, DNS rebinding. The talk will cover how DNS rebinding works, the mitigations imposed by modern browsers and networks, and how each mitigation can be bypassed. I will discuss the notorious unreliability of DNS rebinding attacks that causes many developers to ignore the issue and how to overcome this unreliability.

Finally, I will examine a variety of popular services and tools to understand how they are affected by DNS rebinding. I will be releasing a tool that allows researchers to automate DNS rebinding attacks, the associated mitigation bypasses and generate drop-dead simple proof-of-concept exploits. I will demonstrate this tool by developing exploits for each vulnerable service, ending the talk by exploiting a vulnerable service to obtain remote-code execution, live.

Luke Young

Luke Young is a security researcher originally from the frozen plains of Minnesota who recently migrated to the much warmer state of California. He presented at DEF CON 23 on the topic of exploiting bitflips in memory, DEF CON 24 on the subject of large DDoS attacks and has investigated a variety of well-known products and network protocols resulting in numerous CVE assignments. He spends his free-time maintaining his position as one of the top researchers on various bug bounty platforms and is currently working as a Senior Information Security Engineer at LinkedIn.

@TheBoredEng

"<https://bored.engineer>

[#defcon25/by_track/101/thursday](#)

[#defcon25/By_Day/_thursday](#)

1000 - Where are the SDN Security Talks?

Thursday at 10:00 in 101 Track2

45 minutes | Demo, Tool

Jon Medina*[Protiviti*](#)

Software Defined Networking is no longer a fledgling technology. Google, Amazon, Facebook, and Verizon all rely on the scalability, programmability, flexibility, availability, and yes, security provided by SDN. So why has there only ever been one DEF CON speaker presenting on SDN and security?

This talk will provide a brief introduction to SDN and security, demonstrate ways of compromising and securing a Software Defined Network and will illustrate new ways of using the power of open source SDN coupled with machine learning to maintain self-defending networks.

Jon Medina

Jon Medina (@ackSec) is a security nerd who has worked in networking and security capacities for everything from the Department of Defense, to the Fortune 500, to state and local government. He currently works for Protiviti providing security consulting for a wide variety of clients and industries. His interests outside of work include traveling, hockey, strange beers, and his bulldog. He's spoken at Shmoocon, BSides, and many other security events and conferences.

@ackSec

[#defcon25/by_track/101-Track2/Thursday](#)

[#defcon25/By_Day/_thursday](#)

1100 - From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices

Thursday at 11:00 in 101 Track

45 minutes

Patrick DeSantis*Senior Security Research Engineer, Cisco Talos*

Stringing together the exploitation of several seemingly uninteresting vulnerabilities can be a fun challenge for security researchers, penetration testers, and malicious attackers. This talk follows some of the paths and thought processes that one researcher followed while evaluating the security of several new "out of the box" Industrial Control System (ICS) and Internet of Things (IoT) devices, using a variety of well known exploitation and analysis techniques, and eventually finding undocumented, root-level, and sometimes un-removable, backdoor accounts.

Patrick DeSantis

Patrick DeSantis is a security researcher with Cisco Talos and focuses his efforts on discovery and exploitation of vulnerabilities in technologies that have an impact on the physical world, such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT), and anything else that looks like it's asking to be hacked. Patrick's background includes work in both the public and private sectors, as well as a pile of information security certifications and a few college degrees.

@pat_r10t

#defcon25/by_track/101/thursday

#defcon25/By_Day/_thursday

1100 - Opt Out or Deauth Trying !- Anti-Tracking Bots Radios and Keystroke Injection

Thursday at 11:00 in 101 Track 2

45 minutes | 0025, Demo, Tool, Exploit

Weston Hecker*Principal Application Security Engineer, "NCR"*

It's hard not to use a service now days that doesn't track your every move and keystroke if you absolutely must use these systems why not give them the most useless information possible. Along with the fact that several companies are tracking their customers online now they are taking it to physical brick and mortar stores this talk will be geared looking at the attack surface of instore tracking and attacking these systems for the purpose of overloading their systems or making the information so inaccurate that it becomes useless. Watch as a 32 year old hackers online profile is turned to that of a 12 year old girl who loves horses!

Weston Hecker

With 12 Years Pen-testing, 13 years' security research and programming experience. Weston is currently working on the application security team of NCR Weston has recently Spoken at

DEF CON 22,23 and 24, Blackhat 2016, HOPE11, Hardware.IO 2016, Takdowncon 2016, ICS cyber security 2016, Bsides Boston, Enterprise Connect 2016 ISC2-Security Congress, SC-Congress Toronto and over 60 other speaking engagements from regional events to universities on security subject matter. Working with A Major University's research project with Department of Homeland Security on 911 emergency systems and attack mitigation. Found several vulnerabilities in very popular software and firmware. Including Microsoft, Qualcomm, Samsung, HTC, Verizon.

#defcon25/by_track/101-Track2/Thursday

#defcon25/By_Day/_thursday

1200 - Jailbreaking Apple Watch

Thursday at 12:00 in 101 Track 2

45 minutes | Demo

Max Bazaliy*Security Researcher, Lookout*

On April 24, 2015, Apple launched themselves into the wearables category with the introduction of Apple Watch. This June, at Apple's Worldwide Developer Conference, Apple announced that their watch is not only the #1 selling smartwatch worldwide by far, but also announced the introduction of new capabilities that will come with the release of watchOS 4. Like other devices, Apple Watch contains highly sensitive user data such as email and text messages, contacts, GPS and more, and like other devices and operating systems, has become a target for malicious activity.

This talk will provide an overview of Apple Watch and watchOS security mechanisms including codesign enforcement, sandboxing, memory protections and more. We will cover vulnerabilities and exploitation details and dive into the techniques used in creating an Apple Watch jailbreak. This will ultimately lead to a demonstration and explanation of jailbreaking an Apple Watch, showcasing how it can access important user data and applications.

Max Bazaliy

Max is a Security Researcher at Lookout with more than ten years of experience in areas as reverse engineering, software security, vulnerability research and advanced exploitation. Currently focusing on iOS exploitation, reverse engineering advanced mobile malware and hardware attacks. Max was a lead security researcher at Pegasus iOS malware investigation.

In the past few years, Max was a speaker on various security conferences, including BlackHat, CCC, DEF CON , Ruxcon, RSA and BSides.

Max holds a Masters degree in Computer Science and currently is PhD student at the National Technical University of Ukraine "Kyiv Polytechnic Institute" where he's working on dissertation in code obfuscation and privacy area.

@mbazaliy

#defcon25/by_track/101-Track2/Thursday

#defcon25/By_Day/_thursday

1200 - Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode

Thursday at 12:00 in 101 Track

45 minutes | Demo, Tool

Matt Suiche*Founder, Comae Technologies*

Ethereum is gaining a significant popularity in the blockchain community, mainly due to fact that it is design in a way that enables developers to write decentralized applications (Dapps) and smart-contract using blockchain technology.

Ethereum blockchain is a consensus-based globally executed virtual machine, also referred as Ethereum Virtual Machine (EVM) by implemented its own micro-kernel supporting a handful number of instructions, its own stack, memory and storage. This enables the radical new concept of distributed applications.

Contracts live on the blockchain in an Ethereum-specific binary format (EVM bytecode). However, contracts are typically written in some high-level language such as Solidity and then compiled into byte code to be uploaded on the blockchain. Solidity is a contract-oriented, high-level language whose syntax is similar to that of JavaScript. This new paradigm of applications opens the door to many possibilities and opportunities. Blockchain is often referred as secure by design, but now that blockchains can embed applications this raise multiple questions regarding architecture, design, attack vectors and patch deployments.

As we, reverse engineers, know having access to source code is often a luxury. Hence, the need for an open-source tool like Porosity: decompiler for EVM bytecode into readable Solidity-syntax contracts - to enable static and dynamic analysis of compiled contracts.

Matt Suiche

Matt Suiche is recognized as one of the world's leading authorities on memory forensics and

application virtualization.

He is the founder of the United Arab Emirates based cyber-security start-up Comae Technologies. Prior to founding Comae, he was the co-founder & Chief Scientist of the application virtualization start-up CloudVolumes which was acquired by VMware in 2014. He also worked as a researcher for the Netherlands Forensic Institute.

His most notable research contributions enabled the community to perform memory-based forensics for Mac OS X memory snapshots but also Windows hibernation files.

Since 2009, Matt has been recognized as a Microsoft Most Valuable Professional in Enterprise Security due to his various contributions to the community.

@msuiche

#defcon25/by_track/101/thursday

#defcon25/By_Day/_thursday

1300 - Amateur Digital Archeology

Thursday at 13:00 in 101 Track

45 minutes

Matt 'openfly' Joyce*Hacker at NYC Resistor*

'Digital Archeology' is actually the name of a Digital Forensics text book. But what if we used forensics techniques targetting cyber crime investigations to help address the void in Archeology that addresses digital media and silicon artifacts. At NYC Resistor in Brooklyn we've gotten into the world of Digital Archeology on several occasions and the projects have been enjoyable and educational.

Now, imagine what could happen if a bunch of hackers are able to get their hands on a laptop pulled off of a space shuttle.

Then come to our talk and find out what ACTUALLY happened. I bought a laptop at auction that claimed to be off a Shuttle Mission. It turns out to have been mostly authentic. This will be a little foray into the history of this device and what I could find out about it, and how I did that.

Spoiler Alert: We found out a lot.

Bonus: I may have found the sister laptop of this laptop (serial numbers match)

Matt 'openfly' Joyce

Matt Joyce hates writing in the third person. He is a hacker at NYC Resistor in Brooklyn. He used to do NASA shit for a project called Nebula. He currently is doing this talk in no way representing current or past employers. Matt's last talk was at the American Homebrewer's Association.

#defcon25/by_track/101/thursday

#defcon25/By_Day/_thursday

1300 - Wiping out CSRF

Thursday at 13:00 in 101 Track 2

45 minutes | Art of Defense, Demo

Joe Rozner*Senior Software Security Engineer, Prevoty*

CSRF remains an elusive problem due to legacy code, legacy frameworks, and developers not understanding the problem or how to protect against it. Wiping out CSRF introduces primitives and strategies for building solutions to CSRF that can be bolted on to any http application where http requests and responses can be intercepted, inspected, and modified. Modern frameworks have done a great job at providing solutions to the CSRF problem that automatically integrate into the application and solve most of the conditions. However, many existing apps and new apps that don't take advantage of these frameworks or use them incorrectly are still plagued with this problem. Wiping out CSRF will provide an in depth overview of the various reasons that CSRF occurs and provide payload examples to target those specific issues and variations. We'll see live demos of these attacks and the protections against them. Next we'll look at how to compose these primitives into a complete solution capable of solving most cases of CSRF explaining the limits and how to layer them to address potential short comings. Finally we'll finish by looking at Same Site Cookies, a new extension to cookies that could be the final nail in the coffin, and see how to use the prior solution as a graceful degradation for user agents that don't support it yet.

Joe Rozner

Joe (@jrozner) is a software engineer at Prevoty where he has built semantic analysis tools, language runtimes, generalized solutions to common vulnerability classes, and designed novel integration technology leveraging runtime memory patching. He has a passion for reverse engineering, exploitation, teaching, and sharing research with others. He is the undisputed champion of the Brawndo and Booze competition from DEF CON s past with his Irish Car Mutilator winning in both the drink and dip categories.

@jrozner

#defcon25/by_track/101-Track2/Thursday

#defcon25/By_Day/_thursday

1400 - Hacking the Cloud

Thursday at 14:00 in 101 Track

45 minutes | Demo

Gerald Steere*Cloud Wrecker, Microsoft*

Sean Metcalf*CTO, Trimarc*

You know the ins and outs of pivoting through your target's domains. You've had the KRBTGT hash for months and laid everything bare. Or have you?

More targets today have some or all of their infrastructure in the cloud. Do you know how to follow once the path leads there? Red teams and penetration testers need to think beyond the traditional network boundaries and follow the data and services they are after. This talk will focus on how to take domain access and leverage internal access as a ticket to your target's cloud deployments.

We will also discuss round trip flights from cloud to on-premises targets and what authorizations are required to access your target's cloud deployments. While this talk is largely focused on Microsoft Azure implementations, the concepts can be applied to most cloud providers.

Gerald Steere

Gerald Steere has been a member of the C+E Red Team since joining Microsoft in June 2014. He regularly dives into the deepest corners of Azure looking for vulnerabilities unique to the cloud scale environment and collecting all the creds. Prior to that, he was a security auditor and penetration tester for three civilian Federal agencies, where he acquired a love for obtaining and cracking as many passwords as possible. He has spoken on cloud security topics at multiple BlueHat events and most recently at BSides Seattle.

@darkpawh

Sean Metcalf

Sean Metcalf is founder and principal consultant at Trimarc Security, LLC

(www.TrimarcSecurity.com), which focuses on mitigating, detecting, and when possible,

preventing modern attack techniques. He is one of about 100 people in the world who holds the Microsoft Certified Master Directory Services (MCM) certification, is a Microsoft MVP, and has presented on Active Directory attack and defense at BSides, Shakacon, Black Hat, DEF CON, and DerbyCon security conferences.

Sean has provided Active Directory and security expertise to government, corporate, and educational entities since Active Directory was released. He currently provides security consulting services to customers and regularly posts interesting Active Directory security information on his blog, [ADSecurity.org](https://adsecurity.org).

@pyrotek3

#defcon25/by_track/101/thursday

#defcon25/By_Day/_thursday

1400 - See no evil, hear no evil: Hacking invisibly and silently with light and sound

Thursday at 14:00 in 101 Track 2

45 minutes | Demo, Tool

Matt Wixey*Senior Associate, PwC*

Traditional techniques for C2 channels, exfiltration, surveillance, and exploitation are often frustrated by the growing sophistication and prevalence of security protections, monitoring solutions, and controls. Whilst all is definitely not lost, from an attacker's perspective - we constantly see examples of attackers creatively bypassing such protections - it is always beneficial to have more weapons in one's arsenal, particularly when coming up against heavily-defended networks and highly-secured environments.

This talk demonstrates a number of techniques and attacks which leverage light and/or sound, using off-the-shelf hardware. It covers everything from C2 channels and exfiltration using light and near-ultrasonic sound, to disabling and disrupting motion detectors; from laser microphones, to repelling drones; from trolling friends, to jamming speech and demotivating malware analysts.

This talk not only provides attendees with a new suite of techniques and methodologies to consider when coming up against a well-defended target, but also demonstrates, in a hopefully fun and practical way, how these techniques work, their advantages, disadvantages,

and possible future developments. It also gives details of real case studies where some of these techniques have been used, and provides defenders with realistic methods for the mitigation of these attacks.

Finally, the talk covers some ideas for future research in this area.

Matt Wixey

Matt Wixey is a penetration tester on PwC's Threat and Vulnerability Management team in the UK, and leads the team's research function. Prior to joining PwC, he led a technical R&D team in a UK law enforcement agency. His research interests include bypassing air-gaps, antivirus and sandbox technologies, and RF hacking.

@darkartlab

#defcon25/by_track/101-Track2/Thursday

#defcon25/By_Day/_thursday

1500 - Inside the "Meet Desai" Attack: Defending Distributed Targets from Distributed Attacks

Thursday at 15:00 in 101 Track

45 minutes | Art of Defense

CINCVolFLT (Trey Forgy)*Director of Government Affairs & IT Ninja, NENA: The 9-1-1 Association*

In October of 2016, a teenage hacker triggered DTDoS attacks against 9-1-1 centers across the United States with five lines of code and a tweet. This talk provides an in-depth look at the attack, and reviews and critiques the latest academic works on TDoS attacks directed at 9-1-1 systems. It then discusses potential mitigation strategies for legacy TDM and future all-IP access networks, as well as disaggregated "over-the-top" originating services and the devices on which both the access network providers and originating service providers rely.

CINCVolFLT (Trey Forgy)

CINCVolFLT (Trey Forgy) is Director of Government Affairs for NENA: The 9-1-1 Association. He previously served as a Presidential Management Fellow in the U.S. Department of Homeland Security's Office of Emergency Communications, with rotations in the Federal Communications Commission's Public Safety and Homeland Security Bureau, and the U.S. Department of Commerce's National Telecommunications and Information Administration. A sometimes-piratical sailor and inveterate tinkerer, CINCVolFLT's recent activities have included promoting the use of new location technologies in wireless carriers' networks, and serving as pro bono counsel to QueerCon. He holds a B.S. in Applied Physics and a J.D., both

from the University of Tennessee (GO VOLS!).

@cincvolflt

#defcon25/by_track/101/thursday

#defcon25/By_Day/_thursday

1500 - Real-time RFID Cloning in the Field


Thursday at 15:00 in 101 Track 2

20 minutes | Demo, Tool, Audience Participation

Dennis Maldonado*Adversarial Engineer - LARES Consulting*

Ever been on a job that required you to clone live RFID credentials? There are many different solutions to cloning RFID in the field and they all work fine, but the process can be slow, tedious, and error prone. What if there was a new way of cloning badges that solved these problems? In this presentation, we will discuss a smarter way for cloning RFID in the field that is vastly more efficient, useful, and just plain cool. We will go over the current tools and methods for long-range RFID cloning, then discuss and demonstrate a new method that will allow you to clone RFID credentials in the field in just seconds, changing the way you perform red team engagements forever.

Dennis Maldonado

Dennis Maldonado is a Security Consultant at LARES Consulting. His current work includes penetration testing, red teaming, and security research. Dennis' focus is encompassing all forms information security into an assessment in order to better simulate a real world attack against systems and infrastructure. As a security researcher and evangelist, Dennis spends his time sharing what he knows about Information Security with anyone willing to learn. Dennis co-founded Houston Locksport in  Houston, Texas where he shares his love for lock-picking and physical security as well as Houston Area Hackers Anonymous (HAHA), a meet-up for hackers and InfoSec professionals in the Houston area. Dennis is also a returning speaker to DEF CON having spoken at DEF CON 23 and DEF CON 24.

@DennisMald

#defcon25/by_track/101-Track2/Thursday

#defcon25/By_Day/_thursday

1530 - Exploiting Old Mag-stripe information with New technology

Thursday at 15:30 in 101 Track 2

20 minutes | Demo, Tool, Exploit

Salvador Mendoza*Hacker*

A massive attack against old magnetic stripe information could be executed with precision implementing new technology. In the past, a malicious individual could spoof magstripe data but in a slow and difficult way. Also brute force attacks were tedious and time-consuming. Technology like Bluetooth could be used today to make a persistent attack in multiple magnetic card readers at the same time with audio spoof.

Private companies, banks, trains, subways, hotels, schools and many others services are still using magstripe information to even make monetary transactions, authorize access or to generate "new" protocols like MST(Magnetic Secure Transmission) During decades the exploitation of magstripe information was an acceptable risk for many companies because the difficulty to achieve massive attacks simultaneously was not factible. But today is different.

Transmitting magstripe information in audio files is the faster and easier way to make a cross-platform magstripe spoofer. But how an attacker could transmit the audio spoof information to many magnetic card readers at the same time? In this talk, we will discuss how an attacker could send specific data or achieve a magstripe jammer for credit card terminals, PoS or any card reader. Also, how it could be implemented to generate brute force attacks against hotel door locks or tokenization processes as examples.

Salvador Mendoza

Salvador Mendoza is a security researcher focusing in tokenization processes, mag-stripe information and embedded prototypes. He has presented on tokenization flaws and payment methods at Black Hat USA, DEF CON, DerbyCon, Ekoparty, BugCON and Troopers. Salvador designed different tools to pentest mag-stripe and tokenization processes. In his designed toolset includes MagSpoofPI, JamSpay, TokenGet and lately SamyKam.

@Netxing

Blog: salmg.net

[#defcon25/by_track/101-Track2/Thursday](#)

[#defcon25/By_Day/_thursday](#)

1600 - DEF CON 101 Panel

Thursday at 16:00 in 101 Track

105 minutes | Hacker History, Audience Participation

HighWiz*Founder, DC101*

Malware Unicorn

Niki7a*Director of Content & Coordination, DEF CON*

Roamer*CFP Vocal Antagonizer, DEF CON*

Wiseacre

Shaggy

The DEF CON panel is the place to go to learn about the many facets of DEF CON and to begin your DEF CONian Adventure. Here you will begin your adventure that will include more than just listening in the talk tracks. You can get hands-on experience in the Villages and witness amazing feats of programming in Demo Labs. You may even display your own powers by participating in a contest or two in the Events and Contest Area. The panel will give you what you need to know to navigate DEF CON to your best advantage. We have speakers who will regale you with tales of how they came to be at DEF CON and (hopefully) inspire you with their personal experiences. Oh yeah, there is the time honored "Name the Noob", with lots of laughs and even some prizes.

HighWiz

Born of glitter and moon beams, HighWiz is the things that dreams are made of and nightmares long to be... Years ago, with the help of some very awesome people, he set about to create an event that would give the n00bs of DEF CON a place to feel welcomed and further their own pursuit of knowledge. HighWiz is the fabled Man on the Mountain whom people seek to gain a taste of his forbidden knowledge. He is a rare sighting at DEF CON only to be glimpsed by those lucky few.

Malware Unicorn

As a girl growing up, she was told she could be anything so she decided to be a unicorn. Ever since, she has made it her mission to ensure the truth is out there. Do not attempt to use malware pickup lines on her as she will pull them apart and you risk having your face impaled. Though she is fierce, she is also graceful, peaceful and determined. She is also an awesome artist.

Niki7a

There is truly only one sorceress that ensures the machinations of Def Con continue to move. She is both in tune with the magic and digital functions and is the power behind the CFP board from start to finish as well as the coordination of so many other activities behind the curtain. She works tirelessly year-round to make sure everything runs smoothly. Also, she is fun at parties and awesome AF.

@niki7a

Roamer

Appearing in a cloud of (cigarette) smoke, Roamer is a man full of whiskey and ideas. He has appeared at DEF CON since before (almost) the beginning. He is a renown author, speaker, pontificator and is famous for giving the most entertaining Worldwide Wardrive talk. He is also the Grand Vizier of All Things Vendor - you are welcome.

Wiseacre

Wiseacre was introduced to DEF CON by Roamer. Though he appeared at his first DEF CON because of the Capture the Flag contest, Roamer and HighWiz showed him how to make DEF CON so much more than simply attending the talks. From then on he made a point to participate in as much as he could. Of course, this was all within the limits of social anxiety so, if it allowed participation as a wallflower, he was in! Now, he wants to make sure everyone else gets to know as much as possible about this year's conference. In his private life, Mike hacks managers and is happy anyone listens to him at all. Mike would like to thank Highwiz for everything.

Shaggy

Shaggy has the Voice of Barry White, the brains of Albert Einstein and the soul of Bea Arthur. He has a few philosophies on life: He believes that while the righteous keep moving forward, those with clean hands become stronger and stronger. That the field of battle between God and Satan is the human soul. It is in the soul that the battle rages every moment of life. He also believes that one should Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible. Because You learn to speak by speaking, to study by studying, to run by running, to work by working, and just so, you learn to love by loving. All those who think to learn in any other way deceive themselves.

[#defcon25/by_track/101/thursday](#)

[#defcon25/By_Day/_thursday](#)

1600 - The Last CTF Talk You'll Ever Need: AMA with 20 years of DEF CON Capture-the-Flag organizers

Thursday at 16:00 in 101 Track 2

105 minutes | Hacker History

Vulc@n*Difensiva Senior Engineer, DDTEK*

Hawaii John*CTF organizer, Legit Business Syndicate*

Chris Eagle*CTF organizer, DDTEK*

Invisigoth*CTF organizer, Kenshoto*

Caezar*CTF organizer, Ghetto Hackers*

Myles*CTF organizer, Goon*

Today there is practically a year-round CTF circuit, on which teams hone their skills, win prizes and attain stature. For many, the ultimate goal is to dominate in the utmost competition, DEF CON's CTF, and walk away with a coveted black badge. Capture-the-Flag (CTF) is one of DEF CON's oldest contests, dating back to DEF CON 4. Over the past decades, the perennial contest has matured into an annual event requiring months of preparation and nearly continuous dedication both of players and organizers. Organizers strive to make the events unique while taking extreme measures to prevent games from being gamed. Participants often have to cope with novel challenges while simultaneously demonstrating continued excellence in domains like reverse engineering, vulnerability discovery, exploitation, digital forensics, cryptography, and network security. In this session, we will present the evolution of DEF CON CTF, highlighting key points of advancement in the CTF culture - most of which broke new ground and are now present in other contests run around the world. Capitalizing on the multi-year tenure of recent DEF CON CTF organizers, we are able to concisely represent over 20 years of organizers on a single panel. Where else can you ask cross-generational questions about challenges of running CTF? Where else can you inquire about evolutionary design, and get answers from those that actually did it? Where else can you ask about hidden challenges, secrets, and CTF lore...from whom it originated?

The panelists represent over 20 years of DEF CON CTF organizers. Staples in the CTF community are present comprising of decades of experience in participating and organizing CTFs. On stage we have past organizers representing Legit BS, DDTEK, Kenshoto, Ghetto Hackers, and before – many of which also participated as part of top recurring teams such as Sk3wl of r00t, Ghetto Hackers, Samurai, and Team Awesome. Many also played some role (infrastructure, challenge author, announcer) in the Cyber Grand Challenge culminating last summer at DEF CON. They have received and distributed dozens of black badges. Panelists and the roles they represent for this panel: Hawaii John, Legit Business Syndicate; Chris Eagle, DDTEK; Invisigoth, Kenshoto; Caezar, Ghetto Hackers; Myles, Goon.

Vulc@n

Vulc@n have been involved in the community since DEF CON 11, which in some ways seems recent but upon reflection is clearly more than a decade ago. In his early years he sprinted from talk to talk, dodging curious things like mid-school aged folks with baby chickens, couches in purple-dyed pools, and real dunk tanks. He even sat through talks in the blistering heat in outdoor tents at Alexis Park. Starting with his second year attending, he was pulled more and more into the CTF contest with then new-found and now lifelong friends at Sk3wl

of r00t. Much of his time in the years since has been dedicated to playing in CTF or organizing it (as part of DDTEK). Ever since convincing one of his college professors to finance my first DEF CON trip, the hacker scene has been kind to him. He now finds himself in possession of two black badges (and leather jacket). More recently he was part of the Cyber Grand Challenge development team and was an on-stage referees for the all-computer hacking competition this past summer. In summary, it seems that he just keeps finding novel ways to be very involved with DEF CON and CTF.

@tvidas, @ddtek

Hawaii John

Bio coming soon.

@LegitBSCTF, @hjlbs

Chris Eagle

Bio coming soon.

@cseagle

Invisigoth

Bio coming soon.

@kenshoto

Caesar

Bio coming soon.

Myles

Bio coming soon.

[#defcon25/by_track/101-Track2/Thursday](#)

[#defcon25/By_Day/_thursday](#)