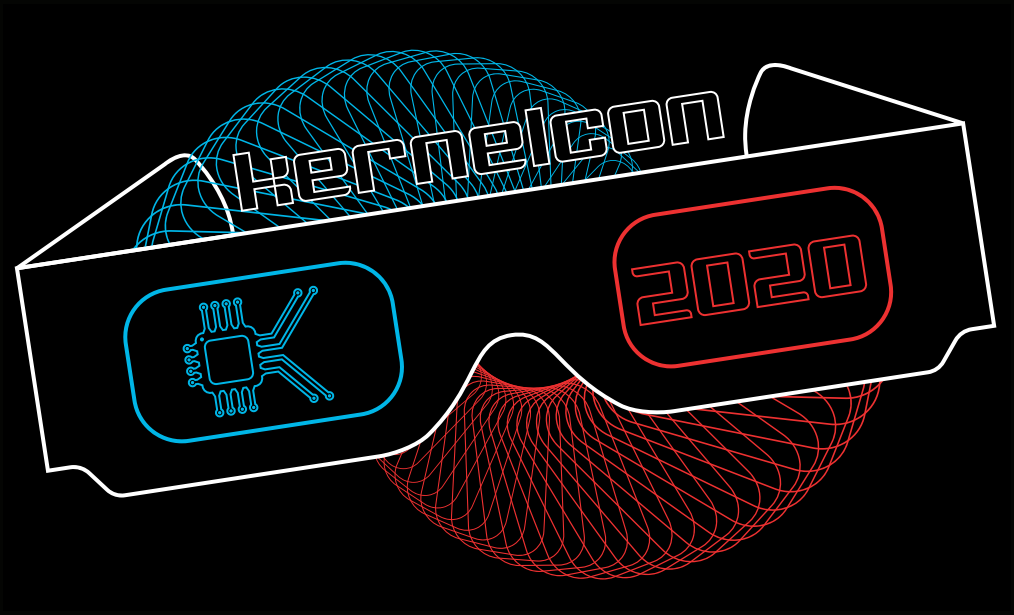


Virtual Program

March 27-28th 2020
Omaha, NE

SCHEDULE DAY 1 - FRIDAY

0830	Stream Open	
0900	Opening Remarks	
0915	Keynote: John Strand	
	Stream: Bat of Doom	Stream: Terrified Chipmunk
1015	Break	Break
1030	Passwords Are Dead? Long Live WebAuthn! Alex Lauerman and Matt South	Exploiting Modern Desktop Applications Matt Austin
1130	A Hacker's Viewpoint: Planning the Attack Robert George and Kristina Krasnolobova	A Secure Design and Implementation of a Smart Home Owen Parkins
1150	Astrophotography - Backyard Robotics for Art and Science Seth Eddy	Dispelling myths of red/blue cyber competition through metrics Kandy Phan
1210	Break	Break
1230	Key Duplication - It's Not Just for the Movies! Tony Virelli	Unleash your Camera with CHDK Aaron Grothe
1330	How Ghidra changed my life Chris Eagle	KetoAppSec: It's All About the FATS David Lindner
1430	Break	Break
1445	The DIY Artificial Pancreas: Hacking Wetware with Open Source Software and Hardware Jay Lagorio	A Red-Teamer's Guide to Building a Blue Team Mark Bayley
1545	Anybody Want to Launch Some Missles? Dan Tentler	Let The Right One In David Boyd
1645	Adventures in Creating a Cybersecurity Dataset Heather Lawrence	How to Pave a Path Forward for InfoSec by Hacking Hearts and Minds Chad Calease

SCHEDULE DAY 2 - SATURDAY

0830	Stream Open	
0900	Opening Remarks	
0915	Keynote: Sophia d'Antoine	
	Stream: Bat of Doom	Stream: Terrified Chipmunk
1015	Break	Break
1030	**Building a Vulnerability Management Program - Avoiding Pitfalls, Managing Risk, and Mastering CYA** Megan Benoit	**The Top 10 Tools For Cloud Penetration Testing** Michael Born
1130	**Bash Bunny Basics** Anthony Bernard	**Hacking your Cybersecurity Career** Ron Woerner
1150	**Pirate Radio: Riding the Ragged Edges** Michael Tomasiewicz	**WannaWorm** Michael Kunz
1210	Break	Break
1230	**Attacking Secondary Contexts in Web Applications** Sam Curry	**Getting started with OSINT** Jamie Maguire
1330	**Better Phishing through Smarter Infrastructure** Chris Patten and Dan Kottmann	**Protecting your Small or Medium Business from Cyber Attacks** Jeff Struik
1430	Break	Break
1445	**Breaking barriers: An introvert's story to InfoSec** Ryen Macababbad	**Bit to Byte** Christopher Wright
1545	**Bio Hack: How Integrative Medicine principles can change the game in Cyber Security** Joseph Wilson	**Kernelcon2020 Badge: nonononoyes** Tyler Rosonke and Aaron Gunning
1645	Own the Con, Closing Ceremonies, Awards	

WELCOME TO KERNELCON

Kernelcon is a community-organized event driven by a passion for connectedness within the information security community. Our second conference will be held March 27th and 28th, 2020 virtually in lieu of our home in Omaha, Nebraska.

Kernelcon takes its name from a mashup of “kernel” from “kernel of corn” - a popular crop grown in the area, and “operating system kernel” - a core, and privileged, component of the operating system responsible for managing computing resources.

CODE OF CONDUCT

Kernelcon provides a forum for open discussion between participants, where radical viewpoints are welcome and a high degree of skepticism is expected. However, insulting or harassing other participants is unacceptable. We want Kernelcon to be a safe and productive environment for everyone. It’s not about what you look like but what’s in your mind and how you present yourself that counts at Kernelcon. We do not condone harassment against any participant for any reason. Harassment includes deliberate intimidation and targeting individuals in a manner that makes them feel uncomfortable, unwelcome, or afraid. Participants asked to stop any harassing behavior are expected to comply immediately. We reserve the right to respond to harassment in the manner we deem appropriate, including but not limited to expulsion without refund and referral to the relevant authorities.

This Code of Conduct applies to everyone participating at Kernelcon - from attendees and instructors to speakers, press, volunteers, and Kernelcon Crew. Anyone can report harassment. If you are being harassed, notice that someone else is being harassed, or have any other concerns, you can:

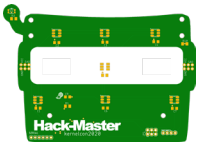
- Contact a Kernelcon Crew Member or Organizer in Discord
- Email report@kernelcon.org

Conference staff will be happy to assist those experiencing harassment to feel safe for the duration of Kernelcon. Remember: The CON is what you make of it, and as a community we can create a great experience for everyone.

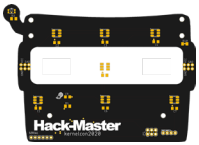
BADGES

Hacker Badge - these are the normal attendee badges. Why do we call us all hackers? Because we are a collection of hobbyists and professionals, blue, purple, and red teamers, students and life-long learners. We are hackers. Hacking is good.

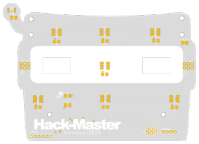
Speaker Badge - these are our esteemed speaker badges. We owe them a debt of gratitude for making the con what it is.



Crew Badge - these are our con volunteers. Looking for help? Reach out to our crew members on Discord and they'll do their best to help you find what you need. They help the event go smoothly.

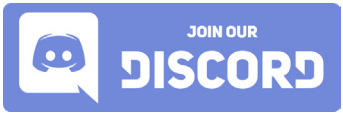


Organizer Badge - these badges are our organizing committee. If you have a con-specific question and/or need, please feel free to reach out to anyone with the organizer badge. They spent months planning and preparing to make Kernelcon what it is.



Instructor Badge - these are our wonderful instructor badges for trainers and workshop facilitators. We owe them a debt of gratitude for making the con what it is.

Eternal Kernel - Possessed by those that have shown their merit by winning a con event.



Roles:

Organizer

Speaker

Instructor

Crew

Hacker

STICKERS

Kernelcon is taking the normal hacker sticker tradition and turning it on its head! Each Kernelcon attendee has a few stickers to trade. Collect all 20! We also put out a call for stickers and the crew selected these following brave contestants:

Smash the Kernel by Rob Temple - The idea behind the sticker is a play on the POP and JMP commands, which obviously can be used to wreak maloc (I mean havoc) on memory and manipulate the stack. AND...if you're going to manipulate memory, well, you might as well Smash the Stack while you're there or were there or are pointing to there...(or Kernel in this case). I think you know what I mean. Congrats Kernelcon on another awesome year!!

Laptop by Zook (@ZookUS) - When I first heard about Kernelcon and the sticker submission program, I knew that I could come up with something that people might like. After a few drinks, I was able to come up with what you see now! The laptop actually features shellcode from the Author "SkuLL-HacKeR" and weighs in at just 19 bytes. It was originally tested on XP SP2 FR and launches calc.exe. I think that I had enough alcohol that day as I never fully completed the side of the popcorn box, for which I was going to write "Kernelcon". I hope that you enjoy my little adventurous creation though! (We added this for you Zook!)

Runza by Kaitlin B (@thetickingnoise) - The inspiration for this sticker idea came from other stickers, such as "hack for ramen." I wanted to make it special to Kernelcon, pulling from signature foods from Nebraska.

OK by Kaitlin B (@thetickingnoise) - Here is another sticker submission, based on the theme of the conference.

VILLAGES (1000 - 1800)

Resume Review (#jobs-hiring-resume)

Did you know your should update your resume every six months, even if you're not looking for a new job? Have a recruiting expert take a look at your resume and assist with advice on making it the best it can be. Sam Harvey, Warren Fish and Sydney Hardin of TEKsystems are volunteering on *Friday, March 27th* at the Kernelcon Jobs, Hiring & Resume village to provide professional resume review assistance. Attendees are welcome to join at any point throughout the day and should expect to spend 15-20 minutes discussing resume updates. After you share a resume the reviewer will help schedule a chat with you to recommend changes and provide general career advice. You might find just what you need to secure your dream job right at Kernelcon!

NARI OT Village (#nari-ot-village)

Almost every enterprise has an IT network - but have you ever seen an OT network? Visit our operational technology (OT) village complete with exercises on OT components. Curious about the traffic? OT PCAP exercises are available for the network investigator in you.

Mental Health and Wellness (#mental-health-wellness)

Instead of a traditional "Chillout village", Kernelcon has partnered with Mental Health Hackers. The Mental Health and Wellness Village offers a common place to allow like-minded individuals to share and grow as a community, to better our mental health and the health of those around us. Check out the village for fidget tables, crafts, adult coloring books, free chair massages and more! Visit https://www.mentalhealthhackers.org/ for more information.

~~TOOOL Lockpicking Village~~ We missed you this year!

Tired of staring at a monitor trying to hack your way through a computer... come try your hand [literally] at hacking hardware! The Open Organisation Of Lockpickers [TOOOL] is set up and ready to give you a new kind of challenge. Gaining access has a different meaning here. TOOOL uses their knowledge to guide you through different types of locks, their vulnerabilities, and how to exploit them. Scrape pin tumblers instead of data!

~~Hardware Hacking Village~~ We missed you this year!

Hardware hackers and novices alike, come learn the secrets of the Kernelcon badge and more at the Hardware Hacking Village. Never soldered? Now's your chance to play with molten metal! Our experts will help teach you how to add the blinky-blink. More experienced? Chat with the people who created the badge, trade SAOs or bring your own electronics project to show off. We will have small project kits and tools available for everyone to practice their soldering skills.

COMPETITIONS (1000 - 1800)

Capture-the-Flag Event (#kerneltron-ctf)

Our Annual Kernelcon Capture the Flag event is back and better than ever, with all new challenges, prizes and a new, fun theme! The competition this year is sure to be fierce with the winning team receiving our coveted Eternal Kernel badges. CTF challenges to include web hacking, reversing, pwning, cryptography, and a whole lot more. In fact, maybe we have already hidden some flags around the internet. Do you have the team to beat this year? If so, we will see you at Kernelcon CTF!

~~WiFi Fox and Hound Challenge~~ We missed you this year!

Have you ever wanted to crack your neighbors WiFi network? We all have at one point or another, but that's illegal, so come on down to the WiFi Fox and Hound where you can crack WiFi networks in a safe, consensual, and legal competition designed to test your abilities in WEP, WPA, and WPA2 cracking. We will be hiding access points around the hotel with various levels of security on them. It will be your job to find them, and break into the networks and recover the key/flag. Once you have the flag enter it in the scoring site to get those points! Contest will run the duration of the conference. Think you have what it takes? Then come show us your 1337 WiFi skillz and compete in the WiFi Fox and Hound event. Even if you're new to WiFi hacking, we'll have plenty of resources to help you along your way. You can even win fabulous prizes!

~~Backdoors & Breaches~~ We missed you this year!

Backdoors & Breaches, and Incident Response card game from Black Hills Information Security & Active Countermeasures has been spreading across the hacking community, and Kernelcon is happy to host one of the first Competitive Backdoors & Breaches events! Stop by on Friday to learn how to play the competitive version of Backdoors & Breaches, and then sign up for the tournament on Saturday. For more information on Backdoors & Breaches you can visit backdoorsandbreaches.com.

TRAINING

This was the training offered at Kernelcon this year. We hope you can join us next year!

Advanced Attack Infrastructure

Jason Lang

Still sending shells directly to your private C2 server? This course will teach you how to proxy your traffic through the cloud (AWS), ensuring your C2 endpoints are protected at all times. We will cover dealing with incoming sandbox connections, domain categorization, infrastructure automation using ansible, as well as complete infrastructure buildout start to phish. :-) Students will come away with full knowledge of how to build out a red team infrastructure capable of handling the demands of modern red teaming, including supporting multiple team members and clients simultaneously while ensuring your C2 servers are protected from prying defenders. While the class is designed for red teamers, defenders are welcome and will learn how modern attack infrastructure is designed and utilized.

Atomic Purple Teaming

Jordan Drysdale | Kent R. Ickler

You've heard this story before. Bad actor walks into a network and pillages the place in swift action. CIO asks "Where did we go wrong?" SysAdmin replies "our password, remote access, workstation restriction, and lack of application whitelisting policies. Oh, and our SIEM didn't notify us. We just weren't ready for that attack." Atomic Purple Teaming (APT) will guide students through attack and defense methodology using the MITRE ATT&CK Framework and the Atomic Red Team tactics to produce a secure enterprise environment. The course covers secure network designs, OSINT based reconnaissance, basic command and control (C2) operations and modern defenses that stop or slow down current adversarial techniques. Network and Active Directory Best Practices will be leveraged as a framework for implementing network and domain protections to harden networks. Students will have an opportunity to attack their own in-class Active Directory environment with Red Team tactics, implement Blue Team defensery, and manage an environment designed to prevent, slow, identify and highlight attacks. Additionally, the course will guide students through configuring no-nonsense attack identification and alerting that is essential to an effective SOC operation. In a live-environment, students will have the opportunity to demonstrate a secured enterprise environment by utilizing the MITE ATT&CK Framework, Red Team tactics and Blue Team defenses to slow, stop, and identify attacks. Implement better security and tell your CIO how everything went right!

TRAINING

Black Hat Go

Chris Patten | Dan Kottmann

Based on the 2020 book Black Hat Go (No Starch Press), this course will guide students on a path to the creation of a basic command-and-control (C2) client/server application. Taught by the book's authors, the course journey begins with a high-level overview of the language, discussing what it is and when it makes sense for development. Next, to ensure students have a basic understanding of the language, we'll review the general syntax, conventions, and idioms. This by no means a comprehensive review of the language but is instead intended to give a brief foundation upon which the subsequent examples will be built. Following this foundational overview, we begin the fun. We start by collaboratively developing a basic HTTP server and a client implant that interacts with the server. As part of this, we'll explore HTTP communications and detail how to very cleanly work with JSON payloads. We'll have the students cross-compile their implants for easy distribution across architectures. As time permits, students will be adding to it the ability to remotely execute operating system commands, increasing security of our interactions by adding authentication and encryption, adding the ability to execute raw shellcode, and creating a concurrent port scanner used by an implant to scan internal network resources.

Control System Analysis and Defense

Brad Miller | Josh Bunstock

Ready to get your hands dirty? NARI's Control System Analysis and Defense workshop is an interactive introduction to the basics of cybersecurity of Industrial Control Systems (ICS) and components. Examine ICS protocols, firewalls, segmentation, device monitoring, and more. You will have the opportunity to interact with live ICS testbeds via multiple hands-on exercises. Leave with a greater understanding of OT equipment and system protocols. Ultimately, you will be equipped with knowledge to protect and defend against malicious attacks.

TRAINING

Hands On Web Application Hacking - Intro

Alex Lauerman | Tyler Rosonke | Matt South

Learn the tools and techniques for conducting a web application penetration test. Get your hands dirty with HTTP and Burp Suite. This workshop will provide a solid introduction to web application penetration testing. This class is designed for those with little to no web application penetration testing experience, although it will move quickly. This class will include hands on challenges where attendees use skills acquired during the class to exploit web applications. Attendees will walk away with a basic understanding of the tools and processes for conducting a web application penetration test.

Introduction to Ghidra

Chris Eagle

This course is designed to introduce students to the essential features of the Ghidra disassembler/decompiler. The course begins with Ghidra installation and project creation, then moves on to cover all of the default Ghidra displays to understand how they can help you in your reverse engineering efforts. Fundamental concepts such as parameter passing and stack frame are covered using binaries from a variety of architectures in order to understand various Ghidra displays and analysis capabilities. Ghidra's handling of complex data types is covered from both the disassemblers and the decompilers point of view. The course conclude with a discussion of configuring and using the Ghidra collaboration server, and an introduction to Ghidra scripting. No previous Ghidra or reverse engineering experience is assumed.

Kubernetes: Build, Secure, Attack

Zach Giezen

Ever wanted to learn Kubernetes but haven't set aside the time? Have a cluster but you haven't secured it yet? Don't know where to start! Want to add container security testing or orchestration security testing to your "bag of tricks"? If you answered yes to one of more of these questions then come join me and others like you for a fun day of hands on exercises and conversation around these exciting topics.

TRAINING

Linux Forensics

Hal Pomeranz

Linux is everywhere - running in the cloud, on cell phones, and in embedded devices that make up the "Internet of Things". Often neglected by their owners, vulnerable Linux systems are low-hanging fruit for attackers wishing to create powerful botnets or mine cryptocurrencies. Ransomware type attacks may target Linux-based database systems and other important infrastructure. As attacks against Linux become more and more common, there is an increasing demand for skilled Linux investigators. But even experiences forensics professionals may lack sufficient background to properly conduct Linux investigations. Linux is its own particular religion, and requires dedicated study and practice to become comfortable. This two-day course is a quick-start into the world of Linux forensics. Learn how to use memory forensics to rapidly triage systems and spot attacker malware and rootkits. Learn where the most critical on-disk artifacts live and how they can help further an investigation. Rapidly process Linux logs and build a clearer picture of what happened on the system.

Network Analysis Workshop

Brad Miller | Josh Bunstock

Have you ever wondered what network traffic looks like? NARI's Network Analysis Workshop employs a hands-on approach to develop a keen understanding of IP networks. You will delve into network traffic to discover the intersection between Information Technology (IT) and Operational Technology (OT). Open source tools such as GrassMarlin and Wireshark will be utilized to test your skills and knowledge of industrial protocols like BACnet. You will walk away with a broader understanding of network topologies, models, and communication. More importantly, you will be able to truly look beyond the ones and zeroes.

WORKSHOPS

Workshops are smaller, shorter, training sessions.

Radio Hacking 101 with RTL-SDR

Gus Gorman

Every security professional, from locksmiths to blue teams, should have an inexpensive RTL-SDR in their toolkit. Radio signals are everywhere, and many of them rely on obsolete or proprietary formats that are easy to intercept & analyze. Learn to catch & exploit these signals in this workshop; Using Linux & open source tools, you'll learn to hack the airwaves. Take home a RTL-SDR.

Friday	10:00am - 12:00pm
Saturday	12:30pm - 2:30pm

Sensing Things With Sensors and Things

Nathan Schlehlein | Clay Dowling

Sure, the cloud is great, but here on the ground there is a lot of data worth observing. Just how does information on stuff like temperature, distance, or direction end up as data? As a participant of this hands-on workshop, you will get the opportunity to fire up and program a ESP32 based microcontroller board (that you get to take home!) and use it to interface, make sense of, and report on data from a variety of sensors.

Friday	12:30pm - 2:30pm	3:00pm - 5:00pm

~~Introduction to Hardware Hacking and IOT: Lightstrip Edition~~

Matt Virus | Jay Keres

We missed you this year!

In this hands-on hacking village, users will be walked through creating a custom, fully open-source LED-strip controller. All software functions with 100% local control – no beaconing to external "cloud" services. A fully-functional android/iphone app provides interface/control to the created LED-controller via local wifi without external connectivity. An open API provides a web interface as well as simple integration into many home automation and alarm systems.

~~Making Light Work of Data Exfiltration~~

Riley Hester | Eric Wright | Ian Trent

We missed you this year!

Attendees will learn how to create a light-based data exfiltration receiver based on the esp32 to circumvent corporate firewalls via vulnerable smart lighting vectors. The esp32 receiver is capable of forwarding data over USB, Bluetooth, or Wifi. Hands on exercises with this sensor will be available to attendees to test their devices interactively with NARI lighting testbeds in the IoT Village.

WORKSHOPS

~~Introduction to Hardware Hacking and IOT: Smartplug Edition~~

Matt Virus | Jay Keres

We missed you this year!

In this hands-on hacking village, users will be walked through modifying a (minimally) functional smart-home outlet plug. In its default state, the smart plug runs feature- limited, insecure firmware and software that depends on cloud connections and, in most cases, beacons to an external address in China. We will replace the software with open- source pieces and configure the plug to run with 100% local-only, non-cloud, control. Users will also be shown how to connect the newly-converted plug into a home- automation platform for software control via MQTT which enables web-based control, voice-based control, and control of state by a physical button.

FRIDAY KEYNOTE - 0900

Now, For Something Completely Different

John Strand | Black Hills Information Security | @strandjs

Over the past two years we have see a perceptible shift in security issues. Traditional architectures like AD and DMZs are falling away and are being replaced with Cloud and IoT. So, how do we approach this new world?

In this talk, John will cover some core tools and techniques we use at BHIS every day to attack organizations. We will also use these tools and techniques to help frame attendees in their approach and mindset to testing these technologies.

Bio

John has both consulted and taught hundreds of organizations in the areas of security, regulatory compliance, and penetration testing. He is a coveted speaker and much loved teacher. John is a contributor to the industry shaping Penetration Testing Execution Standard and 20 Critical Controls frameworks.

SATURDAY KEYNOTE - 0900

In Search of Lost Bytes: Hardware Implants and the Trouble with Supply Chains

Sophia d'Antoine | Hacker in Residence at NYU | @Calaquendi44

Digital markets have quickly grown to international proportions, complexities in materials, development, and distribution have developed accordingly, resulting in market efficiency and, often overlooked, incalculable risks.

There is a fine line between acceptable and irreconcilable risk, while some risks are mitigatable, others are not, and ignoring the facts has disproportionate consequences. This presentation will explore modern supply chain security risks through a technical deep dive of 5G infrastructure and the political battles surrounding it.

However, a wider acknowledgment of the supply chain problem doesn't make it go away. We need to understand the inherent hardware vulnerabilities exposed. Currently, confidence in hardware security relies too much implicit trust — overlooking serious threats. Assurance in this area is hard won, manual, and costly.

To highlight this, several hardware implant techniques will be discussed, showcasing various attack methods as well as the point at which they are most likely to be exploited in a standard supply chain.

Bio

Sophia is the founder of Margin Research, based in New York City, and the Hacker in Residence at NYU. Previously she has served at the NSA as well as a commercial security company. She is an alumnus of RPI where she taught Modern Binary Exploitation and helped run RPISEC, the university CTF team.

Sophia has spoken at over a dozen conferences worldwide on topics ranging from automated exploitation to information operations.
Her current work focuses on finding novel solutions to unique security problems, software vulnerabilities, and information operations.

She has co-authored policy papers on topics in offensive cyber including an Executive Order and a Lawfare article on the risks associated with Huawei 5G. A mostly complete listing of conference talks and publications.

TALKS

A Hacker's Viewpoint: Planning the Attack

Robert George, Kristina Krasnolobova

A lot of work has gone into breaking out the stages of an attack. Unfortunately, many security teams focus on the detection of infiltration, data loss, or response after an attack. This focus skips over a more proactive approach to preventing the attack during the planning stages. There is a plethora of information publically available about a company and its employees that is collected prior to an attack. This information is used to find vulnerabilities in information systems. The information is also used to plan out social engineering which is used to gain system credentials or additional information about a company.

A Red-Teamer's Guide to Building a Blue Team

Mark Bayley

How blue teamers and red teamers think is fundamentally different. This talk will delve into some of those details from a perspective of appreciating the differences – but it will not focus exclusively on them, as it is geared towards how to build a strong security team in general. Some of the aspects of a good blue team is Incident Response team, tuning a SIEM, solidifying network security and other opportunities for a better overall security posture. It will not focus on KU Health system and our systems/solutions, but instead will involve leadership strategies, technical details, and security posturing areas to consider.

A Secure Design and Implementation of a Smart Home

Owen Parkins

Smart homes can be a highly contested cybersecurity topic. Some professionals are fearful of the technology that can be too close to home - and for good reason. With the current political climate regarding foreign made devices, many devices are not safe to have in the home. This should not stop professionals from gaining more experience with a rapidly expanding technology and figuring out a way to use it effectively. This talk describes a design and implementation of a secure smart home.

Adventures in Creating a Cybersecurity Dataset

Heather Lawrence

While the foray to apply machine learning to information security is new, there remain challenges to creating and accessing datasets that are beneficial to security research. This talk is going to discuss our journey in creating an open-source network security dataset, the community-accepted guidelines to creating good data, and the challenges we faced. Moreover, this talk examines the gap between academic datasets and data released by the professional community before providing resources to new datasets that have been released in neighboring areas.

Astrophotography - Backyard Robotics for Art and Science

Seth Eddy

This talk will be an introduction into of amateur robotic astronomy for imaging and science and will discuss the challenges and solutions for building robotic telescopes.

TALKS

Anybody wanna launch some missiles?

Dan Tentler

The computer security industry has several huge problems. These problems routinely coagulate together to from 'digital binary explosives' - naturally, in the wild. We can use these to gain access to places we shouldn't be able to reach. Imagine being able to have access to every spy satellite at once. How many barriers could you see past? What could you assert about a place? Could digital binary explosives get you past any of those barriers? It's broadly known just how ineffective the security industry is right now - but we're all happy living in denial about it. The security posture of large companies who were recently breached and did huge public DFIR campaigns are great examples, and live demos are even better examples - we're doing both. Live, on-stage, we'll discover some companies who have not yet been breached, but are candidates for a breach based on their security posture, and we'll cover how the current 'curriculum' of 'how to get a job in infosec' is partially to blame.

Attacking Secondary Contexts in Web Applications

Sam Curry

This talk explores attacking various 'secondary contexts' in web applications where data is being passed to an underlying internal HTTP server. We will explore the different approaches to targeting limited-access/internal APIs, the very strange interactions between different servers within the stack, and lastly the different types of vulnerabilities present in second stage HTTP services.

Better Phishing through Smarter Infrastructure

Chris Patten, Dan Kottmann

These days, everyone is looking for the phish that is either a generic drive-by or a more targeted campaign, such as a weaponized ransomware attack. Blue teams are smarter, instrumentation is smarter, and detection capabilities have advanced; especially in enterprise networks. Further, set aside all of the click-through/pre-manufactured commodity phishing security awareness services for a moment. The real question, what happens when adversaries aren't so brazen with their tactics and take smarter steps to counter detection? Pre-emptive strike campaigns that are both innocuous (almost forgettable) to glean target details before the real attack, the correct tooling to prevent prying defenders from reaching the command and control redirectors or malware servers, blacklists and whitelists, domain registration misdirection, and quite possibly peering into the void of the vast amounts of signal-to-noise honeypot data trawling the Internet while using it to become more situationally aware. The operators at STACKTITAN will discuss all of these topics and how proprietary tooling has helped shift their perspective on effective phishing techniques. Additionally, REAL mitigation techniques will be discussed to better prepare organizations to defend against these attack campaigns. In conclusion, the presentation will be informative with plenty of opportunity for collaborative discussion.

TALKS

Bash Bunny Basics

Anthony Bernard

Ever wanted to steal passwords and run other programs in seconds with only a small USB sized tool? No? Well, now you can! The Bash Bunny will allow you to program keystroke attacks, which then are executed at lightning speed once you plug it in. In this talk you will learn the basics of this device and a few programs.

Bio Hack: How Integrative Medicine Principles Can Change the Game in Cyber Security

Joseph Wilson

Cyber Security is an exceedingly complex space that requires extreme levels of investment in people, processes, and technology to make a large impact on an organization. Despite the investment, we often sit in the 'spin zone' and accept the status quo and lack of progress. However, there are parallels we can draw from other complex fields (in this case healthcare) to help us consider fundamental or alternative methods for solving the complex security issues we face. Join me in understanding the similarities between patient wellness and Cyber Security and the opportunities that lie ahead for us to improve our capabilities.

Breaking barriers: An introvert's story to InfoSec

Ryen Macababbad

Barriers can slow us down from reaching our goals but they don't have to block us. The key is not letting the gates stop you in your tracks and instead finding a way around or through them. This is hard enough without throwing in the introversion and imposter syndrome common to our industry. Join me while I walk through my journey overcoming the challenges of being an introvert trying to learn while overcoming the imposter syndrome that says I can't. You'll walk away with strategies to create opportunities that will showcase your strengths and ways to overcome the internal monologue that forever tells us we can't.

Building a Vulnerability Management Program - Avoiding Pitfalls, Managing Risk, and Mastering CYA

Megan Benoit

Building a vulnerability management program often feels like eating an elephant that's guarded by sharks — every time you try to take a bite, you're dodging someone that's trying to take a bite out of you. I am going to walk you through building an effective vulnerability management program: avoiding and mitigating common problems, navigating the organizational waters, and getting the most bang for your buck when it comes to reducing your risk. Vulnerability management is more than just running a scan and putting in tickets for remediation — it's about managing the people involved in the scanning and remediation processes and finding a middle ground that reduces your risk and makes operations happy.

TALKS

Dispelling myths of red/blue cyber competition through metrics

Kandy Phan

The DOE CyberForce Competition is an annual college event where student defenders compete against each other, defending their systems from red teams. The goal of this competition is to improve the technical skill sets of the students to prepare them for the work force. However, just randomly throwing red and blue teams together hoping that magic will happen is a recipe for disaster. But it's hard to correct deep-seated wrong views about these cyber competitions. So this year, at the Albuquerque site, we developed a process and automated tooling to collect data during the competition to answer questions such as the average number of vulnerabilities patched before game start time, ability for lateral movement without initial access, detection rate of more advanced C2, etc. This data is really important for us to get insights about the competition so that we can improve it for the students. Hopefully, more competitions will start collecting these types of metrics so that we can improve the state of cyber education events.

Exploiting Modern Desktop Applications

Matt Austin

Let's learn how to attack "Modern Desktop" applications. Specifically we will look at the blurring lines between desktop and web applications, and how embedded (browsers) renders can be exploited, the methods for discovering exploits, and how they can be fixed. On this journey we go over remote code execution vulnerabilities I discovered in apps like Teams, Outlook, Facebook Workplace, chat apps like Slack and Google Chat, and even a Docker sandbox escape. I will also be introducing a new IAST (interactive application security testing) tool I developed to help find these issues. Last and most importantly look at how to prevent / fix these issues in your applications.

Bit to Byte

Christopher Wright

Having to start over again after being fired from a 5-year job, I saw the trend of hacks and saw that cybersecurity was going to be a low unemployment industry. I went back to college and started this new career path at the age of 34. This presentation will showcase the path I have made going from graduating college with a BSIT degree and zero industry experience to getting a SoC analyst job to becoming a project engineer inside of 1 year from date of hire.

Key Duplication - It's not just for the movies!

Tony Virelli

Have you ever seen someone just walking around with a key hanging on thier belt? How about a wall of keys behind a security desk? Better yet, has anyone you know every posted a picture of the keys to the new home they just bought? Well, what if you could take a picture and easily duplicate that key with a 3D Printer? Sound like something from a James Bond film? Well it's not! Better yet, if you can just get a moment alone with a key, you can get an imprint of it in less than 2 minutes, return the key to the owner and then cast a duplicate of that key for later use.

TALKS

Kernelcon2020 Badge: nononoyes

Tyler Rosonke and Aaron Gunning

Ever been curious about how electronic badges, or printed circuit boards (PCB) in general, get made? Come ride along with this year's Kernelcon badge makers, @zonksec and @scotchsec, as they explain the rollercoaster of turning the Hack-Master badge idea into a reality!

Hacking your Cybersecurity Career

Ron Woerner

'How do I find a job in cybersecurity?' This is an issue for both new and experienced professionals. There continues to be a disconnect between those hiring and those looking. This session explains solutions to overcome the cybersecurity hiring gap. Whether attendees are looking to break into cybersecurity or land their next job, they can use hacker skills to make it happen. In this session, I'll explain three traits of a well-rounded cybersecurity professional, three areas for balanced learning, and steps for hacking your career including visualizing your goals, knowing the best path for you, social engineering your next boss, active learning and keeping your skills sharp. This session also presents the difference cybersecurity career paths based on the NIST National Initiative for Cybersecurity Education (NICE). To get the right job, use hacking techniques to break through the hiring process. Learn how here.

Getting started with OSINT

Jamie Maguire

The first step of a Penetration Test is often called Reconnaissance, Information Gathering or OSINT. During this step, Penetration Testers attempt to gather as much information as they can about a target environment by using publicly available information. Unfortunately, this step may be ignored or not completed thoroughly. This is intended to be a 101-level presentation in which we discuss how an attacker may conduct reconnaissance against a target, and what specific information they might be interested in gathering. We will cover specific tools including theHarvester, Shodan, Recon-ng and more. This presentation is intended to give Security Professionals and Administrators an understanding of how attackers conduct information gathering against environments. Audience members will see specific examples of tools and techniques that they can apply to their own environments. We will not cover any new or novel techniques, but my goal is to provide the audience with the knowledge to gather meaningful information quickly.

How Ghidra changed my life

Chris Eagle

Anyone that knows me also knows that I'm a huge IDA Pro fanboy. Ghidra, the NSA's answer to IDA, has been in the public's hands for about a year now, so where does that leave me? Still solidly in the IDA camp, but that doesn't mean that Ghidra hasn't had an impact on my life. Thanks to the magic of open source we can take one of Ghidra's nicest features and bolt it onto IDA to fill some gaps in IDA coverage. In this talk, I'll introduce the 'Binary Lifting Component' (it's kinder name), or just blc for short, plugin for IDA. blc takes the core of Ghidra's decompiler capability and builds an IDA plugin around it to add decompilation capability to IDA for all processors supported by Ghidra.

TALKS

Let The Right One In

David Boyd

Charles Dickens is quoted as saying, 'A very little key will open a very heavy door.' Physical penetration testing is often overlooked when it comes time for a company's annual security assessment. Oftentimes, physical is left out for even a full-scope Red Team exercise. I've heard all of the reasons (excuses) why: 'we have guards,' 'we have locks,' 'card reader access,' 'we know it's an issue, just not a priority,' or 'it seems like cheating,' and the list goes on. I am here to discuss why Physical Penetration Testing/Physical Red Teaming is not only beneficial, but also crucial to a company's security well-being. I will review what physical red teaming is, how physical red teaming differs from traditional physical penetration tests, some of the tactics used in bypassing physical security controls, how closely tied physical security is to the overall posture and effectiveness of security training programs and policies, and will give several scenarios in which a physical intrusion opened several more doors (pun intended) during Red Team excursions.

Passwords are dead? Long live WebAuthn!

Alex Lauerman, Matt South

Password security is getting out of hand. You only need to watch the latest news stories about large-scale breaches or visit the haveibeenpwned site to see the current state of password security. Expecting end users to invent complex passwords for every web site they visit is untenable. Wouldn't it be great if there was some new technology that uses public key exchange and biometrics to get rid of passwords all together? Well, that technology is here. WebAuthn (Web Authentication) is a web standard published in 2019 by the World Wide Web Consortium (W3C). The goal of the project is to standardize an interface for authenticating users to web-based applications and services using public-key cryptography instead of passwords. Despite being an emerging technology, this standard has already been adopted by leading browsers and platforms. This talk aims to shed light the technical details of what WebAuthn is and how it works. We will also cover the security pros and cons of this new standard and make predictions about what this may mean for the future of web application security. This is an introductory talk. You do not need any prior knowledge of web authentication or cryptography to benefit from this talk.

Protecting your Small or Medium Business from Cyber Attacks

Jeff Struik

Small and Medium businesses are prime targets for malicious actors. Lacking the budgetary freedom that larger businesses may have for cyber security and limited personnel resources presents a large bullseye on many small and medium business. This talk addresses various free or built-in options for an organization to use to protect their systems from cyber attacks and reduce their attackable surface.

TALKS

The Beginner's Guide to Pentesting ICS: How NOT to Shut Down A Power Grid

Dan Bougere

Learn what exactly is SCADA/ICS, why it's important, how horrifyingly ancient it all still is, and how to pentest it without kicking over generators or flooding toxic gases everywhere! If you want to hear jaw dropping stories, lose sleep over chemical plants on your commute, or find that nice job niche that's hiring everywhere now is your chance.

The DIY Artificial Pancreas: Hacking Wetware with Open Source Software and Hardware

Jay Lagorio

Technology to manage diabetes revolves around stagnated tech from the 80s and 90s. Hackers took their lives into their own hands by developing open source hardware and software to augment inadequate products. Developing and building a DIY artificial pancreas, its iterations, and real-life examples of will be discussed and at least one will be working on the presenter. Taking the human out of the loop and replacing them with technology increases quality of life. See what happens when hackers decide they're not waiting around for government and the MedTech industry to do better. Managing diabetes revolves around stagnated tech from the 80s and 90s. Hackers took their lives into their hands by augmenting inadequate products after market. Building iterations of a DIY artificial pancreas and real-life examples of will be discussed and at least one will be working on the presenter. Replacing human intervention with technology betters quality of life. See what happens when hackers decide they're not waiting around for government and the MedTech industry to do better.

The Top 10 Tools For Cloud Penetration Testing

Michael Born

As organizations move their traditional on-prem environments to the cloud, penetration testing tools and techniques must also adapt. This talk will highlight the top 10 tools every penetration tester should add to their arsenal when performing a penetration assessment against a cloud environment. Tools covered will work against Azure/Office 365, Google Cloud/G Suite, and AWS.

Unleash your Camera with CHDK

Aaron Grothe

Cannon Hack Development (CHDK) was initially created to allow features in Canon Cameras such as RAW image output to be available on cameras that came without them. Since then additional features have been added to CHDK that have made it more useful to many people. Some of these features are: scripting, high speed photography, 3d pictures, live histograms and many more. This talk will cover all the steps needed to create an SD card with the CHDK software and show some of the features that makes available. We'll also talk about some of the other free firmwares available such as 400plus, Spy Lantern and Magic Lantern.

TALKS

How to Pave a Path Forward for InfoSec by Hacking Hearts and Minds

Chad Calease

Messages transmitted about privacy and security over the past 200 years or so haven't always been very friendly or accessible and many are in direct contrast to today's definitions, expectations, and requirements. We'll take a fast but memorable stroll through history to illuminate a new path forward lit by some quick-win hacks to address these cultural challenges and elevate our understanding of, interest in, and ability to hack how our families, friends, colleagues, clients, and - potentially - how the world-at-large thinks about, understands, and values privacy and information security.

KetoAppSec: It's All about the FATS

David Lindner

The Ketogenic diet has taken form over the past few years and it actually works. So how can we apply something similar to our application security practices? Application security traditionally focuses on tools or manual testing. We traditionally do "static (SAST)" or "dynamic (DAST)" tool assessments and label them as a "full" or "time-boxed" assessment. The driving force is usually budget or lack thereof, so how do we trim down our assessment methodologies yet be efficient, precise and beneficial? There are many ways to be more efficient in the way we AppSec to get the most benefit out of the time we have. Whether it be making risk-based decisions, looking for patterns, understanding frameworks and their built-in protections, we can make intelligent choices and guesses. David Lindner will walk through some tips and tricks that will help consultants and internal testers alike focus on the fat of applications in a shortened timeframe.

Pirate Radio: Riding the Ragged Edges

Michael Tomasiewicz

For the hobbyist, radio is technically fascinating. For the uninitiated, black-magical. What they both have in common? The FCC will be happy to fine the S#!& out of you if you violate the law regarding illegal uses of reserved bands, particularly commercial FM frequencies. We'll talk about why "pirates" pirate on FM, affordable gear options, and how to experiment with the technology without being fined back to the stoneage.

The Top 10 Tools For Cloud Penetration Testing

Michael Born

As organizations move their traditional on-prem environments to the cloud, penetration testing tools and techniques must also adapt. This talk will highlight the top 10 tools every penetration tester should add to their arsenal when performing a penetration assessment against a cloud environment. Tools covered will work against Azure/Office 365, Google Cloud/G Suite, and AWS.

WannaWorm

Michael Kunz

Ever wonder how to build a worm? Mike will demonstrate how to build a ghetto worm using wanna cry. He's also going to talking about some of his work with large scale emulation using the government funded Open Source tool Minimega. Combining the two, he'll use Minimega to run the worm.

THANK YOU TO OUR SPONSORS

PLATINUM

GuidePoint SECURITY
LEADING SECURITY INNOVATION

Check Point
SOFTWARE TECHNOLOGIES

GOLD

fnbo
First National Bank of Omaha

fnts

BRONZE

Secureworks®

CONAGRA BRANDS

TIN

SIRIUS

CONTRAST SECURITY

THANK YOU TO OUR SPONSORS

CTF SPONSOR

splunk> SecureSky

OTHER SPONSORS

TOOOL
The Open Organisation Of Lockpickers

MENTAL HEALTH HACKERS

NEBRASKA APPLIED RESEARCH INSTITUTE
at the University of Nebraska

no starch press

COFFEE

UBT
Union Bank & Trust.
You belong here.℠

SecureSky

POPCORN

UBT
Union Bank & Trust.
You belong here.℠

Secureworks

perspecta™

FOREFRONT 17 SEVENTEEN