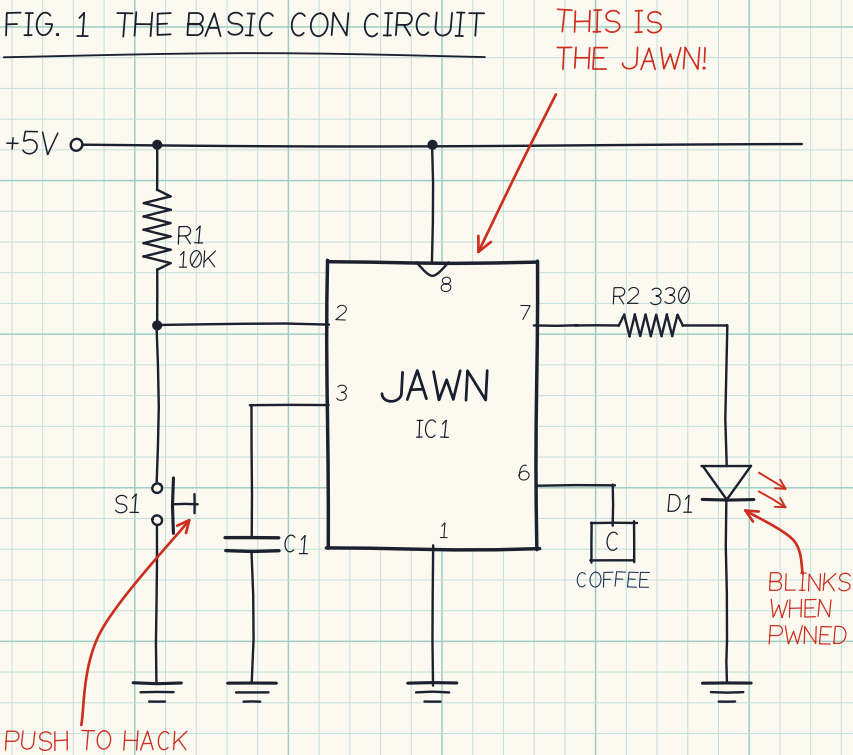


JawnCon™ 0x3

PROGRAM GUIDE

FIG. 1 THE BASIC CON CIRCUIT



PHILADELPHIA, PA
OCTOBER 16-18, 2026

WELCOME JAWNS!

JAWNCON 0x3

WELCOME TO JAWNCON0x3, OUR 4TH YEAR RUNNING! STEP ABOARD OUR JAWNDOLA, SO WE CAN TAKE YOUSE ON A WOODED CRUIZE TO THE INFORMATION SUPERHIGHWAY! THERE'S A LOT TO EXPERIENCE THIS YEAR AS WE'VE EXPANDED IN SPACE AND DURATION. ALL THE TALKS WILL BE IN THE UNIVERSITY COMMONS BUILDING, WITH TRACK 1 BEING DOWNSTAIRS, AND TRACK 2 BEING UPSTAIRS. THE CHILLOUT AND SOLDERING SPACE IS NOW AT MURPHY HALL, UP THE HILL. PLEASE ASK ANY OF OUR STAFF FOR HELP IF YOU NEED IT. FOR IMMEDIATE AND UP TO DATE INFORMATION, YOU CAN GO TO [HTTPS://0x3.JAWNCON.ORG](https://0x3.jawncon.org).

IN THIS GUIDE

CTF & THE BADGE	3
FRIDAY SCHEDULE	5
SATURDAY SCHEDULE	6
SUNDAY SCHEDULE	8
SPEAKERS & ABSTRACTS	9
CHILLOUT SPACE & HAM EXAM	25
NOTES	27

BE EXCELLENT TO EACH OTHER

WI-FI

SSID: **JawnCon0x3**

SIGN IN: [WIFI.JAWNCON.NET](https://wifi.jawncon.net)

ACCEPT THE AUP ON THE PORTAL TO GET ONLINE



CTF & THE BADGE

JAWNCON 0x3

CAPTURE THE FLAG

COME PLAY OUR CTF! OUR CTF FOCUSES ON INTRODUCING PARTICIPANTS TO FUNDAMENTAL CONCEPTS IN TECHNOLOGY INFRASTRUCTURE AND SECURITY IN A CREATIVE WAY. WE DESIGNED IT AS A FUN AND ENGAGING EVENT FOR PARTICIPANTS OF ALL SKILL LEVELS, FROM BEGINNER STUDENT TO SEASONED CURMUDGEON. THE CHALLENGES IN THE CTF SHOWCASE THE INNER WORKING OF THE TECHNOLOGIES THAT BUILT THE MODERN INTERNET AND STILL UNDERPIN IT TODAY. WE SHOWCASE TECHNOLOGIES FROM THE BEGINNING OF COMPUTING TO THE PRESENT DAY, WITH AN EMPHASIS ON HANDS-ON PUZZLE SOLVING.

PUZZLES INVOLVE TECHNICAL SKILL, LATERAL THINKING, AND RESEARCH. YOU'LL ENCOUNTER SOME FUN AND WEIRD CHALLENGES ALONG THE WAY. ABOVE ALL, WE WANT YOU TO HAVE FUN AND LEARN SOMETHING!

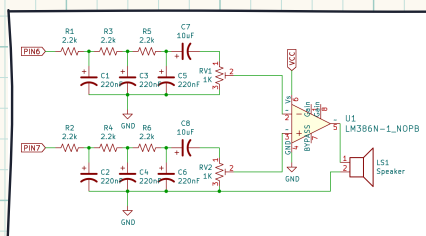
THE BADGE

WE'VE BROUGHT YOU PUNCH CARDS, MODEMS AND PI. THIS YEAR, YOU HAVE A MULTI-FUNCTION CALCULATOR. YES, IT FUNCTIONS AS A CALCULATOR, BUT IT ALSO FUNCTIONS AS A FIDGET DEVICE. THREE GAMES ARE ACCESSIBLE BY PRESSING THE FOLLOWING COMBINATION: 1337=, 1338=, 0203=. THE FIRST GAME IS A HI/LOW NUMBER GUESSING GAME, THE SECOND IS SIMON SAYS WITH DTMF TONES, AND THE THIRD WILL TEST YOUR ABILITY TO DO HEX MATH! OH, AND IF YOU WANT TO ADD ON TO THE BADGE, THAT CARD EDGE CONNECTOR WILL BE USEFUL IN THE SOLDERING STATION AT MURPHY HALL. MORE INFORMATION ABOUT THE BADGE IS AVAILABLE TO BE SEEN AT [HTTPS://JAWNCON.ORG/BADGE.HTML](https://jawncon.org/badge.html)

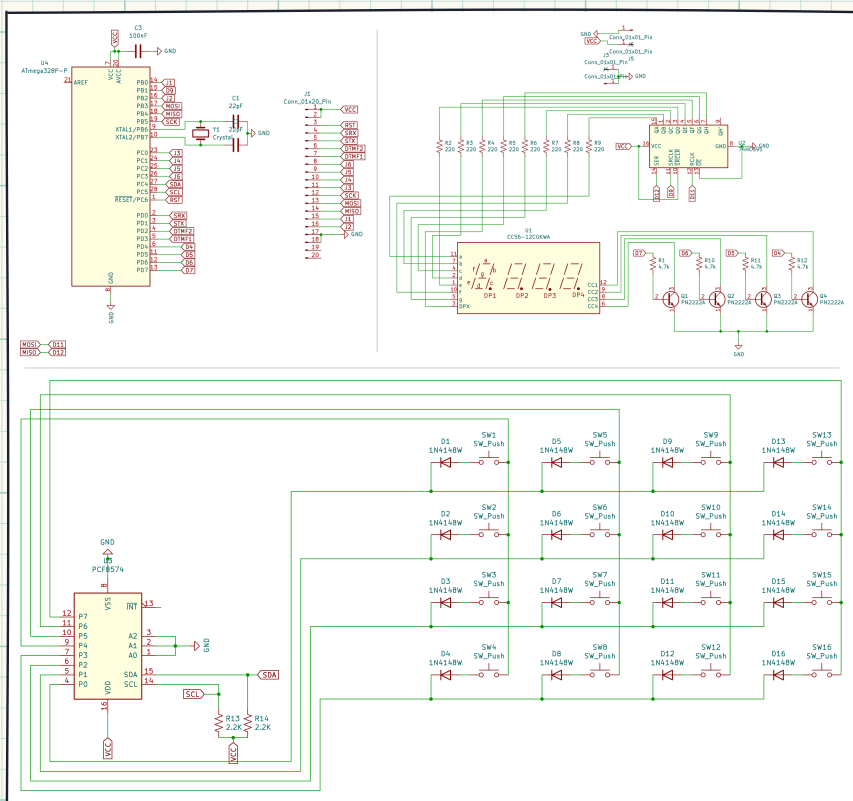
BADGE SCHEMATIC

JAWNCON 0x3

DTMF GENERATOR



THE BADGE



SCHEDULE – FRIDAY

JAWNCON 0x3

TIME	WHAT / WHO	WHERE
9:15 AM	OPENING REMARKS RUSSELL HANDORF	TRACK 1
10:00 AM	KEYNOTE: THE HARDEST EASY PROBLEM I'VE EVER SEEN DR. MATT BLAZE	TRACK 1
11:00 AM	THE WHITE HAT HACKER AND THE COMPUTER FRAUD AND ABUSE ACT MICHAEL LEVY	TRACK 1
1:00 PM	AI GOVERNANCE - THERE'S SO MANY STANDARDS!! WHAT SHOULD I USE???	TRACK 1
	JOSHUA MARPET	
	A BOOT TO THE HEAD: CYBERSECURITY LEARNED FROM THE MOSH PIT AND HOW TO USE THEM BEFORE THE WORLD GOES COMPLETELY TO HELL GEORGE SANDFORD	TRACK 2
2:00 PM	SCREEN TO TABLE: HOW BOARD GAMES CURED MY DIGITAL FATIGUE MIKE D'AMELIO	TRACK 1
	HOW TO MAKE A CYBER DRAGON GARY COHN	TRACK 2
2:30 PM	HAM FOR HACKERS ED WILSON	TRACK 1
3:00 PM	THREAT INTEL IS MUTUAL AID: BUILDING A PEOPLE-FIRST SHARING NETWORK MICHAEL TAGGART	TRACK 1
3:15 PM	HACKER PUBLIC RADIO + WHY YOU SHOULD LISTEN, AND CONTRIBUTE. MURPH NJ	TRACK 2
4:00 PM	STILL POSSIBLE: LAND A CYBERSEC JOB IN THE AI ERA RAYMOND POMPON	TRACK 1
	FROM GAME HACKING TO ECRIME (FEAT. MECCHA CHAMELEON & CSGO) SPEAKER TBA	TRACK 2

SCHEDULE – SATURDAY

TIME	WHAT / WHO	WHERE
9:00 AM	HAM RADIO STUDY AND EXAM NICOLE A2DIM	MURPHY 117
10:00 AM	AI SECURITY MYTHS WE CAN FINALLY STOP REPEATING SPACE ROGUE	TRACK 1
	EVERYDAY FLIPPER, FROM TVS TO TRACKERS: BASIC TASKS FOR THAT FLIPPER ZERO YOU BOUGHT BUT RARELY TOUCHED GREY FOX	TRACK 2
11:00 AM	WHEN RESPONSIBLE DISCLOSURE FAILS: A COLLABORATIVE FRAMEWORK FOR ZERO-DAY REPORTING CHRISTY CARABALLO, WILLIAM ENTRIEN	TRACK 1
1:00 PM	BREAKING PBKDF AND JAVA ENCRYPTION - ADVERSARIAL CRYPTANALYSIS AND TECHNIQUES KEN PYLE	TRACK 1
	POWER WITHOUT BINARIES: BRINGING NATIVE OFFENSIVE TECHNIQUES TO FILELESS RUNTIMES JACOB COVEY	TRACK 2

CONTINUED →

SCHEDULE – SATURDAY (CONT.)

TIME	WHAT / WHO	WHERE
2:00 PM	BRINGING YOUR PRODUCT TO MARKET - "JUST THE HIGHLIGHTS" JONATHAN SPANGENBERG	TRACK 1
	IDENTITY ALL THE WAY DOWN AMANDA DRAEGER	TRACK 2
2:30 PM	VEILID: THE PRIVATE INTERNET WE WERE ALL PROMISED BIANCA LEWIS	TRACK 1
	PUSHING THE LIMITS OF STATIC SITES JEFF GOEKE-SMITH	TRACK 2
3:00 PM	IT TAKES A HARDWARE VILLAGE - THE MAKING OF THE WHOSE SLIDE IS IT ANYWAY DEF CON BADGE DANNY AKACKI	TRACK 1
	APT, MEET OPSEC: TURNING MISTAKES INTO INTELLIGENCE ØXFFARADAY	TRACK 2
4:00 PM	LUA BEFORE LUA: THE RECOVERED WORKS OF LOUISE URSULA ALBRIGHT (APPLE //E, 1987) JORJ BAUER	TRACK 1
	TAKING BACK CONTROL OF YOUR DIGITAL MUSIC: REVIVE YOUR MP3 PLAYERS WITH ROCKBOX SPEAKER TBA	TRACK 2

SCHEDULE – SUNDAY

JAWNCON 0x3

TIME	WHAT / WHO	WHERE
10:00 AM	WARDDRIVING AI VICTORIA WHITAKER	TRACK 1
	SOFTMODEMS ARE COOL NOW: THE DARK ART OF V.34 PHIL PEMBERTON	TRACK 2
10:30 AM	PAGING IN 2026 - FROM CURRENT CARRIERS TO OSS AND HOBBYIST NETWORKS MIKE DANK, NAVEEN ALBERT	TRACK 1
11:00 AM	THOUGHT ON SYSTEM SECURITY ASSESSMENTS BRUCE POTTER	TRACK 2
11:30 AM	HACK THE MISSION: FROM HACKER TO NONPROFIT BOARD PRESIDENT FRANK CLOWES	TRACK 1
1:30 PM	CLOSING REMARKS RUSSELL HANDORF	TRACK 1

SPEAKERS & ABSTRACTS

FRIDAY

OPENING REMARKS

RUSSELL HANDORF

FRI 9:15 AM • TRACK 1

INFORMATION ABOUT WHAT ALL YA'LL JAWN ARE ABOUT TO EXPERIENCE!

KEYNOTE: THE HARDEST EASY PROBLEM I'VE EVER SEEN

DR. MATT BLAZE

FRI 10:00 AM • TRACK 1

ELECTIONS ARE PRETTY IMPORTANT, BUT LATELY, IT SEEMS LIKE WE DON'T TRUST THEM. IRONICALLY, RECENT ADVANCES IN ELECTION TECHNOLOGY, PROCESSES AND ARCHITECTURE MEAN THAT US ELECTIONS ARE PROBABLY AS SECURE AND ROBUST AS THEY'VE EVER BEEN IN HISTORY, YET TRUST IN ELECTIONS SEEMS TO BE AT AN ALL TIME LOW.

THIS TALK WILL GIVE AN OVERVIEW OF HOW ELECTIONS ACTUALLY WORK, THE THREATS AND SAFEGUARDS THEY OPERATE UNDER, AND THE CONFOUNDING PROBLEM OF MAKING THEM NOT JUST TRUSTWORTHY, BUT ACTUALLY TRUSTED.

THE WHITE HAT HACKER AND THE COMPUTER FRAUD AND ABUSE ACT

MICHAEL LEVY

FRI 11:00 AM • TRACK 1

THE COMPUTER FRAUD AND ABUSE ACT (CFAA) WAS FIRST PASSED BY CONGRESS IN 1986. IT HAS BEEN AMENDED MANY TIMES, EXPANDING ITS COVERAGE AND ADAPTING TO THE RAPIDLY CHANGING WORLD OF COMPUTING. ORIGINALLY, ALL "HACKERS" WERE WHITE HATS - PEOPLE INTERESTED IN EXPLORING THE WORKINGS OF COMPUTERS AND NETWORKS. COMPUTERS HAVE INCREASED IN SPEED AND POWER, AND THE INTERNET HAS CHANGED FROM A MILITARY COMMUNICATIONS NETWORK INTO WHAT IT IS TODAY SINCE THE ACT WAS PASSED. WITH THOSE DEVELOPMENTS, SOME HACKERS SAW OPPORTUNITIES FOR PROFIT OR MALICIOUS DAMAGE, CREATING THE DIVIDE BETWEEN WHITE HATS AND BLACK HATS (WITH A FEW IN BETWEEN). THE CFAA IS PROPERLY APPLIED TO THE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

THE WHITE HAT HACKER AND THE COMPUTER FR... (CONT.)

BLACK HATS. BUT LARGE QUESTIONS REMAIN ABOUT WHITE HATS AND THE CFAA. THE CFAA OUTLAWS UNAUTHORIZED ACCESS AND UNAUTHORIZED DAMAGE TO COMPUTERS. BOTH THE COURTS AND THE U.S. DEPARTMENT OF JUSTICE HAVE TAKEN STEPS INTERPRETING THESE PHRASES THAT MAY HELP WHITE-HAT HACKERS. MY TALK WILL DISCUSS THE PATH TO WHERE WE ARE TODAY.

AI GOVERNANCE - THERE'S SO MANY STANDARDS!!
WHAT SHOULD I USE???

JOSHUA MARPET

FRI 1:00 PM • TRACK 1

YOU'RE USING AI. YOU ARE, WHETHER OR NOT ANYBODY APPROVED IT. SO WHEN IT LEAKS YOUR DATA, MISLEADS A CUSTOMER, OR ACTS IN YOUR NAME, WHO'S ACCOUNTABLE? A PILE OF AI GOVERNANCE STANDARDS CLAIMS TO ANSWER THAT: SOME ARE LAW, SOME ARE RISK FRAMEWORKS, SOME ARE SELF-GRADED HOMEWORK, AND A FEW STILL HAVEN'T NOTICED THAT AGENTS EXIST. THIS TALK CUTS THROUGH THEM: WHICH ONE IS ACTUALLY POINTED AT YOU, WHICH ARE THEATER, AND THE GAPS EVERY ONE OF THEM LEAVES OPEN. CERTIFIED, ACCREDITED, SELF-ASSESSED, OR NONE OF THE ABOVE, COME FIND OUT WHICH YOU ACTUALLY NEED.

A BOOT TO THE HEAD: CYBERSECURITY LEARNED
FROM THE MOSH PIT AND HOW TO USE THEM
BEFORE THE WORLD GOES COMPLETELY TO HELL

GEORGE SANDFORD

FRI 1:00 PM • TRACK 2

THE MOSH PIT DOESN'T LIE.

IT STRIPS AWAY TITLES, ORG CHARTS, AND POLISHED LINKEDIN SUMMARIES. WHAT YOU'RE LEFT WITH IS RAW SIGNAL: WHO PICKS YOU UP WHEN YOU GO DOWN, WHO SEES YOU FALL AND KEEPS DANCING, WHO'S THERE TO RELEASE ENERGY TOGETHER - AND WHO SHOWED UP TO HURT PEOPLE.

GEORGE SANDFORD SPENT FORMATIVE YEARS IN THE PHILADELPHIA HARDCORE AND PUNK SCENE - THE TROCADERO, TLA, BASEMENT SHOWS WHERE THE CROWD WAS THE SECURITY MODEL. PHILLY CROWDS HAVE A REPUTATION FOR BEING INTENSE, UNFORGIVING, AND A LITTLE CHAOTIC. THEY'RE ALSO

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

A BOOT TO THE HEAD: CYBERSECURITY LEARNE... (CONT.)

FIERCELY LOYAL, DEEPLY COMMUNAL, AND GENUINELY DANGEROUS WHEN THREATENED. TURNS OUT THAT'S A PRETTY GOOD TEMPLATE FOR A SECURITY TEAM.

WE'RE PAST THE WARM-UP NOW. NATION-STATE ACTORS AREN'T PRETENDING. AI IS ACCELERATING ATTACKS WHILE QUIETLY AUTOMATING AWAY DEFENDERS. MONOCULTURES - ON TEAMS, IN TOOLING, IN THINKING - ARE DYING FAST. AND THE PEOPLE WHO WERE SUPPOSED TO KEEP THINGS SAFE? SOME ARE GONE. SOME ARE THE PROBLEM.

THIS ISN'T A METAPHOR. IT'S OPERATIONAL.

THIS TALK TRANSLATES HARD-WON PIT SURVIVAL SKILLS INTO CONCRETE TEAM-BUILDING AND LEADERSHIP PRACTICE: HOW TO BUILD TEAMS THAT ABSORB IMPACT WITHOUT BREAKING, HOW TO IDENTIFY AND EJECT BAD ACTORS BEFORE THEY CONSOLIDATE INFLUENCE, HOW TO PROTECT YOUR MOST VULNERABLE PEOPLE WHEN THE ENVIRONMENT TURNS HOSTILE, AND HOW TO MAINTAIN FUNCTION - AND HUMANITY - WHEN TRUST IS FRACTURED AND INSTITUTIONS HAVE FAILED.

COMMUNITY ISN'T NETWORKING. IT'S MUTUAL DEFENSE. DIVERSITY ISN'T A CHECKBOX. IT'S OPERATIONAL RESILIENCE. PICKING EACH OTHER UP ISN'T CHARITY. IT'S INFRASTRUCTURE.

YOU'LL LEAVE WITH REAL FRAMEWORKS, NOT INSPIRATION PORN. COME READY TO WORK. LEAVE WITH SCARS AND SKILLS. BECAUSE SITTING THIS ONE OUT WAS NEVER AN OPTION.

SCREEN TO TABLE: HOW BOARD GAMES CURED MY DIGITAL FATIGUE

MIKE D'AMELIO

FRI 2:00 PM • TRACK 1

THE COVID LOCKDOWN OF 2020 MADE ME REALIZE JUST HOW MUCH OF MY LIFE WAS IN FRONT OF A SCREEN: PLAYING ON MY PHONE, WORKING ON MY COMPUTER, AND WATCHING TV. THE WORLD OF BOARD GAMES HELPED ME APPRECIATE HOW IMPORTANT REAL INTERACTIVITY, CONNECTION, AND COMMUNICATION TRULY ARE, AS WELL AS THE NEAR-ENDLESS VARIETY OF THEMES, MECHANISMS, PUZZLES, COMPLEXITIES, AND TYPES OF GAMES AVAILABLE. IF YOU'RE FEELING STUCK IN A DIGITAL LANDSCAPE OR LOOKING FOR A NEW CHALLENGE THAT DOESN'T REQUIRE POWER, JOIN ME AT THE TABLE AND LET'S PLAY!

SPEAKERS & ABSTRACTS (CONT.)

HOW TO MAKE A CYBER DRAGON

GARY COHN

FRI 2:00 PM • TRACK 2

BY POPULAR REQUEST - A TALK ON HOW TO MAKE YOUR VERY OWN POLYGONAL LIGHT-UP DRAGON HEAD MASK! THIS WILL BE BROKEN INTO A TALK + WORKSHOP. AS A FULL BUILD WOULD TAKE MUCH LONGER THAN CAN BE DONE DURING A WORKSHOP, THE WORKSHOP PORTION WILL FOCUS ON SOLDERING 101 - MAKING THE LIGHTING RIG FOR THE HEAD ITSELF.

HAM FOR HACKERS

ED WILSON

FRI 2:30 PM • TRACK 1

SOFTWARE-DEFINED RADIOS (SDRS) LIKE THE RTL-SDR AND HACKRF HAVE MADE RADIO FREQUENCY SNIFFING A STAPLE OF THE HACKER TOOLKIT. HOWEVER, MOST SECURITY RESEARCHERS STOP AT PASSIVE RECEPTION OR LOW-POWER ISM-BAND EXPERIMENTATION. WHY LIMIT YOUR RF EXPLORATION TO MILLIWATTS AND 2.4 GHZ NOISE WHEN AN AMATEUR (HAM) RADIO LICENSE UNLOCKS UP TO 1,500 WATTS OF TRANSMITTING POWER, GIGAHERTZ OF DEDICATED SPECTRUM, AND THE LEGAL FREEDOM TO BUILD AND TEST CUSTOM WIRELESS HARDWARE?

THREAT INTEL IS MUTUAL AID: BUILDING A PEOPLE-FIRST SHARING NETWORK

MICHAEL TAGGART

FRI 3:00 PM • TRACK 1

IFIN, THE INDEPENDENT FEDERATED INTELLIGENCE NETWORK, IS A NEW NONPROFIT DEDICATED TO SHARING THE KNOWLEDGE OF HOW TO COLLECT, ANALYZE, AND EMPLOY THREAT INTELLIGENCE. IN THIS TALK, WE'LL SHARE OUR ORIGIN STORY, HOW WE'RE BUILDING A NETWORK OF PEOPLE THAT PROTECTS EACH OTHER AND THE INTERNET MORE BROADLY, AND HOW YOU CAN GET INVOLVED.

SPEAKERS & ABSTRACTS (CONT.)

HACKER PUBLIC RADIO - WHY YOU SHOULD LISTEN, AND CONTRIBUTE.

MURPH NJ

FRI 3:15 PM • TRACK 2

HACKER PUBLIC RADIO IS A COMMUNITY PODCAST THAT RUNS 5 DAYS A WEEK. IT IS DEDICATED TO SHARING KNOWLEDGE AND HAS BEEN RUNNING IN VARIOUS FORMS FOR NEARLY 20 YEARS. ANYONE THAT HAS ANYTHING THAT IS OF INTEREST TO HACKERS IS WELCOME TO SUBMIT A SHOW.

STILL POSSIBLE: LAND A CYBERSEC JOB IN THE AI ERA

RAYMOND POMPON

FRI 4:00 PM • TRACK 1

LOOK, THE CYBERSEC JOB MARKET IS ROUGH RIGHT NOW. EVERYONE'S TELLING YOU IT'S IMPOSSIBLE TO BREAK IN, THE ENTRY-LEVEL JOBS ALL WANT FIVE YEARS OF EXPERIENCE, AND AI IS GOING TO TAKE THE WHOLE FIELD ANYWAY. BUT HOLD ON, WE STILL NEED GOOD PEOPLE.

I'VE BEEN DOING THIS FOR 30 YEARS - HIRED PEOPLE, LET PEOPLE GO, WATCHED PEOPLE MAKE IT FROM SOME GENUINELY WEIRD STARTING POINTS. PHOTOGRAPHERS. LIBRARIANS. KIDS STRAIGHT OUT OF HIGH SCHOOL. NONE OF THEM HAD A PERFECT RESUME. ALL OF THEM HAD THEIR HEAD RIGHT AND KNEW WHAT TO ACTUALLY WORK ON.

THIS IS THE TALK NOBODY GAVE ME WHEN I WAS STARTING OUT. AS A HIRING MANAGER IN CYBERSEC, I'LL TELL YOU WHAT WE'RE ACTUALLY CHECKING FOR, INCLUDING HOW I STRUCTURE INTERVIEWS. WE'LL ALSO GET INTO WHAT'S REALLY HAPPENING WITH AI IN THIS FIELD AND WHAT YOU SHOULD BE DOING THAT WILL MATTER.

SPEAKERS & ABSTRACTS (CONT.)

FROM GAME HACKING TO ECRIME (FEAT. MECCHA CHAMELEON & CSGO)

SPEAKER TBA

FRI 4:00 PM • TRACK 2

THE OVERLAP BETWEEN GAME HACKING COMMUNITIES AND ECRIME GROUPS HAS NEVER BEEN MORE PREVALENT, WITH THE EMERGENCE OF STOLEN ACCOUNT MARKETPLACES AND GAME HACKING COMMUNITIES THAT RELY ON STOLEN ACCOUNTS TO CONTINUE CHEAT DEVELOPMENT EFFORTS AND CHEATING COMMUNITIES THAT ALSO UTILIZE THESE ACCOUNTS FOR PLAY, WHICH ARE TYPICALLY COMPROMISED THROUGH PHISHING, INFostealers, OR OTHER ACCOUNT TAKEOVER METHODS, SUCH AS SIM SWAPPING. THIS TALK WILL DIVE INTO THE OVERLAP BETWEEN THE TWO GROUPS AND THE PIPELINE THAT ESCALATES FROM CHEATING AND GAMING PLATFORM ACCOUNT TAKEOVER TO CRYPTO THEFT AND PHYSICAL VIOLENCE.

SATURDAY

AI SECURITY MYTHS WE CAN FINALLY STOP REPEATING

SPACE ROGUE

SAT 10:00 AM • TRACK 1

ARTIFICIAL INTELLIGENCE HAS BECOME CYBERSECURITY'S LATEST HYPE CYCLE. VENDORS PROMISE REVOLUTIONARY PROTECTION, HEADLINES PREDICT CATASTROPHIC ATTACKS, AND ORGANIZATIONS STRUGGLE TO DISTINGUISH GENUINE THREATS FROM MARKETING-DRIVEN FEAR, UNCERTAINTY, AND DOUBT.

THIS PRESENTATION EXAMINES SOME OF THE MOST COMMON AI SECURITY MYTHS AND COMPARES THEM TO REAL-WORLD CAPABILITIES AND RISKS. DRAWING ON DECADES OF EXPERIENCE OBSERVING SECURITY TRENDS, SPACE ROGUE EXPLORES CLAIMS THAT AI CAN AUTONOMOUSLY HACK ORGANIZATIONS, REPLACE SECURITY ANALYSTS, AND FUNDAMENTALLY CHANGE THE RULES OF CYBERSECURITY.

ATTENDEES WILL LEARN WHERE AI GENUINELY INCREASES RISK, SUCH AS DATA LEAKAGE, OVERPRIVILEGED AI AGENTS, AND AUTOMATION BIAS, AND WHERE TRADITIONAL SECURITY FUNDAMENTALS REMAIN THE MOST EFFECTIVE DEFENSE. THE SESSION WILL ALSO EXAMINE HOW DEFENDERS CAN LEVERAGE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

AI SECURITY MYTHS WE CAN FINALLY STOP... (CONT.)

AI FOR DETECTION, INVESTIGATION, AND OPERATIONAL EFFICIENCY WITHOUT FALLING VICTIM TO UNREALISTIC EXPECTATIONS.

EVERYDAY FLIPPER, FROM TVS TO TRACKERS: BASIC TASKS FOR THAT FLIPPER ZERO YOU BOUGHT BUT RARELY TOUCHED

GREY FOX

SAT 10:00 AM • TRACK 2

A FEW YEARS AGO, THE FLIPPER ZERO WAS POPULARISED AS THE "SWISS ARMY KNIFE" OF WIRELESS HACKING TOOLS. IT LIT ALL THE INFLUENCER CHANNELS ON FIRE AND GOT ITSELF BANNED IN HOTELS AND COUNTRIES WORLDWIDE. SOME EVEN ACCUSED IT OF STEALING YOUR CAR AND CLONING YOUR CREDIT CARDS. IT REALLY CAN'T DO THOSE... AT LEAST NOT ON ITS OWN. YOU PROBABLY BOUGHT ONE TO SEE WHAT THE TALK WAS ALL ABOUT. NOWADAYS WE RARELY SEE IT IN THE NEWS, CHANNELS, OR SOCIALS. WE RARELY SEE IT IN OUR HANDS OR CAUSING MAYHEM AT LOCAL STORES TOO. THAT MAY BE DUE TO THE FLIPPER ZERO'S BAD REP AS A HACKING TOOL ONLY, AND NOT A USEFUL ADDITION TO A HOUSEHOLD TOOLBOX. WE'LL COVER WHAT THE FLIPPER ZERO DOES WITH REAL-WORLD AND USEFUL EXAMPLES. WE MIGHT EVEN DO A BIT OF "HACKING", BUT NOTHING THAT WILL GET YOU ARRESTED OR KICKED OUT OF A RESTAURANT (NO PROMISES). BRING YOUR OWN TO JOIN IN THE HANDS-ON ACTIVITIES, OR JUST SIT BACK AND TAKE SOME NOTES. A LAPTOP AND USB CABLE TO LINK IT WITH YOUR FLIPPER WOULD BE HELPFUL TOO.

WHEN RESPONSIBLE DISCLOSURE FAILS: A COLLABORATIVE FRAMEWORK FOR ZERO-DAY REPORTING

CHRISTY CARABALLO, WILLIAM ENTRIKEN

SAT 11:00 AM • TRACK 1

TRADITIONAL RESPONSIBLE DISCLOSURE CAN BECOME A BLACK HOLE WHEN VULNERABILITY REPORTS DISAPPEAR INTO UNRESPONSIVE OR INEFFECTIVE CHANNELS. RATHER THAN TREATING VENDOR NOTIFICATION AS THE END OF THE RESEARCHER'S RESPONSIBILITY, THIS TALK EXPLORES A

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

WHEN RESPONSIBLE DISCLOSURE FAILS: A... (CONT.)

COLLABORATIVE MODEL IN WHICH TRUSTED, ETHICAL RESEARCHERS WORK TOGETHER TO UNDERSTAND AND ADDRESS SECURITY PROBLEMS WHILE VENDOR NOTIFICATION OCCURS IN TANDEM.

BREAKING PBKDF AND JAVA ENCRYPTION - ADVERSARIAL CRYPTANALYSIS AND TECHNIQUES

KEN PYLE

SAT 1:00 PM • TRACK 1

BREAKING ENCRYPTION ISN'T HARD-IT'S JUST TAUGHT POORLY.

USING DECADES-OLD OPENJDK PBKDF FLAWS, FORGOTTEN RFCs, HASH COLLISIONS, AND A FEW SEMANTIC EDGE CASES, WE'LL COMPROMISE MULTIPLE CRYPTOGRAPHIC SYSTEMS WITH LITTLE MORE THAN A HANDFUL OF CAREFULLY CHOSEN VALUES AND SEVERAL "USELESS" TOOLS.

THIS TALK EXPLORES HOW IMPLEMENTATION BUGS, LEGACY COMPATIBILITY, AND ARCHITECTURAL ASSUMPTIONS CAN UNDERMINE OTHERWISE SOUND CRYPTOGRAPHY-AND WHY THE REAL ATTACK SURFACE IS OFTEN EVERYTHING AROUND THE ALGORITHM.

POWER WITHOUT BINARIES: BRINGING NATIVE OFFENSIVE TECHNIQUES TO FILELESS RUNTIMES

JACOB COVEY

SAT 1:00 PM • TRACK 2

ADVANCED STEALTH TRADECRAFT, INCLUDING SYSCALL DISPATCHING, UNMANAGED MEMORY ACCESS, AND RUNTIME EVASION, IS TYPICALLY DESIGNED FOR COMPILED BINARIES.

THIS TALK EXPLORES WHAT HAPPENS WHEN THOSE TRADITIONALLY NATIVE CAPABILITIES ARE TRANSLATED INTO A FILELESS RUNTIME.

POWERSHELL WAS CHOSEN AS THE TARGET RUNTIME BECAUSE IT IS BROADLY AVAILABLE IN WINDOWS ENVIRONMENTS AND EXPOSES SURPRISINGLY LOW-LEVEL .NET AND UNMANAGED FUNCTIONALITY WHILE OFTEN REMAINING ENABLED IN ENTERPRISE SETTINGS.

RATHER THAN TREATING POWERSHELL AS "JUST AN AUTOMATION TOOL," THIS RESEARCH ASKS HOW FAR A FILELESS SCRIPTING RUNTIME CAN BE PUSHED TOWARD NATIVE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

POWER WITHOUT BINARIES: BRINGING NATIVE... (CONT.)

OFFENSIVE CAPABILITY DEVELOPMENT. I WILL WALK THROUGH THE TECHNICAL IMPLEMENTATION REALITIES INCLUDING AMSI, CLR BEHAVIOR, MODERN AV/EDR VISIBILITY, AND WHERE AI-ASSISTED WORKFLOWS ACCELERATED DIFFICULT INTEROPERABILITY AND TRANSLATION CHALLENGES.

THROUGH A PROGRESSION OF WORKING AND FAILED IMPLEMENTATIONS FOR A FILELESS PROCESS INJECTOR, ATTENDEES WILL SEE HOW TRADITIONALLY NATIVE TRADECRAFT EVOLVES FROM STANDARD C AND ASM TO WINAPI, NTAI, DIRECT SYSCALLS, AND INDIRECT SYSCALLS PERFORMED ENTIRELY WITHIN POWERSHELL. TECHNIQUES DISCUSSED INCLUDE P/INVOKE, MARSHALLING, UNMANAGED INVOCATION, SHELLCODE LOADING, PROCESS INJECTION, NTDLL PARSING, AND SYSCALL STRATEGIES WITHIN A FILELESS CONTEXT.

A PRE-RECORDED POC DEMONSTRATION WILL SHOW THE RESULTING FRAMEWORK SUCCESSFULLY OPERATING IN A FILELESS EXECUTION MODEL TO PERFORM PROCESS INJECTION. THIS WILL BE FOLLOWED BY A DISCUSSION OF OBSERVABILITY, DETECTION OPPORTUNITIES, AND DEFENSIVE IMPLICATIONS. THE FRAMEWORK WILL BE PUBLICLY AVAILABLE AT THE TIME OF THE TALK.

FOR DEFENDERS, THIS TALK HIGHLIGHTS MEANINGFUL OPPORTUNITIES FOR TELEMETRY, DETECTION ENGINEERING, AND DEFENSIVE PRIORITIZATION.

BRINGING YOUR PRODUCT TO MARKET - "JUST THE HIGHLIGHTS"

JONATHAN SPANGENBERG

SAT 2:00 PM • TRACK 1

"I HAVE A GREAT IDEA, I SHOULD BE ABLE TO MAKE MONEY WITH THIS, WHAT DO I DO NEXT?" THIS COMMUNITY IS FULL OF IDEAS AND TENDS TO BE VERY SKILLED IN BRINGING TECHNOLOGY TO LIFE AT "PROJECT SIZE". THIS TALK WILL HIT THE HIGHLIGHTS OF THE THINGS THAT NEED TO BE CONSIDERED TO MONETIZE YOUR PROJECT AS A BUSINESS VENTURE. WE'LL HIT THE BIG ROCKS ON WHAT GOES INTO A BUSINESS PLAN THAT WILL LET YOU SEEK INVESTMENT, HOW TO FORECAST DEMAND AND REVENUE, AND FIGURE OUT ROI. WE'LL HIT THE MAJOR CONSIDERATIONS AROUND SUPPLY CHAIN, WAREHOUSING, AND LOGISTICS. MOST IMPORTANTLY WE'LL TALK ABOUT WHAT ROLE YOU NEED TO PLAY IN YOUR BUSINESS AND WHY A

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

BRINGING YOUR PRODUCT TO MARKET - "JUST ... (CONT.)

VISIONARY ISN'T ALWAYS "CEO".

THE GOAL HERE ISN'T A FULL BUSINESS COURSE, IT'S AN INTRO TO GET YOU THINKING ABOUT WHAT YOU NEED TO KNOW, AND WHAT STEPS YOU'D NEED TO TAKE.

IDENTITY ALL THE WAY DOWN

AMANDA DRAEGER

SAT 2:00 PM • TRACK 2

WHEN YOU THINK OF "EXCITING TOPICS IN SECURITY", RARELY DO YOU THINK ABOUT IDENTITY. BUT IDENTITY UNDERPINS NEARLY EVERY OTHER ACTIVITY THAT WE AS SECURITY PROFESSIONALS UNDERTAKE. IT IS, ARGUABLY, THE HARD PROBLEM IN SECURITY WITH ASPECTS THAT YOU HAVE LIKELY NEVER THOUGHT OF BEFORE. COME EXPLORE SOME OF THE RARELY VISITED CORNERS OF IDENTITY SO THAT YOU, TOO, CAN START SEEING IDENTITY EVERYWHERE YOU LOOK!

VEILID: THE PRIVATE INTERNET WE WERE ALL PROMISED

BIANCA LEWIS

SAT 2:30 PM • TRACK 1

THE CULT OF THE DEAD COW (CDC) IS BREAKING THE INTERNET WITH VEILID, AN OPEN-SOURCE, PEER TO PEER, MOBILE-FIRST, NETWORK APPLICATION FRAMEWORK. VEILID GOES ABOVE AND BEYOND EXISTING PRIVACY TECHNOLOGIES AND HAS THE POTENTIAL TO COMPLETELY CHANGE THE WAY PEOPLE USE THE INTERNET. VEILID HAS NO PROFIT MOTIVE, WHICH PUTS IT IN A UNIQUE POSITION TO PROMOTE IDEALS WITHOUT THE COMPROMISE OF CAPITALISM. WITH VEILID, THE USER IS IN CONTROL, IN A WAY THAT IS APPROACHABLE AND FRIENDLY, REGARDLESS OF TECHNICAL ABILITY.

THIS FRAMEWORK SHARES SOME SIMILARITIES WITH IPFS AND TOR IN ITS OVERALL DESIGN, BUT IT IS BUILT TO DELIVER BETTER PERFORMANCE WHILE NATIVELY SUPPORTING ALL SERVICES THROUGH A PRIVATELY ROUTED NETWORK. IT ALLOWS DEVELOPERS TO CREATE FULLY DECENTRALIZED APPLICATIONS WITHOUT DEPENDING ON A BLOCKCHAIN OR TRANSACTION-PROCESSING LAYER AS THE FOUNDATION. THE FRAMEWORK CAN EITHER BE INTEGRATED DIRECTLY INTO END-USER APPLICATIONS OR OPERATED AS A STANDALONE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

VEILID: THE PRIVATE INTERNET WE WERE ALL... (CONT.)

HEADLESS NODE BY ADVANCED USERS WHO WANT TO CONTRIBUTE RESOURCES AND HELP STRENGTHEN THE NETWORK. THOUSANDS HAVE ALREADY JOINED THE VEILID NETWORK, INTEGRATING IT INTO THEIR DAILY LIVES AND BUILDING PRIVACY-FOCUSED PROJECTS ON TOP OF IT.

TOGETHER, WE CAN GIVE THE WORLD THE PRIVATE INTERNET WE SHOULD HAVE HAD ALL ALONG.

PUSHING THE LIMITS OF STATIC SITES

JEFF GOEKE-SMITH

SAT 2:30 PM • TRACK 2

MOST EVERYBODY HAS HEARD OF STATIC SITE GENERATION AT THIS POINT. TYPICALLY FIRST THOUGHT OF AS A MECHANISM TO GENERATE DOCUMENTATION SITES FOR GITHUB WITH JEKYLL, WE FOUND ANOTHER USE CASE: ONLINE HISTORICAL COLLECTIONS. IT'S NOT JUST MARKDOWN AND IT'S NOT JUST TEXT. THE WEB BROWSER IS AN IMMENSELY POWERFUL SYSTEM, AND NEARLY EVERY FEATURE WE HAD COULD BE REPLACED BY IN BROWSER CAPABILITIES.

BUT WHAT OF THE THINGS THAT CAN'T BE DONE IN BROWSER? DOES IT HAVE TO BE A WEB CONNECTION CONNECTED TO A FULLY EMPOWERED DYNAMIC BACK END, OR COULD WE BUILD SOMETHING MORE ROBUST AND BASIC?

IT TAKES A HARDWARE VILLAGE - THE MAKING OF THE WHOSE SLIDE IS IT ANYWAY DEF CON BADGE

DANNY AKACKI

SAT 3:00 PM • TRACK 1

ULTIMATELY, THIS IS A TALK ABOUT COMMUNITY. NO GOOGLE SEARCH, NO DATASHEET, NOR ANY NUMBER OF AI PROMPTS CAN MATCH THE CRITICALITY OF BEING ABLE TO LEAN ON A COMMUNITY OF MAKERS ALL HELL BENT ON CONQUERING CODE AND ELECTRICITY. TO GET FROM PROTOTYPE TO PCB, IT TRULY TAKES A HARDWARE VILLAGE.

TO BUILD OR NOT TO BUILD? WELL, AFTER THE FIRST TIME YOU MAKE AN LED GO BLINK, THAT ISN'T EVEN A QUESTION. THINGS ESCALATE EXPONENTIALLY AFTER THAT FIRST HARDWARE SUCCESS. IT TOOK ME 6 MONTHS FROM THE FIRST TIME I REALLY DOVE INTO A KIT FROM HACKERBOXES.COM, FUMBLING THE ENTIRE WAY, TO CREATING MY FIRST EVER BADGE FOR THE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

IT TAKES A HARDWARE VILLAGE - THE MAKING... (CONT.)

10 YEAR ANNIVERSARY FOR MY WHOSE SLIDE IS IT ANYWAY CONTEST AT DEF CON 34.

THIS TALK BEGINS AT THE BEGINNING, FROM RE-LEARNING HOW TO SOLDER A SINGLE PIN, TO STARING AT A KICAD SCREEN QUESTIONING ANY POSITIVE THING MY MOTHER EVER TOLD PEOPLE ABOUT ME. I WILL LAY BARE EVERY FAILURE THAT LED TO EVERY SUCCESS IN THE GOAL OF PUTTING SOME BLING AROUND THE NECKS OF OUR CONTESTANTS.

APT, MEET OPSEC: TURNING MISTAKES INTO INTELLIGENCE

0XFFARADAY

SAT 3:00 PM • TRACK 2

THREAT REPORTS FREQUENTLY HIGHLIGHT THE SOPHISTICATED ATTACKS CONDUCTED BY ADVANCED PERSISTENT THREATS (APTS), BUT FAR LESS ATTENTION IS GIVEN TO THEIR OPSEC FAILURES. THESE MISTAKES CAN BE LEVERAGED TO GAIN VALUABLE INTELLIGENCE AND GIVE THE SECURITY COMMUNITY AN UPPER HAND. THIS TALK WILL COVER A HANDFUL OF REAL-LIFE OPSEC FAILURES, THE INTELLIGENCE THEY REVEALED, AND THE SKILLS AND PLATFORMS REQUIRED TO TURN ADVERSARY MISTAKES INTO ACTIONABLE INTELLIGENCE.

LUA BEFORE LUA: THE RECOVERED WORKS OF LOUISE URSULA ALBRIGHT (APPLE //E, 1987)

JORJ BAUER

SAT 4:00 PM • TRACK 1

IN EARLY 2021, AN APPLE 10MB PROFILE HARD DRIVE SURFACED AT AN AUCTION AND PASSED, MONTHS LATER, INTO A PILE OF APPLE //E EQUIPMENT INHERITED BY THE PRESENTER - WHO BUILT RECOVERY HARDWARE FOR IT (PUBLICLY DOCUMENTED AT THE TIME) WITHOUT UNDERSTANDING WHAT HE HAD. FIVE YEARS ON, A CLOSE READING OF THE RECOVERED PRODOS VOLUME REVEALED THE COMPLETE WORKING ENVIRONMENT OF LOUISE URSULA ALBRIGHT (B 1938-?), A CHIPPEWA FALLS, WISCONSIN HIGH-SCHOOL MATHEMATICS TEACHER WHO, IN 1987, APPEARS TO HAVE ACCOMPLISHED SOMETHING THE HISTORICAL RECORD INSISTS DID NOT HAPPEN: A SELF-HOSTING DYNAMIC LANGUAGE "LUA" ON THE APPLE //E, SIX YEARS BEFORE "LUA" EXISTED. HER INITIALS, INKED AS A

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

LUA BEFORE LUA: THE RECOVERED WORKS OF... (CONT.)

FILE EXTENSION, EXPLAIN THE SYSTEM'S NAME; THE COINCIDENCE OF 1993 IS A MATTER THIS PRESENTATION DECLINES TO LITIGATE.

THE RECOVERED VOLUME HOLDS A 10KB BYTECODE VM IN MERLIN-8 ASSEMBLY; A 20KB COMPILER WRITTEN IN ITS OWN LANGUAGE AND COMPILED BY ITSELF; AND - MOST PRECIOUS! - THE BOOTSTRAP LADDER BY WHICH ONE PERSON CLIMBED FROM "NO COMPILER EXISTS" TO "THE COMPILER COMPILES ITSELF," USING NOTHING BUT MERLIN-8 2.58 AND A RAMWORKS 1MB CARD. WE WILL PERFORM THE RECOVERED WORKS ON PERIOD INSTRUMENTS: MERLIN WILL ASSEMBLE THE VM BYTE-FOR-BYTE BEFORE YOUR EYES; THE MACHINE WILL COMPILE ITS OWN COMPILER.

IN THE TRADITION OF PROF. PETER SCHICKELE'S RESEARCHES INTO P.D.Q. BACH: THE HISTORY IS INVENTED AND THE PRESENTER ADMITS IT CHEERFULLY. BUT EVERY ARTIFACT SHOWN IS REAL. EVERY DEMONSTRATION RUNS ON REAL PERIOD HARDWARE. THE FICTION IS THE STORY, BUT THE ENGINEERING IS REAL.

TAKING BACK CONTROL OF YOUR DIGITAL MUSIC:
REVIVE YOUR MP3 PLAYERS WITH ROCKBOX

SPEAKER TBA

SAT 4:00 PM • TRACK 2

IN TODAY'S DIGITAL WORLD, PEOPLE HAVE BECOME ENTHRALLED AND ENSNARED IN DIGITAL MUSIC SERVICES THAT CLAIM USER FREEDOM AND USER CONTROL ARE ANYTHING BUT, AND WITH SERVICES LIKE SPOTIFY, AMAZON MUSIC, AND APPLE MUSIC, AMONG OTHERS, GETTING WORSE WITH USER FREEDOM AND USER CONTROL OF OUR OWN MUSIC LIBRARIES, THINGS MAY LOOK BLEAK, BUT THERE ARE WAYS OF TAKING BACK CONTROL OF OUR MUSIC AND OUR LIVES. WITH THE REVIVAL OF OFFLINE MUSIC AND PHYSICAL MEDIA, WE NEED A SOLUTION FOR OUR OLD MP3 PLAYERS AND BREAKING THE OLD ECOSYSTEMS THEY WERE TIED TO. THE FREE SOFTWARE JUKEBOX SOFTWARE ROCKBOX OFFERS THAT FREEDOM. THIS TALK WILL COVER WHAT ROCKBOX IS AND HOW WE CAN USE IT TO GAIN DIGITAL FREEDOM FOR OUR OLD DEVICES, AND ALSO COVER DIGITAL SOVEREIGNTY AND RECLAIMING OUR OLD TECH.

SPEAKERS & ABSTRACTS (CONT.)

SUNDAY

WARDDRIVING AI

VICTORIA WHITAKER

SUN 10:00 AM • TRACK 1

THIS TALK DISCUSSES BOTH THE VALUE AND SHORTCOMINGS OF USING AI TO AID OSINT ANALYSIS. IT DETAILS THE RESULTS OF AN EXPERIMENT DESIGNED TO PRESSURE TEST THE ANALYTICAL CAPABILITIES OF THREE FRONTIER LLMs USING OPEN-SOURCE TELECOMMUNICATIONS DATA.

SOFTMODEMS ARE COOL NOW: THE DARK ART OF V.34

PHIL PEMBERTON

SUN 10:00 AM • TRACK 2

SOFTMODEMS USED TO BE THE BANE OF THE EARTH (OR AT LEAST THE LINUX PART), BUT NOW THEY'RE A KEY PART OF FAX OVER VOIP. THE BTX AND VIEWDATA 1200/75 BAUD FSK MODES ARE EASY ENOUGH, BUT WHAT ABOUT 28,800 OR 33,600 V.34? WHAT DON'T THE ITU TELL YOU IN THE V.90 SPEC? WHY DID SOME SOFTMODEM DSPs COMPARE SO POORLY TO A "REAL MODEM"? AND MIGHT SOFTMODEMS ACTUALLY BE COOL NOW?

PAGING IN 2026 - FROM CURRENT CARRIERS TO OSS AND HOBBYIST NETWORKS

MIKE DANK, NAVEEN ALBERT

SUN 10:30 AM • TRACK 1

WHILE PAGERS ONCE RULED THE '90s, THESE COMMUNICATIONS DEVICES HAVE GENERALLY FALLEN OUT OF FAVOR WITH THE POPULARITY OF CELL PHONES AND TEXT MESSAGING. PAGERS ARE STILL USED BY MANY PEOPLE TODAY, AND THE TECHNOLOGY AND INFRASTRUCTURE TO RUN IT IS STILL THERE, BUT ASPIRING INDIVIDUALS CAN ALSO MAKE USE OF THE UNDERLYING PROTOCOLS AND VINTAGE EQUIPMENT TO CREATE AND OPERATE PAGING IMPLEMENTATIONS OR BUILD SMALL SITES FOR THEIR OWN OR EXISTING PROJECTS.

THIS TALK WILL COVER THE CURRENT LANDSCAPE OF PAGING, AN OVERVIEW OF THE PROTOCOLS, PROVIDER CONSOLIDATION AND CURRENT SUPPORT, SECURITY CONSIDERATIONS AND ATTACK VECTORS, AND HOW ALPHANUMERIC PAGING CAN BE

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

PAGING IN 2026 - FROM CURRENT CARRIERS T... (CONT.)

DONE TODAY. FURTHER, WE WILL COVER AN INTEGRATION OF PAGING SUPPORT INTO OPEN SOURCE SOFTWARE, SHOWING HOW TO EASILY SUPPORT/MAKE USE OF VARIOUS PAGING PROTOCOLS TODAY. WE WILL ALSO EXPLORE HOW TO JOIN AND USE DAPNET, A WORLDWIDE DECENTRALIZED PAGING NETWORK FOR AMATEUR RADIO OPERATORS, ALLOWING USERS TO BUILD AND OPERATE SMALL PAGING SITES WITH INEXPENSIVE OR SURPLUS HARDWARE EASILY AND LEGALLY.

THOUGHT ON SYSTEM SECURITY ASSESSMENTS

BRUCE POTTER

SUN 11:00 AM • TRACK 2

ASSESSING A SYSTEM'S SECURITY IS MORE THAN FINDING VULNERABILITIES WITH TOOLS OR LLM'S. SECURITY IS ONE OF A BROAD SET OF NON-FUNCTIONAL REQUIREMENTS (SUCH AS SCALABILITY, PERFORMANCE, RELIABILITY, ETC) THAT WE EXPECT OUR SYSTEMS TO HAVE. UNDERSTANDING HOW TO ASSESS A FULL SYSTEM, INCLUDING UNDERSTANDING WEAKNESSES IN CONTEXT, IMPACTS ON OPERATIONS DUE TO SYSTEM COMPLEXITY, AND JUDGING RISK IS PART ART, PART SKILL, AND A LOT OF EXPERIENCE.

THIS TALK WILL COVER THE PHILOSOPHY AND STRATEGY AROUND SECURITY ASSESSMENTS. THIS WON'T BE A DEEP DIVE INTO VULN DISCOVERY (THO, I WILL TOUCH ON IT). RATHER, IT'S AN ATTEMPT TO PAINT A PICTURE OF A SYSTEM WHERE SECURITY IS ONE PIECE WITHIN MANY. I'LL COVER TECHNIQUES TO GAIN BROAD UNDERSTANDING OF A SYSTEM, BUILDING LISTS OF FUNCTIONAL AND NON-FUNCTIONAL SECURITY REQUIREMENTS, FIND AREAS OF HIGH COMPLEXITY AND HIGH RISK, AND HOW TO STRUCTURE THE ACTUAL ASSESSMENT.

HACK THE MISSION: FROM HACKER TO NONPROFIT BOARD PRESIDENT

FRANK CLOWES

SUN 11:30 AM • TRACK 1

HACKERS ALREADY KNOW HOW TO GIVE BACK. WE BUILD SHMOOCON, JAWNCON, BSIDES, AND LOCAL COMMUNITIES, WHILE ORGANIZATIONS SUCH AS HACKERS FOR CHARITY HAVE APPLIED TECHNICAL TALENT DIRECTLY TO HUMANITARIAN WORK. BUT ANOTHER HIGH-IMPACT OPPORTUNITY IS HIDING IN PLAIN SIGHT: ESTABLISHED NONPROFITS NEED CAPABLE BOARD

CONTINUED →

SPEAKERS & ABSTRACTS (CONT.)

HACK THE MISSION: FROM HACKER TO NONPROF... (CONT.)

MEMBERS WHO CAN HELP THEM MAKE CONSEQUENTIAL DECISIONS AND REMAIN HEALTHY.

THIS FAST-PACED TALK FOLLOWS AN OFFENSIVE-SECURITY LEADER'S PATH FROM FIRST-TIME BOARD MEMBER TO PRESIDENT OF THE DELAWARE SYMPHONY ORCHESTRA. IN 25 MINUTES, HE WILL UNPACK THE REAL BOARD WORK: SELECTING A MUSIC DIRECTOR AND CEO, NAVIGATING THE MUSICIANS' COLLECTIVE BARGAINING AGREEMENT, SETTING STRATEGY, OVERSEEING FINANCIAL HEALTH AND DONOR RELATIONSHIPS, AND ASKING HOW A 120-YEAR-OLD INSTITUTION CAN REACH YOUNGER AUDIENCES.

ATTENDEES WILL LEARN WHAT BOARDS ACTUALLY DO, WHERE HACKER INSTINCTS HELP, WHEN THEY HURT, WHAT TO ASK BEFORE JOINING, AND HOW TO CREATE IMPACT WITHOUT BECOMING THE UNPAID HELP DESK. HACKERS ALREADY HELP BUILD COMMUNITIES; BOARD SERVICE LETS US HELP SUSTAIN THE INSTITUTIONS THOSE COMMUNITIES DEPEND ON.

CLOSING REMARKS

RUSSELL HANDORF

SUN 1:30 PM • TRACK 1

LET'S WRAP THIS UP!

CHILLOUT & HAM EXAM

HAM RADIO STUDY & EXAM

HAM RADIO STUDY AND EXAM

NICOLE A2DIM

SAT 9:00 AM • MURPHY 117

STUDY AND TAKE THE HAM RADIO EXAMS!

TAKE A STUDY SESSION STARTING IN THE MORNING SO THAT BY AFTER LUNCH, YOU'LL FEEL MORE PREPARED TO TAKE THE EXAM! HERE IS A STUDY GUIDE YOU SHOULD REVIEW TO HELP YOU AHEAD OF TIME. SCAN BELOW TO SIGN UP!



SIGN UP
HAM.STUDY

CHILLOUT SPACE

OPEN DAILY FROM 8:30 AM. DROP IN ANY TIME!

AND TWO BABY ZEBRAS: CARE AND FEEDING OF ZEBRA ID PRINTERS

WALT ZARNOCH, MIKE BAKER

OPEN DAILY FROM 8:30 AM

STOP BY FOR A FUN SHOWING OF THE CARE AND FEEDING OF ZEBRA ID PRINTERS.

LEAVE WITH A CUSTOM PRINTED BADGE, AND A PEEK BEHIND HOW EVERYDAY CARDS ARE MADE.

PHILLY RADIO AND MESH CHILLOUT SPACE

CALEB FREY, EMILY BODA

OPEN DAILY FROM 8:30 AM

MESHTASTIC AND MESHCORE ARE AN OPEN SOURCE PROJECT THAT REPURPOSES INEXPENSIVE LORA RADIOS INTO A PEER-TO-PEER, OFF-GRID, ENCRYPTED COMMUNICATIONS PLATFORM WITHOUT REQUIRING A LICENSE LIKE AMATEUR RADIO.

THE NETWORK IN PHILLY HAS GROWN SIGNIFICANTLY OVER THE PAST FEW YEARS AND HAS NEW USERS JOINING EVERY DAY.

JOIN US TO LEARN MORE ABOUT THESE TECHNOLOGIES, TELL US ABOUT YOUR EXPERIENCES, OR TAKE A LOOK AT SOME OF THE HARDWARE OPTIONS WE'LL HAVE ON DISPLAY.

CONTINUED →

CHILLOUT & HAM EXAM (CONT.)

PHILLY RADIO AND MESH CHILLOUT SPACE (CONT.)

PHILLY MESH IS A GROUP OVER 1,000 STRONG WITH CURIOUS PEOPLE INTERESTED IN WIRELESS TECHNOLOGY, AND WE ARE EXCITED FOR OTHERS TO JOIN US ON OUR LEARNING JOURNEY. SEVERAL OF OUR MEMBERS HAVE EVEN USED THIS TECHNOLOGY AS A STEPPING STONE INTO GETTING THEIR TECHNICIAN RADIO LICENSE AND BEYOND!

TOOOL LOCKPICKING VILLAGE

LEO NENDZA

OPEN DAILY FROM 8:30 AM

LOOKING FOR A PLACE TO HANG OUT WHILE YOU WAIT FOR THE NEXT TALK TO START? OR HOW ABOUT A PLACE TO REST YOUR LEGS BUT NOT YOUR HEAD? THEN COME CHECK OUT AT TOOOL'S LOCKPICKING VILLAGE AT JAWNCON! WHETHER YOU'RE A NOVICE WHO JUST STUMBLED UPON LOCKPICKINGLAWYER, A SEASONED SAFECRACKER, OR SOMEWHERE IN BETWEEN, COME CHILL WITH US AS WE POP SOME LOCKS!

PHILTEL

MIKE DANK, NAVEEN ALBERT

OPEN DAILY FROM 8:30 AM

PHILTEL WILL HAVE A SELECTION OF PAYPHONES ON "FREE PLAY" FOR ATTENDEES TO USE. THESE PHONES CAN CONNECT TO THE PSTN AND MAKE/TAKE CALLS FROM IT, BUT IT IS ALSO CONNECTED TO PHREAKNET, A HOBBYIST TELEPHONY NETWORK CATERING TO PHREAKS; TANDEM-STACKING, RED-BOXING, BLUE-BOXING, AND OTHER TECHNIQUES ARE ALL FAIR GAME HERE! IN ADDITION TO PAYPHONES WE WILL HAVE OTHER TELEPHONY EQUIPMENT FOR DISPLAY AND USE! WE ARE CONSIDERING BRINGING VIDEO PHONES, A WEBTV, AN AT&T SCEPTRE TERMINAL, A RADIO PHONE PATCH SO RADIO AMATEURS CAN CALL OUR PHONES, AND MORE!

EX MACHINA PARLOR RANGE DAY

LEO NENDZA

OPEN DAILY FROM 8:30 AM

IF YOU'RE A POTENTIAL HOMELAB ENTHUSIAST, SYSTEM ENGINEER, OR CYBER RANGE DEVELOPER COME AND CHECK OUT THE EMP CREW'S CYBER RANGE DAY! WE'LL BE SHOWCASING OUR PORTABLE CYBER RANGE KIT WE TOOK TO DEFCON AND BLACKHAT USA THIS YEAR. YOU'LL GET TO PLAY AROUND IN OUR RANGE WITH OUR NEW TENGU MARAUDER STRYKER UNITS AND ROBOTS IN AN EMULATED IOT RANGE.

NOTES

JAWNCON 0x3

SCRIBBLE HERE!

JawnCon™0x3

THIS CON WAS MADE POSSIBLE
BY OUR SPONSORS



JPMorganChase



VOLUNTEERS, SPEAKERS & ATTENDEES – YOU ARE THE JAWN.