2018 BSides Las Vegas

On the Highway to Shell

August 7-8, 2018
Tuscany Suites & Casino
Las Vegas, USA
BSides Las Vegas is a nonprofit organization designed to advance the body of Information Security knowledge by providing an annual, two-day open forum for discussion and debate for security engineers and their affiliates.

We produce a conference that is a source of education, collaboration, and continued conversation for information technologists and those associated with this field.

The technical and academic presentations at BSidesLV are given in the spirit of peer review and advanced knowledge dissemination.

This allows the field of Information Security to grow in breadth and depth, and continue in its pursuit of highly advanced, scientifically based knowledge.
Almost nothing about preparing an event like this is easy. I’m sure you know this, because so many of you are engaged in organizing or volunteering for community events all over the world. Everyone, from the staff and volunteers, speakers, sponsors, and participants are part of making BSidesLV happen.

This year was a bumpy one for many the BSLV staff. Changes in tooling and changes in the personal lives of many of our team created an environment that was often way more stressful than we’re used to dealing with, but we love bringing you BSides Las Vegas. We stayed focused on our mission and pulled together as a team. We hope that we have been able to craft an event that is seamless and engaging.

The BSides global movement exists because so many are willing to put in the hard work to create these spaces for sharing information and opportunities—thank you for being part of this amazing community!

We are relieved and excited to bring you this year’s edition of BSides Las Vegas. We hope that you engage with people, ideas, and opportunities that change your life in some small way. If that happens, please let us know. We’ll need that fuel to propel us through the next planning cycle.

To everyone on the staff, as always, my love and gratitude.
Thank you for joining us! We’re glad you’re here. With so much going on in Las Vegas this week, you had a lot of options to choose from. You chose wisely.

Coming into Vegas a day or two ahead of DEF CON isn’t easy for a lot of us. It means extra lodging, at least one extra day out of the office, and extra expenses all around. But it also means extra education and exposure to topics that won’t be covered later this week, a chance to meet up with old friends ahead of the madness to come, and the opportunity to expand your network above and beyond the colleagues you’ll be seeing over the next few days.

We have a lot of great talks on the schedule and TEN amazing tracks of content for you to choose from:

- **Ground Floor** is new this year, and it’s literally on the ground floor of the hotel, at the Copa Room. It features foundational talks on topics relevant to security practitioners today.
- **I Am The Cavalry**, where the community is working together to make The Internet of Things a safer place for our neighbors, our children, our parents, and our friends.
- **Groundtruth** is all about off-the-record talks on subjects best discussed AFK. No press, no recording, no streaming, no names. Just you and your peers, talking about what matters, behind closed doors. This is one conversation you’ll almost certainly miss entirely if you’re not present.
- **Breaking Ground** covers new and ongoing research, presented by speakers that want your feedback, insight, and opinion.
- **Common Ground** covers an assortment of other topics that are nonetheless near and dear to the heart of InfoSec.
- **Proving Ground** gives first-time speakers a platform to have their voice heard in a welcoming environment, with the support of a mentor that has been assisting them in their preparation and practice runs.
- **GroundTruth** is focused on innovative computer science and mathematics as applied to information security: natural language processing, machine learning, statistics, and all manner of big data manipulation and analysis.
- **Training Ground** features workshops and classes to give students hands-on experience learning valuable information security skills, such as Red Team, Blue Team, Technical, and Policy.

**NOTE:** Training Ground sessions are hosted at the Platinum Hotel, just Northwest of the Tuscany.

- **Hire Ground**, is aimed at helping our Participants find employment, getting their resume up to snuff, and working on their interviewing skills and receiving career advice.

Video recording will also be posted to our YouTube channel (and to archive.org) a month or so after the event, so check back to catch video of the sessions you missed because the hallway track was just too good to leave. Special thanks to Source of Knowledge, our streaming and recording provider, for enabling us to get our content out to the world.

Don’t forget the events! We have a **Lockpick Village**, where you can practice your picking or show off your skills by teaching someone new, as well as the **Pros vs. Joes CTF**, pitting Red Team against Blue to teach the Joes new defense and offense skills in a fun, controlled environment.

Our **Silent Auction** this year will benefit our Supported Charities. **The Diana Initiative**, **Hak4Kidz** and as always, the **EFF**. The 50/50 Raffle will be split 50/50 with our Grand Prize winner and BSidesLV, so we can put the money toward good use next year and keep the education flowing. Both the Silent Auction and Raffle winners will be pulled during happy hour on Tues and Wed as well as during closing.

Of course, no InfoSec conference would be complete without after-hours activities.

On Tuesday, the **QueerCon mixer** down at the pool starts at 20:00, and the return of **The New Hacker Pyramid** starts at 21:30 in the Chill-Out Room. Wednesday night starting at 22:00, we have the **BSidesLV Pool Party**, with musical guests An Hobbes at 22:00, DJ Jackalope at 23:30, Circuit Static at 00:30 and closing out the evening from 02:00-03:30, we have Alchymyst from Armada Music!

This IS a pool party, so bring your swimsuit and badge, and we’ll provide the beats, the beverages, the bites, and the beach toys.

There is a lot that can be gained from attending a BSides conference. Please, let us know what it means to you. If you have comments that weren’t personally conveyed, please drop us an email at info@bsideslv.org. We’d love to hear from you. We’re sure you won’t be disappointed. We certainly hope you’re delighted.

From all of us at Team BSidesLV, participate, have fun, and help us spread the BSides ethos: Education! Communication! Collaboration!

---

**The BSidesBus Schedule**

**Monday:** Start at McCarran International Airport (LAS) at 12:00 and run a continual loop to Tuscany Hotel until 23:59.

**Tuesday:** Start at LAS at 06:00, drop-off at Tuscany Hotel, continue to Mandalay Bay for pick-up, continue to LAS for pick-up, return to Tuscany. Repeat loop until 01:00 Wednesday morning.

**Wednesday:** Start at LAS at 06:00, drop-off at Tuscany Hotel, continue to Mandalay Bay for pick-up, continue to LAS for pick-up, return to Tuscany. Repeat loop until 14:00, then cut LAS from the route, and change the run to Mandalay Bay/The Flamingo/Tuscany from 14:00 to 04:00.

**Thursday–Sunday:** Run a continual, 24-hr loop between The Flamingo and Mandalay Bay. Between Thursday and Sunday, the shuttle from LAS will end at Tuscany Hotel, continue to Mandalay Bay/The Flamingo/Tuscany from 14:00 to 04:00.

The #BSidesBus is back. You could have caught the shuttle from LAS starting at noon on Monday, but you can STILL use it to get around to those other two conferences, too!
We at BSidesLV expect that our Participants are here for education, communication and collaboration, and we know that the majority of you are here for just that. Occasionally though, we have to reiterate the rules, so that it’s been said out-loud and there’s no misunderstanding of expectations. To that end, we present you with the following:

**Code of Conduct**

We have NO TOLERANCE for physical/verbal/sexual harassment of any human! Our Code of Conduct is “Be Excellent to Each Other” AKA the Golden Rule.

Failing that, it is “Do not be an Ass” or we will kick your ass out!

Asking questions of a speaker during their talk, to get clarity or debate a point is NOT being an ass—heckling or haranguing the speaker IS. If you are not sure, ask, or err on the side of basic decency and common courtesy. If what they are doing would not be acceptable to have done to you, your best friend, your worst enemy, your sister, niece, daughter, brother, nephew, son, mother, father, or any human being, do not let them treat anyone else that way—whether you know them or not. If someone asks you to stop—stop.

If you are having an issue with a BSidesLV participant of ANY badge type, find a radioed member of our Safety Team in the red BSidesLV t-shirts (or any staff member in a purple shirt). They will call our Safety & Medical Response Team (S.M.R.T), who will assist you in determining the next steps for you to feel safe and heard.

“Staff reserves the right to determine what constitutes “Being an Ass.”

Photo, Video, and Recording Device Policy

Ensure you have the permission from anyone you photograph or record. This includes those in the background of your shot. “Crowd shots” from the front (facing the crowd) are strongly discouraged. No photo/video/audio recording in the Underground Track, period.

If you’ve accidentally taken a picture without permission, delete it. If you are asked by a participant to delete/blur a picture they did not give you permission to take, do so immediately. We ask Press photographers to adhere to this policy, as well. A Press badge is not a pass to break these rules.

Upon a first infraction, you will receive one warning from BSidesLV Staff. Upon a second infraction you will be asked to give up your device to BSidesLV Safety & Security for the duration of the Con or to leave the Con with your device, your choice. You may return to the Con once you have deposited your device in a secure location, offsite.

There is one official BSidesLV Photographer. She will have a professional camera and a Staff badge. She is aware of this policy and is not immune, except in cases where she has been requested to document activities, official parties, presentations, etc., for BSidesLV PR purposes. If you believe that she is breaking these rules, or abusing her privilege, please bring it to the attention of BSidesLV Safety Operations or any BSidesLV Staff member.

**Thank you for your cooperation!**
We think it’s important to color outside the lines.

Our mission is ambitious—ready to be part of the bigger picture?

www.rapid7.com/careers
Jim Christy will discuss the history and future of using Digital Forensics to solve almost any investigation, including his role leading Cyber Ops for the D.B. Cooper Cold Case Team.

In 1971, a man named Dan Cooper (Press misidentifies him as D.B. Cooper and that name has stuck) hijacked a Northwest Orient flight showing a flight attendant a bomb in his briefcase. He demanded and received $200,000 cash and 4 parachutes. After releasing the passengers, he directed the flight crew to fly him to Mexico with a refueling stop in Reno, NV. Somewhere over Washington State, it is believed D.B. Cooper parachuted out of the airliner via the rear stairway with the ransom, never to be heard from again. For law enforcement, this is the only unsolved skyjacking in American history.

Christy put together an online task force to help Colbert’s team prove the real identity of D.B. Cooper, starting with the evidence from Colbert’s 2016 documentary and continuing through a surprising number of online sources and contacts for a 45-year-old case. It only took them six years to prove what had eluded countless investigators in all that time. Learn all about the techniques that brought them success and join Jim Christy after the Keynote for an extended Q&A session and meet & greet in our Underground track!

Jack Daniel is co-host of Security Weekly and served as director of the National Information Security Group (NAISG). He is co-founder of Security BSides, and his Uncommon Sense Security blog has been named to the Security Bloggers Network Hall of Fame. He currently serves as resident strategist at Tenable, and mixes a mean Negroni.
Common Ground

Topics of general interest to the security community, e.g., lock-picking, hardware hacking, mental health/burnout, law, privacy, regulations, risk, activism, technical tutorials, etc.

TUESDAY

- **Who Wants to Be A Regulator: The IoT Security Game Show**
  - 11:30–12:25
  - Allan Friedman, Jen Ellis, Wendy Knox Everette, Whitney Merrill

- **How to Start a Cyber War: Lessons from Brussels - EU Cyber Warfare Exercises**
  - 14:00–14:55
  - Chris Kubecka

- **Red Teaming a Manufacturing Network (Without Crashing It)**
  - 15:00–15:55
  - Johnny Medina, Kyle Cucci

- **An Encyclopedia of Wiretaps**
  - 17:00–17:55
  - Wendy Knox Everette

- **You’re just complaining because you’re guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software Used In the Criminal Justice System**
  - 18:00–18:55
  - Jeanna N. Matthews, Nathan Adams, Jerome Greco

WEDNESDAY

- **All Your Cloud Are Belong To Us - Hunting Compromise in Azure**
  - 10:00–10:55
  - Nate Warfield

- **Security Awareness Training Refresh**
  - 11:00–11:55
  - Lauren Clausen

- **Where are the reinforcements?**
  - 12:00–12:25
  - Brady Nielsen

- **Who Maed Dis; A beginners guide to malware provenance based on compiler type.**
  - 14:00–14:55
  - Lucien Brule

- **LibreSSL - Moving the Ecosystem Forward**
  - 15:00–15:55
  - Brent Cook

- **Solving for Somebody Else’s Problem: Hacking Devs for Better Security**
  - 17:00–17:55
  - Sarah Gibson

- **Watch Out For That Bus! (Personal Disaster Recovery Planning)**
  - 18:00–18:55
  - David Minch
Ground Floor is new this year, and it’s literally on the ground floor of the Tuscany, at the Copa Room. It features foundational talks on topics relevant to security practitioners today. **NOTE:** Certain talks will be held in Florentine G, where Proving Ground talks are also hosted.

### TUESDAY

**GF** Hillbilly Storytime - Pentest Fails
Florentine G
11:00–11:55
Adam Compton

**GF** From CTF to CVE: How Application of Concepts and Persistence led to a Vulnerability Disclosure
Copa Room, Tuscany Casino Floor
11:30–12:25
Joe Gray

**GF** Get on the Eye Level: Tailoring the Security Talk
Florentine G
11:30–12:25
Fahmida Y Rashid

**GF** Who Watches the Watchers?: Understanding the Internet’s Background Noise
Copa Room, Tuscany Casino Floor
14:00–14:55
Curt Barnard

**GF** Lessons Learned by the WordPress Security Team
Copa Room, Tuscany Casino Floor
15:00–15:55
Aaron D Campbell

**GF** (De)Serial Killers
Copa Room, Tuscany Casino Floor
10:00–10:55
Erez Yalon

**GF** Not your Mother’s Honeypot - Another name for Threat Intel
Florentine G
10:00–10:55
Kat Fitzgerald

**GF** Applied Quantitative Risk Analysis
Copa Room, Tuscany Casino Floor
11:00–11:55
Michael Rich

**GF** Invoke-NoShell
Copa Room, Tuscany Casino Floor
12:00–12:25
Gal Bitensky

**GF** Security and DevOps are really Best Friends
Copa Room, Tuscany Casino Floor
14:00–14:55
Emily Gladstone Cole

**GF** Don’t Bring Me Down: Are You Ready for Weaponized Botnets?
Copa Room, Tuscany Casino Floor
15:00–15:55
Cheryl Biswas

### WEDNESDAY

**GF** Another one bites the dust: Failed experiments in infrastructure security analytics and lessons learned from fixing them
10:00–10:55
Ram Shankar Siva Kumar

**GF** PowerShell Classification: Life, Learning, and Self-Discovery
11:00–11:55
Derek Thomas

**GF** Can data science deal with PAM?
12:00–12:25
Lella Powell

**GF** Tracking Malicious Logon: Visualize and Analyze Active Directory Event Logs
14:00–14:55
Shusei Tomonaga, Tomoaki Tani

**GF** Decision Analysis Applications in Threat Analysis Frameworks
15:00–15:55
Emily Shawgo

---

**GT** 101 ways to fail at getting value out of your investments in security analytics, and how not to do that
11:30–12:25
Jon Hawes

**GT** An Introduction to Machine Learning and Deep Learning
14:00–14:55
Hillary Sanders

**GT** Stop and Step Away from the Data: Rapid Anomaly Detection via Ransom Note File Classification
15:00–15:55
Mark Mager

**GT** Sight beyond sight: Detecting phishing with computer vision.
17:00–17:55
Daniel Grant

**GT** Catch me, Yes we can! - Pwning Social Engineers using Natural Language Processing Techniques in real-time
18:00–18:55
Ian G. Harris, Marcel Carlsson
Hire Ground

GT Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era
15:30–15:55
Andrea Marcelli

GT Hackademia: The 2018 Literature Review
17:00–17:55
Falcon Darkstar Momot, Brittany “Straithe” Postnikoff

GT Arbitrary Albatross: Neutral Names for Vulnerabilities at Volume
18:00–18:55
Art Manion and Leigh Metcalf

Hire Ground

A career focused track to provide the tools needed for job search and overall career planning. Talks and panels on recruiting and hiring practices, improving chances of being recruited, interviewed, and hired. Resume review by industry recruiters. Career coaching available on a first-come, first-served basis. Opportunities for job seekers to network with representatives from our Hire Ground sponsors.

TUESDAY

HG Hire Ground Kickoff
11:30–12:00
Lesley Carhart

HG From Hacker to Serial Entreprenuer
12:30–13:25
Matt Devost

HG You're Good and You Should Feel Good
14:30–15:00
Victor Wieczorek

HG The Long Way Around – from Software Engineering to Cyber Security (How Choosing Wrong Turned out to be Right)
15:00–15:30
Margaret White

HG Redefining the Hacker
17:30–18:00
Manju Mude

HG What Did We Learn from Today? Recruiter Panel
18:00–18:30
Kris Rides, Briana Fernandez, Scott Handley

WEDNESDAY

HG The Key to Managing High Performance Security Teams
10:00–11:00
Mike Murray

HG Increasing Retention Capacity
11:00–11:30
Andrea Little Limbago

Paranoids at Oath:

Visit oath.com/careers for current openings.
I Am The Cavalry

**HG** Fast-track your Hacking Career - Why Take The Slow Lane?
14:00-14:30
Joe Klein

**HG** Community Career Panel or How to Get More than a T-Shirt Working at a Con
14:30-15:00
Cindy Jones, Magen Wu, Kristen Kenner, Kathleen Smith

I Am the Cavalry

Security that affects public safety and human life. Discussions cover medical devices, cars, and other connected technologies with a higher consequence of failure; issues where security overlaps with the human condition; and building skills to influence change outside the echo chamber. IATC’s mission is to gather ambassadors from diverse fields, and put them to work with a common objective to be “Safer, Sooner, Together.”

**IATC** Engaging the Media: Telling Your Story
15:00-15:55
Steve Ragan, Sean Gallagher, Paul Wagenseil, Iain Thomson

**IATC** A Good Day to Die? IoT End of Life
17:00-17:55
Jessica Wilkerson, Allan Friedman, Karl Grindal, Karim Farhat, Ishan Mehta

**IATC** Cyber Safety Disclosure
18:00-18:55
Nina Alli, Suzanne Schwartz, Jay Radcliffe, Joshua Corman

**IATC** Stupid Hacker Tricks: Bridging Airgaps and Breaking Data Diodes
10:00-10:25
Monta Elkins

**IATC** Building ambassadors to reduce friction, drive change, and get sh*t done
10:30-11:25
Katie LeDoux

**IATC** Hacking the Public Policy API
11:30-12:25
Travis Moore, Maurice Turner, Jessica Wilkerson

**IATC** CVE CVSS NVD OMGWTFBBQ
14:00-14:55
Tom Millar, Katie Trimble, Art Manion, Seth Carmody, Josh Corman

**IATC** Engaging Policymakers at the State Level
15:00-15:55
Maurice Turner, Joe Hall, David Forsey

**IATC** Transforming Industries for Fun and Safety (Panel)
17:00-17:29
Pete Cooper, Jeff Troy

**IATC** Transforming Industries for Fun and Safety (Presentation)
17:30-17:55
Beau Woods, David Rogers

**IATC** Cavalry is ALL OF US
18:00-18:55
Joshua Corman, Beau Woods, and special guest appearances

**IATC** Engaging the Media: Telling Your Story
15:00-15:55
Steve Ragan, Sean Gallagher, Paul Wagenseil, Iain Thomson

**IATC** A Good Day to Die? IoT End of Life
17:00-17:55
Jessica Wilkerson, Allan Friedman, Karl Grindal, Karim Farhat, Ishan Mehta

**IATC** Cyber Safety Disclosure
18:00-18:55
Nina Alli, Suzanne Schwartz, Jay Radcliffe, Joshua Corman

**IATC** Stupid Hacker Tricks: Bridging Airgaps and Breaking Data Diodes
10:00-10:25
Monta Elkins

**IATC** Building ambassadors to reduce friction, drive change, and get sh*t done
10:30-11:25
Katie LeDoux

**IATC** Hacking the Public Policy API
11:30-12:25
Travis Moore, Maurice Turner, Jessica Wilkerson

**IATC** CVE CVSS NVD OMGWTFBBQ
14:00-14:55
Tom Millar, Katie Trimble, Art Manion, Seth Carmody, Josh Corman

**IATC** Engaging Policymakers at the State Level
15:00-15:55
Maurice Turner, Joe Hall, David Forsey

**IATC** Transforming Industries for Fun and Safety (Panel)
17:00-17:29
Pete Cooper, Jeff Troy

**IATC** Transforming Industries for Fun and Safety (Presentation)
17:30-17:55
Beau Woods, David Rogers

**IATC** Cavalry is ALL OF US
18:00-18:55
Joshua Corman, Beau Woods, and special guest appearances

**Ground1234!**

Focused on the (in)security of passwords and other authentication solutions, Ground1234! brings together security researchers, password crackers, and experts in password security from around the globe (we miss you, Per!), in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.

**Ground1234!**

Focused on the (in)security of passwords and other authentication solutions, Ground1234! brings together security researchers, password crackers, and experts in password security from around the globe (we miss you, Per!), in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.

**Ground1234!**

Focused on the (in)security of passwords and other authentication solutions, Ground1234! brings together security researchers, password crackers, and experts in password security from around the globe (we miss you, Per!), in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.

**Ground1234!**

Focused on the (in)security of passwords and other authentication solutions, Ground1234! brings together security researchers, password crackers, and experts in password security from around the globe (we miss you, Per!), in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.

**Ground1234!**

Focused on the (in)security of passwords and other authentication solutions, Ground1234! brings together security researchers, password crackers, and experts in password security from around the globe (we miss you, Per!), in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.
Proving Ground

Guardians of GitHub
17:00–17:55
Joshua Danielson, Dileep Gurazada

Ransombile, yet another reason to ditch SMS
18:00–18:55
Martin Vigo

Our Mentorship and Scholarship track for first time (inter)national speakers. Proving Ground is an opportunity for new presenters to learn from established ones, and find their voice. There are no limits to the security-related topics that can be addressed in Proving Ground, and our presenters offer up original and interesting research, theory, or practical tutorials on a fascinating array of subjects.

TUESDAY

Social engineering at scale, for fun
14:00–14:25
Sara-Jayne Terp
MENTOR: Brittany Postnikoff

Implementing the Three Cs of Courtesy, Clarity, and Comprehension to Optimize End User Engagement
14:30–14:55
Courtney Klevermang
MENTOR: Chris Eng

Building A Teaching / Improvement Focused SOC
15:00–15:25
Andrew Gish-Johnson
MENTOR: Ming Chow

Modern Political Warfare: A Look at Strategy and TTPs
15:30–15:55
Sina Kashefi
MENTOR: Brendan O’Connor

Legendary Defender - The Voltron Analogy
17:00–17:25
Brian Carey
MENTOR: Patrick McNeil

Not your Grandpa’s Password Policy
17:30–17:55
Kevin T Neely
MENTOR: Russell Buttutini

Vulnerability Management 101: Practical Experience and Recommendations
18:00–18:25
Eric Bryan
MENTOR: Magen Wu

Cruising the MJ Freeway: Examining a large breach in legal Cannabis
18:30–18:55
Rex
MENTOR: Soldier of FORTRAN

Our mission at Semmle is to secure the software that runs the world. We do that through our products, QL and LGTM, which make source code truly searchable, allowing people to ask deep semantic questions of their software, and get accurate answers.

Leading tech companies including Google, Microsoft and Mozilla use QL to hunt down and prevent zero-days that would otherwise be impossible to find.

Our dedicated team of security researchers work closely with software companies and the open source community to find security vulnerabilities in widely-used software, disclosing the details responsibly, publishing write-ups on our blogs, and taking what we find to improve our open source QL queries and libraries.

We’re hiring!

If you share our passion for security or software development, we’d love to talk to you. We’re hiring for many positions, including our security research, QL and LGTM teams. Don’t worry too much about experience, we believe raw talent matters most.

semble.com/careers
# Training Ground

## Wednesday

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker</th>
<th>Mentor</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00–12:00</td>
<td>The current state of adversarial machine learning</td>
<td>Diamond Room, Platinum Hotel</td>
<td>Heather Lawrence</td>
<td>Hyrum Anderson</td>
</tr>
<tr>
<td>14:00–15:25</td>
<td>Treble or Trouble: Where Android’s latest security enhancements help, and where they fail</td>
<td>Emerald Room, Platinum Hotel</td>
<td>Tamir Zahavi-Bruner</td>
<td>Sneha Rajguru</td>
</tr>
</tbody>
</table>

## Training Ground

Workshops and classes to give students hands-on experience learning valuable information security skills. Red Team, Blue Team, Technical, Policy; Training Ground aims to provide something for participants of many differing areas of focus and responsibility. **NOTE: Training Ground sessions are hosted at the Platinum Hotel, just Northwest of the Tuscany.**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker</th>
<th>Mentor</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:00–17:00</td>
<td>Introduction to Cryptographic Attacks</td>
<td>Emerald Room, Platinum Hotel</td>
<td>Gabriel Ryan, Justin Whitehead</td>
<td></td>
</tr>
<tr>
<td>17:00–18:30</td>
<td>Windows Internals and Local Attack Surface Analysis using Powershell</td>
<td>Opal Room, Platinum Hotel</td>
<td>James Forshaw</td>
<td></td>
</tr>
</tbody>
</table>

---

# Underground


<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker</th>
<th>Mentor</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:30–12:25</td>
<td>Q&amp;A with Jim Christy</td>
<td></td>
<td>Jim Christy</td>
<td></td>
</tr>
<tr>
<td>14:00–15:00</td>
<td>Advanced APT Hunting with Splunk</td>
<td>Diamond Room, Platinum Hotel</td>
<td>Ryan Kovar, Dave Herrald, John Stoner</td>
<td></td>
</tr>
<tr>
<td>14:00–15:00</td>
<td>Attack &amp; Defense in AWS Environments</td>
<td>Ballroom, Platinum Hotel</td>
<td>Vaibhav Gupta, Sandeep Singh</td>
<td></td>
</tr>
<tr>
<td>14:00–15:00</td>
<td>Smart Contracts: Hello World</td>
<td>Diamond Room, Platinum Hotel</td>
<td>John Amirrezvani, bspar</td>
<td></td>
</tr>
<tr>
<td>14:00–15:00</td>
<td>Endpoint Monitoring with Osquery and Kolide Fleet</td>
<td>Opal Room, Platinum Hotel</td>
<td>Rodrigo “Sp00KeR” Montoro, Felipe “Pr0teus” Espósito</td>
<td></td>
</tr>
</tbody>
</table>

---

# TUESDAY

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker</th>
<th>Mentor</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00–11:55</td>
<td>Advanced Wireless Attacks Against Enterprise Networks</td>
<td>Ballroom, Platinum Hotel</td>
<td>Gabriel Ryan, Justin Whitehead</td>
<td></td>
</tr>
<tr>
<td>08:00–11:55</td>
<td>HAM Crams and Exams</td>
<td>Diamond Room, Platinum Hotel</td>
<td>Matt Cheung</td>
<td></td>
</tr>
<tr>
<td>08:00–11:55</td>
<td>Evil Mainframe Hacking Mini</td>
<td>Opal Room, Platinum Hotel</td>
<td>James Forshaw</td>
<td></td>
</tr>
</tbody>
</table>

---

# TUESDAY

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker</th>
<th>Mentor</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00–12:25</td>
<td>Q&amp;A with Jim Christy</td>
<td></td>
<td>Jim Christy</td>
<td></td>
</tr>
<tr>
<td>14:00–15:00</td>
<td>Snake Oil &amp; The Security Industry</td>
<td></td>
<td>Dave Cole</td>
<td></td>
</tr>
</tbody>
</table>
**Special Events**

**A Peek into the Cyber Security of the Aviation Industry**

15:00–15:55
Nitha Rachel Suresh

**That Buzzword Bingo Rapid Debates Panel Thing**

17:00–18:55
Jen Ellis, Josh Corman, Chris Nickerson, Robert Graham, Lesley Carhart

**How A Fortune 500 Company Suppressed Our Research Through Legal Threats**

14:00–14:55
T Prophet, Falcon Momot

**Why Can’t We Be Friends? (Get Spotted With A Fed)**

15:00–15:55
Russel Handorf

**Ask The EFF**

17:00–18:25
Nate Cardozo, Kurt Opsahl, Nash Sheard, Eva Galparin, Cooper Quentin

---

**Public Ground**

Platinum Hotel Boardroom

**Tuesday 11:30–18:55**

**Wednesday 10:00–18:55**

Made possible by a generous grant from the William and Flora Hewlett Foundation, Public Ground will foster greater inclusion in public policy dialog by building lasting bridges between the cybersecurity research, public policy, and journalist communities. This space will facilitate office hours to bring together, birds-of-a-feather for high-trust, high-collaboration engagement.

---

**Pros vs Joes CTF**

Chill-out Room (Florentine C&D)

**Tuesday & Wednesday**

Pros vs Joes is a Capture the Flag event where inexperienced users learn from seasoned professionals in a fierce competition of attack and defend. Blue Teams of Joes work with Pro Captains to compete against other defending Teams, protecting horrifically vulnerable networks from assault by a dangerous and relentless Professional Red Team. For two days the battle will rage on an ethereal field rife with desktops and servers, Linux and Windows, systems and software both old and new. On day one, Blues lock down their systems against the onslaught. On day two, Blue Teams turn Purple and can go offensive, attacking the other competing teams. After the dust settles each day, Blue and Red discuss events to help further mentoring and learning of defensive and offensive tradecraft. Come witness the teams do battle after weeks of preparation. Only the strongest will survive, but all will learn and have fun!

---

**Lockpick Village**

Chill-out Room (Florentine C&D)

**Tuesday & Wednesday**

Want to try your hand at the art of lockpicking? Come visit the Lockpick Village! We bring the locks and picks, you bring a sense of curiosity. We’ll also be holding contests and beginner sessions on both days of the conference. All skill levels welcome - volunteers will be on hand to help you get started!

---

**Charity Silent Auction Bidding Opens**

Chill-out Room (Florentine C&D)

**Tuesday 9:00–9:15**

As a member of the InfoSec Community, you no doubt understand the pressing need for community support groups. BSides Las Vegas has a deep tradition of fostering and helping these groups, this year is no different. BSides will be holding its annual Charity Silent Auction and Raffle with all the proceeds going to three specific groups:
- Electronic Frontier Foundation (eff.org)
- The Diana Initiative (dianainitiative.org)
- Hak4Kidz (hak4kidz.com)

Our efforts to help make these groups grow and succeed can’t take effect unless we have the support of everyone in our community. Winning Bids will be announced during the Closing Ceremonies.

---

**Can You Solve These Puzzles?**

Easy: WannaCry communicated with IPs from which countries?

Hard: Can you find the WannaCry kill switch domain?

Hint: Go to VirusTotal Graph (virustotal.com/graph) and click “Load example”.

Solved the puzzle? Or need another hint? Stop by the VirusTotal table for your prize.

---

Global Malware Intelligence Services
1. Go to the silent auction table before any of the drawings and deposit the entry half of the tickets from your swag bag into the appropriate bucket.
2. Show up before one of the drawings and purchase raffle tickets from the team at the silent auction table. The raffle items will be at the silent auction table throughout the conference, so swing by to peruse through your choices. All tickets deposited during one draw period will be discarded afterwards and are not eligible for other draws. But this means two things:
   1. You have control over which draw period or periods you participate in, maximizing chance for the prizes you desire.
   2. NO LONG ASS DRAW AT THE CLOSING CEREMONIES.
I know, we’re proud of the idea as well. Only took a few years to figure it out...

SE   Pros vs Joes CTF: Play begins!
Chill-out Room (Florentine C&D)
9:00-9:15

SE   Lockpick Village: Beginner lesson
Chill-out Room (Florentine C&D)
11:30-12:00

SE   Lockpick Village: Contest
Chill-out Room (Florentine C&D)
14:30-15:00

SE   Pros vs Joes CTF: Contest play ends!
Chill-out Room (Florentine C&D)
15:45-16:00

SE   Lockpick Village: Contest
Chill-out Room (Florentine C&D)
16:00-16:30

SE   Charity Raffle: Draw 2
Chill-out Room (Florentine C&D)
End of Happy Hour

SE   Pros vs Joes CTF: End of Day Hotwash
Chill-out Room (Florentine C&D)
17:00-17:30

SE   QueerCon Mixer
The Tuscany Pool
20:00-23:30
Queercon is excited to be part of BSides Las Vegas again this year. Join us at the Tuscany pool from 8:00 PM until 11:30 for the Queercon BSides Mixer!

SE   The New Hacker Pyramid
Chill-out Room (Florentine C&D)
21:30-23:30
“We keep screwing up, and yet they keep asking us to return.” The New Hacker Pyramid returns yet again at BSidesLV 2018. Join us for games, drinks, and retro-fun. There will be prizes, audience participation, a number of secret guest appearances, and an EXTRA SPECIAL EVENT that you will have to be there to see! Things are so secret WE don’t even know what they are!

SE   Charity Silent Auction Bidding Closes
Chill-out Room (Florentine C&D)
18:30-18:45
Last chance to place your bid on the excellent array of goodies donated to benefit our supported charities! Come to the closing ceremony to see who paid how much for what!

SE   Charity Raffle: Draw 3
Chill-out Room (Florentine C&D)
Mid-point of Closing Ceremony

SE   BSides Las Vegas 2018 Closing Ceremony
Chill-out Room (Florentine C&D)
19:00-20:00
Come join us as we say goodbye to the 2018 edition of BSides Las Vegas! Contest winners, winning raffle numbers, and silent auction high bidders will be announced.

SE   BSides Pool Party
The Tuscany Pool
22:00-04:00
Come chill out by the pool! Drink, eat, and float around the Tuscany’s fantastic pool while listening to An Hobbes, Jackalope, Circuit Static, and others playing all of the best music you’ve never heard before. Don’t forget your swimsuit and conference badge!
Nina Alli
Cyber Safety Disclosure
I Am The Cavalry, 15:00-15:55, Wednesday
co-presenting with Suzanne Schwartz, Jay Radcliffe, and Joshua Corman
Nina Alli is a healthcare information security researcher and the Project Manager of the DEF CON BioHacking Village. Her work is focused predominately on Electronic Medical Records for it is the ultimate medical device, its information interactions and interoperability capabilities, how the US Government polices its healthcare system, Actionable Data Analysis, and STEM education.

John Amirrezvani
Smart Contracts: Hello World
Training Ground, 14:00-17:55, Wednesday
co-presenting with bspar
Security researcher with interests in Cryptocurrency & Privacy

Hyrum Anderson
The current state of adversarial machine learning
Proving Ground, 18:00-18:25, Wednesday
mentor to Heather Lawrence

Brandon Arvanaghi
Attacking Ethereum dApps
Breaking Ground, 17:00-17:55, Tuesday
Brandon Arvanaghi is a Security Engineer at Gemini, specializing in blockchain security research, smart contract auditing, and secure dApp development. Brandon is an active researcher in Ethereum wallet security and has written frameworks to discover vulnerabilities in dApps. Before Gemini, Brandon was a security consultant at Mandiant, where he focused on sandbox hardening and evasion. Prior to working in the industry, Brandon conducted research on automated attack plan generation at Vanderbilt University.

Uptycs
Osquery Powered Security Analytics Platform
Curious about osquery?
Uptycs is a well funded startup looking for talented Front-End, Back-End and CSIRT engineers. Come help us build the first scalable osquery-powered security analytics platform for fleet visibility, intrusion detection, vulnerability management and compliance.

Come chat in-person or send your resume to jobs@uptycs.com
Cheryl Biswas  
Unifying the Kill Chain  
Proving Ground, 14:30–14:55, Wednesday  
mentored by Paul Pols  

Don’t Bring Me Down: Are You Ready for Weaponized Botnets?  
Ground Floor, 15:00–15:55, Wednesday  

Cheryl Biswas, aka @3ncr1pt3d, is a Strategic Threat Intel Analyst with TD Bank in Toronto, Canada. Previously, she was a Cyber Security Consultant with KPMG and worked on GRC, privacy, breaches, and DRP. She has done project management, vendor management and change management. Also, child management. She has an ITIL certification and degree in Political Science. Her areas of interest include APTs, mainframes, ransomware, ICS SCADA, and building threat intel. She actively shares her passion for security as a volunteer at conferences, encouraging diversity through “The Diana Initiative”, writing and speaking.

Gal Bitensky  
Invoke-NoShell  
Ground Floor, 12:00–12:25, Wednesday  

Gal Bitensky 30 years old geek from Tel-aviv. He is a senior analyst and security researcher, currently repelling attackers on enterprise scale at Minerva. “Full stack researcher” experienced in anything from debugging exploit kits to ICS protocols reverse engineering.

Dan Borges  
Tuning The Warp Drive with Laforge: New Tool for Building Security Competitions  
Proving Ground, 12:00–12:15, Wednesday  
co-presenting with Alex Levinson  

Dan Borges is an information security professional with over 15 years in computer science. Dan participates in a number of cyber security competitions each year, being from the National CCDC Red Team, to leading a Blue Team in Press Versus Joes, and helping run the Collegiate Penetration Testing Competition (CPTC). He has been publishing a blog on infosec education for more than 10 years.

Lucien Brule  
Who Maed Dis; A beginners guide to malware provenance based on compiler type.  
Common Ground, 14:00–14:55, Wednesday  
Malware Research Intern @EndgameInc @ RPISEC member  

Eric Bryan  
Vulnerability Management 101: Practical Experience and Recommendations  
Proving Ground, 18:00–18:30, Tuesday  
mentored by Magen Wu  
NorthState Technology Solutions Security Engineer  

bspar  
Smart Contracts: Hello World  
Training Ground, 14:00–17:55, Wednesday  
co-presenting with John Amirrezvani  

Briana Butler  
The Effect of Constraints on the Number of Viable Permutations of Passwords  
Ground1234!, 18:00–18:55, Tuesday  
co-presenting with Randy Abrams  
Engineering - Engineering Data Analyst  

Russell Butturini  
Not your Grandpa’s Password Policy  
Proving Ground, 17:30–17:55, Tuesday  
mentored by Kevin T Neely  

Ezra Caltum  
JARVIS never saw it coming: Hacking machine learning (ML) in speech, text and face recognition - and frankly, everywhere else  
Proving Ground, 15:00–15:55, Tuesday  
co-presenting with Guy Barnhart-Magen  

Aaron D. Campbell  
Lessons Learned by the WordPress Security Team  
Ground Floor, 15:00–15:55, Tuesday  

Aaron is the WordPress Security Team lead, has been a regular contributor to WordPress for more than ten years, and is currently funded by GoDaddy to work full time on the WordPress open source project. He’s been called both a coffee snob and a beer snob, but considers both to be compliments. When not buried in code, he enjoys spending time with his wife and son, riding his motorcycle, and reading sci-fi/fantasy books.

Nate Cardozo  
Ask The EFF  
Underground, 17:00–18:25, Wednesday  
co-presenting with Kurt Opsahl, Nash Sheard, Eva Galparin, and Cooper Quentin  

Nate Cardozo is a Senior Staff Attorney on EFF’s civil liberties team where he focuses on cybersecurity policy and defending coders’ rights. Nate has litigated cases involving electronic surveillance, freedom of information, digital anonymity, online free expression, and government hacking. His other projects include defending encryption, fighting software export controls, preserving automotive privacy, and assisting surveillance law reform efforts. As an expert in technology law and civil liberties, Nate works on EFF’s Who Has Your Back report and regularly assists companies in crafting rights-preserving policies and advising on compliance with legal process. A 2009-2010 EFF Open Government Legal Fellow, Nate spent two years in private practice before returning to his senses and to EFF in 2012. When he’s not brewing beer with his EFF colleagues, Nate serves on the boards of directors of the First Amendment Coalition and the South Asian Film Preservation Society. Nate has a B.A. in Anthropology and Politics from U.C. Santa Cruz and a J.D from U.C. Hastings where he has taught first-year legal writing and moot court.

Brian Carey  
Legendary Defender - The Voltron Analogy  
Proving Ground, 17:00–17:25, Tuesday  
mentored by Patrick McNeil  
Senior Security Consultant at Rapid7  

Lesley Carhart  
Hire Ground Kickoff  
Hire Ground, 11:30–12:00, Tuesday  

That Buzzword Bingo Rapid Debates Panel Thing  
Underground, 17:00–18:35, Tuesday  
co-presenting with Jen Ellis, Josh Corman, Chris Nickerson, and Robert Graham  

Lesley Carhart, Principal Threat Hunter at Dragos, Inc., is recognized as a subject matter in cybersecurity incident response - regularly speaking on the topic at conferences and universities. She has spent the last 9 years of her 19 year IT career specializing in information security, with a focus on response and analysis of nation state adversaries. Lesley is highly active in the security community, working to train the next generation of analysts through blogs, career clinics, and volunteerism. She also serves as a Cyber Transport Systems NCO in the United States Air Force Reserves. @Hacks4Pancakes

Marcel Carlsson  
Catch me, Yes we can! - Pwning Social Engineers using Natural Language Processing Techniques in real-time  
Ground Truth, 18:00–18:55, Tuesday  
co-presenting with Ian G. Harris  

Marcel Carlsson has presented at security and hacking conferences all over the world e.g. EAST FCS, Nordic Security Conference, Shákon, HackMiami, CONFidence and POC.

Seth Carmody  
CVE CVSS NVD OMGWTFBBQ  
(Wednesday Edition)  

I Am The Cavalry, 14:00–14:55, Wednesday  
co-presenting with Tom Millar, Katie Trimble, Art Manion, and Josh Corman
Lily Chalupowski
The Chrome Crusader
Ground@34, 11:30–12:25, Tuesday

Lily works with GoSecure on Threat Intelligence and started her journey being mostly self-taught making hacking tools in her spare time. Chameleon (custom base64 steganography), Badger (DLL Security Enumeration including ASLR Entropy), Dirty-Needle (DLL Injection Tool) and more. She has presented at the Atlantic Security Conference on PE File Structure Security Enumeration and Custom Base64 Steganography, Hask (Halifax Area Security Ktichen) on using file upload vulnerabilities to obtain shell access to a webserver using injection techniques, she has also presented at Digital Discovery Camp for kids on Phishing Awareness and SQLi with interactive demos helping children understand Cyber Security and how to keep an ethical approach, at the same time she is making Cyber Security a more attractive profession to young people.

Leeren Chang
Active Directory Password Blacklisting
Ground@34, 14:00–14:55, Tuesday

I am a software engineer currently working for Yelp’s corporate security team. The project I described in the abstract was one that I led. While undertaking the project, I was shocked to see how few corporations were utilizing employee password filtering countermeasures against dictionary attacks, and how misunderstood increasing password complexity as a solution to the issue was. I would love to spread my knowledge on this topic to better educate the public on the most effective password-based policies to follow.

Matt Cheung
Introduction to Cryptographic Attacks
Training Ground, 8:00–11:55, Tuesday

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol. Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh’s crypto 1 course offered on Coursera and the Matanzos/crypto1/pals challenges. From this experience he has given talks and workshops at the Boston Application Security Conference and the DEF CON Crypto and Privacy Village.

Clarence Chio
Bypassing Antivirus Engines using Open Sourced Malleable C2 Software, MSFVenom, Powershell and a bit of Guile
Proving Ground, 17:00–17:55, Wednesday

Ming Chow
Building A Teaching / Improvement Focused SOC
Proving Ground, 15:00–15:25, Tuesday

Lauren Clausen
Security Awareness Training Refresh
Common Ground, 11:00–11:55, Wednesday

Emily Gladstone Cole
Security and DevOps are really Best Friends
Ground Floor, 14:00–14:55, Wednesday

Emily is a Senior Security Engineer for Agari Data, Inc., an email security company.

Adam Compton
Hillbilly Storytime - Pentest Fails
Ground Floor, 11:00–11:55, Tuesday

Adam Compton has been a programmer, researcher, professional pentester, father, husband, and farmer. Adam has over 18 years of programming, network security, incident response, security assessment, and penetration testing experience. Throughout Adam’s career, he has worked for both federal and international government agencies as well as within various aspects of the private sector.

Brent Cook
LibreSSL - Moving the Ecosystem Forward
Common Ground, 15:00–15:55, Wednesday

Brent Cook is a Senior Manager at Rapid7 for the Metasploit project. He also contributes to the OpenBSD, LibreSSL, and OpenNTPD projects.
The #BSidesBus is back. Our friendly, complimentary shuttle will be available at LAS airport terminals 1 & 3, Tuscany, Flamingo, and Mandalay Bay through DC26. Schedule on page 7.

Special Thanks to The Hewlett Foundation for sponsoring PUBLIC GROUND at the Platinum.
Joshua Corman is a Founder of I am The Cavalry and Joseph Zadeh co-presenting with Beau Woods, Rod Soto, Suzanne Schwartz, and Jay Radcliffe.

Cyber Safety Disclosure co-presenting with Tom Millar, I Am The Cavalry, 14:00–14:55, Wednesday

Joshua Danielson

Guardians of GitHub

Ground1234!, 17:00–17:55, Wednesday

copresenting with Dileep Gurazada

With a decade of experience in both public and private sectors, Josh Danielson has served a variety of industries throughout his security career; from academia and government contracting, to the financial sector. Josh has received a Master of Science degree in Information Management from Syracuse University, and currently holds multiple certifications including CISSP-ISSAP and CISM.

Matt Devost

From Hacker to Serial Entrepreneur

Hire Ground, 12:30–13:25, Tuesday

copresenting with Allan Friedman, Matt Gallagher, Steve Ragan, and Paul Wagenseil

Monta Elkins

Stupid Hacker Tricks: Bridging Airgaps and Breaking Data Diodes

I Am The Cavalry, 10:00–10:25, Tuesday

Monta Elkins is currently “Hacker-in-Chief” for FoxGuard Solutions, an ICS patch provider. He is a security researcher/consultant and BFFs with the elusive #TrooperBR549. Considered by many of his friends to be the Chuck Norris of ICS Cybersecurity, Monta enjoys his tenure as Security Architect, and Radford University hired him as their first Information Security Officer. As the World’s Foremost Cordless Drill Hacker/Musician, Monta has been a speaker at more security and ICS conferences than even his enormous ego can remember. Monta is the totally-safe-for-work “Coke and Strippers” YouTube channel creator. 
https://tinyurl.com/6ypmbw4

Jen “Cat Herder” Ellis

Who Wants to Be A Regulator: The IoT Security Game Show

I Am The Cavalry, 14:00–14:55, Tuesday

copresenting with Joseph Cox, Sean Gallagher, Steve Ragan, and Paul Wagenseil

That Buzzword Bingo Rapid Debates Panel Thing

Underground, 10:00–10:25, Tuesday

copresenting with Joseph Cox, Sean Gallagher, Steve Ragan, and Paul Wagenseil

Jen Ellis is the vice president of community and public policy at Rapid7, a leading provider of analytics and automation for security and IT operations. Jen’s primary focus is on building productive collaboration between those in the security community and those operating outside it. She works extensively with security researchers, technology providers and operators, and various government entities to help
them understand and address cybersecurity challenges. She believes effective collaboration is our only path forward to reducing cyber-crime and protecting consumers and businesses. She has testified before Congress and spoken at a number of security industry events including SXSW, RSA, Derbycon, Shmoocon, SOURCE, UNITED, and various BSides.

Chris Eng
Implementing the Three Cs of Courtesy, Clarity, and Comprehension to Optimize End User Engagement
Proving Ground, 14:30–14:55, Tuesday
mentor to Courtney Kievernagel

Felipe “Pr0teus” Espósito
Endpoint Monitoring with Osquery and Kolide Fleet
Training Ground, 14:00–18:00, Wednesday
co-presenting with Rodrigo “Sp0oKeR” Montoro

Felipe “Pr0teus” has 10 years experience in TI, masters degree in Computer Systems and Networking. His interests include Network Covert Channels, Information visualization, Log analysis and Incident Response. Currently working for the Rio de Janeiro state court as Network Security Administrator, working hard to make the government’s environment as responsive against threats as possible. Felipe has spoken at a number of security and open source conferences such as Latinoware, FISL (Porto Alegre), H2HC (São Paulo), MindTheSec (Rio de Janeiro & São Paulo), BHack, BSides (Las Vegas & São Paulo).

Wendy Knox Everette
Who Wants to Be A Regulator: The IoT Security Game Show
Common Ground, 11:30–12:25, Tuesday
co-presenting with Allan Friedman, Karl Grindal, Karim Farhat, and Ishan Mehta

Wendy Knox Everette (@wendyck) is a hacker lawyer who works as a Senior Security Advisor at Leviathan Security Group. She began her career as a software developer at Amazon.com and Google, before going to law school, where she focused on national security law and computer security issues. She interned with the FTC, FGC, and several other three letter agencies, before completing a fellowship with ZwillGen in Washington, D.C., and then moving to Washington State where she advises companies on risk and security regulations.

Karim Farhat
A Good Day to Die? IoT End of Life
I Am The Cavalry, 17:00–17:55, Tuesday
co-presenting with Jessica Wilkerson, Allan Friedman, Karl Grindal, and Ishan Mehta

Karim Farhat is a Research Assistant and PhD student at the Georgia Institute of Technology, School of Public Policy. His work as a Research Associate at the Internet Governance Project (IGP) focuses on the institutional and standards environment evolving around the Internet of Things. Karim’s other research interests include the economics of information security and Internet governance. Before joining Georgia Tech, Karim was active in the Internet Society chapter of his native Lebanon, particularly through his involvement with the Internet governance and start-up arenas. Karim also worked in DC for an indie film company and has a Master in Media Studies from Ohio University.

Bianna Fernandez
What Did We Learn from Today? Recruiter Panel
Hire Ground, 18:00–18:30, Tuesday
co-presenting with Kris Rides and Scott Handley

Bianna Fernandez has been supporting Amazon’s security team for the last year and a half, focusing on all technical recruitment needs. In her own words: “Amazon has been unlike any company I have worked for. The culture combined with the relentlessness to build a high caliber team has been a welcoming and rewarding challenge!”

Kat Fitzgerald
Not your Mother’s Honeypot - Another name for Threat Intel
Ground Floor, 10:00–10:55, Wednesday

I took my parents’ stereo apart at the age of 7 to find out where the music came from. I am based in Chicago and a natural creature of winter, you can typically find me sipping Casa Noble Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos against a barrage of attackers. And I have honeypots all over the world.

Allan Friedman
Who Wants to Be A Regulator: The IoT Security Game Show
Common Ground, 11:30–12:25, Tuesday
co-presenting with Jen Ellis, Wendy Knox Everette, and Whitney Merrill

Allan Friedman has spoken at a number of security industry events including SXSW, RSA, Derbycon, Shmoocon, and various BSides. Allan has over 15 years of experience in international cybersecurity and technology policy. His experience and research focuses on economic and market analyses of information security. He has designed, convened, and facilitated national and international multi-stakeholder processes that have produced real results on cutting edge issues. Allan has significant experience in the press, has been featured in global media including CNN, NPR, and major American and international papers. He is frequently invited to speak or keynote to industry, academic, and public audiences.

David Forsey
Engaging Policymakers at the State Level
I Am The Cavalry, 18:00–18:55, Tuesday
co-presenting with Maurice Turner and Joe Hall

David is a policy analyst with the National Governors Association’s Center for Best Practices, where he helps governors’ offices and state agencies craft cybersecurity policy.
Previously, he worked on surveillance reform and encryption policy as National Security Fellow at Third Way. He has a law degree from Georgetown University Law Center and graduated magna cum laude from the University of Virginia.

James Forshaw
Windows Internals and Local Attack Surface Analysis using PowerShell
Training Ground, 8:00–11:55, Tuesday
James is a security researcher in Google’s Project Zero specializing in Microsoft Windows. He has been involved with computer hardware and software security for over 10 years looking at a range of different platforms and applications. With a great interest in logical vulnerabilities he’s been listed as the #1 researcher for MSRC, as well as being a Pwn2Own and Microsoft Mitigation Bypass bounty winner. He has spoken at a number of security conferences including Black Hat USA, CanSecWest, Bluehat, HTB, and Infitr8. He’s also the author of the book Attacking Network Protocols available from NoStarch Press.

Dimitri Fousekis
How I Met Your Password
Ground1234, 11:00–12:25, Wednesday
Hacker & Tinkerer or Things(Also CTO) Bitrack Cyber Security

Sean Gallagher
Engaging the Media: Know Your Target
I Am The Cavally, 14:00–14:55, Tuesday
co-presenting with Jen “Cat Herder” Ellis, Joseph Cox, Steve Ragan, and Paul Wagenseil
Engaging the Media: Telling Your Story
I Am The Cavally, 15:00–15:55, Tuesday
co-presenting with Steve Ragan, Paul Wagenseil, and Iain Thomson

Sean Gallagher is the Information Technology Editor and National Security Editor at Ars Technica. A former naval officer, information security officer and government IT contractor, Sean has reported on and performed lab testing on security and privacy issues in various guises for more than two decades.

Tom Gallagher
What is Agile and how can I use it well?
Proving Ground, 14:00–14:25, Wednesday
mentor to Nicole Schwartz

Eva Galperin
Ask The EFF
Underground, 17:00–18:25, Wednesday
co-presenting with Nate Cardozo, Kurt Opsahl, Nash Sheard, and Cooper Quintin

Eva Galperin is EFF’s Director of Cybersecurity. Prior to 2007, when she came to work for EFF, Eva worked in security and IT in Silicon Valley and earned degrees in Political Science and International Relations from SFU. Her work is primarily focused on providing privacy and security for vulnerable populations around the world. To that end, she has applied the combination of her political science and technical background to everything from organizing EFF’s Tbr Relay Challenge, to writing privacy and security training materials (including Surveillance Self Defense and the Digital First Aid Kit), and publishing research on malware in Syria, Vietnam, Kazakhstan. When she is not collecting new and exotic malware, she practices aerial circus arts and learning new languages.

Michael Gianarakis
iOS Runtime Hacking Crash Course
Breaking Ground, 11:00–11:55, Wednesday

Michael Gianarakis is the co-founder and CEO of Assetnote, a platform for continuous monitoring of your external attack surface. Michael has presented his mobile security research at various industry events and meetups including, DEF CON, Black Hat Asia, Thotcon, Rootcon, and Hack in the Box. Michael is also actively involved in the local security community in Australia where he is one of organizers of the monthly SecTalks meetup as well as the hacker camp TusKCon.

Sarah Gibson
Solving for Somebody Else’s Problem: Hacking Devs for Better Security
Common Ground, 17:00–17:55, Wednesday
Sarah Gibson fell into application security and found she liked it. For the past two years she has been in a role where she consults with development teams on security issues found in their projects. Assisting them with understanding and fixing their security bugs.

Spencer Gietzen
Pacu: Attack and Post-Exploitation in AWS
Breaking Ground, 15:00–15:55, Wednesday
With a background in software development, Spencer Gietzen is a penetration tester with Rhino Security Labs. His primary focus as a penetration tester is security relating to Amazon Web Services post exploitation and configuration, where he has found success in discovering vulnerabilities and attack vectors through extensive research.

Brad Girardeau
Deploying WebAuthn at Dropbox Scale: Second Factor and Beyond
Ground1234, 15:00–15:55, Wednesday
Brad thinks it’s helpful if people could add and multiply large random numbers in their head, or at least remember them. Instead he’s trying to make up for our inabilities with WebAuthn and added support for it to Dropbox, where he works on the product security team. He graduated from Stanford with a BS/MS in computer science, specializing in theory and security.

Daniel Grant
Sight beyond sight: Detecting phishing with computer vision.
Ground Truth, 17:00–17:55, Tuesday
Daniel Grant is a Data Scientist at Endgame where he focuses primarily on multi-class malware identification, model validation, and system behavioral analysis. He has an MS in Operations Research from Georgia Tech.

Joe Gray
From CTF to CVE: How Application of Concepts and Persistence led to a Vulnerability Disclosure
Ground Floor, 11:30–12:25, Tuesday
Senior Security Architect(Do to wording, I am unsure if you want a full speaker bio beyond job title, so submitting below) Joe Gray joined the U.S. Navy directly out of High School and served for 7 years as a Submarine Navigation Electronics Technician. Joe is currently a Senior Security Architect at IBM and maintains his own blog and podcast called Advanced Persistent Security. In his spare time, Joe enjoys attending information security conferences, contributing blogs to various outlets, training in Brazilian Jiu Jitsu (spoken taps out A LOT!), and flying his drone. Joe is in the inaugural winner of the DerbyCon Social Engineering Capture the Flag (SECTF) and was awarded

Robert Graham
That Buzzword Bingo Rapid Debates Panel Thing
Underground, 17:00–18:55, Tuesday
co-presenting with Jen Ellis, Josh Corman, Chris Nickerson, and Lesley Carhart
Robert Graham has been the creator of well-known cybersecurity tools over the last two decades, including the first IPS, the BlackICE intrusion detection system, sidejacking, and most recently masscan, a tool that can scan the entire Internet in less than a few minutes. You’ve probably seen his name infesting your web server logs as he and others use masscan on a regular basis to scan the Internet. His blog can be found at https://blog.erratasec.com, and his code can be found at https://github.com/robertdavidgraham.

Eva Galperin
Ask The EFF
Underground, 17:00–18:25, Wednesday
co-presenting with Nate Cardozo, Kurt Opsahl, Nash Sheard, and Cooper Quintin

Eva Galperin is EFF’s Director of Cybersecurity. Prior to 2007, when she came to work for EFF, Eva worked in security and IT in Silicon Valley and earned degrees in Political Science and International Relations from SFU. Her work is primarily focused on providing privacy and security for vulnerable populations around the world. To that end, she has applied the combination of her political science and technical background to everything from organizing EFF’s Tbr Relay Challenge, to writing privacy and security training materials (including Surveillance Self Defense and the Digital First Aid Kit), and publishing research on malware in Syria, Vietnam, Kazakhstan. When she is not collecting new and exotic malware, she practices aerial circus arts and learning new languages.

Michael Gianarakis
iOS Runtime Hacking Crash Course
Breaking Ground, 11:00–11:55, Wednesday

Michael Gianarakis is the co-founder and CEO of Assetnote, a platform for continuous monitoring of your external attack surface. Michael has presented his mobile security research at various industry events and meetups including, DEF CON, Black Hat Asia, Thotcon, Rootcon, and Hack in the Box. Michael is also actively involved in the local security community in Australia where he is one of organizers of the monthly SecTalks meetup as well as the hacker camp TusKCon.

Sarah Gibson
Solving for Somebody Else’s Problem: Hacking Devs for Better Security
Common Ground, 17:00–17:55, Wednesday
Sarah Gibson fell into application security and found she liked it. For the past two years she has been in a role where she consults with development teams on security issues found in their projects. Assisting them with understanding and fixing their security bugs.

Spencer Gietzen
Pacu: Attack and Post-Exploitation in AWS
Breaking Ground, 15:00–15:55, Wednesday
With a background in software development, Spencer Gietzen is a penetration tester with Rhino Security Labs. His primary focus as a penetration tester is security relating to Amazon Web Services post exploitation and configuration, where he has found success in discovering vulnerabilities and attack vectors through extensive research.

Brad Girardeau
Deploying WebAuthn at Dropbox Scale: Second Factor and Beyond
Ground1234, 15:00–15:55, Wednesday
Brad thinks it’s helpful if people could add and multiply large random numbers in their head, or at least remember them. Instead he’s trying to make up for our inabilities with WebAuthn and added support for it to Dropbox, where he works on the product security team. He graduated from Stanford with a BS/MS in computer science, specializing in theory and security.

Daniel Grant
Sight beyond sight: Detecting phishing with computer vision.
Ground Truth, 17:00–17:55, Tuesday
Daniel Grant is a Data Scientist at Endgame where he focuses primarily on multi-class malware identification, model validation, and system behavioral analysis. He has an MS in Operations Research from Georgia Tech.

Joe Gray
From CTF to CVE: How Application of Concepts and Persistence led to a Vulnerability Disclosure
Ground Floor, 11:30–12:25, Tuesday
Senior Security Architect(Do to wording, I am unsure if you want a full speaker bio beyond job title, so submitting below) Joe Gray joined the U.S. Navy directly out of High School and served for 7 years as a Submarine Navigation Electronics Technician. Joe is currently a Senior Security Architect at IBM and maintains his own blog and podcast called Advanced Persistent Security. In his spare time, Joe enjoys attending information security conferences, contributing blogs to various outlets, training in Brazilian Jiu Jitsu (spoken taps out A LOT!), and flying his drone. Joe is in the inaugural winner of the DerbyCon Social Engineering Capture the Flag (SECTF) and was awarded

Robert Graham
That Buzzword Bingo Rapid Debates Panel Thing
Underground, 17:00–18:55, Tuesday
co-presenting with Jen Ellis, Josh Corman, Chris Nickerson, and Lesley Carhart
Robert Graham has been the creator of well-known cybersecurity tools over the last two decades, including the first IPS, the BlackICE intrusion detection system, sidejacking, and most recently masscan, a tool that can scan the entire Internet in less than a few minutes. You’ve probably seen his name infesting your web server logs as he and others use masscan on a regular basis to scan the Internet. His blog can be found at https://blog.erratasec.com, and his code can be found at https://github.com/robertdavidgraham.
a DerbyCon Black Badge. Joe has contributed material for the likes of AlienVault, ITSP Magazine, CSO Online, and Dark Reading.

Jerome Greco
You’re just complaining because you’re guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software Used In the Criminal Justice System
Common Ground, 18:00–18:55, Tuesday
co-presenting with
Jeanna N. Matthews and Nathan Adams
Jerome Greco is a public defender in the Digital Forensics Unit of the Legal Aid Society in New York City. Along with four analysts, he works with attorneys and investigators in all five boroughs on issues involving historical cell-site location information, cell phone extraction, electronic surveillance technology, social media, and hard drive analysis, among other fields. He is currently engaged in challenging the NYPD’s use of cell-site simulators, facial recognition, and the execution of overbread search warrants for electronic devices. Prior to his work with the Digital Forensics Unit, he was a trial attorney in the Legal Aid Society’s Manhattan and Staten Island criminal defense offices. He graduated magna cum laude from New York Law School in 2011 and received his B.A. from Columbia University in 2008.

Karl Grindal
A Good Day to Die? IoT End of Life
I Am The Cavalry, 17:00–17:55, Tuesday
co-presenting with Jessica Wilkerson, Allan Friedman, Karim Farhat, and Ishan Mehta
Karl is a policy analyst and information security researcher based in Atlanta, GA. He is a Research Associate with the Internet Governance Project, and a Ph.D Candidate at the Georgia Institute of Technology’s School of Public Policy. Karl previously served as the Director of Research for Cyber Conflict Studies Association (CCSA), a non-profit dedicated to advancing a research agenda on cyber conflict. Karl has a Master’s of Public Policy with a concentration in Technology Policy from Georgetown University and completed his undergraduate studies with a Bachelor’s of Arts in Government from Wesleyan University.

Vaibhav Gupta
Attack & Defense in AWS Environments
Training Ground, 14:00-15:55, Wednesday
co-presenting with Sandeep Singh
Vaibhav is working as a Security Researcher with Adobe Systems. His expertise lies in infusing design and architecture level security in applications hosted on in-house and cloud environments. With ~9 years of InfoSec exposure, he has strong experience in attacking and defending applications including the ones hosted on the cloud. He is co-leading the OWASP and Null community in Delhi region and has delivered multiple talks at the local and international stage.

Dileep Gurazada
Guardians of GitHub
GroundTruth, 17:00-17:55, Wednesday
co-presenting with Joshua Danielson
A strong engineering background along with knowledge in infrastructure and application security vulnerabilities has allowed Dileep to develop cutting edge solutions for a wide-ranging set of use cases. With an M.S in Computer Science from the University of Texas at Dallas, Dileep is currently an application security engineer at Copart.

Joe Hall
Engaging Policymakers at the State Level
I Am The Cavalry, 18:00-18:55, Tuesday
co-presenting with Maurice Turner and David Forsey
Joseph Lorenzo Hall is the Chief Technologist and Director of the Internet Architecture project at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring the internet remains open, innovative and free. Hall’s work focuses on the intersection of technology law and policy, working to ensure that technical considerations are appropriately embedded into legal and policy instruments. Supporting work across all of CDT’s programmatic areas, Hall provides substantive technical expertise to CDT’s programs, and interfaces externally with CDT supporters, stakeholders, academics, and technologists.

Scott Handley
What Did We Learn from Today? Recruiter Panel
Hire Ground, 18:00-18:30, Tuesday
co-presenting with Kris Rides and Briana Fernandez
Talent Acquisition Manager at Sentek Global, a DOD and commercial cybersecurity firm based in San Diego, CA. With over a decade of experience in talent management, Scott is currently focusing on commercial and DOD grade cybersecurity. He also serves in the United States Navy as a Public Affairs Officer (PAO).

Russel Handorf
Why Can’t We Be Friends? (Get Spotted With A Fed)
Underground, 15:00-15:55, Wednesday
TLDR- Cyber Ninjas, you’re invited.

Ian G. Harris
Catch me, Yes we can! - Pwning Social Engineers using Natural Language Processing Techniques in real-time
Ground Truth, 18:00-18:55, Tuesday
co-presenting with Marcel Carlsson
Before joining this company, Eugene led the launch of Symantec’s Security Response Center in Singapore. In which, he created a regional multi-functional security team, focusing on attack investigations. Eugene is best known for his contributions to the Linux kernel. He was with Red Hat’s product security team. He was also a security officer of the upstream Linux kernel security team.

ENDGAME. The Only Agent You’ll Ever Need
- Replace AV
- Stop ransomware, malware, phishing, and fileless attacks
- Automated threat hunting

ENDGAME ARTEMIS
Visit our table to learn more!
Christopher Simon Hanlon
Disabling Encryption to Access Confidential Data
Proving Ground, 15:30–15:55, Wednesday
mentored by John Seymour
Chris Hanlon has reported multiple data leak vulnerabilities to Google, been invited to the Google Security Hall of Fame, and maintained servers, desktops, and firewalls for hundreds of businesses.

Jon Hawes
101 ways to fail at getting value out of your investments in security analytics, and how not to do that
Ground Truth, 11:30–12:25, Tuesday
Jon manages Security Data Analytics for a global energy company. In his spare time he likes longboarding down hills. Fast.

Dave Herrald
Advanced APT Hunting with Splunk
Training Ground, 8:00–17:55, Wednesday
co-presenting with Ryan Kovar and John Stoner
Dave Herrald is a veteran security technologist. He holds a gaggle of security certs including the GIAC GSE #79. Dave works on Splunk’s Security Practice team and he rides bikes and skis for sanity. @daveherrald

Cindy Jones
Community Career Panel or How to Get More than a T-Shirt Working at a Con
Hire Ground, 14:30–15:00, Wednesday
co-presenting with Megan Wu, Kristen Renner, and Kathleen Smith
Cindy brings works with Rapid7 as a Principal Security Consultant with Advisory Services. Cindy spends a good chunk of her time by leading the Reg team for BSidesLV, volunteers for DerbyCon, and is 2IC for Workshops at DEF CON. Her favorite color is purple and she doesn’t use that as a security question.

Michael Kajiloti
SiliVaccine: North Korea’s Weapon of Mass Detection
Breaking Ground, 14:00–14:55, Tuesday
co-presenting with Mark Lechtik
Michael is a security researcher with interests ranging from reverse engineering & malware to cryptocurrencies. He currently works as the malware research team leader in Check Point, and enjoys teaching and lecturing on the things he is passionate about.

Aamil Karimi
Incorporating Human Intelligence (HUMINT) into An Information Security Team
Proving Ground, 15:00–15:25, Wednesday
mentored by Rachael Lininger
Principal Intelligence Analyst + HUMINT Lead, Optiv Security

Sina Kashefi pour
Modern Political Warfare: A Look at Strategy and TTPs
Proving Ground, 15:30–15:55, Tuesday
mentored by Brendan O’Connor

Courtney Kievernagel
Implementing the Three Cs of Courtesy, Clarity, and Comprehension to Optimize End User Engagement
Proving Ground, 14:30–14:55, Tuesday
mentored by Chris Eng

Joe Klein
Fast-track your Hacking Career – Why Take The Slow Lane?
Hire Ground, 14:00–14:30, Wednesday
For over 40 years, Joe Klein has played many roles in the Cyber Security domain, from Chief Security Officer, incident handler, forensics engineer, cyber intelligence, auditor, trainer, mentor, and administrator of boxes with blinky lights. He has spoken at many national and international venues such as Black Hat, DefCon, BSides, SecTor, TorCon, SANS, SecurityDays, and of course HOPE. Over his career, he has performed hundreds of security audits, assessments, and penetration tests for commercial and government agencies. He enjoys Earl Gray Tea, hot, his favorite number is 42, and he has a weeping angel painting on his wall.

Ryan Kovar
Advanced APT Hunting with Splunk
Training Ground, 8:00–17:55, Wednesday
co-presenting with Dave Herrald and John Stoner
Ryan Kovar fought in the cyberwars and has been doing cybery things for almost 20 years. Now he is a Principal Security Strategist at Splunk building cool stuff, talking about security things, and helping other people fight their battles. He hates printers. @meansec

Chris Kubecka
How to Start a Cyber War: Lessons from Brussels - EU Cyber Warfare Exercises
Common Ground, 14:00–14:55, Tuesday
Chris Kubecka is an experienced, committed, energetic and certified digital security expert who is passionate about solutions. Over 20 years of professional experience ranging from military, government, public and private business. Prior to establishing HypaSec in 2015, Chris established and headed network and security operations teams, ICS security, international joint intelligence teams, EU/UK privacy group for EMEA and South American (outside Saudi Arabia) for Aramco Overseas Company, part of Saudi Aramco. She was
Competition (CCDC). Previously, Alex worked for the National Collegiate Cyber Defense of Uber, he is a core member of the red team threat assessment, and investigations. Outside experience in red teaming, incident response, Alex Levinson is a Senior Engineer at Uber with co-presenting with Dan Borges Breaking Ground, 12:00–12:25, Wednesday.

Tool for Building Security Competitions

Tuning The Warp Drive with Laforge: New

Alex Levinson
Tuning The Warp Drive with Laforge: New Tool for Building Security Competitions

Breaking Ground, 12:00–12:25, Wednesday
co-presenting with Dan Borges

Alex Levinson is a Senior Engineer at Uber with experience in red teaming, incident response, threat assessment, and investigations. Outside of Uber, he is a core member of the red team for the National Collegiate Cyber Defense Competition (CCDC). Previously, Alex worked as a Senior Consultant at Lares Consulting.

Andrea Little Limbago
Increasing Retention Capacity

Hire Ground, 11:00–11:30, Wednesday

Dr. Andrea Little Limbago is the Chief Social Scientist at Endgame, where she researches and writes on geopolitics, cybersecurity, and data science, while also directing the company’s technical content. Her writing has been featured in numerous outlets, including Politico, the Hill, VentureBeat, Forbes, War on the Rocks, and Dark Reading. She also has presented at numerous conferences, including SXSW, DerbyCon, Enigma, and BSidesLV.

Andrea previously worked in academia and at the Joint Warfare Analysis Center. While at JWAC, Andrea received the Command’s top award for technical excellence for her analytic support across the Department of Defense. Andrea holds a PhD in Political Science from the University of Colorado at Boulder.

Rachael Lininger
Incorporating Human Intelligence (HUMINT) into an Information Security Team

Proving Ground, 15:00–15:25, Wednesday
co-mentoring with Aamil Karimi

Guy Barnhart-Magen
JARVIS never saw it coming: Hacking machine learning (ML) in speech, text and face recognition - and frankly, everywhere else

Breaking Ground, 15:00–15:55, Tuesday
co-presenting with Ezra Calturn

Guy is a member of the BSidesTLV organizing team and recipient of the Cisco “black belt” security ninja honor - the highest cyber security advocate rank. With over 15 years of experience in the cyber-security industry, he held various positions in both corporates and start-ups. He is currently a security research manager at Intel, where he focuses on AI Security, reverse engineering and researching various embedded systems.

Mark Mager
Stop and Step Away from the Data: Rapid Anomaly Detection via Ransom Note File Classification

Ground Truth, 15:00–15:55, Tuesday

Senior Malware Researcher at Endgame—Throughout his career in software engineering and computer security, Mark has served in prominent technical leadership roles in the research and development of advanced computer network operations tools and has provided malware analysis and reverse engineering subject matter expertise to a diverse range of government and commercial clients in the Washington, D.C. metropolitan area.

Art Manion
CVE CVSS NVD OMGWTFBBQ (Wednesday Edition)

I Am The Cavalry, 14:00–14:55, Wednesday
co-presenting with Tom Milliar, Katie Trimble, Seth Carmody, and Josh Corman

Arbitrary Albatross: Neutral Names for Vulnerabilities at Volume

Ground Truth, 18:00–18:55, Wednesday
co-presenting with Leigh Metcalf

Art Manion is the Vulnerability Analysis Technical Manager at the CERT Coordination Center (CERT/CC), part of the Software Engineering Institute at Carnegie Mellon University. He has studied software security and computer network operations tools and has provided malware analysis and reverse engineering subject matter expertise to a diverse range of government and commercial clients in the Washington, D.C. metropolitan area.

Andrea Marcelli
Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era

Ground Truth, 15:30–15:55, Wednesday

Eugene has a keen interest in applying visualization and machine learning techniques to address computer security problems.

Jeanna N. Matthews
You’re just complaining because you’re guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software

Used in the Criminal Justice System

Common Ground, 18:00–18:55, Tuesday
co-presenting with Nathan Adams and Jerome Greco

Dr. Matthews is an associate professor of Computer Science at Clarkson University and a 2017-18 fellow at Data and Society. She is member of the Executive Committee of US-ACM, the U.S. Public Policy Committee of ACM and one of the co-chairs of their subcommittee on algorithmic transparency and accountability. She was a speaker and DEFCON 23 and 24, both times on the topic of vulnerabilities in virtual networks. Her broader research interests include virtualization, cloud computing, computer security, computer networks and operating systems.
Jeanna received her Ph.D. in Computer Science from the University of California at Berkeley and is an ACM Distinguished Speaker.

**Patrick McNeil**
**Legendary Defender - The Voltron Analogy**

Proving Ground, 17:00–17:25, Tuesday
mentor to Brian Carey

Johnny Medina is a Red Team Lead at General Motors, responsible for leading logical and physical penetration testing security assessments globally. He has over 8 years of experience in Information Security in both the government and corporate sectors, filling diverse roles such as Security Advisor, Information Systems Security Officer, and Information Assurance Engineer. Johnny has a bachelor’s in Technology Management and holds certifications including CISSP, GFE and GSEC. Kyle Cucci is a Security & Privacy Researcher in Technology Management and holds certifications including OSCP, Security +, and CISSP. During non-work hours, Kyle enjoys tinkering with open-source security tools and bug hunting.

**Jeanna Shearer**
**Proving Ground, 15:00–15:55, Tuesday**
codifying with Remy Topp, Karim Farhat, and Kurt Hebershuber

Johnny Medina is a Red Team Lead at General Motors, responsible for leading logical and physical penetration testing security assessments globally. He has over 8 years of experience in Information Security in both the government and corporate sectors, filling diverse roles such as Security Advisor, Information Systems Security Officer, and Information Assurance Engineer. Johnny has a bachelor’s in Technology Management and holds certifications including CISSP, GFE and GSEC. Kyle Cucci is a Security & Privacy Researcher in Technology Management and holds certifications including OSCP, Security +, and CISSP. During non-work hours, Kyle enjoys tinkering with open-source security tools and bug hunting.

**Keith Cantiello**
**Proving Ground, 16:00–16:50, Tuesday**
codifying with Remy Topp, Karim Farhat, and Kurt Hebershuber

Johnny Medina is a Red Team Lead at General Motors, responsible for leading logical and physical penetration testing security assessments globally. He has over 8 years of experience in Information Security in both the government and corporate sectors, filling diverse roles such as Security Advisor, Information Systems Security Officer, and Information Assurance Engineer. Johnny has a bachelor’s in Technology Management and holds certifications including CISSP, GFE and GSEC. Kyle Cucci is a Security & Privacy Researcher in Technology Management and holds certifications including OSCP, Security +, and CISSP. During non-work hours, Kyle enjoys tinkering with open-source security tools and bug hunting.

**Taylor Winklevoss**
**I Am The Cavalry, 12:00–12:55, Tuesday**
codifying with Karim Farhat, Kurt Hebershuber, and Remy Topp

Johnny Medina is a Red Team Lead at General Motors, responsible for leading logical and physical penetration testing security assessments globally. He has over 8 years of experience in Information Security in both the government and corporate sectors, filling diverse roles such as Security Advisor, Information Systems Security Officer, and Information Assurance Engineer. Johnny has a bachelor’s in Technology Management and holds certifications including CISSP, GFE and GSEC. Kyle Cucci is a Security & Privacy Researcher in Technology Management and holds certifications including OSCP, Security +, and CISSP. During non-work hours, Kyle enjoys tinkering with open-source security tools and bug hunting.

**Michael A. Caruso**
**Proving Ground, 16:00–16:50, Tuesday**
codifying with Remy Topp, Karim Farhat, and Kurt Hebershuber

Johnny Medina is a Red Team Lead at General Motors, responsible for leading logical and physical penetration testing security assessments globally. He has over 8 years of experience in Information Security in both the government and corporate sectors, filling diverse roles such as Security Advisor, Information Systems Security Officer, and Information Assurance Engineer. Johnny has a bachelor’s in Technology Management and holds certifications including CISSP, GFE and GSEC. Kyle Cucci is a Security & Privacy Researcher in Technology Management and holds certifications including OSCP, Security +, and CISSP. During non-work hours, Kyle enjoys tinkering with open-source security tools and bug hunting.

**Ishan Mehta**
**A Good Day to Die? IoT End of Life**

I Am The Cavalry, 17:00–17:55, Tuesday
co-presenting with Jessica Wilkerson, Allan Friedman, Karl Grindal, and Karim Farhat

Ishan is a policy advisor for the National Security Program at Third Way. Focusing on cybersecurity, he aims to work at the intersection of technology and policy and bring the two worlds closer. He has a double master’s degree from the Georgia Institute of Technology in Computer Engineering and Public Policy. He spent time in Silicon Valley working as an engineer for Intel. As a graduate student researcher for the Internet Governance Project, he has contributed to research on cybersecurity attribution, Internet governance and digital trade. During his time in Atlanta, he worked in local politics and led a digital rights activists group. He is most proud of his efforts that led to the veto of a poorly written cybersecurity bill.

**Whitney Merrill**
**Who Wants to Be A Regulator: The IoT Security Game Show**

Common Ground, 11:30–12:25, Tuesday
co-presenting with Allan Friedman, Jen Ellis, and Wendy Knox Everette

Whitney Merrill is a privacy attorney at Electronic Arts (EA). Recently, she served her government as an attorney at the Federal Trade Commission where she worked on a variety of consumer protection matters including data security, privacy, IoT, and deceptive marketing and advertising. She also runs the Crypto & Privacy Village which appears at DEF CON each year. Whitney has spoken at a number of hacker & infosec conferences including, Chaos Communication Congress, DEF CON, Shmoocon, BSides LV, IndiSec World, and THOTCON. In everything Whitney does, she fights for the users.

**Leigh Metcalf**
**Arbitrary Albatross: Neutral Names for Vulnerabilities at Volume**

Ground Truth, 18:00–18:55, Wednesday
codifying with Art Manion

Leigh Metcalf is a Senior Consultant at Shadytel, and helps people get their security bugs fixed.

**Tom Millar**
**CVE CVSS NVD OMGWTFBBQ**
(Wednesday Edition)

I Am The Cavalry, 14:00–14:55, Wednesday
co-presenting with Katie Tribble, Art Manion, Seth Carmody, and Josh Corman

Tom Millar is a Technical Advisor to the Under Secretary of the Department of Homeland Security (DHS)’s cybersecurity and infrastructure protection arm, the National Protection and Programs Directorate. Mr. Millar was a member of US-CERT for 10 years, serving as its Chief of Communications for most of that time. In that role, he has worked to strengthen US-CERT’s information sharing capabilities, increased the level of public, private and international partner engagement, and supported initiatives to improve information exchange by both humans and machines, such as the standardization of the Traffic Light Protocol and the development of the Structured Threat Information eXpression.

**David Minch**
**Watch Out For That Bus! (Personal Disaster Recovery Planning)**

Common Ground, 18:00–18:55, Wednesday
co-presenting with Udi Yavo

David Minch is a cybersecurity engineer, focusing on exploiting and securing critical systems. He has a blend of technical and non-technical experience that helps him practice balanced security. In his free time, he enjoys playing with his overly complicated home network, especially a new-to-him Dell R610 running more VMs than necessary for a house. When he isn’t doing security, he’s probably destroying his house, serving his cats, or drinking orange crushes (it’s a Maryland thing).
Rodrigo “Sp0oKeR” Montoro
End-to-End Monitoring with Osquery and Kolide Fleet
Training Ground, 14:00–17:55, Wednesday
co-presenting with Felipe “Pr0teus” Esposito
Rodrigo “Sp0oKeR” Montoro has 18 years experience deploying open source security software (firewalls, IDS, IPS, HIDS, log management) and hardening systems. Currently he is Senior Security Engineer & Researcher at Neuway. Previously worked as a SO/PO Researcher at Clavis, Senior Security Administrator at Sucuri. Also worked as a Researcher at Spiderlabs, focusing on IDS/IPS Signatures, Modsecurity rules, and new detection research. Author of two patents involving discovery of malicious digital documents and analyzing malicious HTTP traffic. Rodrigo is currently coordinator and Snort evangelist for the Brazilian Snort Community. Rodrigo has spoken at a number of open source and security conferences (OWASP AppSec, Toorcon (USA), BHHC (San Paulo and Mexico), SecTor (Canada), CNAI, SOURCE Boston & Seattle, SANS DEF, ZoneCon (Amazon Internal Conference), BSides (Las Vegas and São Paulo), Black Hat Brazil).

Manju Mude
Redefining the Hacker
Hire Ground, 10:00–11:00, Wednesday
Ms. Mude is an Information Security, Risk and Compliance Leader with almost 20 years of experience in information security, business leadership, compliance and risk management, within the high-tech and financial services industries.

Dennis Murphy
Intro to Industrial Control System Network Analysis
Training Ground, 8:00–17:55, Tuesday
Director, US Cybersecurity Operations

Mike Murray
The Key to Managing High Performance Security Teams
Hire Ground, 10:00–11:00, Wednesday
Mike Murray for the past decade has been focused on information security in many diverse forms. He has led an information security consulting practice within industry leading organizations including GE Healthcare and Neohapsis or as an entrepreneur/founder of The Hacker Academy and MAD Security, where they bootstrapped the company to over $25M in revenue in the first 4 years. For the past year, he has been building out the global research function at Lookout, where we’re leading detection of malware, vulnerabilities and risky applications on mobile platforms. Mike has built global information security programs and has a proven track record of implementing pragmatic and results-driven security organizations which balance risks against business imperatives and rewards. As the Threat Intelligence Lead for the MITRE ATT&CK team, Katie focuses on applying cyber threat intelligence to ATT&CK and evangelizing how that helps analysts. She has worked in threat intelligence and network defense for nearly a decade, with much of that time spent helping Security Operations Centers navigate how to apply intel to defenses. Katie hails from a liberal arts background with degrees from Smith College and Georgetown University’s School of Foreign Service. When she’s not losing her mind over group aliases, Katie enjoys deadlifting, baking cookies, and teaching teenage girls about cybersecurity.

Kevin T Neely
Not your Grandpa’s Password Policy
Proving Ground, 13:30–17:55, Tuesday
mentored by Russell Buttirinni
Information Security Manager

Katie Nickels
ATT&CKing the Status Quo: Improving Threat Intel and Cyber Defense with MITRE ATT&CK
Breaking Ground, 11:30–12:25, Tuesday
co-presenting with John Wunder

2-second visibility of all your assets
qualys.com/2seconds
Brendan O’Connor
Modern Political Warfare: A Look at Strategy and TTPs
Proving Ground, 15:30–15:55, Tuesday
mentor to Sina Kashefi

Kurt Opsahl
Ask The EFF
Underground, 17:00–18:25, Wednesday
co-presenting with Nate Cardozo, Nash Sheard, Eva Galparin, and Cooper Quentin
Kurt Opsahl is the Deputy Executive Director and General Counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech and privacy law, Opsahl counsels on EFF projects and initiatives. Opsahl is the lead attorney on the Coders’ Rights Project, and is representing several companies who are challenging National Security Letters. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on Kelly v. Arribasoft, MGM v. Grokker and CoStar v. LoopNet. For his work responding to government subpoenas, Opsahl is proud to have been called a “rabid dog” by the Department of Justice. Prior to Perkins, Opsahl was a research fellow to Professor Pamela Samuelson at the U.C. Berkeley School of Information Management & Systems. Opsahl received his law degree from Boalt Hall, and undergraduate degree from U.C. Santa Cruz. Opsahl co-authored “Electronic Media and Privacy Law Handbook.” In 2007, Opsahl started out as a help-desk technician and network administrator, before moving into software development, and then into journalism. He is currently the managing editor at Decipher. Over the past decade and a half, Fahmida Y Rashid has written for various infotech trade publications including Dark Reading, InfoWorld, CSO, CRN, PCMag, and SecurityWeek.

Paul Pols
Unifying the Kill Chain
Proving Ground, 14:30–14:55, Wednesday
mentored by Cheryl Biswas
Ethical hacker. Author. Lecturer.

Leila Powell
Can data science deal with PAM?
Ground Truth, 12:00–12:25, Wednesday
I’m a data scientist working in security. I used to use supercomputers to study the evolution of galaxies as an astrophysicist. Now I tackle more down-to-earth challenges, helping companies use different data sets to understand and address security risk. As part of the team at Panasée (a London based security start up), I work with security functions in global financial firms, applying data science to help solve strategic and operational challenges.

Cooper Quentin
Ask The EFF
Underground, 17:00–18:25, Wednesday
co-presenting with Nate Cardozo, Kurt Opsahl, Nash Sheard, and Eva Galparin

Jay Radcliffe
Cyber Safety Disclosure
I Am The Cavalry, 15:00–15:55, Wednesday
co-presenting with Natha Alli, Suzanne Schwartz, and Joshua Corman
Having spent fifteen years spent in the field of computer security, Jay Radcliffe has used just about every device made within the last decade. He gained notoriety in 2011 for presenting groundbreaking research on security vulnerabilities in medical devices at a world-renowned security conference. Bloomberg hailed the impact this research had on Congress and the FDA in a 2014 article on the “Top 10 Greatest White-Hat Hacks” of all time. He holds a Master’s degree in Information Security Engineering from SANS Technology Institute as well as a Bachelor’s degree in Criminal Justice/Pre-Law from Wayne State University.

Steve Ragan
Engaging the Media: Know Your Target
I Am The Cavalry, 14:00–14:55, Tuesday
co-presenting with Jen “Cat Herder” Ellis, Joseph Cox, Sean Gallagher, and Paul Wagenseil
Prior to joining the journalism world in 2005, Steve Ragan spent 15 years as a freelance IT contractor focused on infrastructure management and security. He’s a father of two and rounded geek with a strong technical background.

Sneha Rajguru
Mobile Application Hacking - Master Class
Training Ground, 8:00–17:55, Tuesday
Treble or Trouble: Where Android’s latest security enhancements help, and where they fall
Proving Ground, 18:30–18:55, Wednesday
mentored to Tamir Zahavi-Brunner
Sneha works as Security Consultant with Payatu Software Labs LLP. Her areas of inter-
Yothin Rodanant  
Overlooked tactics for attacking hardened Active Directory environment  
Breaking Ground, 17:00–17:55, Wednesday  
copresenting with Hao Wang and Joshua Theimer  

Yothin Rodanant is a Manager in Ernst & Young LLP’s Advanced Security Center (ASC). Yothin has eight years of hands-on experience performing penetration testing, security research and cyber-investigations. Yothin is currently responsible for overseeing the development of various assessment methodologies, including Red Team, external and internal penetration testing, web application security assessments, physical security assessments, wireless assessments and social engineering tests. In this role, he regularly contributes cutting-edge hacking techniques to the team members. His areas of research include Active Directory security and accelerated password cracking.

David Rogers  
Transforming Industries for Fun and Safety (Presentation)  
I Am The Cavalry, 17:30–17:55, Wednesday  
copresenting with Beau Woods  

David Rogers runs Copper Horse Solutions Ltd, a software and security company based in Windsor, UK, focusing on security and privacy research for the Internet of Things. David chairs the Device Security Group at the GSM Association and sits on the Executive Board of the Internet of Things Security Foundation. He is a Visiting Professor in Cyber Security and Digital Forensics at York St John University and teaches Mobile Systems Security at the University of Oxford. Prior to his 20 years in the mobile industry in security and engineering roles, David worked in the semiconductor industry. Most recently he authored the UK’s ‘Code of Practice for Security in Consumer IoT Products and Associated Services’, in collaboration with DCMs, NCSC, ICO and industry colleagues.

Gabriel Ryan  
Advanced Wireless Attacks Against Enterprise Networks  
Training Ground, 8:00–11:55, Wednesday  
copresenting with Justin Whitehead  

Gabriel Ryan is a penetration tester and researcher with a passion for wireless and infrastructure testing. He currently serves a co-founder and principle security consultant for Digital Silence, a Denver based consulting firm that specializes in impact driven penetration testing and red team engagements. Prior to joining Digital Silence, Gabriel worked as a penetration tester and researcher for Gotham Digital Silence, contributing heavily to their wireless security practice and regularly performing large scale infrastructure assessments and red teams for Fortune 500 companies. Some of Gabriel’s most recent work includes the development of EAPHammer, an 802.11ac focused tool for breaching WPA2-EAP networks. On the side, he serves as a member of the BSides Las Vegas senior staff, coordinating wireless security for the event. In his spare time, he enjoys producing music, exploring the outdoors, and riding motorcycles.

Hillary Sanders  
An Introduction to Machine Learning and Deep Learning  
Ground Truth, 14:00–14:55, Tuesday  

Hillary Sanders is a senior software engineer on the Sophos data science team, which focuses on building and analyzing Sophos’ deep learning models. She is also a co-author of the upcoming book, Malware Data Science.

Michael Rich  
Applied Quantitative Risk Analysis  
Ground Floor, 11:00–11:55, Wednesday  

Mike became hopelessly enthralled with computer and network security towards the end of his 20-year career with the Air Force. Though, truth be told, he was cracking Bulletin Board Systems and stumbling onto Telnet logs on his CoCo 2 & 3 back in the late 80s. After a brief stint as a government contractor he went full commercial and has been enjoying himself greatly. Mike is currently the Director of IT Security, Infrastructure, and Operations at Motion Picture Industries Pension and Health Care Plan. Google it. In his spare time Mike codes, hacks, and exploits white-line tunneling through the Los Angeles traffic firewalls. He spoke at DEFCON 24. At DEFCON 25 he was a member of Gateherder’s DCDarknet winning team, specializing in binary reversing and exploitation. He has also published a couple of times in 2600. His absolute favorite piece of IT paper is his OSCP. You should get yours.

Kris Rides  
What Did We Learn from Today? Recruiter Panel  
Hire Ground, 18:00–18:30, Tuesday  
copresenting with Briana Fernandez and Scott Handley  

Kris is Co-Founder of Tiro Security a Cyber Security Staffing and Professional services company. He has been working in recruitment for over 20 years and is heavily involved in the InfoSec community. When not sitting on panels and advising CISO’s on security recruitment you will find him either snowboarding or scuba diving with sharks.

Rex  
Cruising the MJ Freeway: Examining a large breach in legal Cannabis  
Proving Ground, 18:30–18:55, Tuesday  
copresented by Soldier of FORTRAN  

Long-time web developer, recent security enthusiast. Interested in OSINT, getting pwned in CTF, and casual locksport (emphasis on the casual).

Suzanne Schwartz  
Cyber Safety Disclosure  
I Am The Cavalry, 15:00–15:55, Wednesday  
copresenting with Nina Alli, Jay Radcliffe, and Joshua Corman  

Suzanne B. Schwartz, MD, MBA is the Associate Director for Science and Strategic Partnerships in the Center for Devices and Radiological Health (CDRH) at the FDA. Suzanne’s programmatic efforts in medical device cybersecurity extend beyond incident response to include increasing awareness...
ness, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH) as well as fostering collaborations across other parts of government and the private sector. Suzanne was recently recognized with an award for Excellence in Innovation at FDA’s Women’s History Month on March 1st 2018 for her work in Medical Device Cybersecurity.

**John Seymour**
Disabling Encryption to Access Confidential Data

**Amir Shaked**
Fighting Fraud in the Trenches

**Emily Shawgo**
Decision Analysis Applications in Threat Analysis Frameworks

**Kathleen Smith**
Community Career Panel or How to Get More than a T-Shirt Working at a Con

**Nashe Sheard**
Ask The EFF

**Maty Siman**
Serverless Infections: Malware Just Found a New Home

**Sanjeev Singh**
Attack & Defense in AWS Environments

**Emily has recently graduated from Carnegie Mellon University with a master’s degree in Public Policy and Management with a concentration in Cybersecurity Management. She also has an undergraduate degree in Psychology and Political Science from Carlow University. Emily’s interests lie in penetration testing, threat analysis, and applying the study of human behavior to the field of cybersecurity.**

**Kathleen Smith**
Community Career Panel or How to Get More than a T-Shirt Working at a Con

**Sandeep Singh**
Attack & Defense in AWS Environments

**Ask The EFF**
Underground, 17:00–18:25, Wednesday

**VP R&D @ PerimterX, Developer & Hacker**

**VP R&D @ PerimterX, Developer & Hacker**

**VP R&D @ PerimterX, Developer & Hacker**

**Closing**

**John Stone**
Advanced APT Hunting with Splunk

**Sandeep Singh**
Attack & Defense in AWS Environments

**Emily’s interests lie in penetration testing, threat analysis, and applying the study of human behavior to the field of cybersecurity.**

**Emily Shawgo**
Decision Analysis Applications in Threat Analysis Frameworks

**Kathleen Smith**
Community Career Panel or How to Get More than a T-Shirt Working at a Con

**Nashe Sheard**
Ask The EFF

**VP R&D @ PerimterX, Developer & Hacker**

**VP R&D @ PerimterX, Developer & Hacker**

**VP R&D @ PerimterX, Developer & Hacker**

**VP R&D @ PerimterX, Developer & Hacker**
free time (which, as of this writing, he has a lot of these days), he searches for jobs while blogging about travel hacking and writing columns for The Hacker Quarterly. If you want to hire him, he would make a great product manager or technical program manager.

**Talha Tariq**

**Securing Robots at Scale**

*Breaking Ground, 14:00-14:55, Wednesday*

Talha Tariq is the CISO at Anki, a consumer robotics and AI company where he leads security and privacy engineering efforts. He has 15 years of experience building and scaling security programs from startups to large Fortune 100 organizations. Previously he was CISO for FinancialForce, Director of Security Consulting at PwC, and has held various security engineering and leadership positions at Microsoft and NCR. He has broad security and privacy engineering experience and patents building trusted platforms for cloud and IoT devices. He has also led variety of engagements around the world, advising clients, across a range of industries, on matters related to significant sensitive data breaches, intellectual property thefts, hacking events, forensic investigations, security program development, security operations, threat and vulnerability assessments. Talha holds a BS in Computer Science & MS in Information Security from Royal Holloway, University of London.

**Sara-Jayne Terp**

**Social engineering at scale, for fun**

*Proving Ground, 14:00-14:25, Tuesday*

**mentored by Brittany Postnikoff**

Data scientist at AppNexus (online advertising exchange), sometimes professor at Columbia University; always causing trouble somewhere. Data nerd, specialising in complex business and social problems. Current interest in misinformation mechanisms and counters; current work in large-scale auction systems; background in applied AI, military information systems, autonomous vehicle system design, data strategy, crowdsourcing, crisis data and transport data systems; experience in all sorts of strange areas.

**Joshua Theimer**

**Overlooked tactics for attacking hardened Active Directory environment**

*Breaking Ground, 17:00-17:55, Wednesday*

**co-presenting with Hao Wang and Yothin Rodanant**

Joshua Theimer is a senior manager in Ernst & Young LLP’s Advanced Security Center (ASC) where he evaluates and implements sustainable enterprise information security programs for the Fortune 500. He is currently leading the entire attack and penetration practice of ASC, and having a wide range of client engagements focused on assessing Active Directory security.

**Iain Thomson**

**Engaging the Media: Telling Your Story**

*I Am The Cavalry, 15:00-15:55, Tuesday*

**co-presenting with Steve Ragan, Sean Gallagher, and Iain Thomson**

Iain has spent the last 25 years covering the computing, science and aviation industries, including spells as technical editor of PC Magazine, reviews editor of PC Advisor and is currently news editor with The Register covering security and space issues. He has lived in the Bay Area for the decade and, when not writing, spends his time sailing, reading, and stroking demanding cats.

**Derek Thomas**

**PowerShell Classification: Life, Learning, and Self-Discovery**

*Ground Truth, 11:00-11:55, Wednesday*

**Applied Security Researcher**

**Shusel Tomonaga**

**Tracking Malicious Logon: Visualize and Analyze Active Directory Event Logs**

*Ground Truth, 14:00-14:55, Wednesday*

**co-presenting with Tomoaki Tani**

**Jeff Troy**

**Transforming industries for Fun and Safety (Panel)**

*I Am The Cavalry, 17:00-17:29, Wednesday*

**co-presenting with Pete Cooper**

GE Aviation IT Risk Security Operations Leader. Oversees the Intelligence, Detection, Response and Remediation functions. Implemented the Kill Chain strategic model into the collection, development, analysis and management of strategic and tactical indicators of network intrusion groups. The SecOps team specializes in reverse engineering and in-depth analysis of malware and network intrusion attacks. Our team innovates and builds tools to automate the processing of intelligence from collection, through analysis and finally to deployment to detection/ prevention tools.

**Kathleen “Katie” Trimble**

**CVE CVSS NVD OMGWTFBBQ (Wednesday Edition)**

*I Am The Cavalry, 14:00-14:55, Wednesday*

**co-presenting with Tom Miller, Art Manion, Seth Carmody, and Josh Corman**

Ms. Trimble is the section chief of the Vulnerability Management and Coordination section in the NCCIC. Previous to this position, she served as the Senior Communications Sector analyst in the DHS Office of Cyber and Infra-structure Analysis (OCIA), where she operated as the focal point for efforts related to wired communications between interagency government partners, DHS components, and private industry in response to National Security Council requirements. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism/force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

**Maurice Turner**

**Hacking the Public Policy API**

*I Am The Cavalry, 11:30-12:25, Tuesday*

**co-presenting with Travis Moore and Jessica Wilkerson**

**Engaging Policymakers at the State Level**

*I Am The Cavalry, 18:00-18:55, Tuesday*

**co-presenting with Joe Hall and David Forsey**

Maurice Turner is Senior Technologist at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring the internet remains open, innovative and free. Supporting work across all of CDT’s programmatic areas, Turner focuses on the Election Security and Privacy Project identifying and updating election cybersecurity practices and infrastructure, and working through potential remedies. Nearly a decade of municipal management experience is complemented by numerous private-sector technology positions, fellowships, and internships. As a TechCongress Congressional Innovation Fellow in 2017, he served the Republican staff of the Senate Homeland Security and Governmental Affairs Committee (reporting to Chairman Sen. Ron Johnson) supporting cybersecurity issues.

**Martin Vigo**

**Ransomible, yet another reason to ditch SMS**

*Ground1234!, 18:00-18:55, Wednesday*

Martin Vigo is a Product Security Lead and Researcher responsible for Mobile security Identity and Authentication. He helps design...
secure systems and applications, conducts security reviews, penetration testing and generally helps keep “the cloud” secure. Martin has also been involved in educating developers on security essentials and best practices. Martin has presented several topics including breaking password managers, exploiting Apple’s Facetime to create a spy program and mobile app development best practices. These were given at conferences such as Blackhat EU, EKoparty, Kaspersky Security Analyst Summit and Shakacon.

Paul Wagenseil
Engaging the Media: Know Your Target
I Am The Cavalry, 14:00–14:55, Tuesday
co-presenting with Jen “Cat Herder” Ellis, Joseph Cox, Sean Gallagher, and Steve Ragan

Paul Wagenseil handles security and privacy coverage for Tom’s Guide and Laptop Magazine. He has also been a warehouse manager, a car deliveryman, a bartender, a ditch digger, a fry cook and a dishwasher. He graduated from college with a degree completely unrelated to his present job.

Hao Wang
Overlooked tactics for attacking hardened Active Directory environment
Breaking Ground, 17:00–17:55, Wednesday
co-presenting with Yohin Rodnanit and Joshua Theimer

Hao Wang is a manager in Ernst & Young LLP’s Advanced Security Center (ASC). Hao has more than seven years of Attack & Penetration testing and Cyber Investigation experience. Hao has utilized his experience as a lead tester on a wide array of red team and purple team assessments. Hao serves as a core technical team member for ASC, regularly contributing new hacking techniques to the team. His areas of research include advanced Active Directory attack against Microsoft ESAE, exploit development for both point of sale systems and gaming systems, and cyber threat hunting.

Nate Warfield
All Your Cloud Are Belong To Us - Hunting Compromise In Azure
Common Ground, 10:00–10:55, Wednesday

Nate Warfield is a Senior Security Program Manager for the Microsoft Security Response Center. He spent nearly 20 years designing, building and troubleshooting enterprise & carrier-grade networks for Fortune 500 companies while simultaneously moonlighting as a Grey Hat. He learned BASIC at 8 years old, hacked his first BBS over 2400 baud dialup at 13 and has dabbed with everything from reverse engineering and network exploitation to breaking Magstripe,RFID/NFC and bricking Bluetooth devices. In his current role he manages security reports for vulnerabilities which affect Azure Cloud, Hyper-V and Windows server products. He devotes his spare cycles to hunting hacked virtual machines in Azure, adding functionality to OSINT tools like Shodan and teaching others how to hunt Threats Like A Boss.

Margaret White
The Long Way Around – from Software Engineering to Cyber Security (How Choosing Wrong Turned out to be Right)
Hire Ground, 15:00–15:30, Tuesday

Margaret White is an award-winning Management Professional recognized and promoted for outstanding leadership in operational risk management, technology strategy execution, process improvement and effective cost cutting. She received early practical leadership training in Bank of America’s Global Technology and Operations Foundations for Success Program. A top performer at the Bank of America since 2003, Margaret is a trusted advisor and strategic partner to senior level management. Technical teams relied upon to outline and map long-term proactive risk management strategy for systems and processes. She is uniquely qualified to translate business drivers and needs to a technical audience and technical concepts to bottom-line terminology that clearly demonstrates IT’s value as a partner to the business. She is a proven team leader for 30 high-performance professionals, serving as manager, mentor, and motivator, providing responsible oversight of budgets or project budgets as large as $36M. Margaret is respected as a subject matter expert influencing and encouraging implementation of new technologies and methodologies that improve quality, productivity and efficiency. An experienced IT Project Manager with ‘Lean for Six Sigma’ training and implementation, practiced in the utilization of methodologies including SDLC, Waterfall, Agile and Six Sigma.

Justin Whitehead
Advanced Wireless Attacks Against Enterprise Networks
Training Ground, 8:00–11:55, Wednesday
co-presenting with Gabriel Ryan

Justin Whitehead is an Army infantry veteran with over a decade of service. After retiring from the military, he went on to have a successful 7-year career in computer forensics and incident response. In 2015, he became a penetration tester at One World Labs, working under renowned security researcher Chris Roberts. He now serves as CEO and Co-Founder of Digital Silence, bringing a unique attention to detail and blend of blue and red team experience to the company. When he’s not focused on his role as a security professional, Justin happily pursues his hobby of synchronized figure skating.

Jessica Wilkerson
Hacking the Public Policy API
I Am The Cavalry, 11:30–12:25, Tuesday
co-presenting with Travis Moore and Maurice Turner

A Good Day to Die? IoT End of Life
I Am The Cavalry, 17:00–17:55, Tuesday
co-presenting with Allan Friedman, Karl Grindal, Karim Parhat, and Ishan Mehta

Jessica Wilkerson is a Professional Staff Member with the House Committee on Energy and Commerce, covering cybersecurity issues across the Committee’s broad jurisdiction. As part of that work, she has investigated issues in the telecommunications, commercial, energy, and healthcare sectors. She has a background in mathematics and computer science.

Heath Wickline
Cavalry is ALL OF US
I Am The Cavalry, 18:00–18:55, Wednesday
co-presenting with Joshua Corman, Beau Woods, Rod Soto, and Travis Moore

Victor Wieczorek
You’re Good and You Should Feel Good
Hire Ground, 14:30–15:00, Tuesday

Victor Wieczorek is Practice Lead for Guided-Point’s Threat & Attack Simulation team. He has a broad range of experience in both defensive and offensive security roles. His prior work included delivering various security projects to a wide spectrum of clients with a primary focus on penetration testing, social engineering, and security architecture design. As a penetration tester holding both the Offensive Security Certified Expert (OSCE) and Offensive Security Certified Professional (OSCP) certifications, he has helped organizations identify a multitude of weaknesses with a focus on root cause remediation.
Beau Woods
IATC Kickoff
I Am The Cavalry, 11:30–11:59, Tuesday
co-presenting with Joshua Corman
Transforming Industries for Fun and Safety (Presentation)
I Am The Cavalry, 17:30–17:55, Wednesday
co-presenting with David Rogers
Cavalry is ALL OF US
I Am The Cavalry, 16:00–18:55, Wednesday
co-presenting with Josh Corman, Rod Soto, Travis Moore, Heath Wickline, and Joseph Zadeh

Beau Woods is a leader with the I Am The Cavalry grassroots initiative, a Cyber Safety Innovation Fellow with the Atlantic Council, Entrepreneur in Residence at the US Food and Drug Administration, and Founder/CEO of Stratigos Security. Beau has consulted with Global 100 corporations, the White House, members of Congress, foreign governments, and NGOs on some of the most critical cybersecurity issues of our time. Beau’s focus is on Internet of Things (IoT) technologies where cybersecurity intersects public safety and human life issues, including healthcare, automotive, energy, oil and gas, aviation, transportation, and other sectors.

Magen Wu
Vulnerability Management 101: Practical Experience and Recommendations
Proving Ground, 18:00–18:30, Tuesday
mentor to Eric Bryan
Community Career Panel or How to Get More than a T-Shirt Working at a Con
Hire Ground, 14:30–15:00, Wednesday
co-presenting with Cindy Jones, Kristen Renner, and Kathleen Smith

John Wunder
ATT&CKing the Status Quo: Improving Threat Intel and Cyber Defense with MITRE ATT&CK
Breaking Ground, 11:30–12:25, Tuesday
copresenting with Katie Nickels

John is a principal cybersecurity engineer at MITRE working on cyber threat intelligence and how to detect attacks using cybersecurity analytics. He supports MITRE’s work on ATT&CK, and is a co-chair of the STIX Subcommittee in the OASIS Cyber Threat Intelligence Technical Committee. He believes that cyber threat intelligence can improve security for everyone, and works across MITRE’s sponsors to make it easier, faster, and more effective. Besides all this cyber stuff, John likes to record music, try and fail to convince his dog to actually chase a ball, and go camping.

Michael Wylie
Deep Dive into NMAP & Network Scanning
Training Ground, 14:00–17:55, Tuesday
Your taxes are being leaked
Breaking Ground, 10:00–10:55, Wednesday

Michael Wylie, MBA, CISSP is the co-founder of Corporate Blue, an Information Systems and Security consulting firm that serves clients in their pursuit of mitigating cyber threats. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, risk management, and training. Michael has developed and taught numerous courses for the Department of Defense, Moorpark College, and clients around the country. Michael holds credentials from certifying bodies such as ISC2, Cisco, VMware, Dell, EC-Council, CompTIA, and more.

Erez Yalon
(De)Serial Killers
Ground Floor, 10:00–10:55, Wednesday
co-presenting with Omri Misgav

Erez Yalon has more than 15 years of experience in cyber-security with a proven track record in leading cutting edge cyber-security R&D projects. Prior to enSilo, Erez spearheaded the direction of the cyber-security unit at the National Electronic Warfare Research & Simulation Center of Rafael Advanced Defense System and served as its CTO. Additionally, he developed and led Rafael’s cyber training programs. Erez’s achievements at Rafael have been recognized, winning him excellence and innovation awards on complex security projects. Prior to Rafael, Erez served as a system architect at the IDF. He holds a BA in Computer Science from the Open University. Erez is also the first Cyber Security R&D team.

Joseph Zadeh
Cavalry is ALL OF US
I Am The Cavalry, 18:00–18:55, Wednesday
co-presenting with Beau Woods, Josh Corman, Rod Soto, Travis Moore, and Heath Wickline

Joseph Zadeh studied mathematics in college and received a BS from University California, Riverside and an MS and PhD from Purdue University. While in college, he worked in a Network Operation Center focused on security and network performance baselines and during that time he spoke at DEFCON and Torcon security conferences. Most recently he joined JASK.AI as Chief Data Scientist. Previously, Joseph was part of Splunk UBA and the data science consulting team at Greenplum/ Pivotal helping focused on Cyber Security analytics and also part of Kaiser Permanentes first Cyber Security R&D team.

Tamir Zahavi-Brunner
Treble or Trouble: Where Android’s latest security enhancements help, and where they fail
Proving Ground, 18:30–18:55, Wednesday
mentored by Sneha Rajguru

Tamir Zahavi-Brunner (@tamir_zb) is a mobile security researcher at Zimperium. Tamir’s main interests are reverse engineering and vulnerability research. Tamir’s current focus is Android security research. Previously, Tamir dealt with researching and reversing Linux and proprietary embedded systems.
BSidesLV is a do-ocracy, a year-round, part-time project, and a labor of love for everyone listed here, in service of this community. Without our Senior Staff, this little learning shindig of ours would be a beautiful mess. Because of their hard work and dedication, it’s simply beautiful. We couldn’t do this without them, and they all deserve a heartfelt THANK YOU for making BSides Las Vegas what it is. Please make sure you let them know what you’ve gotten out of BSidesLV because of them. While they hear it internally (we hope often enough), external kudos go a long way to let them know that you appreciate what we’ve created here and that their hard work isn’t going unnoticed.

Board of Directors
Genevieve Southwick, President, CEO (@banasidhe)
Jack Daniel, Treasurer, CFO (@jack_daniel)
Justin Tiebs, Secretary (@JMP_EBP)
Ally Miller, General Director (@selenakyle)
Iftach Ian Amit, General Director (@liamit)
Dave Lewis, General Director (@gattaca)
Jessica Archer, General Director (@j3ssa)
As much as the Senior Staff work year-round to ensure planning and logistics comes off without a hitch, the volunteer teams listed here are the heart and soul of the conference. Each and every one of them are integral to operations and ensuring that the tracks and events run smoothly during the event. We couldn’t do this without them either and we’re grateful that they have chosen to become part of the BSidesLV family.

**General & SafetyOps Volunteers**

- aabywan
- Zee
- DN7
- kamenrunnaa
- Masha
- MrBill
- Ryan B
- Will Baggett
- xy22y
- Sagar Belure
- Carfl
- 3ncr1pt3d (Cheryl)
- BridgetteB
- Lauren
- chaocipher
- zeuz2you
- mystech7
- The S0vvy_Geek
- gi0cann
- Brian
- Fellype
- Rusty Shackleford
- Rebecca
- BScout
- Lucas Cioffi
- Bill C
- Lauren
- chaocipher
- zeuz2you
- mystech7
- The S0vvy_Geek
- gi0cann
- Brian
- Fellype
- Rusty Shackleford
- Rebecca
- BScout
- Lucas Cioffi
- Bill C
- Zonii
- Joe C
- Sara
- Ari
- elastic ninja
- Banshee
- Amy
- Loy
- Mario Dean
- Joe
- s3q
- hashtagcyber
- Christy
- Jenny
- DigiWarfare
- Craig M
- Lisa Mckee
- Cléo
- j3len4
- Will
- epicarmi
- jdmurray
- Vahnu
- Failible
- Priyank N
- Running Tree
- Michael P
- Jason
- Alan
- imp0ster
- jayprez
- Syntax
- Vivienne P
- Darsh
- JohnRE
- Kirsten Benner
- n3bb13
- Levi
- Mikesf0et
- Kris Rides
- Gary Rimar
- Christopher Roberts
- liza
- BrianCanFixIT
- Harshit
- tmanapat

*itwaslikethiswhenifoundit / ifoundditthisway
Ryan Flint
flummer
Aleks Freitas
Yuki
Jason Gaudard
Hook
Dan G
iDigitalFlame
Bill H
Evader / ajithatti
Jennifer Havermann, Hire Ground
secitup
Webbreacher
r4t1x
Ayan
Agent_Jacob
voteblake
liath
Maya
surfersdve
David K
gizmom0nk
@zulu_caPWN
Steven K
webjedi
kr1msn
Jonathan
Mandy
tehExodus
Harshit
tmanapat

A Personal Note from the Volunteer Coordinator: These Volunteers not only help with something I am very passionate about, they manage to put a smile on my face each and every day. I couldn’t do it without them. Thank You Everyone!!!!
Thanks for joining us for our 9th annual BSidesLV. We hope to see you again next year. And speaking of next year, here are a few dates of note:

The 2019 Sponsor Prospectus will be released on September 28, 2018.

Donor Drive will open on April 1, 2019 and run until it’s sold out—No Foolin’!

Proving Ground Call for Mentors will open on February 1, 2019 and close on March 1, 2019.

Proving Ground Call for Papers will open on February 1, 2019 and close on April 1, 2019.

Proving Ground Mentor/Mentee matches delivered on April 14, 2019.

Acceptance and rejection letters for General CFP go out on June 20, 2019.

BSides Las Vegas 2019 will be held August 6–7, 2019.

The General Call for Papers will open on April 1, 2019 and close on May 15, 2019.

All this information and more will be updated at bsideslv.org.

Join our low-volume mailing list: bsideslv.org/contact-us

Follow us on Twitter @bsideslv

Because of our sponsors, BSides Las Vegas is able to provide a vendor-neutral, free as in beer, free as in speech event year after year.

Please take a minute to thank them for their support. You can find them at the sponsor tables in the Chill-Out Room, in Hire Ground, and throughout the conference with Gold badges. Or give them a shout-out on social with #BSidesLV #Sponsors.
We regret to inform you that **DEF CON has been cancelled**. Thank you for attending BSides Las Vegas.