DEFCON 30 Voting Village Speaker Schedule 2022

Twitch: https://www.twitch.tv/votingvillagedc
YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Day/Date: Friday 08/12/22
Time: 10:00am
Speaker: **Brigadier General Teri (Terin) D. Williams,**
Vice Director of Operations (Cyber), National Guard Bureau
Talk: *Election Cyber Security in the National Guard*

Date/Date: Friday 08/12/22
Time: 11:00am
Talk: Welcome by Election Integrity Foundation Board
Speaker: **Matt Blaze, Harri Hursti, Philip Stark, David Jefferson, Jody Westby, Catherine Tayrien**
Talk: Introducing EIF board

Date/Date: Friday 08/12/22
Time: 12:00am
Talk: The State of Election Security Training
Speaker: **Jerome Lovato, Consultant**
Talk: The State of Election Security Training

Day/Date: Friday 08/12/22
Time: 1:00pm
Speaker: **Nicole Tisdale, Director of The White House National Security Council (2021-2022) - Director of The U.S. Committee on Homeland Security (2009-2019)**
Talk: Truly Maligned - How Disinformation Targets Minority Communities to Create Voter Suppression

Synopsis: Eliminating early voting days, denying mail-in ballots, complicating voter ID laws, closing polling places, and removing voters from voting rolls. All of these are examples of voter suppression, but a less discussed element of the same tactic is *voter depression*. Voter depression negatively affects how we feel, the way we think, and how we act when it comes to voting or participating in democracy. Disinformation fuels voter depression and targets minority communities.

This discussion will focus on how political disinformation in the U.S. has been collected and disseminated in cyberspace by foreign and domestic actors via technology & social media platforms to depress voting and civic participation. We will focus specifically on how election disinformation targets minority communities, especially Black communities, by leveraging the unaddressed issues and grievances of racism and inequality. We will also share how the cyber community can help defend and empower minority communities to fight disinformation.

Day/Date: Friday 08/12/22
Time: 2:00pm
Panel: Information Operations
Will Not Be Streamed
Panelists To Be Announced

Synopsis: Discussion about how information operations have changed from 2015 to today and what we can predict about the future. Additionally, the panel will cover how war was once fought on land, then progressed to sea, then underwater and air, followed by space and cyber. We have to realize that information space warfare is the new domain of war.

Day/Date: Friday 08/12/22
Time: 4:00pm
Speaker: Speaker: **Patrik Neu, Ory Systems GmbH**
Talk: Open Source Zero Trust Security using Ory Keto

Synopsis: Local laws around voting vary widely. Building secure authorization that implements all of them is challenging. Future voting systems built on tested open source components will reduce the attack surface and improve trust in the system. In this session, we will first examine various authorization challenges that arise in voting

contexts. As a possible solution, we will discuss the usage of a highly flexible open source authorization system based on Ory's open source efforts to implement Google Zanzibar, and how an implementation within a voting system would work.

Day/Date: Saturday 08/13/22
Time: 10:00am
Speaker: **Assistant Professor Drew Springall, Auburn University**
Talk: Dominion ImageCast X CVEs and reflections on CVD for election systems

Synopsis: In February of this year, we worked with CISA to conduct the first Coordinated Vulnerability Disclosure (CVD) related to an active, widely-used voting system (the Dominion Democracy Suite 5.5-A system) in order to disclose multiple vulnerabilities found through analysis and testing of the system as used in the state of Georgia (ICSA-22-151-01). Though initiated prior to and not focused on the November 2020 election, our research and efforts to disclose occurred in its shadow and with the November 2022 election on the horizon. Along with the urgency, overlapping primary elections ensured that the importance of "getting it right" was not lost but along the way, we discovered that "right" meant very different things to the various stakeholders. In this talk, we'll share our experiences and lessons-learned from this journey, discuss how the advisory-sausage is actually made, and offer our analysis and opinions on the use of the standard CVD process for voting system vulnerabilities going-forward.

Date/Date: Saturday 08/13/22
Time: 11:00am
Speaker: **Ivo de Carvalho Peixinho, Cybercrime Researcher and Forensic Expert**
Talk: Three Time's a Charm: Our Experience at the Public Hacking Trials of the Brazilian Election Systems

---

Day/Date; Saturday 08/13/22
Time: 12:00pm
Speaker: **Michael Moore, Information Security Officer for the Maricopa County Recorder's Office & Nate Young, Director of IT for the Maricopa County Recorder's Office**
Talk: United We Stand

Synopsis: Election security is largely not cybersecurity – we'll review some of the checks and balances in place: Logic and Accuracy testing, Post-Election statistically significant hand count, air gapped Election Management Systems (EMS). We'll also review improvements we've worked towards including physical security hardening, threat intelligence sharing, incorporating least privilege methodologies, advocating for security improvements from the Election Assistance Commission (EAC) as well as our EMS vendors, and being the originators of the EMS Gateway CIS (Center for Internet Security) benchmark. Lastly, we'll inform the audience on how they can do their part - fight Mobile Device Management (MDM), demand intellectual integrity from themselves and those around them, normalize requesting citations, volunteer to work for elections and speak up if something seems wrong!

Day/Date: Saturday 08/13/22
Time: 2:00pm
Panel: Election Forensics
Will Not Be Streamed
Panelists To Be Announced

Day/Date: Saturday 08/13/22
Time: 4:00pm
Speaker: **Will Baggett, CCEE, CFE**
Talk: Digital Forensics and Voting Machines

Synopsis: This talk is new to the information security community. The purpose is to outline the process we use at the Voting Village to analyze machines in a professional, neutral manner with the goal of improving voting security and integrity. While in Las Vegas for data recovery and E-discovery work for a client, I attended DefCon 2017. By happenstance I visited the Voting Village, organized by Harri Hursti.

Dozens of machines were on display for DefCon participants to 'hack' and find vulnerabilities. As I had my digital forensic toolkit with me, I asked Harri if the Windows CE and Windows XP devices had been professionally imaged and analyzed. Within minutes, I was presented with a pristine Windows CE machine. I imaged the device with BlackBag's MacQuisition and began triage analysis with BlackBag's BlackLight system.

The system was used for local, state, and national elections, initially purchased by Fairfax County, Virginia and placed into service, October 2002. The machine was last used in November 2014. I met with Harri at DefCon 2018 and performed the same tasks for thirty seven additional voting machines. The systematic lack of security was found on every single device nationwide. The same pattern was repeated at DefCon 2019.

I will discuss the professional methods we use to image devices at the Voting Village prior to the general public accessing the machines and the two-person finding verification method in use as well as the best practice of multiple tools. (Imaged with write-blocking hardware, analyzed with BlackLight and Autopsy, with a deleted file recovery tool afterwards.) I will discuss the findings we have discovered in the voting village: The operating system had not been updated since purchase. Votes were compiled into cleartext (votes.txt) onto a removable media drive and in some instances, uploaded to a FTP server, unencrypted. Hundreds of USB drives had been inserted into the machines since deployment. Voters access the machines as ‘administrator’ with all votes being cast on the admin account. Admin and security usernames and passwords are found online due to the relevant state sunshine laws.

I will present our findings as to what was absent from the machines: No firewall or antivirus programs are present. No audit trail for USB drives or voting record integrity was found. No voter information was found. No evidence of tampering has been found.