August 4, 2022

Media Alert: Intel at Black Hat, Diana Initiative

Intel experts present briefings, theatre sessions and more at Black Hat USA 2022 and The Diana Initiative 2022.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Join Intel experts on-site at Intel's booth and for presented sessions at this year's Black Hat USA 2022 and The Diana Initiative 2022, taking place in Las Vegas and virtually starting August 6.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20220804005134/en/

Join Intel experts on-site at Intel's booth and for presented sessions at this year's Black Hat USA 2022, taking place in Las Vegas and virtually starting August 6. (Credit: Intel Corporation)

Intel will host an exhibition at Black Hat in the Business Hall at the Mandalay Bay Convention Center, booth #1460. Intel's booth on the show floor will feature some of Intel's security innovations, plus live demos, real-world use cases and theatre sessions on Intel's Project Circuit Breaker, research from Intel Labs on security and privacy, confidential computing with Intel® Software Guard Extensions (Intel® SGX), Intel® Threat Detection Technology (Intel® TDT) on the Intel vPro® platform powered by 12th Gen Intel® Core™ and more. Anjuna, Eclypsium, Fortanix, Grip Security and JupiterOne will also participate in theatre sessions on-site.

For a full look at Intel's theatre session schedule at booth #1460, see below (all times PDT; schedule subject to change).

Project Circuit Breaker: A Community of Elite Hackers *Presented by Intel*	Wed., Aug. 10 | 10:15 – 10:30 a.m.
Security First Culture: Security is a Mindset, Not Just a Feature *Presented by Intel*	Wed., Aug. 10 | 10:45 – 11 a.m. Thu., Aug. 11 | 1:45 – 2 p.m.
Firmware Security: Detecting Vulnerabilities Below the OS *Presented by Intel and Eclypsium*	Wed., Aug. 10 | 11:15 – 11:30 a.m. Wed., Aug. 10 | 4:45 – 5 p.m. Thu., Aug. 11 | 2:15 – 2:30 p.m.
Introduction to Hardware-based Threat Detection *Presented by Intel*	Wed., Aug. 10 | 11:45 a.m. – noon Wed., Aug. 10 | 3:45 – 4 p.m. Thu., Aug. 11 | 2:45 – 3 p.m.

Lists vs. Graphs: Looking Beneath the Attack Surface *Presented by Intel and JupiterOne*	Wed., Aug. 10 | 1:15 – 1:30 p.m. Wed., Aug. 10 | 5:15 – 5:30 p.m.
Fortanix Confidential AI & Intel SGX: Accelerating the Use of AI/ML *Presented by Intel and Fortanix*	Wed., Aug. 10 | 1:45 – 2 p.m. Thu., Aug. 11 | 10:15 – 10:30 a.m. Thu., Aug. 11 | 3:15 – 4 p.m.
Accelerating Adherence to Industry Security Standards *Presented by Intel*	Wed., Aug. 10 | 2:45 – 3 p.m. Thu., Aug. 11 | 10:45 – 11 a.m.
Confidential Computing 101 *Presented by Intel and Anjuna*	Wed., Aug. 10 | 2:15 – 2:30 p.m. Thu., Aug. 11 | 11:15 – 11:30 a.m.
SaaS Security Control Plane Leveraging NLP-Based Discovery *Presented by Intel and Grip Security*	Wed., Aug. 10 | 3:15 – 3:30 p.m. Thu., Aug. 11 | 11:45 a.m. – noon

At The Diana Initiative 2022, a diversity-driven conference committed to helping all underrepresented people in information security, Intel will present a talk on fuzzing and Miki Demeter, security researcher at Intel, will close the conference as the final keynote speaker. The keynote is focused on how to take the initiative in one's career journey and is scheduled to start at 4:30 p.m. PDT, Thursday, Aug. 11.

Find out why security begins at the hardware level and how Intel's innovative technologies and research are moving the industry forward.

Black Hat USA 2022

When: Aug. 6-11

Where: Mandalay Bay Convention Center, Las Vegas, and virtual

Intel Talks at Black Hat USA 2022:

Project Circuit Breaker, A Community of Elite Hackers
Presented by Katie Trimble-Noble, director of Product Security and Bug Bounty at Intel. Project Circuit Breaker is a community of elite hackers – fixers and breakers – who hunt bugs in firmware, hypervisors, GPUs, compromising chipsets, pwning processors and other equipment. Missions include live hacking events on the latest Intel products, and even some pre-release opportunities, immersive training, and capture the flag events. Game Masters, Intel engineers, work closely with participants, and the community is encouraged to learn from each other. This isn't your usual Bug Bounty program. Challenges focus on some of the biggest hurdles, and bounties are multiplied.

When: 8-8:15 a.m. PDT, Wednesday, Aug. 10
Where: Virtual and on-demand session
Registration: https://www.blackhat.com/us-22/registration.html

Fault-Injection Detection Circuits: Design, Calibration, Validation and Tuning
This session, presented by Daniel Nemiroff, senior principal Engineer at Intel and Carlos Tokunaga, principal engineer at Intel Labs, covers the tunable replica circuit (TRC), a fault-injection detection circuit that has been integrated into Intel® Converged Security and Management Engine (Intel® CSME) in the recent 12th Gen Intel Core processor. This is Intel's first foray into active fault-injection attack detection in high-volume products like CPUs and chipsets.

Since a timing failure is the primary goal of fault-injection attacks and has been shown as the vehicle to cause unsigned code to run on other security engines, using the TRC to explicitly detect timing failures is Intel's current approach to fault-injection detection in client security engines. Unlike traditional analog voltage and clock monitors, the TRC detects timing failures that result from voltage, clock, temperature and other glitch attacks, like electromagnetic radiation. This session will introduce the TRC technology, how the TRC was integrated into Intel CSME, the process for calibrating the TRC in high volume manufacturing (HVM), as well as the false-positive and fault-injection testing that occurred in our physical attack labs.

When: 3:20-4 p.m. PDT, Wednesday, Aug. 10
Where: Islander FG (Level 1)
Registration: https://www.blackhat.com/us-22/registration.html

The Diana Initiative 2022

When: Aug. 10-11

Where: The Westin Las Vegas Hotel & Spa, Las Vegas

Intel Talk at The Diana Initiative 2022:

Fuzzing: A Must Have in Your Bug-Hunting Arsenal
Fuzz testing, aka fuzzing, is a dynamic software testing mechanism designed to detect a wide spectrum of bugs and potential security vulnerabilities from memory corruption to deadlocks, from undefined behavior to exception handling. In combination with appropriate program instrumentation, fuzzing has proven its effectiveness to software developers, security validators as well as security researchers. Although fuzzing can greatly assist in bug finding, it has its own sets of challenges, such as coverage wall and effective input generation. This talk, presented by Priyam Biswas, offensive security researcher at Intel, will explore the common roadblocks in fuzzing and some of the best practices to overcome these challenges as well as how to best utilize the potential of fuzzing to find bugs and security. In addition, this talk will highlight how fuzzing can be adopted in the firmware domain despite the tight coupling with the target hardware platform.

When: 8:30-9:30 a.m. PDT, Thursday, Aug. 11
Where: The Westin Las Vegas Hotel & Spa, Las Vegas
Registration: https://www.eventbrite.com/e/the-diana-initiative-2022-tickets-84434470775

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore’s Law, we continuously work to

advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

© Intel Corporation. Intel, the Intel logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220804005134/en/

Jennifer Foss
1-425-765-3485
jennifer.foss@intel.com

Source: Intel Corporation