hardwear.io
Hardware Security Conference and Training

Press Release

Security experts to reveal global security trends and priorities at Hardwear.io USA event

Hardwear.io announces the 3rd Hardware Security Training & Conference to be held online, 5-10th July 2021 featuring Keynote Speakers from the Korea Advanced Institute of Science and Technology and Dalhousie University of Canada.

Conference is endorsed by Google, NCC Group, NVIDIA, Synacktiv and NXP.

USA – June 23rd 2021: Hardwear.io, USA's virtual platform for hardware research and innovation, welcomes hundreds of hardware security experts and academia to its 6-day event, July 5-10, 2021. Keynote Speakers will share the latest security research and attack threats to help the hardware and security community to defend their products. More speakers from NCC Group, Google's OpenTitan project, Riscure and more will share practical insight and tools to the hardware security community.

Antriksh Shah, founder of Hardwear.io, says, "Many vendors do not always treat hardware security as a priority because of the time and effort involved. That is why platforms and virtual conferences such as Hardwear.io are useful to help InfoSec professionals learn about the latest research and tools they need to protect their IoT devices."

Day one's Keynote Speaker is professor Yongdae Kim from Korea Advanced Institute of Science and Technology who will test the security of modems and networks and share the future direction for automatic testing. Professor Kim is a pioneer in telecom security, having more than 20 years of experience in security issues related to 2G, 3G, 4G and 5G, while spending significant time working with various chip manufacturers on baseband.

Hardwear.io's Keynote Speaker of day two is Colin O'Flynn, assistant professor at Dalhousie University of Canada, who will highlight major hardware attacks and share thoughts on the future of hardware security and increasing accessibility throughout the industry. He is the inventor of ChipWhisperer, a complete, open-source toolchain for side-channel, power analysis and glitching attacks.

Conference Talks:

- *Dr. Jiska Classen, Postdoc at TU Darmstadt: Interacting with *OS hardware from user space* - repurposing daemons to access chips and wireless protocols while keeping most of their functionality intact in Apple products;

- *Joshua Beaker, Security Analyst at Riscure: Proving the efficacy of software countermeasures for fault injection* - providing applicable defensive knowledge of preventing a large amount of fault injection attacks with only software;

- *Chris Frantz, Site Reliability Engineer at Google OpenTitan project: Secure Builds for Secure Software* - revealing exclusive technical details about Google OpenTitan, a project used by millions around the globe;

- *Ta-Lun Yen, Threat Researcher at Trend Micro: Enabling dynamic analysis of Legacy Embedded Systems in full emulated environment* - stressing the significance of emulation tools by showing how their emulation methods allows to transplant any given kernel-mode binaries into our controlled environment;

- *Mathieu Stephan, Electronics Engineer: The Mooltipass Open Source Hardware Authentication Ecosystem* - presenting Mooltipass, an entirely open-source framework providing hardware-based authentication solutions;

- *Eric Evenchick, Technical Director at NCC Group: Building CANtact Pro: An Open Source CAN Bus Tool - exposing a new tool used for automotive reverse engineering which operates by dissecting the CAN protocol, injecting malicious code thus surrendering control over automotive systems to the hacker;*

- *Andrew Zonenberg, Associate Principal Security Consultant at IOActive: Boost your hardware reversing with glscopeclient* - introducing glscopeclient, a tool for controlling instruments and analyzing streaming waveforms at speeds in excess of 2 Gbps, using GPU acceleration when available;

- *John McMaster: talk to be announced soon*

Training sessions:

- Protecting the CAN bus by Ken Tindell, CTO of Canis Automotive Labs
- Assessing and Exploiting PLCs by Justin Searle, Director of ICS Security at InGuardians,
- IC Reverse Engineering & Code Dump by Olivier Thomas, CTO of Texplained
- Reverse Engineering Firmware with Ghidra by Eric Evenchick, Technical Director at NCC Group
- BootPwn: Breaking Secure Boot by Experience by Niek Timmers & Cristofaro Mune, Founders of Raelize
- EMFI and Voltage Fault injection attacks with Raiden by Grzegorz Wypych, Security Researcher at IBM XForce & Adam Laurie, Partner at IBM XForce

- Optimizing Crypto on Embedded Microcontrollers by Peter Schwabe, Research Group Leader at Radboud University & Matthias Kannwischer, PhD Student at Radboud University

Antriksh added, “If there is a vulnerability on the software side, it can be easily patched, but if there is a vulnerability on the hardware side, it can mean the hardware manufacturer may have to rebuild everything from scratch**.** The research projects presented at Hardwear.io USA will be used by people who build and secure new silicon products. Members of the audience will become aware of such vulnerabilities, and they will be more sensitive to preventing and fixing them in future products. Moreover, such research also helps companies identify counterfeit products available in the market. This is especially important, as the COVID-19 pandemic has disrupted the balance between supply and demand and counterfeit chips are spreading due to the global semiconductor shortage.”

Hardwear.io USA will be held **virtually** for the second time. Over 1500 hardware security experts from the industry and academia participated in first-ever virtual Hardwear.io USA conference in 2020. The event kicks off with 7 training sessions for 4 days from 5th July 2021, while the Conference will happen between the 9th–10th of July.

Attendees at Hardwear.io will have the opportunity to network and find solutions to address business needs. In addition to the training sessions and conference talks, Hardwear.io has come up with extracurricular activities highly beneficial as they provide its audience useful soft and hard skills through fun and entertaining activities:

- Fix-Up, a unique networking event for the attendees to network and find their next hardware research collaboration or business partner.
- Hospital Under Siege CTF (8th July), a scenario-driven Capture the Flag contest, where participants compete on both real and simulated medical devices. Challenges will draw from expert areas including forensics, RF hacking, network exploitation techniques, web security, protocol reverse engineering, hardware hacking, and others.
- Capture the Signal CTF (9-10th July), a new challenge-based CTF contest that focuses exclusively on the reverse engineering of radio signals. Participants will have to examine a series of increasingly complex radio signals to extract key information leading them to the final exit signal.
- Wall Puzzle Contest (9-10th July), a cryptographic challenge where puzzles are posted at random times during the conference. Participants must check all the sessions to solve all the challenges with knowledge of cryptography, physics, chemistry, electronics, computers, mathematics, history, and vexillogy.

To see the full agenda of the event, please go to the Hardwear.io website online.

Organizer	Hardwear.io USA 2021
Event Summary	3rd Edition Hardware Security Training & Conference
Venue	Online, Zoom & Discord
Date of Training	July 5th to 8th 2021
Date of Conference	July 9th to 10th 2021
URL:	https://hardwear.io/usa-2021/

About Hardwear.io

Hardwear.io was founded in 2015 by Antriksh Shah with the aim to provide the Hardware & Security community with a platform to discuss & solve issues pertaining to hardware security. It hosts events in the USA and Netherlands as well as webinars and training sessions. The objective of the hardwear.io conference revolves around key concerns in hardware, firmware, & related protocols. More information is available at the Hardwear.io website, www.hardwear.io. Follow Hardwear.io on Twitter and on LinkedIn. The organization offers several resources for hardware security professionals on its YouTube Channel.

About Hardwear.io Security Trainings & Conference

Hardwear.io Security Trainings & Conference is a platform dedicated for the hardware security community where researchers showcase and discuss their innovative research on attacking and defending hardware. Present in The Netherlands, Germany, and the US, Hardwear.io provides advanced, hands-on trainings designed for hardware security professionals from industry, academia and government alike.

Media Contact

For further details regarding media participation, please contact Antriksh Shah by emailing antriksh@payatu.com.

All the announcements regarding the event will be posted on Hardwear.io social media channels. Twitter: @hardwear_io, Facebook: hardwear.io, LinkedIn: @hardwear.io