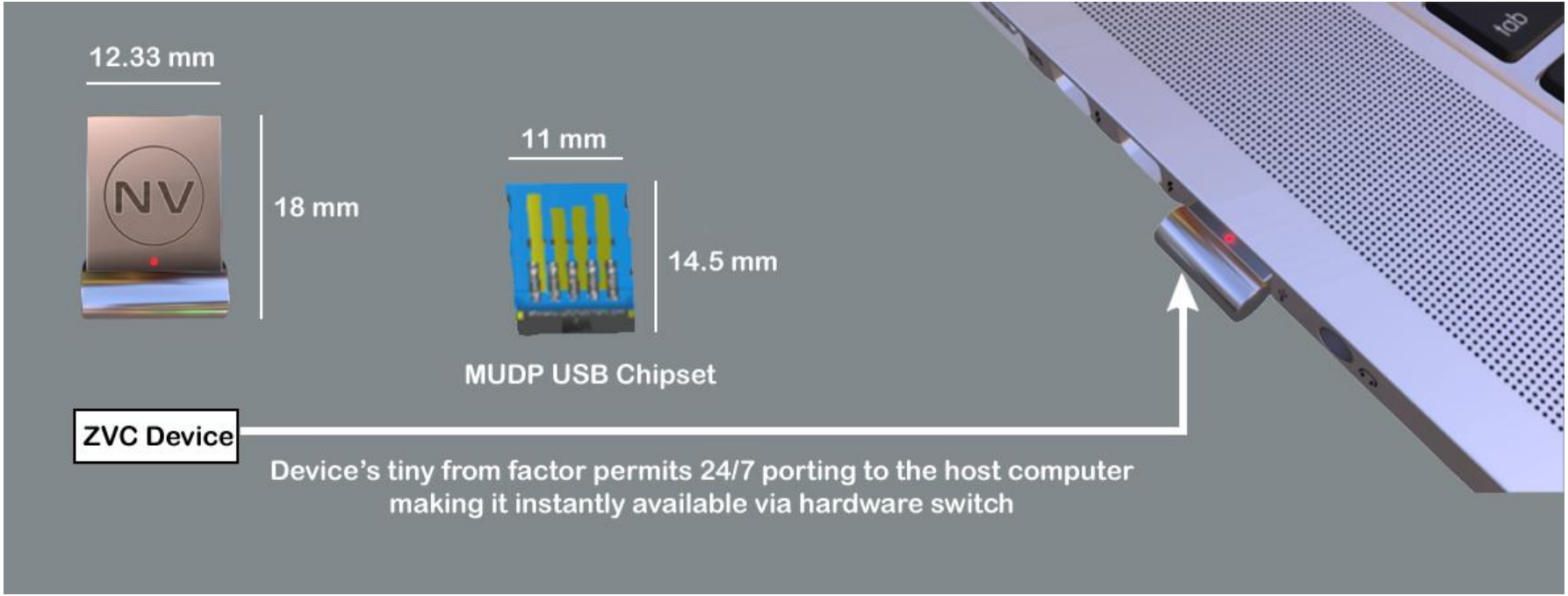
Review Open Call: Stage 1
ZVC: Zero Vulnerability Computing

Blockchain 5.0 OÜ

Virtual Wall (imec)

FEC10

Jan 27, 2022



ZERO VULNERABILITY COMPUTING (ZVC) PARADIGM FOR COMBATING COMPUTER VULNERABILITIES

What is ZVC?

- Cybercrime is a €5.56 trillion industry and hack attacks happen every 39th seconds.
- These hack attacks fall under two major categories:

1. **Vulnerability-related computer hacks** take advantage of the attack surface inherently present in all computers that malwares exploit;
2. **PII (Personally Identifiable Info)-related hacks** that result from ID/credentials/PII theft, e.g., brute-force, dictionary-attacks, etc.

- Zero Vulnerability Computing (**ZVC**) concept focuses on zeroing computer vulnerabilities by completely obliterating the attack surface that's inherent in legacy systems with 2 novel approaches;

1. **Firstly**, preventing any direct installation or execution of 3rd party app (SOS), and,
2. **Secondly** integrating an instantly switchable offline data storage within an online host computer itself. (ICOS).

- The current proposal represented a fairly restricted, simplistic & narrow implementation of the radical ZVC concept.
- The experiment aimed at transforming a USB-mountable hardware device into a novel vehicle for securing the cryptocurrency transactions as well as PII data from hack attacks

Objectives of the Experiment

While our long-term vision is to get rid of all the computers of vulnerabilities, this proposal addressed our short-term goal to build a minimalist prototype using USB that validates ZVC technology, and at the same time builds a product that has multi-billion market - Hardware Wallets.

Objectives:

1. Designing and Prototyping a ZVC device based on a MUDP 3.0 chipset with a tiny form factor
2. Building a cryptocurrency wallet application that supports crypto transaction as a hardware wallet
3. Provide a switchable In-Computer Offline Storage so that sensitive user data remains offline while the ZVC device remains mounted on the computer.
4. Testing the ZVC by switching ON the ZVC device to execute a cryptocurrency transaction and making the mock malware application that launches an attack on the ZVC device by attempting to contemporaneously execute a malware code on the ZVC device
5. Validating the unhackability of the ZVC device by demonstrating that the mock malware script that successfully infects a normal computer hardware but fails to infect (execute or write any data to) the ZVC hardware wallet device

Background & Motivation for the Experiment

- Blockchain 5.0 Ltd is an Estonian SME actively involved in developing innovative technologies that are beyond state of the art. The company has participated in several Horizon projects in the past 2 years.
- In one of our recent Horizon 2020 proposals, ZEROV we proposed a radical cybersecurity technique to circumvent computer OS related vulnerabilities by completely obliterating the attack surface, using a specially designed Supra OS (SOS) software.
- While the full scale ZEROV development involves highly intricate and challenging Supra OS (SOS) software, we discovered that a minimalist SOS script is easier to implement and potentially transforms a USB-mountable hardware device into a novel vehicle for securing the transactions as well as PII data from hack attacks.
- The end product was highly relevant and valuable to one of our consortium partners, in bringing a new level of security to their customers' cryptocurrency transactions as a hardware wallet.
- In pursuit of our mutual interests, we presented this proposal for testing and validating a prototype of the world's first ZVC-powered, always connected, instantly accessible cryptocurrency hardware wallet integrated within an online computer.

Experiment Set Up: Overview

- Building a tiny minimalist ZVC Proof of Concept (PoC) hardware device compatible with the Linux OS using USB MUDP 3.0 chipset.

- Remotely accessing at least 2 virtual wall testbed nodes (PC Gen6 Linux computers) with JFed tool and get access to their UI using XRDP, we designated these nodes as Node0 (Target Node) and Node1 (Hacker Node).

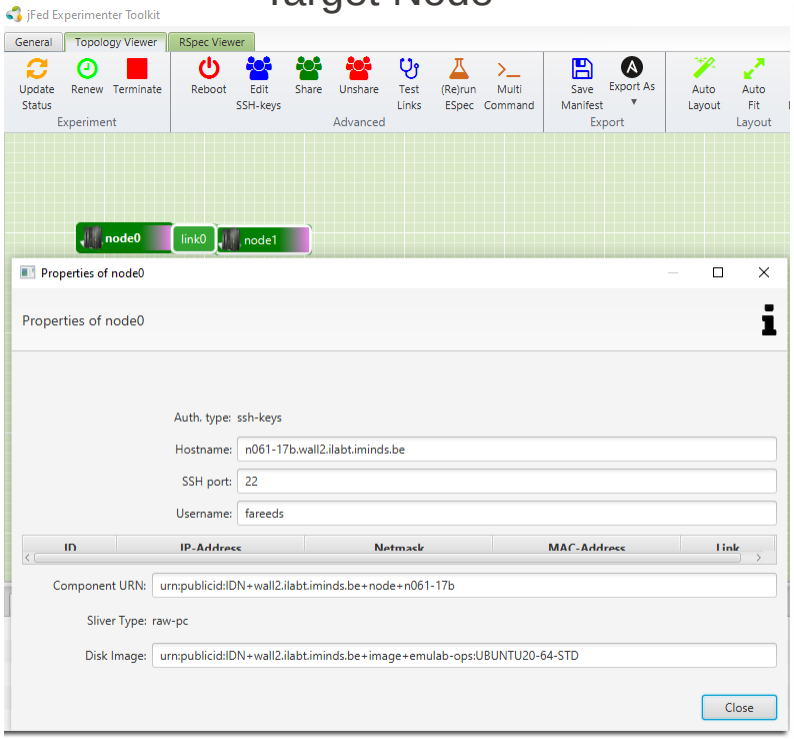
- Mounting ZVC hardware device (with SOS & ICOS software) in the first USB port of Node0 or target node. Contemporaneously mount a similar hardware wallet without ZVC program on the target node's second USB port. This serves as a control device.

- Installing a mock malware software on Node1 (hacker node) designed to detect, infect and steal data from any device mounted on a USB port of another computer Node0 (target node) by executing malware script on the USB-mounted target device of target node.

- Execute the mock malware application on the hacker node, which identifies the target node and infects any hardware device mounted on the target node's USB ports and simultaneously run the inbuilt wallet applications on the ZVC device and the Control device mounted on the target node and check if the malware is able to copy files from target node to the hacker node.

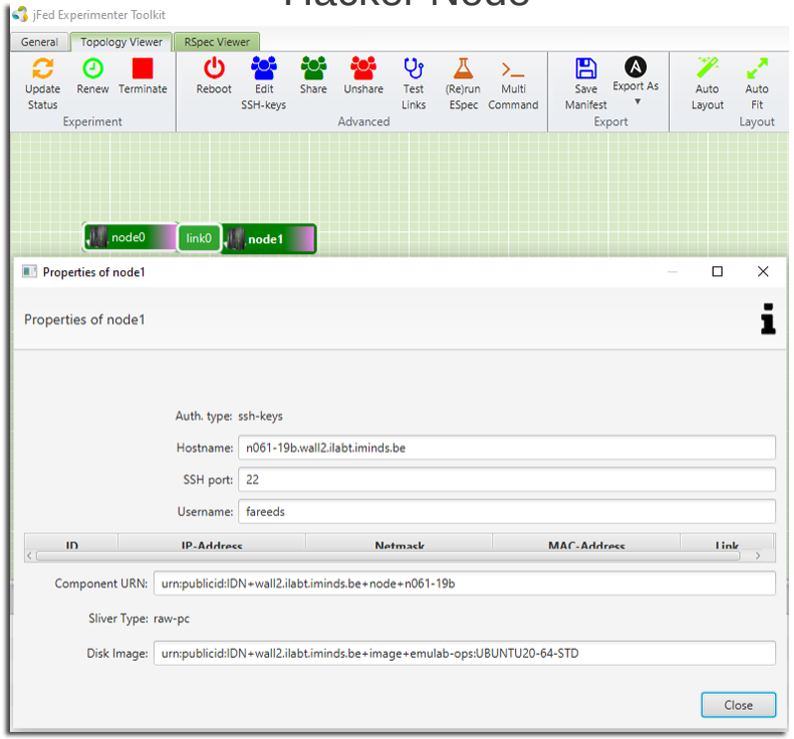
Node Set Up on Virtual Wall 2 testbed

Target Node



Node0

Hacker Node

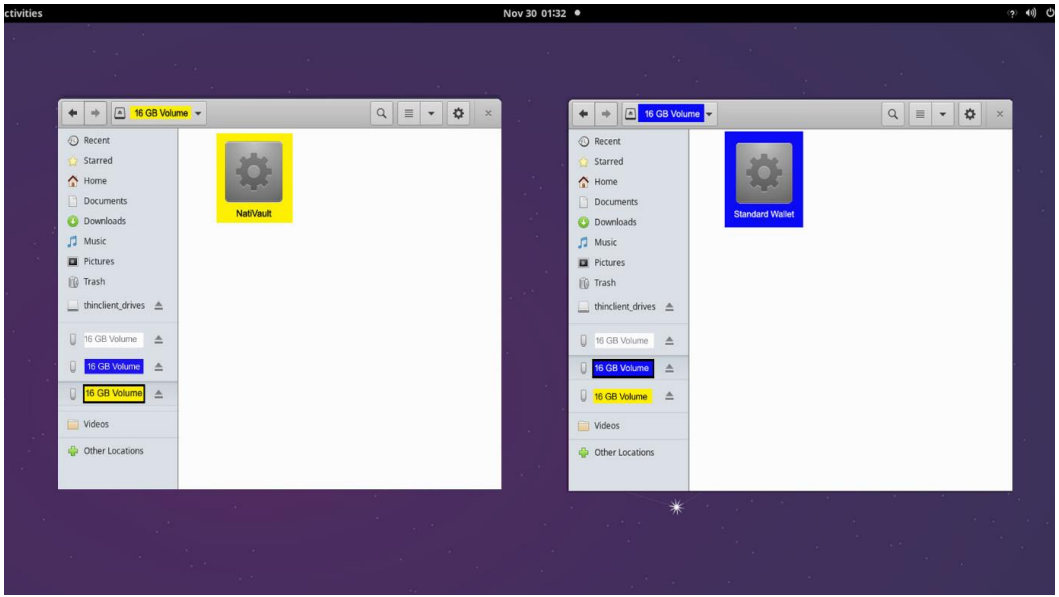


Node1

Device Arrangement on Node 0

Mounted ZVC device & Control device

Control & ZVC device arrangement on Node0 UI

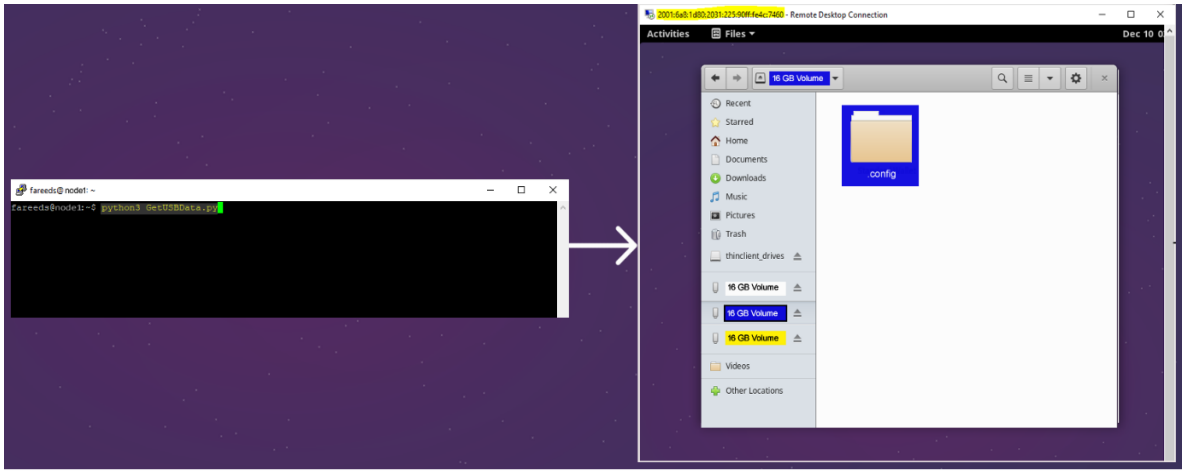


The significant difference between the files in ZVC device and Control device can be noted as the wallet application in ZVC device (Yellow) integrates SOS and ICOS program scripts to create the ZVC ecosystem, whereas Standard Wallet app (Blue) in the control device is a normal cryptocurrency wallet application.

Experiment

CASE1: CONTROL DEVICE MOUNTED AND ONLINE ON NODE0 AND TRANSMITTING MALICIOUS PROGRAM FROM NODE1 TO NODE0

- To test if the malware program was able to perform any action over the Control device, we mounted the Control device over one of the USB ports of Node0 (Target Node) and transmitted the Malware program from Node1 (hacker node) to the Node0, target node.
- The malware program was designed to infect the hardware mounted on the USB port of Node0 and steal data and bring it back to the hacker node (Node1)



SSH of Node 1 UI of Node 0

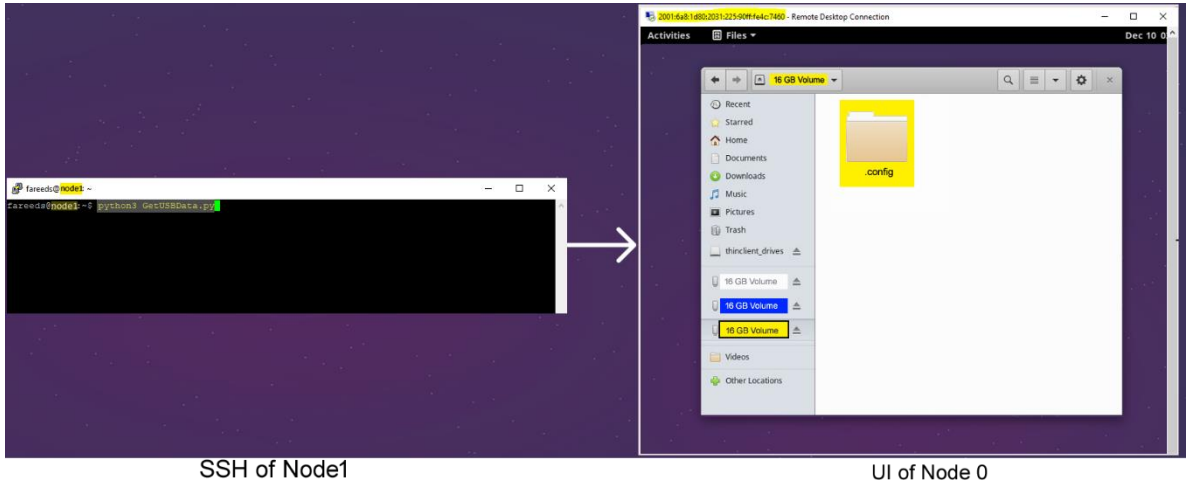
Hacking Command for Target Node0 with Control Device

We performed the transaction using the standard wallet application stored inside the control device and checked if the malware was able to steal the sensitive user data and bring it back to the hacker node.

Experiment

CASE2: ZVC DEVICE MOUNTED AND ONLINE ON NODE0 AND TRANSMITTING MALICIOUS PROGRAM FROM NODE1 TO NODE0

- To test if the malware program was able to perform any action over the ZVC device, we mounted the ZVC device over one of the USB ports of Node0 (Target Node) and transmitted the Malware program from Node1 (hacker node) to the target node.
- The malware program was designed to infect the hardware mounted on the USB port of Node0 and steal data and bring it back to the hacker node (Node1)



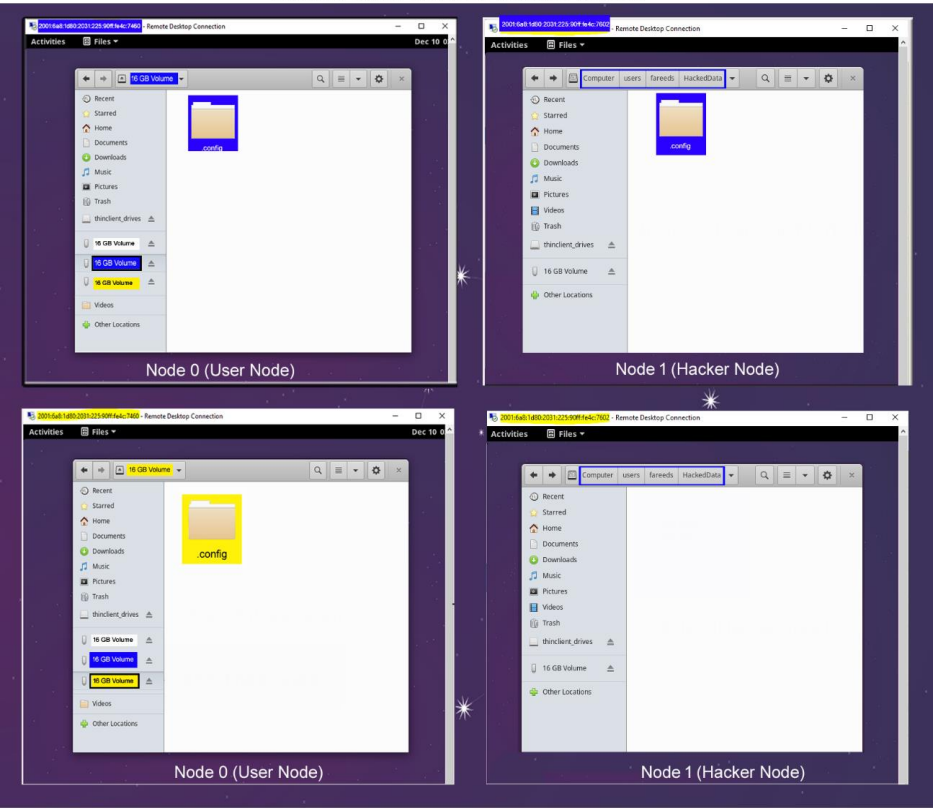
SSH of Node1 UI of Node 0

Hacking Command for Target Node0 with ZVC device

We performed the transaction using the wallet application endowed with SOS and ICOS scripts, stored inside the ZVC device and checked if the malware was able to steal the sensitive user data and bring it back to the hacker node.

Experiment Results

Case1: With control device online



Case2: With ZVC device online

Case1 demonstrated that sensitive files from Node0 (Target Node) was copied to Node1 (Hacker Node), marked in Blue, when the Control Device, without SOS and ICOS components, was connected to the Node0.

Case2; When the ZVC device with SOS and ICOS scripts was connected to Node0, the malware could not copy any files from Node0 to Node1.

Thus, The experiment validated the security and unhackability of a ZVC powered hardware wallet device as a thin client designed as a tiny form-factor permanently USB mountable hardware wallet for storing sensitive data.

Impact: Technology Development Approach

- In one of our previous Horizon 2020 proposals ZEROV, we proposed a radical cybersecurity technique to circumvent computer OS related vulnerabilities by completely obliterating the attack surface, using a specially designed Supra OS (SOS) software.

- Supra OS (SOS) software that restricts any access to the third-party applications was firstly designed to be implemented over the OS in the BYOD (Bring Your Own Devices) settings.

- While the full scale ZEROV development in BYOD setting involved highly intricate and challenging Supra OS (SOS) software, we discovered that a minimalist SOS script is easier to implement in a controlled thin client USB devices to create a novel ZVC ecosystem that can potentially sanitize the USB device.

Business Impact

Commercialization: Out-licensing of the technology to NatiVault Limited, a startup especially founded to commercialize a new class of secure 24*7 connected hardware wallet and authenticator.

Research Partnerships: A Consortium of 10 EU cybersecurity partners including 3 cybersecurity centres of excellence for a Horizon 2020 call for Improved security in open-source and open-specification hardware in connected devices. The ZVC4IoT consortium will integrate ZVC into mobile phones, tablets, and other IoT devices.

Research Hypotheses: The results of this F4FP experiment have helped us formulate 2 hypotheses for further exploration. The details of which will be soon disclosed in the EIC Accelerator Stage 2 submission under H2020 program for which ZVC has already qualified.

Feedback for Fed4fire

- Fed4Fire+ affiliate facilities are state-of-the-art and a boon for SMEs that mostly don’t have such infrastructure in-house to test and validate their research.
- The Fed4fire resources available are really advanced and can be accessed 24*7.
- ZVC involved many aspects that needed to be tested before its market adaptation.
- Minimalistic SOS and ICOS approach that we could successfully test with Fed4Fire’s support has really simplified our product development approach and also the market entry strategy.
- Fed4fire, offering these testing tools free of cost and in a remotest possible way has turned out really beneficial for the project ZVC.

Feedback: Used Resources & Tools

- We conducted the ZVC experiment by accessing the distributed computer hardware network of virtual wall 2 testbed infrastructure.
- The nodes we selected for this experiment were: n061-17b & n061-19b nodes of virtual wall 2 that supported connecting multiple USB devices at one go.
- The nodes were flexible enough to be programmed as per our experiment protocol.
- We used Jfed to access the remote nodes, JFed is really an exciting tool to get access to the remote PCs. The SSH command line portrays a really easy way to run various Linux commands and simulates the real time experience for the experimenters.
- JFed provides really easy to use interface even for the first timers and also the resources are categorically distributed over the tool which makes it easy for the beginners.
- We also used XRDP tool to get remote access to the node UI. As ZVC predominantly needed to be accessed with local commands, it would not have been possible otherwise.
- The best part of conducting experiment with Fed4fire resources is that the testing facilities can be customised easily as per the need of the experiment.

Feedback: Added Value to F4F+

- Fed4Fire+ offered an excellent opportunity and resources for experimenting our cutting edge solutions.
- The experience thus far has enabled us to take our project to the next level by validating our assumptions and further building upon our solutions.
- It is also a platform that provides continuous opportunity for the innovative technologies to be presented at a global level and offers wider visibility on the EU forums.
- The best thing about conducting experiment with fed4fire+ is that it provides wider access to the testbed resources and a single point testing solution for validating the technologies.
- Availability of budget, easy procedures and access to resources and availability of tools, all made the choice easy for us.

Feedback

Following components really make Fed4fire a preferred choice for experiments like ZVC;

1. Diversity of available resources
2. Single point technical assistance
3. Easy setup of the experiments
4. Continuous support from the FED4FIRE+ on both technical as well as administrative front
5. Budget for conducting the experiment
6. Support and documentation details

Thanks to the experiment we conducted within Fed4FIRE+, we got an opportunity to test and validate the revolutionary ZVC concept and we are eagerly working towards commercializing this very promising technology as the world's first always-connected hardware wallet with our partner, NatiVault Limited, UK.


Co-funded by the
European Union


Co-funded by the
Swiss Confederation

This project has received funding from the European Union's Horizon 2020 research and innovation programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under grant agreement No 732638.

WWW.FED4FIRE.EU