Zero Vulnerability Computing

CONCEPT

Computer Hack Attacks can be broadly classified as;

1. Vulnerability-related computer hacks happening through attack surface provided by computer permissions
2. PII (Personally Identifiable Info)-related hacks

Zero Vulnerability Computing (**ZVC**) concept focuses on zeroing computer vulnerabilities by completely obliterating the attack surface 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).

GOALS

1. Prototyping a ZVC device based on a MUDP 3.0 chipset & Building a cryptocurrency wallet application that supports crypto transaction as a hardware wallet
2. 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.
3. 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.

EXPERIMENT SETUP

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

RESULTS

Case1: Control device 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.

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.

Results Case1: The sensitive files from Node0 (Target Node) was copied to Node1 (Hacker Node), when the Control Device, without SOS and ICOS components, was online on the Node0.

Case2: ZVC device 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 Node0.

We performed the transaction using the ZVC wallet application 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.

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

CONCLUSIONS

The ZVC components, SOS and ICOS, rendered the ZVC enabled hardware wallet device immune to any type of hack attack carried out from a remote server.

The experiment thus 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.

POST MORTEM

With the successful completion of the ZVC experiment, company is moving fast towards commercialization of the ZVC technology by Out-licensing the Hardware wallet technology to NatiVault Limited, a startup especially founded to commercialize a new class of secure 24*7 connected hardware wallet and authenticator.

We have been successful in achieving Research Partnerships by forming 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.