What makes Yoroi safe? A Deep Dive into its Security Features

emurgo.io

Yoroi, the light weight Cardano wallet,derives its name from the incredibly ornate ancient armor worn by Japanese samurai. The armor was a combination of iron and leather exquisitely constructed over nearly a year. This article explores some of the security centered features, and core technologies, behind the modern armor designed for your web browser and ADA funds.

There are a number of browser based wallets for both Cardano and other cryptocurrencies. Some browser based wallets are websites that you have to access on the public Internet, while other wallets are actually extensions that you can install on your browser.

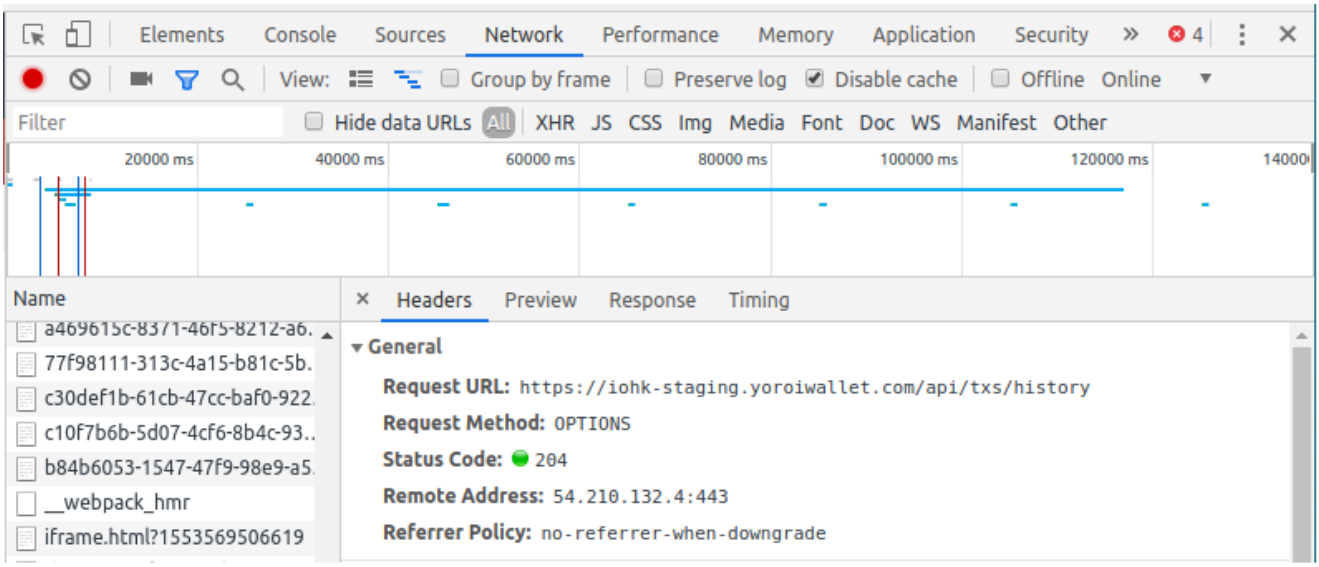
EMURGO, as the official, and commercial, venture arm of Cardano — the first peer-reviewed third generation blockchain — chose to develop a browser based *extension* due to a number of security issues with web based wallets. Often times, unofficial web based wallets will encourage you to run a local copy of their Javascript code to create your private key and password; there is no guarantee the code is clean and most people don't want to have to look at every line of code themselves. In contrast, Yoroi has been developed by the official organizations behind Cardano, namely EMURGO and IOHK. Furthermore, there is no guarantee that a website based wallet won't quietly get hacked, or snooped on, by a third party at some point, given the tremendous incentive to do so.

Another reason EMURGO chose to create a browser extension was due to the cases where DNS hijacking occurred and people were redirected from a wallet to a different website that stole their money. Typos of a website domain name can also lead to similar issues. An extension doesn't have this problem.

Similarly, people have linked to fake versions of Daedalus where the application people downloaded was actually a virus. Yoroi doesn't have this problem, however, since the Chrome store ensures you download the right application.

The fact Yoroi runs in Chrome allows us to develop faster as there are well-made APIs we can rely on and it also protects the user as the extension runs inside its own sandbox. Chrome, in general, makes it easier to inspect packets so you can check that Yoroi is not sending your private key to our servers. With the Chrome developer tools you are able to see exactly what data is passed to the EMURGO/IOHK servers.

Select the **Network** tab from the developer tools main menu and you can see the polling process, for example. The Yoroi wallet will periodically send your wallet address and the dateFrom value, which tells the staging server to get all transactions after that date. Currently, Yoroi has to poll the IOHK servers to get your transaction history and to execute transactions. You can see all of the HTTP POST requests in the yoroi-backend-api.js file. While the Yoroi light wallet will always depend upon our servers, the transaction broadcast is a temporary situation and will be changed once Shelley is released.



Select the **Network** tab from the developer tools main menu

The Chrome permission system also lets you know exactly what we have access to. Right now, Chrome says that Yoroi has access to your entire browsing history; traditionally, this is referred to as an over privileged extension, however, the code does not actually compile, or read, your history. This is a misleading message by Chrome and we will fix it, but the development team just hasn't had the time yet.

You can only have one copy of Yoroi running at the same time and the way we ensure that is true is to check if you have a different Yoroi tab open. And in order to do that, we need to scan through all your tabs open at the moment. Since, theoretically, you could constantly scan open tabs to, over-time, know the user's entire browsing history, Chrome displays the worst-case scenario message which is the warning that the "app can see your whole browsing history." We don't actually do that, however.

The permissions that websites have to see your wallet details is also an issue EMURGO developers are thinking about. Some wallets, such as Metamask, inject a web3 instance into every page in order to interact with websites. Wallet interactivity with websites is important for distributed app usage and helps drive adoption of the underlying cryptocurrency. Developers at EMURGO plan to integrate a URI scheme so that Yoroi can have similar functionality without exposing wallet addresses, or transaction information, to every site you visit.

Understanding the risks of a hot wallet mean you have to understand your responsibilities as a user. Your encrypted private key is stored in Chrome's local storage space. Storing your encrypted private key locally means you actually own your ADA. However, it is also important to secure the computer on which your wallet resides.

If you can dedicate an entire machine to your Yoroi wallet, trading activities, and other crypto funds, then that is ideal. If you can't do that then you may want to use a virtual machine for web browsing, torrents, or streaming media in addition to using an effective antivirus program and adblocker. Making sure your machine is on an isolated network from the rest of your family, or office, is also imperative. Lastly, checking the security of your router/firewall is necessary.

Your encrypted private key is safe with Yoroi, but, as stated above, you have to be extra careful about creating a secure environment where no one can snoop on your wallet password when you enter it. Your wallet password is different from the 15 word mnemonic. Your private key is encrypted using the

mnemonic and your wallet password as the salt. So if someone physically steals your computer you can simply install Yoroi on another computer and use your 15 word mnemonic/recovery phrase to access your funds as that phrase gives you direct access to your private key. The Cardano-rust password encryption code uses the standard HMAC-SHA512 functions along with pbkdf2 and ChaCha20 Poly1305.

Currently, while Yoroi supports the HD Wallet format, it only allows one account. You can still generate as many arbitrary addresses as you like using the "Generate new address" button, however. Yoroi Mobile supports more than one account with each having its own mnemonic and Bip-44 compliant wallet.

Yoroi supports importing Daedalus paper wallets, but not the creation of paper wallets natively at the moment. Yoroi supports both Trezor and Ledger hardware wallets. Storing your keys offline and using a light wallet when needed for smaller transactions can provide both extra safety and ease of use.

There has been a significant push in the cryptocurrency industry to adopt secure languages for development. Rust is generally considered to be one of these secure languages. TheCardano-rust package handles all of the cryptography in Yoroi. This is the same Rust code used to power the Rust fullnode that IOHK is creating.

In order to connect Yoroi to the Cardano-rust crypto libraries, WASM is used. WASM, also known as WebAssembly, is a "binary instruction format for a stack-based virtual machine. Wasm is designed as a portable target for compilation of high-level languages like C/C++/Rust, enabling deployment on the web for client and server applications." It has some security features worth noting.

WASM is strongly typed, and memory is limited/sandboxed to ajavascript array buffer, so WASM cannot access memory out of bounds or access other Javascript memory. The Cardano-rust code is compiled to WASM and then called through Javascript bindings. In the near future, WASM bindings will be automatically generated, so developers will have an easier time exploring the code for their own purposes.

EMURGO'S lead developer, Sebastien Guillemot, says that, "a lot of blockchains are now usingRust since it allows for very fast execution, and good support, for avoiding memory problems at compile time, along with good interoperability with WASM." If you are interested in talking with other Cardano developers, or have questions, you can explore the Cardano-Rust gitter chat room.

Hopefully, now you have a better understanding of the security features, and components, behind the Yoroi light wallet. The developers at EMURGO are thinking about security first when it comes to the Yoroi. Explore the Yoroi source code on github or visit Yoroi.com and install the extension yourself today.

About EMURGO
EMURGO drives the adoption of Cardano and adds value to ADA holders by building, investing in, and advising projects or organizations that adopt Cardano's decentralized blockchain ecosystem. EMURGO leverages its expertise in blockchain R&D as well as its global network of related blockchain and industry partners to support ventures globally.

EMURGO is the official commercial and venture arm of the Cardano project, registered in Tokyo, Japan since June 2017 and in Singapore since May 2018. EMURGO is uniquely affiliated and works closely with IOHK to grow Cardano's ecosystem globally and promote the adoption of the Cardano blockchain. To learn more about the project, visit the EMURGO website.

||**Click here to subscribe to the EMURGO Newsletter**||

Follow EMURGO on Social Media

- Official Homepage: emurgo.io
- Twitter (English): @emurgo_io
- Twitter (Japanese): @Emurgo_Japan
- Youtube: EMURGO
- Telegram: EMURGO Announcements
- Facebook: @emurgo.io
- Instagram: @emurgo_io
- LinkedIn: @emurgo_io

About Yoroi Wallet

- Yoroi Twitter: @YoroiWallet
- Yoroi Homepage: https://yoroi-wallet.com/

About Cardano

- Cardano Forum: https://forum.cardano.org/
- Cardano Telegram: https://t.me/CardanoGeneral
- Cardano Reddit: