Wristband uses encryption to grant access to devices

November 11 2014, by Nancy Owano

A Kickstarter project aims to give you a Bluetooth Low Energy-enabled wristband that replaces keys and passwords. Everykey from the Cleveland, Ohio-based company of the same name, Everykey, is a fashionable band that can be instantly disabled if your Everykey ever gets lost or stolen. You call the team or go online to deactivate it. A message is immediately sent to all of your devices letting them know that they should not unlock for your wristband. The team would overnight you a new wristband at a discount. As the team says in their promotional video, it pretty much "unlocks your life." When the Everykey wristband is within range of a user's device, the wristband will allow the user to bypass that device's password or physically unlock it automatically. When the wristband is out of range, the device automatically re-enables security mechanisms.

They say their security is military-grade. (Everykey uses AES 128-bit encryption), and they also highlight an "obsession with design and usability." Fashion, they said, was their "north star." Color options were selected to reflect a unique personality. The band has a silicon exterior with a lightweight metal skeleton. Everykey works with Mac OS 10.9 (Mavericks), Windows 8.1, and Android 4.4 (KitKat). They are currently developing support for jailbroken versions of iOS as well as Ubuntu 14+ (Linux). The circuit board is powered by their custom bent lithium-polymer battery. The team said that you would need to charge it about once a month. After the battery runs out, you can charge Everykey using an included Micro USB to USB cable.

How it works: The wristband broadcasts encrypted information to identify itself, which only your devices can decrypt. The team said: "Everykey broadcasts an encrypted Bluetooth 4.0 message at least once every second. Each time this message is broadcast, it's changed, preventing a hacker from sniffing a message and re-broadcasting it. Because each message is encrypted, there's no way to derive one message from the previous message, so each encrypted message that's broadcast is non-deterministic and pseudorandom. Your devices will only unlock for the most recent message, so a hacker is unable to unlock your devices by re-broadcasting an old message. Only devices that you've set up with your Everykey will have the ability to interact with your Everykey, all other connections are rejected. A device still has to verify its legitimacy through an encrypted handshake in order to interact with your wristband."

Does Everykey work on every web site? They said, "We developed the Everykey browser extension by testing it on hundreds of websites and although we can't guarantee it to work on every website, our software has been able to work with every website we've tested it on. All major websites (Facebook, Twitter, Gmail, etc) work with Everykey."

Supporters who pledge $50 get a wristband in any available color, with an estimated delivery date of March.

Future plans include the release of an SDK, allowing other access control technologies to integrate with Everykey. They said this means the wristband may start a car, turn on lights and even replace credit cards.

More information: www.prweb.com/releases/everyke … er/prweb12262874.htm
www.kickstarter.com/projects/e … places-keys-and-pass

Citation: Wristband uses encryption to grant access to devices (2014, November 11) retrieved 9 April 2024 from https://techxplore.com/news/2014-11-wristband-encryption-grant-access-devices.html