Cracking a $2 million crypto wallet

In early 2018, Dan Reich and a friend decided to spend $50,000 in Bitcoin on a batch of Theta tokens, a new cryptocurrency then worth just 21 cents apiece. At first, they held the tokens with an exchange based in China, but within weeks, a broad crackdown on cryptocurrency by the Chinese government meant they would soon lose access to the exchange, so they had to transfer everything to a hardware wallet. Reich and his friend chose a Trezor One hardware wallet, set up a PIN, and then got busy with life and forgot about it.

By the end of that year, the token had sunk to less than a quarter of its value, come back up, and then crashed again. Reich decided he wanted to cash out, but his friend had lost the paper where he'd written the PIN and couldn't remember the digits. They tried guessing what they thought was a four-digit PIN (it was actually five), but after each failed attempt, the wallet doubled the wait time before they could guess again. After 16 guesses, the data on the wallet would automatically erase. When they reached a dozen tries, they stopped, afraid to go further.

Reich gave up and wrote off the money in his mind. He was willing to take the loss — until the price started to rise again.

From a low of around $12,000, the value of their tokens started to skyrocket. By the end of 2020, it would be worth more than $400,000, rising briefly to over $3 million. It would be hard to get into the wallet without the PIN — but it wasn't impossible. And with potentially millions on the line, Reich and his friend vowed to find a way inside.

The only way to own cryptocurrency on the blockchain is to have sole possession of a private key associated with a block of currency — but managing those keys has been a, sometimes high-stakes, challenge from the beginning. You can't sell or spend your currency without the key (or the string of words used to derive the key, also called the seed) — but if anyone else gets hold of it, they can grab your coins in a single anonymous transaction from anywhere in the world. You can store your key in a software wallet on an exchange service's server or in a software wallet on your own computer or mobile phone — but those are vulnerable to remote attack if anyone on the internet is able to get your key.

Hardware wallets, the size of a USB stick, are meant to solve that problem, storing the key locally, off the internet, and signing transactions inside the secure wallet when you insert the device into a computer and enter the PIN. But if you forget the PIN and don't have the key written down, you're generally out of luck and can no longer access your currency on the blockchain.

more than 3.7 million Bitcoins are lost to owners
This happens more often than you might think. The cryptocurrency data firm Chainalysis estimates that more than 3.7 million Bitcoins worth $66.5 billion are likely lost to owners. Currency can be lost for many reasons: the computer or phone storing a software wallet is stolen or crashes and the wallet is unrecoverable; the owner inadvertently throws their hardware wallet away; or the owner forgets their PIN or dies without passing it to family members.

As the value of their inaccessible tokens rapidly rose in 2020, Reich and his friend were desperate to crack their wallet. They searched online until they found a 2018 conference talk from three hardware experts who discovered a way to access the key in a Trezor wallet without knowing the

PIN. The engineers declined to help them, but it gave Reich hope.

“We at least knew that it was possible and had some directional idea of how it could be done,” Reich says.

Then they found a financier in Switzerland who claimed he had associates in France who could crack the wallet in a lab. But there was a catch: Reich couldn’t know their names or go to the lab. He’d have to hand off his wallet to the financier in Switzerland, who would take it to his French associates. It was a crazy idea with a lot of risks, but Reich and his friend were desperate.

COVID and lockdowns slowed their plans in 2020, but in February 2021, with the value of their tokens now $2.5 million, Reich was making plans to fly to Europe, when suddenly they found a better option: a hardware hacker in the US named Joe Grand.

Grand is an electrical engineer and inventor who has been hacking hardware since he was 10. Known by the hacker handle “Kingpin,” he was part of the famed L0pht hacker collective that, in 1998, testified to the US Senate about a vulnerability that could be used to take down the internet or allow an intelligence agency to spy on traffic. In 2008, he co-hosted the Discovery Channel’s “Prototype This” show and currently teaches hardware hacking to organizations and companies that design complex systems and want to understand how hackers can attack their products.

“If he screwed something up, there was a good shot that it would never be able to be recovered”
Reich, an electrical engineer himself who owns a software company, had a better ability than most to assess if Grand had the skills to pull off the hack. After a single conversation, he knew they’d found the right person. “I remember thinking, ‘Wow, this is perhaps one of the brightest electrical

engineers I’ve ever met,’” he recalls.

Grand, who has a custom lab in his family’s Portland backyard, purchased several identical wallets to the one Reich and his friend owned and installed the same version of firmware on them. Then he spent three months doing research and attacking his practice wallets with various techniques. They agreed that Reich, who lives in New Jersey, wouldn’t fly out to Portland with his wallet until Grand succeeded to crack three wallets using the same technique.

“If he screwed something up, there was a good shot that it would never be able to be recovered,” says Reich.

Luckily for Grand, there was previous research to guide him. In 2017, a 15-year-old hardware hacker in the UK named Saleem Rashid had developed a method to successfully unlock a Trezor wallet belonging to tech journalist Mark Frauenfelder and helped him free $30,000 in Bitcoin.

a fault-injection method — also known as glitching
Rashid found that when the Trezor wallet was turned on, it made a copy of the PIN and key that was stored in the wallet’s secured flash memory and placed the copy in RAM. A vulnerability in the wallet allowed him to put the wallet into firmware update mode and install his own unauthorized code on the device, which let him read the PIN and key where it was in RAM. But the installation of his code caused the PIN and key stored in long-term flash memory to erase, leaving only the copy in RAM. This made it a risky technique for Grand to use; if he inadvertently erased the RAM before he could read the data, the key would be unrecoverable.

In any case, Trezor had altered its wallets since then so that the PIN and key that got copied to RAM during boot-up got erased from RAM when the device was put into firmware update mode.

So Grand looked instead to the method used in the 2018

conference talk that Reich had also examined previously. The researchers in this case found that despite Trezor removing the PIN and key that got copied to RAM during boot-up, the PIN and key were showing up in RAM during another stage. They found that at some point during the firmware update mode, the PIN and key were being temporarily *moved* to RAM – to prevent the new firmware from writing over the PIN and key – then *moved* back to flash once the firmware was installed. So they devised a technique dubbed "wallet.fail." This attack used a fault-injection method – also known as glitching – to undermine security protecting the RAM and allow them to read the PIN and key when they were briefly in RAM.

There are three levels of security available for the microcontroller used in Trezor wallets – RDP2, the most secure, which doesn't let you read the RAM, and RDP1 and RDP0, which do. Trezor wallets are configured to use RDP2 to prevent someone from reading the RAM, among other things.

But by doing a fault injection attack against the chip – which affects voltage going to the microcontroller – the wallet.fail team found they could downgrade the security from RDP2 to RDP1. They could then force the wallet into firmware update mode, sending the PIN and key into RAM, and read them. It was similar to Rashid's attack, except the fault injection got them access to RAM without needing to exploit code.

The technique was great for a research project but risky for Reich's wallet. Because the PIN and key were *moved* to RAM during the firmware update and not just copied, there was only one version on the wallet during this period. Do something wrong, and Grand could inadvertently wipe the RAM, along with the key and PIN. As it was, each time he glitched his practice wallets, they froze.

After nearly three and a half hours, the computer finally called out
But while trying to troubleshoot the problem, Grand stumbled

on a better solution. He found that in the version of firmware installed on Reich's wallet, the key and PIN still got copied to RAM when the device was powered on. If Grand glitched the device at the right moment, he could downgrade the security to RDP1 and read RAM. And because the key and PIN were merely copied to RAM at this point and not moved, unlike the wallet.fail scenario, this meant they still existed in flash if Grand inadvertently wiped the RAM. It was a much safer solution that elegantly borrowed from both prior attacks.

The only problem was the glitching required thousands of tries — powering up the wallet repeatedly and using different parameters to affect the voltage to the microcontroller each time, in an attempt to hit the exact moment that would let him downgrade the microcontroller's security. It took three to four hours using an automated script, and there was no guarantee it would work on Reich's wallet, even if it worked on the practice wallets. Reich likened the excruciating wait to sitting through a stakeout.

Grand designed his program so that if and when the glitch worked, his computer would call out: "Hack the planet!" — a nod to the 1995 film *Hackers*. When the time came to do the hack for real last May, Reich flew to Portland for two days. They spent the first day getting everything set up — they filmed the hack with a professional crew — and the next day, Grand launched his script.

Then they waited. And waited some more. Then they ate pizza and waited some more.

After nearly three and a half hours, the computer finally called out: "Hack the planet!" On Grand's screen, he could see the key and five-digit PIN. Reich and his friend were now $2 million richer.

He immediately moved the Theta tokens out of their account and sent a percentage of the booty to Grand for his services.

It was a thrilling moment for Grand – and not just because of the money that was at stake. “It kind of reinvigorated me… and helped me decide what I should be doing with my skills,” he says.

“with enough time and effort and resources, anything is hackable”

Since last May, he’s been speaking with others who lost access to their funds, with the hope of helping more people crack their wallets. This includes James Howells in Wales, who inadvertently threw his hardware wallet in the trash in 2013 and lost access to Bitcoin now worth half a billion dollars. He’s been trying for years to convince his local council to let him dig through the dump. The city tracks where residential trash is buried and told him there’s a good chance they could locate the area where his wallet might be but have so far refused his request.

Grand has also been speaking with someone whose wallet is on a broken phone, which would require forensic repair techniques and a couple who lost the password to a software wallet stored on their computer.

But Grand doesn’t want to just crack wallets – he also wants to help make them more secure. He plans to report vulnerabilities he finds to the vendor when they’re patchable, so they can’t be exploited by criminals or others who might seize an owner’s wallet. Does this mean he’ll run out of vulnerabilities to hack at some point?

Grand doesn’t think so. There will always be people with older unpatched versions of firmware on their wallets – like Reich – and he’s confident newer devices will still be vulnerable in different ways even if they’re patched.

“It depends on the design, but with enough time and effort and resources, anything is hackable,” he notes.

Trezor already fixed part of the problem Grand exploited in

later versions of its firmware. The wallets no longer copy or move the key and PIN into RAM at all. Pavol Rusnak, co-founder and CTO of SatoshiLabs, which makes Trezor wallets, said it now stores them in a protected part of flash that isn't affected during firmware upgrades.

But a core issue with the chip that allows fault injection still exists and can only be fixed by the chip maker — which the maker has declined to do — or by using a more secure chip. Rusnak says his team explored the latter, but more secure chips generally require vendors to sign an NDA, something his team opposes. Trezor uses open-source software for transparency, and when Rusnak's team discovered a flaw in one secure chip they considered using, the chip maker invoked the NDA to prevent them from talking about it.

This means Trezor wallets may continue to be vulnerable to other hacking techniques. Grand is already working on one new method for hacking the STM32 microcontroller used in the wallets. It will work even on wallets with the newest, more protected firmware. He says he won't release the details publicly, however, because the ramifications go beyond wallets.

"The STM32 is used in billions of devices around the world," he says, and the issue he found can't be patched. "Which is both awesome and scary."

https://www.theverge.com/2022/1/24/22898712/crypto-hardware-wallet-hacking-lost-bitcoin-ethereum-nft