Neha Narula Follow
Director, Digital Currency Initiative at the MIT Media Lab. I work on scaling applications and platforms for the internet.
Sep 7, 2017 · 7 min read

Cryptographic vulnerabilities in IOTA

Last month, Ethan Heilman, Tadge Dryja, Madars Virza, and I took a look at IOTA, currently the 8th largest cryptocurrency with a $1.9B market cap. In its repositories on GitHub, we found a serious vulnerability—the IOTA developers had written their own hash function, Curl, and it produced collisions (when different inputs hash to the same output). Once we developed our attack, we could find collisions using commodity hardware within just a few minutes, and forge signatures on IOTA payments. We informed the IOTA developers, they patched their system, and we wrote a vulnerability report. **The current version of IOTA does not have the vulnerabilities we found**, but there's more to be said about how this happened and what's going on with cryptocurrencies right now.

> *In 2017, leaving your crypto algorithm vulnerable to differential cryptanalysis is a rookie mistake. It says that no one of any calibre analyzed their system, and that the odds that their fix makes the system secure is low*
>
> *— Bruce Schneier*

Who's responsible for vetting cryptocurrency technology?

The cryptocurrency space is heating up—Protocol Labs raised $200M for Filecoin, Bancor raised $150M, and Tezos raised $232M. Some are heralding this as a new funding model: a new way of monetizing distributed networks and applications. I'm enthusiastic about the underlying technology, but urge serious caution around ICOs. The SEC has already issued warnings, suspended traditional trading on companies doing token sales, and caused one company to revert its ICO.

Though the technology is exciting, the due diligence required to make sound investments in the technology isn't keeping up with the pace of the hype. Aside from the financial risk, I don't think developers and investors are thoroughly evaluating these systems technically, either. Many investors are relying on signaling—if enough well-known institutions like universities or large companies sign on as investors or advisors, it indicates approval of the project and its software. The problem is that some of these technologies have serious issues, and the large companies and well-known individuals either aren't doing due diligence and investing the resources and time needed to evaluate the projects with which they are partnering, or aren't sharing their findings with everyone else. The cryptocurrency space still doesn't have a good way to assess these projects.

An early example of this was The DAO. Slock.it listed curators, who approved investment proposals on the website. It looked like those curators—including prominent Ethereum researchers like Vitalik Buterin, Gavin Wood, and Vlad Zamfir—were standing behind the code and the system. But the curators didn't realize that users would view their agreement to help curate as endorsement and approval of the entire DAO. The DAO turned out to have a major security vulnerability, and users lost their tokens until the Ethereum Foundation stepped in to reverse the loss.

You might think that IOTA, a cryptocurrency worth over a billion dollars, and working with organizations like Microsoft, University College London, Innogy, and Bosch, BNY Mellon, Cisco, and Foxconn (through the Trusted IOT Alliance) would not have fairly obvious vulnerabilities, but unfortunately, that's not the case. When we took a look at their system, we found a serious vulnerability and textbook insecure code.

> "In 2017, leaving your crypto algorithm vulnerable to differential cryptanalysis is a rookie mistake. It says that no one of any calibre

analyzed their system, and that the odds that their fix makes the system secure is low," states Bruce Schneier, renowned security technologist, about IOTA when we shared our attack.

Vulnerability report

We discovered a vulnerability in IOTA after reviewing their code on GitHub in July. We disclosed what we found to the IOTA team on July 14th, and have been in contact with them since then as we discovered new issues and exploits. IOTA issued a patch that addresses the vulnerabilities we found on August 7th. **IOTA no longer has the vulnerabilities we found, they have been fixed.** To learn more about the details of our attack, you can view the full disclosure and review our attack examples. We sent a draft of this report to the IOTA team and they gave some feedback which we considered in the version we're sharing today. The IOTA team has raised more general objections to the report and whether this is a vulnerability that should be of concern.

Please don't roll your own crypto

A cryptographic hash function takes an arbitrary amount of input and produces unpredictable output with a fixed size. The idea is that given an output, it's very hard to find an input that maps to that output, and given an input and output, it's very hard to find *another* input that maps to the same output. When two inputs map to the same output, that's called a *collision*. Being able to easily find collisions means the cryptographic hash function is broken.

Cryptographic hash functions are important for cryptocurrencies because usually a transaction is hashed before it's signed. So if you can break a hash function, you can potentially break signatures as well, meaning that the mechanism used to determine if a transaction is a valid and authorized spend is broken. The mathematical integrity that cryptocurrencies provide hinges on this relationship being secure.

The golden rule of cryptographic systems is "don't roll your own crypto." If asked, any security researcher will tell you to only use well-understood and well-tested cryptographic primitives when building a system. Cryptographic hash functions, in particular, go through years of vetting and testing before they are deemed robust enough to use in critical software. For example, the SHA-3 competition took nine years (from 2006 to 2015) to thoroughly cryptanalyze the candidates and select Keccak as the finalist.

So when we noticed that the IOTA developers had written their own hash function, it was a huge red flag. It should probably have been a huge red flag for anyone involved with IOTA.

Problems with IOTA's hash function

We found that IOTA's custom hash function Curl is vulnerable to a well-known technique for breaking hash functions called differential cryptanalysis, which we then used to generate practical collisions. We used our technique to produce two payments in IOTA (they call them "bundles") which are different, but hash to the same value, and thus have the same signature. Using our techniques, a bad actor could have destroyed users' funds, or possibly, stolen user funds.

One part of IOTA we were not able to investigate, since the code is not open source, is its trusted coordinator. Currently, the trusted coordinator, which the IOTA developers run and plan to remove in the future, signs the latest good state of the system (as determined by the coordinator). The coordinator might prevent some problems caused by colliding transactions, but without it, an attacker could have potentially "forked" the IOTA tangle—divided it into two irreconcilable pieces. We do not think the coordinator would have prevented the burning user funds or stealing attacks because the original transaction is not relayed to the network, so the coordinator wouldn't be able to tell the second, colliding transaction was an attack.

We show the details of our proposed attacks, one which destroys user funds and one which steals IOTA from a user, in this repository. When we found this vulnerability, we notified the IOTA developers. They have switched to a new hash function they wrote, based on the well-known SHA3. They quickly turned around code and set the steps in motion to hard fork their system and change all user addresses. Right now, our specific attacks have been fixed, but we do want to note that IOTA is still using the old Curl hash function in some places in its software.

We discovered the vulnerability by reading public resources made available by the IOTA developers, including their repositories on GitHub and posts in the IOTA forum, and we validated it by using publicly available IOTA binaries and sending our bundles to the IOTA developers over email. Tadge Dryja first noticed that that the Curl hash function looked suspicious, and brought in Ethan Heilman, who did the bulk of the cryptanalysis to figure out how to create collisions. I implemented a practical attack, and Madars Virza did an independent analysis to try to directly invert the hash function using algebraic techniques (which has not yet been successful, and is not included in the report). We never submitted our colliding transactions to the network, or otherwise interacted with the IOTA network.

I think it's important to reiterate that the IOTA developers do not agree with our characterization of this as an issue of concern. Our report lays out more details about why we are concerned.

Trits and trytes and other red flags

There are other red flags—unlike every other program running on your laptop or phone, IOTA uses ternary instead of binary. Since all computer hardware today uses binary, IOTA converts to ternary in software, which is less efficient and more complex. This complexity prevents IOTA from benefiting from existing security analysis tools that are designed to work with binary, and makes the code harder to read and understand. Another inefficiency is that transactions in IOTA are 10KB (in contrast, Bitcoin transactions are on average 600B), meaning that this is not well-suited to devices with limited storage, like those used for IoT, one of the developers' primary use cases. The current IOTA tangle requires a trusted party (the coordinator) for security, suggesting that in its current form it's not ready to run as a truly permissionless, decentralized system. Others have written about IOTA's use of a trusted coordinator and asked about the incentive structure—whether users of their system have an incentive to converge the tangle if each acted selfishly.

Conclusion

The digital currency space is still new, and we are confident that robust, useful technologies will continue to emerge and gain adoption. But the fact that none of IOTA's partners raised these concerns about a glaring vulnerability in a ~$2B cryptocurrency, or spoke about the other red flags, is worrisome. While one of the most important features of blockchains is removing the need for trusted third parties, most people don't have the time or background to thoroughly evaluate the software, which means that trust is still needed: trust in the developers of the project, or someone else capable of evaluating the software. I think it's important that the public is aware of our investigation and what we found. In this space, extraordinary claims warrant extraordinary evidence; there's a need to temper large claims with rigorous due diligence, and right now, that is not happening nearly enough. Large organizations and well-known individuals should not lend their names and reputation to technology they have not vetted.

— -

Neha Narula is the Director of the Digital Currency Initiative at the MIT Media Lab.