KENNESAW STATE UNIVERSITY

COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

CS 4850-01 | FALL 2023 | SP-24 RED | SECURITY IN BLOCKCHAIN

WEAK RANDOMNESS

GAREK MILENDER

INSTRUCTOR: SHARON PERRY

INTRODUCTION

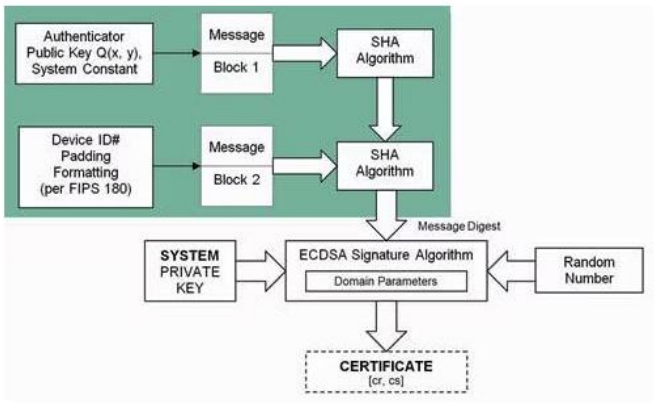
In this paper, we will briefly investigate weak randomness and how it can be exploited. It is an exceedingly small yet large problem inside of the blockchain system and can allow for people's private keys their signatures to be taken and used to take some of their bitcoin. We will also see some small items that could help in prevention as well as some mitigation methods to make it less useful as an exploit to attackers.

What is Weak Randomness?

Weak randomness is an exploit using the randomly generated number for encryption in blockchain. This is exploited in the way that ECDSA works. ECDSA is an elliptic curve digital signature algorithm. This algorithm uses elliptical curve cryptography keys.

What is ECDSA?

The elliptical curve used in creating the digital signal in the ECDSA algorithm makes the signing process more secure and more efficient. ECDSA has 3 main functions generating key pairs, signatures, and verification. The first step is to generate the key pairs. The private key is generated first then the public key. The public key is created using the public key times G. G being the elliptical curve point. Next, they generate signatures. The signing algorithm takes the message and the private key as input and outputs a signature. Next up is the signature verification method. This accepts the message and the signature returning a Boolean indicating whether the signature is valid. This is done by having the message hashed using the same hash as the signature usually SHA-256. Next the modular inverse is calculated of the signature. Followed by the random point is recalculated decompressed for the x coordinate and then compared to verify the signature.



This image from embedded shows where ECDSA fits into blockchain and where it is used in the verification process.

Random Number

In the above image you can see where the random number goes in, and it is seen going inside the ECDSA. This is where the weakness occurs in the nonce that is generated by combining half the message bits and the signing key together. In this way an attacker can create a fake ECDSA signature that looks valid on the surface. By exploiting this number, the attacker is said to be able to retrieve the ECDSA private key if they know the nonce used to generate a signature. The nonce in bitcoin is a uniquely randomly generated number that is used to create the hash for the previous block address. Sometimes this vulnerability can also occur when the random number is generated the same as another that was previously generated.

PREVENTION

The way to prevent this from happening is mainly creating a list of weak sequences of numbers and repeat numbers not allowing for the randomly generated number to be one of the past numbers. This would allow no repeats making it harder for the attacker to use this exploit. Also adding to this list to decrease numbers that are reused should be previously breached numbers. This makes them not truly random but adds a layer of security to the verification algorithm. Other than this there is not to much prevention to be done other than figuring out a new more secure way to verify and hash keys and signatures.

MITIGATION

Some third-party people include Chain links random functions and VeeDos verifiable Delay function can be used to add more randomness to the chain making it slightly more difficult for the attacker to get the bitcoin. These solutions do cost extra money however they are not as susceptible to prediction by the attacker in guessing the randomly generated number of when the block is mined.

CONCLUSION

Weak randomness in ECDSA verification can lead to data breaches in bitcoin. A random number being reused or a pattern emerging in the random number can all be used by attackers to find a user's private key or signature to the block. Possibly having a list removing recently used random numbers or leaked numbers could help in prevention. Better mitigation methods are available yet costly but can help aid in confusing attackers and not making it easy to predict the next number. Weak randomness is more of an accepted risk in certain blockchain wallets unless a better more effective way of securing the private keys can be found.

REFERENCES

Author links open overlay panelZiyu Wang a b, et al. "Ecdsa Weak Randomness in Bitcoin." *Future Generation Computer Systems*, North-Holland, 3 Sept. 2019, www.sciencedirect.com/science/article/abs/pii/S0167739X17330030.

Hussein1, Nisreen T., and Ali H. Kashmar2. "IOPscience." *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, 1 Nov. 2020, iopscience.iop.org/article/10.1088/1757-899X/928/3/032022#:~:text=One%20of%20Blockchain%20vulnerabilities%20is,even%20the%20user's%20fund%20theft.

Kalaycı, Muhammet. "The ECDSA (Elliptic Curve Digital Signature Algorithm) Explained." *Medium*, Medium, 6 Feb. 2023, medium.com/@mkklyci/the-ecdsa-elliptic-curve-digital-signature-algorithm-explained-db052557a6f9.

Liguori, Martin. "Preventing the Source of Randomness Vulnerability." *Blockchain Development Company*, 9 Mar. 2023, www.infuy.com/blog/preventing-the-source-of-randomness-vulnerability/.

Staff, Embedded. "Using the Elliptic Curve Digital Signature Algorithm Effectively." *Embedded.Com*, 2 Feb. 2014, www.embedded.com/using-the-elliptic-curve-digital-signature-algorithm-effectively/.