A Study on Digital Currency: The Safety of Future Money

T. Syahrul Reza
Associate Professor (Lektor Kepala)
Institut Ilmu Sosial dan Manajemen STIAMI
Email : ts.reza@stiami.ac.id

ARTIKEL INFO

Keywords—Cryptosystem; *Cryptoanalysis; Cryptography; Information Security;Bitcoin; Cryptocurrencies.*

ABSTRACT

Cryptography, as the most critical aspect of the never-ending evolving information technology era, is being criticized in its privacy aspect. Information outbreaks make users doubtful on relying on their own information in current cryptosystems. this study present professional countermeasures and attempts to define how the existing cryptology functioned being used worldwide by using Bitcoin as the prime. By understanding the current world phenomenon, it would be easier to answer the question of how secure and reliable cryptology actually is.

INTRODUCTION

To understand the term cryptology we have to go back to 1935, where the term cryptology was first heard of. Cryptology, the practice, and study of techniques for secure communication, concerned with the message / plain text confidentiality, integrity, non-repudiation, and authentication [1]. When dealing with cryptography techniques, always keep in mind that someday, there will be a way to break it. The idea is to find a way to go down with grace. This paper attempts to define the function of cryptography techniques and learn the cryptography capabilities until its being said obsolete and broken.

In the cryptology essence, there are two types of cryptography encryption type, symmetric and asymmetric. The asymmetric cryptography technique, such as RSA that relies on prime factorization is hard to be tempered. It is claimed that even if some of the utility numbers are compromised, the encryption is still intact. However, there is also an algorithm that gives disclosure to a decryption key that attempts to compromise the ciphertext, such as Las Vegas algorithm that provides a quicker factorization to break RSA.

Key size or key length is the size in bits of the key used in a cryptographic algorithm. An algorithm‟s vital length is distinct from its cryptographic security. The security of an algorithm cannot exceed its key length, but it can be smaller. Keys are used to controlling the operation of a cipher so that only the correct key can convert the encrypted text or ciphertext to plaintext. A key should, therefore, be large enough so that an attack on it can take a long time to decrypt.

Nowadays, we extend the number of encryption key digits, naively thinking, that raising key digits takes longer time and more power for attackers to decrypt it. Yes, its allegedly true that there is a super-speed and powerful computer machine that can take care of heavy encryption-decryption algorithm. However, is the existence of it necessarily means that there are no longer hopes for every encryption out there?

Each encryption system has different cryptographic complexity. The actual degree of security achieved overtime varies, as more computer machinery power and more powerful mathematical methods become available. Hence, cryptologists tend to look at algorithms and key length as indicator signs of potential vulnerability and move to longer key size and more difficult algorithm.

THE BITCOIN

What more can cryptography benefit us? It is formally known that the function of the cryptographic system is to secure day to day connections. Whereas the more complex algorithm and the longer secret key means the more secure the cryptography is. One of the useful function of the beauty and the state of the art mathematical functionality of cryptography can be used to create a crypto-currency. By using this case, this paper will elaborate more on how secure cryptography is.

The currency-cryptograph case that will be more elaborated is called Bitcoin. Bitcoin is an open source, peer-to-peer payment network and digital currency introduced in 2009.

Bitcoin has been called a crypto-currency because it uses public-key cryptography for security. Users send payments by broadcasting digitally signed messages that transfer ownership of Bitcoins, which is also the name for the unit currency. A decentralized network of specialized computers verifies and timestamps all transactions using a proof-of-work system.

Bitcoins are digital coins which are not issued by any government, bank, or organization, and rely on cryptographic protocols and a distributed network of users to mint, store, and transfer. Bitcoin itself is the name given to the new digital, internet-based form of currency.

Bitcoin is mostly an imaginary piece of code, with no intrinsic value. Bitcoins are like the rewards for a correct answer to a specific math problem. Both the problem and the answer are entirely unique. There will be a limit of about 21 million of these special solution rewards known as the “BTC.” Hence, the rate of new Bitcoin creation will be halved every four years until there are 21 million BTC. This invented term refers to the form of mathematics that generates the rarity behind the solutions that earn the Bitcoin rewards. Bitcoin is often represented as BTC, or 1 BTC is 1 Bitcoin.

Actually, those users who gain Bitcoin is those hosts that serve as Bitcoin peer and successfully calculate and solve decryption data, thus the rewarded point on this successful attempt called Bitcoin reward. Those users that are trying to accumulate Bitcoin rewarded is called Bitcoin miner. A miner acts like a historian logging and verifying new transactions in the public ledger. As an incentive to update the ledger, the miner receives a predetermined amount of Bitcoin when his block is linked to the Blockchain. Each block is an independent challenge: the first miner to compute the proof gets paid while the rest get nothing and have to start over on a new block. Each miner‟s problem is distinct because it depends on the previous block, outstanding transactions and the unique payment to themselves. Thus, a faster computer does not guarantee victory but does increase the probability of winning.

Since Bitcoin is open-source based, we can see every single line of codes used in Bitcoin transactions. Nobody owns Bitcoin, the most famous client is maintained by a community of open-source developers. It is publicly stated that Bitcoin verifies every transaction with the same state-of-the-art encryption that is used in military and government applications. The entire history of Bitcoin transactions is publicly available. The user of the Bitcoin itself is made anonymous, within the system, users are identified by the public- keys only.

Bitcoins is the example of how a cryptosystem can be beneficial, not only for monetary improvement but also to study how the electronic exchange could grow digitally. This phenomenon could not be done without cryptography involvement. If the cryptosystem is broken, everything will be fallen apart. The cryptographic code for Bitcoin is virtually impossible to crack. That brings all the focus for hackers to use more basic brute force methods of shutting down exchanges and getting Bitcoins. A DDoS is a Distributed-Denial-of- Service attack that sends huge numbers of bot data visitors that overload servers. When an exchange gets hit, inevitably the value of Bitcoins fallen. Hackers would be motivated to get profit from the devalued BTC's. When the exchange gets back up and running, the values of BTC‟s climb and the hackers have their revenues. It is also possible that the hackers simply want to crash the service.

The DDOS attack could be prevented, as long as the main cryptography frame is still secured. After an in-depth investigation of Bitcoin, it's being found that Bitcoin uses no fancy cryptography, its design actually reflects a surprising amount of ingenuity and sophistication natural countermeasure to malware is to split private keys into random shares, using standard threshold cryptography techniques and distribute them onto multiple locations.

Bitcoin is based on public-key cryptography where each transaction is referenced by two keys: the public key that encrypts incoming payments and the private key that decrypts them. These keys are represented by long numbers to make encryption secure against brute-force guessing. Although it is possible to use the same account (public key) for all incoming and outgoing transactions, people who desire anonymity would generate unique public keys for each transaction. They would give out a unique address to receive and store one-time payments from other senders, rather than using a single static address as we do with bank accounts. Otherwise, the public can deduce how much money there is in each address and how the owners spend it by looking at the public history.

Bitcoin shows that a simple, yet robust and secure cryptosystem could be achieved. Now, lets questioned how secure data security out there is, since it is being announced that there is exist such super-computer that could crack any encryption available.

GOVERNMENT SURVEILLANCE PROGRAM

The most significant information leaks in history are associated with the big journalism namely Wikileaks.org. WikiLeaks has combined high-end security technologies with journalism and principles. Like other media outlets conducting investigative journalism, WikiLeaks accept anonymous sources of information. However, one of the WikiLeaks not so anonymous sources is Edward Snowden.

According to NSA Director Keith Alexander, Snowden was a system administrator at the NSA, and it gave him enough security privileges to access data remotely, browse it freely, as well as take it off its home servers and copy it onto portable drives. This is how the information was leaked. A key reason behind Snowden"s success may have been that the data was not very clearly compartmentalized, specialists in one area could easily browse information they would never plausibly need, provided they had the right security clearance. Another advantage is that he manages to successfully social-engineers about 25 login id and password from other personnel.

Snowden reveals that the National Security Agency can infiltrate even the most airtight encryption technologies has done, no matter how theoretically “secure” it may appear to be. As described in top secret documents supplied Snowden, the NSA has spent the better part of a decade and billions of dollars in an all-out war on encryption or “digital scrambling,” targeting popular data-protection technologies such as HTTPS, SSL, and VPN, among others .

This disclosed document reveal that the NSA has been able to crack or circumvent a large part of the encryption technologies that protect sensitive online information such as medical records, proprietary trade secrets, banking systems, and e-commerce transactions. Various encryption technologies such as SSL and HTTPS are commonly used to protect private email accounts, Internet chats, Web searches, and online credit card purchases, but the NSA"s cryptanalysis efforts (utilizing elaborate supercomputers) have managed to bypass practically all of the major security protocols that exist today.

Nowadays, encryption of electronic data is an essential part of modern life. It secures the financial networks link, protects e- commerce systems, stop cellphone calls from being listened to and guards confidential records. Between the claimed state-of- the-art encryption of Bitcoin, which is an active currency exchange that relies on its cryptosystem function, and proof that NSA is indeed owned all cryptosystem ever existed, it leaves us again, is cryptography broken?

Before further discussion, it is necessary to sit back and explain what the definition of is broken that we are going to elaborate. Google adjectively defines broken as “having been fractured or damaged and no longer in one piece or in working order.” Thus, to answer the question above, we have to conquer which side of cryptography that is been fractured, damaged, and no longer in working order.

While it might be true that NSA eavesdrops every communication on the Internet, on one side of the coin, many attackers also trying to penetrate government system. We have to understand why we try to surveil each other. For attackers, the attempt to break encryption may be motivated to against government or any organization. This era motivated to launch an attack with more effective and cheaper methods, such as bt sitting in front of computers and virtually breaking in. It is easier than physically climbing the targeted building. Any authorization entry into telecommunication system or message was considered an intellectual crime. Some do it for the thrill, the others are motivated by money or to become famous [9]. Let's now try to understand the other side of the coin, the part where government surveille on us.

Quoting from Bruce Schneier, the primary way the NSA eavesdrops on Internet communications is thru the network [10]. They have invested in enormous programs to automatically collect and analyze network traffic. The NSA also attacks network devices directly: routers, switches, firewalls, etc. Most of these devices have surveillance capabilities already built in; the trick is to surreptitiously turn them on. This is an especially fruitful avenue of attack; routers are updated less frequently, tend not to have security software installed on them, and are generally ignored as a vulnerability. The NSA also devotes considerable resources to attacking endpoint computers. This kind of thing is done by its Tailored Access Operations (TAO) group. TAO exploits can serve up against the individual computer (whether running Windows, Mac OS, Linux, iOS, or something else) and a variety of tricks to get them on to your computer.

There must be a strong motive why do the NSA decide to have a supercomputer to encrypt all information available. If the NSA wants to get access in to our computer, it'll definitely in. And again, there must be a strong motive why do they need to access an individual endpoint. Anything that requires NSA to attack individual endpoint computers is significantly more costly and risky.

By understanding their motives, it will help to determine whether the cryptosystem out there is no longer secure and what security aspect that already damaged and also which cryptosystem that is no longer in working order.

The NSA's focus on doing surveillance is on citizens safety; they do not exist merely to infringe on personal constitutional rights. A government that takes a purely idealistic approach to the modern world will leave its people totally vulnerable to outside threats. Modern terrorists online are a real risk, through this surveillance it will help NSA recognize and prevent attacks before they even happen, especially after 9/11.

To some people, it is preferable to have „someone‟ listening to a phone call, then having a devastating terrorist attack to happen. Even though it may be an invasion of privacy, the NSA is attempting to help, and the priority is to save lives. As long as there is nothing to hide against the nations, this surveillance should not even matter. Even though the NSA is able to read emails, texts, and other communication, that doesn't mean that they necessarily are.

People need to understand the extent to which the government actually monitors network communication. Digital surveillance focuses on a few data points: if several people appear to be in a network of communication with a known terrorist(s) or criminal(s), then their priority is increased. The data examined is specifically limited to meta data, unless someone is a definite threat. Metadata is very general; it only includes time, duration, and participants in a phone call, or time and recipients/ sender of an email.

Privacy is worth sacrificing for safety. Despite the fact that we all deserve privacy, losing our privacy is not harming anyone. There is a huge difference between NSA collecting and encrypting massive amounts of data and targeting individuals. In order to target a particular citizes as a subject to constitutional protections, a detailed vetting process is employed to establish sufficient probable cause, and these procedures are designed to pass the scrutiny of any U.S. court since the objective would be to eventually prosecute those aiding or abetting terrorist. Collective safety is more important than personal privacy.

People also need to understand that technology has evolved, and so has the crime. Inspecting must do so as well. Ignoring the fact that crimes are set up on the internet is absurd. The motivation is to safeguard the national security, not to sneak around personal lives. Government surveillance is a public service, hence a little infraction of people’s privacy is worth the value of saving lives. People should be more educated on what government surveillance is and how it benefits them.

This surveillance program is constitutional, non-abusive, and necessary to stop terrorism a national security threat. The fourth amendment of the constitution does not outlaw any searches of people, houses, papers, and effects no matter what the warrant. It just states that a search must be warranted by oath or affirmation. This means that NSA surveillance, (which is warranted by FISA court and any other courts to have been brought the case) is constitutional because it is approved by the judicial branch of government. NSA surveillance is not abusive. It is confidential, and even if some small mistakes or errors occur (inevitable in any choice), they are greatly outweighed by the benefits of national security.

COUNTERMEASURES

Most of the motives of the surveillance can safely sum up by saying that its it is providing national security at a minimal risk operation for the greater good. Yes, they do have a state-of- the-art superpower technology that can decrypt any surveillance data they had, but again, with great power comes great responsibility. NSA watches us, but they also being watched. If the NSA can modify the encryption algorithm or drop a Trojan on your computer, all the cryptography in the world doesn't matter at all. But this surveillance is not meant to harm any civilization. Thus, it is not considered as a cybercrime.

Cybercrime is simply a more high-tech version of old real-world" crimes. Any crimes committed to breaking cryptography is an old-fashioned crime to gain any valuables, or in this case, valuable information. Cybercrime is defined as any offense committed using a computing device, personal computer and computer networks, including smartphones [5]. The NSA surveillance is not for terrorism reasons, but for prevention of the cyberespionage and cybercrime reason. If we still would want to remain secure against the network, we need to do our best to ensure that the encryption can operate unimpeded. Below are the Schneier [10] steps on how to hide from NSA:

1. Hide in the network. Implement hidden services. Use Tor to anonymize yourself. Yes, the NSA targets Tor users, but it's work for them. The less obvious you are, the safer you are.
2. Encrypt communications. Use TLS. Use IPsec. Again, while it's true that the NSA targets encrypted connections and it may have explicit exploits against these protocols, we're much better protected than if we communicate in the clear.
3. Assume that while our computer can be compromised. If we have something really important, use an air gap. Schneier methods are to use a brand new computer that has never been connected to the Internet. If he wants to transfer a file, he encrypts the file on the secure computer and walks it over to Internet computer, using a USB stick. To decrypt something, he reverses the process. This might not be bulletproof, but it is pretty good.
4. Be suspicious of commercial encryption software, especially from large vendors. Schneier assumes that most encryption products from large US companies have NSA- friendly back doors, and many foreign ones probably do as well. It is prudent to assume that foreign products also have foreign-installed backdoors. Closed-source software is easier for the NSA to backdoor than open-source software. Systems relying on master secrets are vulnerable to the NSA, through either legal or more clandestine means.
5. Try to use public-domain encryption that has to be compatible with other implementations. For example, it is harder for the NSA to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving the NSA a lot more freedom to make changes. Moreover, because BitLocker is proprietary, it is far less likely those changes will be discovered. Prefer symmetric cryptography over public-key cryptography. Prefer conventional discrete- log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can.

NSA has turned the fabric of the Internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defense is to make surveillance of us as expensive as possible. A piece of advice from Schneier is to trust the math. Mathematicians build a range for strong encryption method. They are varied so people can choose the encryption that suits their needs. Encryption is our friend. Use it well, and to do our best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA.

CONCLUSION

Ensuring a strong cryptographic system is certainly not an easy task. Still, it is something that everyone has probably aimed to achieve as he or she wants to protect his or her information against newly launched attacks for a safer information system. This article has shown an understanding of the available cryptosystems currently functions. Bitcoin shows how a cryptosystem is becoming a reliable medium for new digital currencies, whereas the arguably broken cryptosystems are indeed existed but not without any countermeasures. It is therefore important to understand from whom we need to protect our information against with. The current commercial cryptosystem still provides secured encryption to asses our necessities.

REFERENCES

Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A., Handbook of Applied Cryptography ISBN 0-8493-8523-7

Garret, J. Making, Breaking Codes: An Introduction to Cryptology. Prentic-Hall, Inc. The United

States of America. 2001.

Davis, J. "The Crypto-Currency". The New Yorker, November 2013.

Brito, J., Castillo, A. Bitcoin: A Primer for Policymakers. Mercatus Center. George Mason University, October 2013.

Dorit, R., Shamir, A. "Quantitative Analysis of the Full Bitcoin Transaction Graph". Cryptology ePrint Archive, October 2012.

Forrester, D., Solomon, M. Bitcoin Explained: Today's Complete Guide to Tomorrow's Currency, Kindle, 2013.

Reid, F.; Harrigan, M., "An Analysis of Anonymity in the Bitcoin System," Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) , vol., no., pp.1318,1326, 9-11 Oct. 2011 doi: 10.1109/PASSAT/SocialCom.2011.79

Pentago, C. NSA Supercomputers Crack a Variety of Common Encryption Technologies, October 2013 retrieved from http://www.news24.com/MyNews24/NSA-Supercomputers-Crack-a-Variety-of-Common-Encryption-Technologies-20130930

Warren, P., Streeter, M. "Cyber Crime & Warfare: All That Matters", McGraw-Hill, US, 2013

Schneier, B. Schneier on Security: A blog covering security and security technology. Retrieved from: https://www.schneier.com/blog/archives/2013/09/how_to_remain_s.html Sept., 2013.