Sentinel Protocol

Security Intelligence Platform for Blockchain

Abstract

The rapid development of computer technology in the 21st century has led to the manifestation of sophisticated and intelligent threats that hinder further innovation. While the essence of cryptocurrency is decentralization, this has also become its greatest weakness. As the decentralized cryptocurrency system lacks a threat defense system, the burden for security has thus far been placed squarely upon the shoulders of individuals and corporations. Sentinel Protocol overcomes the disadvantage of decentralization by turning it into an advantage for security. By utilizing a collective intelligence system created through harnessing the power of decentralization, Sentinel Protocol combines cryptographic functions and intelligence-based threat analysis algorithms to create a secure, innovative ecosystem.

Uppsala Foundation

2018.03.28

Chapter 1

Introduction

Decentralization, which is at the heart of cryptocurrency technology and works as its ideology, involves both innovation as well as innate anxiety. The cause of both is autonomy. Autonomy based on anonymity can only be achieved with great responsibility imposed on the system. When faced with reality, the side effects based on said autonomy are the most evident in countless cybercrime cases. In addition, a fundamental defense system to protect against such cybercrime has not yet been built.

There are three main security issues facing the average cryptocurrency user: The first problem is that ordinary users are exposed to hacks far too easily. The second problem is that while attackers can often identify us, we cannot easily identify them. Lastly, the damage such attackers inflict upon us is our responsibility. How can we solve these fundamental problems? In the end, the responsibility lies with us all. However, everyone acting individually will not be able to provide a solution to the issue of cryptocurrency security. Instead, we must utilize our collective intelligence to act together in our mutual self-interest through a decentralized cyber security ecosystem. Our decentralized AI system detects unknown patterns of the attacker(s), disseminates the information throughout the ecosystem, and protects all members through collective intelligence, while maintaining the fundamental autonomy of decentralization.

Chapter 2

Statement of Problem

Generally, the difference in defense level against security threats between individual users and business users is a simple one. How much budget do you have to invest in technology and human resources? For added objectivity, examine at the IT Security Spending Trends [1] published by the SANS Institute. In 2016, financial institutions typically spent the most on IT security, averaging from 10-12% of their annual budgets of $500,000-$1Mil. Government agencies came in at second place, spending between 7-9% of their annual budgets ranging from $1Mil-$10Mil. Other industries, such as education and healthcare, spent less, but are still increasing their annual IT security spending at a steady rate. A report from Cybersecurity Ventures[2] predicted that the cybersecurity market size will grow by $1 trillion (US) from 2017 to 2021, as the constantly increasing number of cybercrimes have already exceeded the critical level.

Take a look at the means to which end-users must go in order to defend themselves, while corporate users are protected by numerous security solutions and professionals. Unfortunately, at best, you cannot get away with using poor quality security software, inferior hardware, or a having a personal lack of expertise. As blockchain technology has evolved, various scams and cybercrimes have also developed. One of the most well-known fields of cybercrime is ransomware, a new type of cybercrime that takes the user's data hostage and demands monetary compensation via bitcoin in exchange for the release of the user's data. It is expected that the ransomware "market" will expand to $17.36 billion by 2021. Perhaps here, bitcoin is undergoing an ironic situation where its monetary value is most significantly used through cybercrime as currency of choice for cyber criminals

The DAO case of 2016 was the first major security vulnerability incident of the blockchain age, which exposed about 15% of the total Ethereum to hackers due to attacks on code vulnerabilities. As a result, tens of thousands of investors suffered financial loss. The only means of solving this problem was the implementation of the "hard fork"[3], which violated the philosophical beliefs of blockchain immutability. At the root of this recent catastrophe rests the unflinching difficulty of decentralization, combined with the strong autonomy that has gone hand in hand with individual responsibility for so long.

Chapter 3

Security of Decentralization

Nowadays, everyone has at least one email address. It is impossible to imagine a business card without an email. However, this common necessity of our modern lives also presents a vulnerability. Consider the phishing email, in which malicious macros are inserted into attached document files such *.doc, *.xls, *.ppt, etc., which then infect the user when he or she opens the infected document file, or clicks on attached links. In July 2017, a major Korean cryptocurrency exchange, Bithumb, was hacked, and the confidential information of 31,000 customers and companies was stolen, just by the opening of one infected file. The perpetrator of this phishing attack has yet to be identified.

Phishing is not limited to email. In the case of telephone phishing, there are a variety of fraudulent methods that have tricked many individuals into giving up their personal information over the telephone to a criminal pretending to be the operator of the cryptocurrency exchange. For example, a hacker may pretend to be an administrator, claiming that the user's account has been hacked. In this case the hacker will claim that as the administrator, he needs the user's personal information to reset the password of the account in order to stop the hacking. Through manipulation and exploitation of the psychological weaknesses of the user, the hacker gains access to the account.

Another type of bitcoin related hacking can occur during the Initial Coin Offering (ICO), by creating a fake ICO fundraising site and giving false information, by hacking the fundraising address and replacing it with the address of the hacker.

The key to these various hacks is that they occur because victims are easy to target due to the open nature of the internet. The ideology of decentralization is central to both cryptocurrency and the internet, but it is impossible to say that blockchain implements perfect autonomy. Autonomy in openness is subject to individual responsibility. Decentralization is not a magical solution to all problems, and we do not live in a fantasy world in which the only actors on the internet act with the best of intentions. We need to face reality. Bad actors are taking aim at this place, and the ideology of decentralization must develop a philosophy of security.

Chapter 4

Reputation System on Blockchain

At the root of bitcoin lies the blockchain[4], a complete peer-to-peer system that does not require the control of a central agency, but which is completed using a consensus algorithm, through which the remittance of electronic money is completed within a network without mutual trust. In the process of settlement, there is the rule of the distributor that all records are shared; however, commercialization of realistic financial products is difficult in terms of information disclosure of sensitive personal property apart from the technical aspects. On the other hand, without a guarantee of real identity, we cannot take part in a variety of financial services, and as time goes by, the rules and regulations become even stronger. One alternative is the consortium blockchain, although it still does not make the most of the benefits of public decentralization.

The fundamental question of what the best solution to inherit the advantages of public decentralization is this: If the information is fully disclosed and accumulated, does it become more valuable or less valuable?

If a blockchain-based reputation system and information related to cybercrimes that are currently occurring are all shared within a blockchain distributed policy, then the decentralized nature of the blockchain will protect the majority system. The biggest problem in operating within existing reputation systems is manipulation and destruction of information. When an individual or group with malicious intent manipulates the reputation of an organization or system, or hacks a blockchain-based system to manipulate its recorded reputation, the latter case is the part that is naturally resolved by the advantage of the data integrity of the blockchain. However, in a reputation system scoring the quality of information rather than a transaction, an attack such as a Sybil attack cannot be easily defeated by the basic characteristics of the blockchain, because of the subjective nature of the pre-manipulated information which allows it to be recorded, despite the transaction reputation. This part, however, makes it possible to solve through the power of collective intelligence.

Chapter 5

Collective Intelligence

While the reputation of information related to cybercrimes has been combined with the blockchain, it has the advantage of being able to prevent and protect many imitative crimes due to the shared economic principles of the data, but more importantly, the cybercrime investigation framework can be completed. For example, there is a prejudice that cybercriminals targeting cryptocurrency cannot grasp users' information due to their autonomy. But this is incorrect.

Essentially, the blockchain is a system that shares information transparently. All transactions are recorded in a distributed ledger, and can be verified without special permission. This means that it is possible to trace these transactions. In fact, the flow of cryptocurrency transactions that has been hijacked by cybercrime is easily traceable. Ironically, however, the most common way to avoid that trail is via money laundering using cryptocurrency exchanges and coin shift systems. If you do not exchange money, you lose the cash value of the coin. A virtuous cycle occurs, because there is an exchange. The same applies to autonomous transaction coins, such as Dash, Zcash, and Monero, that hide transaction information, as eventually they need an exchange to cash out in order to enhance traceability through the Interactive Cooperative Framework associated with transaction analysis projects such as BlockSci.[6]

It is not impossible to cooperate with the cryptocurrency exchanges in relation to cybercrime. They are also striving to protect users in strict regulations; therefore, most cryptocurrency exchanges require that they meet the provision that they cannot cooperate without the consent of the police or government investigative agencies in order to meet the basic obligation to protect the confidentiality of the users. However, cryptocurrency regulation is different between countries around the world, and it is almost impossible to receive help from experts who have expertise in cryptocurrency in local investigative agencies. Even worse, most countries do not treat cybercrimes that are related to cryptocurrency as a real financial crime. In the end, it is a reality that only good people who are not protected by the legal system will suffer financial loss.

It is the blockchain itself that contains information regarding all the existing, occurring, and suspicious cybercrimes in an immutable database that can fill this enormous hole in the current legal system that serves an obstacle to a decentralized investigation system. All information can be made instantly transparent to the individuals, exchanges, projects, security firms, governments, etc., and most importantly, it can be tracked within one system by all people around the world. A reputation system that is managed by collective intelligence also means simplicity. This means that exchanges can refer to this system and take the proactive action of trusting the system's reputation without the requirement for complex legal evidence which previously has given users a sense of helplessness. This can prevent and control the many cybercrimes that occur within the cryptocurrency industries. People or institutions that have been thoroughly verified, qualified, and certified by a majority of experts will be authorized to update the results of the investigation.

Chapter 6

Artificial Intelligence

The mechanism of artificial intelligence is simply to model a large quantity of good quality data using an optimized algorithm. Attackers often employ intelligent use of an unexpected number of attacks to exploit system vulnerabilities over long periods of time when targeting an individual, group, government, business, or organization. Thereafter, a command and control communication channel is established with the hacker's external command tower. It is not so easy to grasp the behavior of an attacker who has already successfully entered an internal network. Most existing security technologies do not have a way to doubt the behavior of a seemingly legitimate entity in making an exact binary representation of an attack as a signature. For this reason, many attacks are perceived as normal users' daily patterns.

Let us consider for a moment, the grasshopper and the hairworm. Hairworms infect grasshoppers and other insects which reside on dry land, even though hairworms must reproduce in a wetland environment. An infected grasshopper looks, and initially acts, no different than any other grasshopper. However, after the hairworm is ready to reproduce, the grasshopper's behavior begins to change. Through secretion of chemicals, the hairworm takes control of the grasshopper's mind, causing it to seek out water, and – in effect – commit suicide by drowning. Thus, the hairworm can emerge and begin the next stage of its life cycle.

The key to machine learning security technology is to keep track of changes in behaviors, not changes in the appearance. Think about the grasshopper. While the hairworm controls the grasshopper's brain, the grasshopper will behave outside of the normal range of its typical activities, including aberrant behavior such as seeking out wetlands, even though externally it appears normal and healthy. This unusual behavior can enable entomologists to detect infected grasshoppers by observation alone. Similarly, if we compare the correlation of changes in minor behaviors rather than the changes in appearance, even if nothing specific has gone wrong, this can allow us to recognize the empirical risks in advance, and provide a high probability of disaster prevention.

There are two ways that Sentinel Protocol can use the blockchain and artificial intelligence together. The first is the machine learning-based blockchain security client wallet that collects a user's or node's information and creates model behaviors of all the aspects, such as normal activities of your computer usage patterns, including transaction patterns. When suspicious behavior occurs, the security wallet recognizes the probability of threat, and blocks the execution of the process. Detailed information is reported to the collective intelligence group, and shared with the reputation system. All information is shared through the API to everyone who would like to use it, and it is extended to the most accurate and secure global intelligence system in the world.

The second is to construct a Fraud Detection System (FDS) using data from the blockchain. Essentially, Sentinel Protocol's anomaly detection is associated with a consensus system. The collective intelligence group or individuals who are certified by a majority of experts (or initially by the Uppsala Foundation during the early stages of SIPB), acts as an "International Cybercrime Police

Force" known as The Sentinels. They are responsible for research and analysis, and have special authority to update their reputation system. They receive rewards through Sentinel Protocol's shared economy system. To prevent insider threats, the Fraud Detection System (FDS) is installed to monitor and detect abnormal behavior for collective intelligence as well as ordinary users' abnormal transactions.

Chapter 7

Security Features

Security Intelligence Platform for Blockchain (SIPB, or Sentinel Protocol) has the following unique security features:

- Threat reputation database (TRDB)
- Machine learning (ML) engine integrated security wallet (S-Wallet)
- Distributed malware analysis sandbox (D-Sandbox)

Threat reputation database (TRDB)

Threat reputation database (TRDB) can tackle two problems lied in existing cybersecurity industry. The first problem is centralized database of the security firms. Keeping threat information on one centralized place makes it vulnerable to information manipulation and abuse. The database becomes an obvious target of Sybil attack, or server hacking and service interruption. This is a fundamental problem of the centralized 'client-server' model of the Internet. In October 2017, for example, Russian state hackers stole NSA materials using the well-known antivirus company Kaspersky's antivirus software. Basically, hackers used the security tools to find vulnerabilities of the target. The decentralized nature of blockchain can mitigate such issue as its immutability makes it difficult to tamper with the data. This increases the security stability of the server that provides the data.

Another problem is the lack of shared knowledge among security vendors. The greater the collected risk information, the higher the chance of preventing cyber crimes. However, each security vendor compiles threat information on its own as if it is the winner takes it all game, since there's no incentive for vendors to collaborate and create one comprehensive database. Anton Chuvakin, research VP at Gartner once said that, "It is truly maddening to see examples of bad guys sharing data, tricks, methods and good guys having no effective way of doing it." It is the ordinary people who pays this huge inefficiency. Good will alone doesn't scale, so TRDB uses incentive scheme which is explained in chapter 11. Security experts and vendors are encouraged to contribute to building the threat database under the consensus mechanism and feedback from participants, or Delegated Proof of Stake (DPOS). Through collective intelligence, TRDB can most efficiently and effectively collect hacker's wallet address, malicious URI, phishing address, malware hashes, just to name a few.

TRDB is only updated by security experts in order to eliminate the systematic errors such as false positives. General users can also participate, however, using two methods: auto reporting and manual reporting. If users allow auto reporting, unknown threats that are automatically detected from the machine learning-based security wallet go into the database. Through manual reporting user can report risk information which will be validated by the community afterwards. TRDB will be provided as an API, so any individual or organization (e.g. cryptocurrency wallet projects, cryptocurrency exchanges, and security vendors) can make use of the information.

Machine learning engine integrated security wallet (S-Wallet)

S-Wallet has the functionality of antivirus software. However, the fundamental difference is that antivirus software is best able to respond to new threats only by receiving the latest updates via a centralized server for all new known signatures. This approach is difficult to respond to unknown threats such as zero-day attacks. On the other hand, S-wallet analyzes the threat tendency and history to proactively respond to unknown threats or zero-day attacks. Thus, S-Wallet does not need signature updates. This unsupervised learning approach is especially effective against threats like ransomware.[7] While S-wallet leverages collective intelligence from connected TRDB, it provides basic blocking services for the following information:

- Cryptocurrency wallet address filtering
- URL/URI filtering
- Data filtering
- Fraud Detection System

It is important to understand that the machine learning technology enables the Fraud Detection System (FDS) on all distributed ledgers and identifies transactions that are reported for misuse or stolen, thereby preventing the secondary damage.

Distributed malware analysis sandbox (D-Sandbox)

Sandbox is a security mechanism to run untested or unverified programs and code on a separate virtual machine without risking the application or host. D-Sandbox is where potential threat is submitted via a ticket system and analyzed through collective intelligence.

D-Sandbox has two outstanding advantages. First, it is significantly cost effective. It guarantees infinite scaling through distributed systems. A security appliance with regular sandbox has been bounded by the capability of running virtual machines. Even the high-cost security appliances were very limited in analyzing malware this way. Also, the regular sandbox system was highly unstable as it could not guarantee high capability such as high throughput, high bandwidth, higher usage than expected. This often led to system performance degradation and malfunctioning, which not only harmed the user experience but also resulted malware infection in the end.

Second advantage is that while D-Sandbox can solve the waste of computing power in Proof of Work (PoW), it can also build a better security ecosystem. Indeed, the computing power to generate the hash value is a waste. The nodes participating in Sentinel Protocol's network can use their computing power to analyze malware additionally. After all, the advantage of a decentralized system is that idle resources can be utilized where they are needed. Individual users will be of help by provisioning the sandbox through a virtual machine, boosting the overall security ecosystem.

Chapter 8

Sentinel Protocol Ecosystem

The following describes use-cases in the ecosystem of the Security Intelligence Platform for Blockchain (SIPB, or Sentinel Protocol):

Interactive Cooperation Framework (ICF, or Sentinel Portal)

One of the biggest obstacles to business continuity in the cryptocurrency industry is security. Customer hacking incidents and their related costs have tremendously increased recently but appropriate security measures have not taken place yet. It is difficult to cover all security elements if the industry is growing so rapidly, but it should not be the excuse. Some crypto exchange platforms lack security expertise from the initial system design to the full operation. Customer service specialists cannot be the cybersecurity specialists but they are certainly doing the double-duty as of now. Sentinel Protocol overcomes this problem by providing an essential framework that runs by trusted cryptocurrency security experts and their collective intelligence. Just by joining the Sentinel Protocol community, crypto users can easily obtain knowledge and assistance on all security issues. They can also deploy security solutions provided by the Sentinel Protocol. Inefficiency costs will be reduced to businesses and individuals alike. This framework will enhance the overall security of the crypto world and flourishes on the fundamental principle of decentralization.

A beta release will be announced at https://www.sentinelprotocol.io

Anti-theft system

While more real world applications for cryptocurrency are built every day, there is no system to validate the integrity of the crypto assets. This means even the stolen crypto assets can be abused as a payment for commercial services as long as the hacker splits them through tumbling and mixing. Just like in the real world where card companies block the use of stolen credit/debit card, Sentinel Protocol will track all the stolen cryptocurrencies and share this information to any crypto service provider. Then, stolen crypto assets cannot be used or converted to fiat money. This protection scheme will keep cryptocurrency under regulatory constraints.

Malformed transaction prevention

Addresses registered as scams, and all derived addresses, will be shared within Sentinel Protocol community in real time thanks to the nature of blockchain. As long as Sentinel Protocol is applied, further spread of damage can be prevented. One of the applicable uses is during ICOs, where thousands of people are involved for a short period of time and address could be tampered. Even if hacker changes the address, all users are automatically notified for the original abnormal address and newly changed addresses. This can totally change the security industry paradigm since

there was no solidified platform that could act like this before. There was no systematic method to prevent thousands of individual users to get notified of an attack and prevent the damage spread all at the same time.

Unknown Threat Prevention (User Scenario)

Hacker Malloy uploads a software into a well-known cryptocurrency online community. He made this software to be undetectable by reputable threat-checking website such as VirusTotal or anti-virus programs. Dozens of community users including Alice downloads this seemingly mining software. (Unfortunately, most users do not know how to check the integrity of an original file via md5, sha, etc.). Once Malloy notices that his miner (backdoor) is downloaded, he replaces it with the clean, normal file. By then, the first mining software (backdoor) user has already been compromised and all information is collected by Malloy--both the passphrase of the private key of the wallet and the credential of the cryptocurrency exchange have been stolen. However, it is difficult to ascertain how the system was compromised, as Alice – a mere ordinary user – does not have any of the necessary investigative skills or tools to investigate this cybercrime.

Meanwhile, the same online community user Bob uses Sentinel Protocol's security wallet. Bob also downloads the corrupted mining software. However, the machine learning engine within S-Wallet detects that the file is highly suspicious. The engine blocks the execution, even if the file hasn't been labeled as known attack and it hadn't been detected by any antivirus software thus far. As soon as the file execution is blocked, corresponding information is automatically submitted to Sentinel Protocol. Then, The Sentinels, the group of trusted security experts, analyzes the root cause of the threat. This analyzed information is registered in the Threat Reputation Database (TRDB) and also reported to the online community where the file was originally found. Through more detailed analysis of the timestamp and the uploader, Malloy is identified as the hacker. Meanwhile, Malloy realizes that he cannot distribute his mining software elsewhere, since real-time defense systems of the Sentinel Protocol database is employed everywhere.

Transaction traceability (User Scenario)

Hacker Malloy has a wallet of seized coins which he hacked from many people. Prior to cashing, he distributes coins on a number of sub-addresses to avoid tracing. This is possible due to the nature of the cryptocurrency wallet. Alice is one of Malloy's victims. As soon as Alice finds out her coins are stolen, she reports it to Sentinel Protocol. The Sentinels, a group of trusted security experts, confirms the incident, and registers the case information into the Threat Reputation Database (TRDB). Sentinel Protocol will automatically track all sub-addresses derived from the original addresses registered. This will be shared to all crypto services including the exchanges that have integrated Sentinel Protocol. If Malloy tries conversion, the exchange system that has already been notified receives a high priority alarm, and it will cut off any chance for hacker Malloy to make use of the seized coins. It won't be easy for Alice to have the coins back, since current judicial systems across international border doesn't help her much if she lives in Europe while the cryptocurrency exchange is based in the States. Alice starts to actively promote her case and the advantage of using Sentinel Protocol in the hope of Sentinel Protocol having greater presence

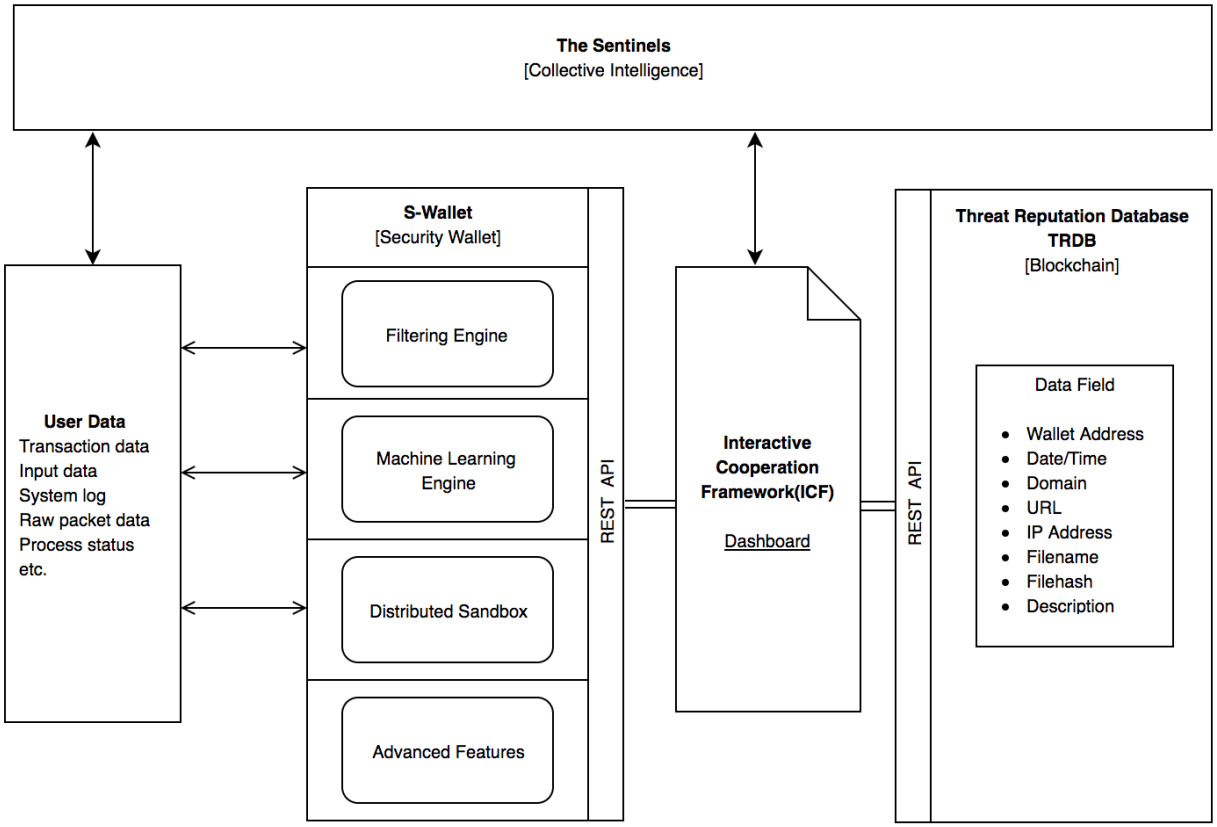
worldwide. One day, Sentinel Protocol becomes as much influential as to replace the complex documentation and legal identity verification required by the Interpol to report hacking.

Chapter 9

Architecture

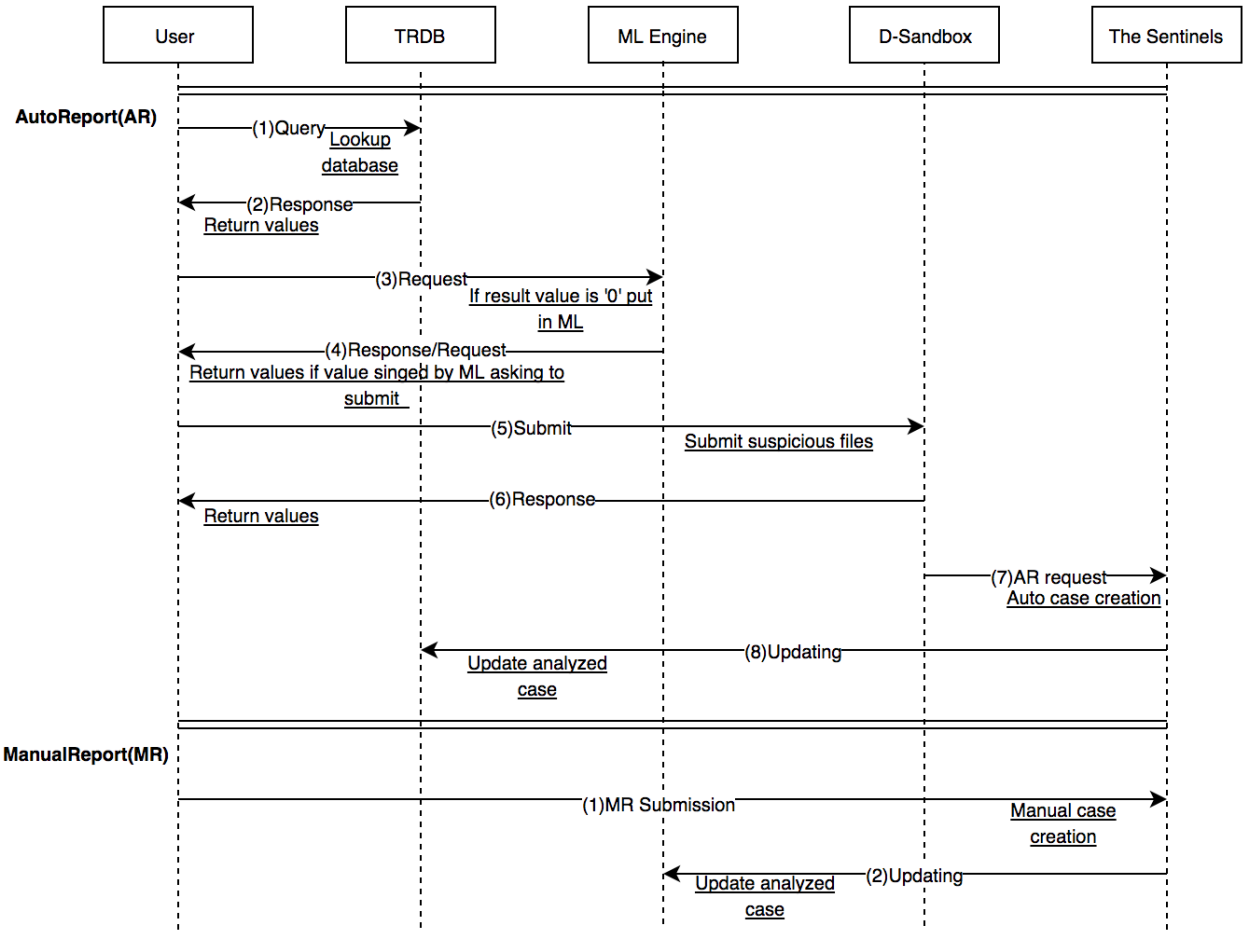
Sentinel Protocol will provide all security services through its integrated security wallet. However, each part is designed to enable third party interworking through API. Basically, the integrated security wallet is implemented through two functions: ‘Auto Reporting" and ‘Manual Reporting.’

[Technology Architecture: Security Intelligence Platform for Blockchain]



- S-Wallet: Integrated security wallet
- User Data: User input, transaction data, system logs, and packet data
- Filtering Engine: Cryptocurrency address filtering, scam related domain, URL, IP and file filtering
- Machine Learning Engine: Local machine learning engine for behavior analysis
- Distributed Sandbox: Distributed malware analysis sandbox
- Threat Reputation DB: Intelligence DB containing cybercrime information
- Plugin Features: In future, more enhanced security functions will be added, such as VPN, Integrated with 3rd cryptocurrency wallet
- The Sentinels: Certified and qualified collective intelligence group and individuals
- Interactive Cooperation Framework (ICF): Sentinel Portal, which is the dashboard for The Sentinels and public user activities such as root cause analysis, incident response, and statistics of worldwide activities.

[Security Intelligence Platform for Blockchain (SIPB) Process Flow]



If a domain, url, cryptocurrency wallet address, file download, etc., are attempted through a link or redirection during execution of a security wallet, the following occurs:

Auto Report (AR)

The auto report is an intelligence framework to optimize the analysis of unknown threat.

1) Query: asks Threat DB to research potential scam/harm of reported information
2) Response: Threat DB provides data field of information that has been registered
3) Request: If queried address is identified as scam/harm, it will be simply blocked. Even if it's not identified as something new, files are downloaded, and a new process is started asking the ML engine to analyze it
4) Response/request: The ML engine analyzes suspicious behavior of files or processes and blocks as unknown threat(s), and asks the user whether to report this information or not.
5) Submit: If user has enabled the submit option (optional on/off), the information goes to a distributed sandbox for sandboxing
6) AR request: An auto reporting case is created and shared to the ICF dashboard
7) Analysis response: The Sentinels analyze the unknown threat using a sandbox or additional tools
8) Updating: Updated threat information is sent to the Threat DB

Manual Report (MR)

The user can also manually report scam information.

1) MR Submission: Domain, url, and scam address and files of any suspicious information can be reported directly to The Sentinels.
2) Updating: After verification of the scam information, updated information is sent to the Threat DB.

Chapter 10

Consensus

The basic mechanism of Proof of Work (PoW) gives the right to block generation and its corresponding benefits when the results reach an approximation of the given target difficulty through mining. The process of finding the results requires extensive computational work that involve trial and error, so it is difficult for all but a few to achieve it. Therefore, the person who has gone through these difficult processes may become a delegate to represent the majority. The problem is that the massive waste of electricity in the process of finding this delegate is inefficient. As a result, people have come across other methods of improving consensus. Subsequently, an ideal algorithm was created, which is Proof of Stake (PoS), that increases the probability of delegation by amount of stake hold. However, the limitations of the system delegated by the two algorithms are not 100% free from the 51% attack, as the delegator cannot distinguish between good intentions and malicious intentions of majority.

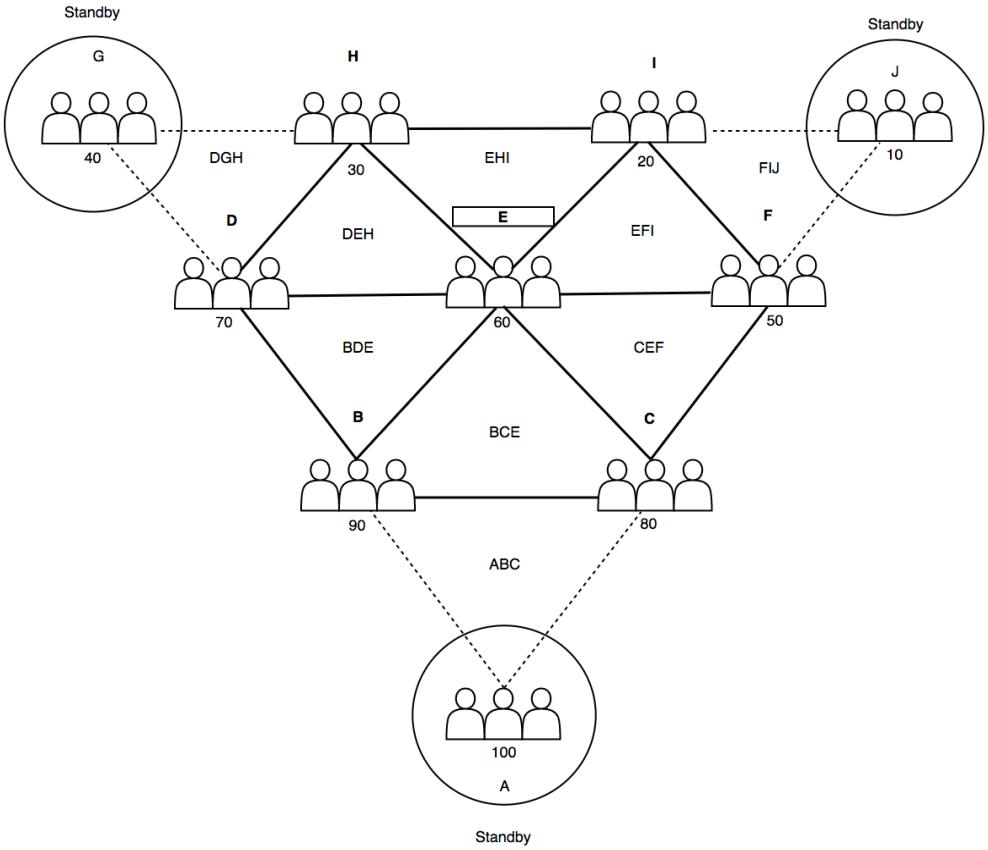
The consensus of Sentinel Protocol essentially uses the idea of the Delegated Proof of Stake (DPoS)[8], introduced from BitShares invented by Daniel Larimer. The Sentinels, delegated by the Uppsala Foundation, are a group of proven institutions or individuals with the necessary qualifications, such as the security team at the cryptocurrency exchanges, global cyber security research firms, or group of white hackers or individual white hackers; all of them are experts who have proven their status and experience. In reality, the risk is dramatically reduced and thus consensus is optimized. However, the gap between the social engineering viewpoint and the algorithm is undeniable, as mentioned above. In order to solve this problem, the score of reputation is separated by another share, Sentinel Point (SP), where UPP is the circulation currency. Sentinel Points can only be obtained by acting as a member of The Sentinels. For example, it analyzes the cases registered with AP and MP, records the relevant information in the Threat database, and then, based on the data, many ecosystems of various industries receive help. Another way is that based on their performance, people can actually vote on their reputation. The system that is delegated by obtaining a reputation score, defined as the Proof of Protection (PoP) in Sentinel Protocol. If a dishonest Sentinel Protocol's actions intend harm, such as a Sybil attack or forking a chain, he will lose his reputation score as a punishment. As with the slasher of Ethereum[9], this eliminates the "nothing at stake" issue, as representatives are threatened with loss of both reputation and qualification.

The advantage of the reputation system, especially this structure, is that it is almost impossible to become a bad actor, as individuals are representatives of trust in their professional field. Technically, in this trust structure, a large number of delegated Sentinels are unnecessary; that would only serve to increase randomness for securing consensus and add unnecessary delay. Therefore, the consensus structure of Sentinel Protocol has small group only of only seven Sentinels charged with validation of transactions, generating blocks, and updating the Threat database. According to the reputation ranking, a total ten Sentinels are chosen, with seven designated as Active while three are designated as Standby. The three Sentinels will remain in Standby, unless needed to reduce network latency and delays. The PoP synchronous algorithm and asynchronous

Byzantine Fault Tolerance (BFT)[10] are supported as redundant consensus algorithms in case of significant network fragment, massive DDOS attack, or other unexpected event causing the majority of The Sentinels to lose communications with each other.

Sentinel Protocol's Proof of Protection (PoP) is to designed to be simple and efficient in terms of latency, scalability and reliability.

[High Level Consensus Diagram]



- 10 delegated reputation Sentinels form the inverted pyramid structure shown above
- The group of people in the diagram represents The Sentinels (individual or organizational)
- The score underneath each group of people shows the Sentinel Points earned by their contribution
- A, G, and J correspond to each of the three endpoints that become Standby
- Nodes in hexagon are randomly granted a block generation
- The small triangle structure is intended to tag the smallest multicast groups to minimize broadcast for efficiency
- Minimized consensus process seven fixed nodes.
- In case of BFT implemented for 'n = 3f + 1' structure, up to 10 nodes can be operated with three Standby and E becomes Master.
- Standby charged with Denial of Service (DoS) resistance as well as high availability the nodes A, G, and J perform backup of the peer node. (For stabilized consensus, The Sentinels build a robust network security environment but cannot be completely free from attacks such as DDoS.)

Chapter 11

Incentive System

Sentinel Protocol aims to create a self-sustaining cyber security ecosystem in a moderate timeframe without requiring centralized guidance or organization. An effective cyber security ecosystem requires an exchangeable cryptocurrency as a direct means to compensate for the usage of goods or services; also, it requires an independent value which represents an individual's subjective contribution to improve the cybersecurity ecosystem. Thus, Sentinel Protocol has a circulating cryptocurrency named UPP (Uppsala) for the use of the goods and services provided by Security Intelligence Platform for Blockchain (SIPB) and SP (Sentinel Points) for the staking value of The Sentinel Protocol's reputation.

Early contributors will receive greater incentives; once Sentinel Protocol reaches a certain level of intelligence or timeframe, an automatic reduction of UPP rewards for relatively similar contributions will be implemented to benefit early contributors. This incentive system is designed to encourage both the ones who need help from cyber security experts, as well as those experts (either individuals or organizations) to participate.

[UPP (Uppsala)]

- UPP is a currency for goods and services provided by SIPB, such as the advanced security features of the security wallet
- UPP also can be used in a case opened for detailed cyber forensic service, consultancy, vulnerability assessment, and/or other activities requiring The Sentinel Protocols' help
- Usage fees can be collected in a smart contract by a DEX (decentralized exchange) platform such as Kyber Network
- Initially 500,000,000 UPP will be generated and distributed for the early stage cybersecurity community builders
- Throughout 20 time-vestings, additional UPP will be generated; following the inflation ratio described below, and distributed to contributors who make Sentinel Protocol a better place by Proof of Protection
- To incentivize the early participants or early Sentinels, the initial inflation ratio will be set between 3~7%, then each logarithmic decrement percentage will be reduced as the round goes until reaching (near) 0% inflation ratio
- 30% of UPP revenue by advanced feature usage fee, case processing fee, and/or future development by the Foundation will be also vested together with inflation UPP as a reward to community contributors
- Each round of vesting is executed when total generated Sentinel Point hits a target value or certain weeks of timeframe; whichever comes sooner. Detailed scheme will be officially announced
- 15% of initial UPP will be reserved for Uppsala Foundation
- 15% of initial UPP will be reserved for business development, development funds, legal funds, advisory incentives, other organizational activities requiring funds, etc.
- 2% of initial UPP will be reserved for advisory incentives
- 8% of initial UPP will be reserved for any unforeseen business activities
- The remainder of UPP (60% of initial UPP) will be distributed in the market for Sentinel Protocol early contributors, users, contributors, supporters, etc.
- Initial UPP exchange ratio will be available on the official homepage

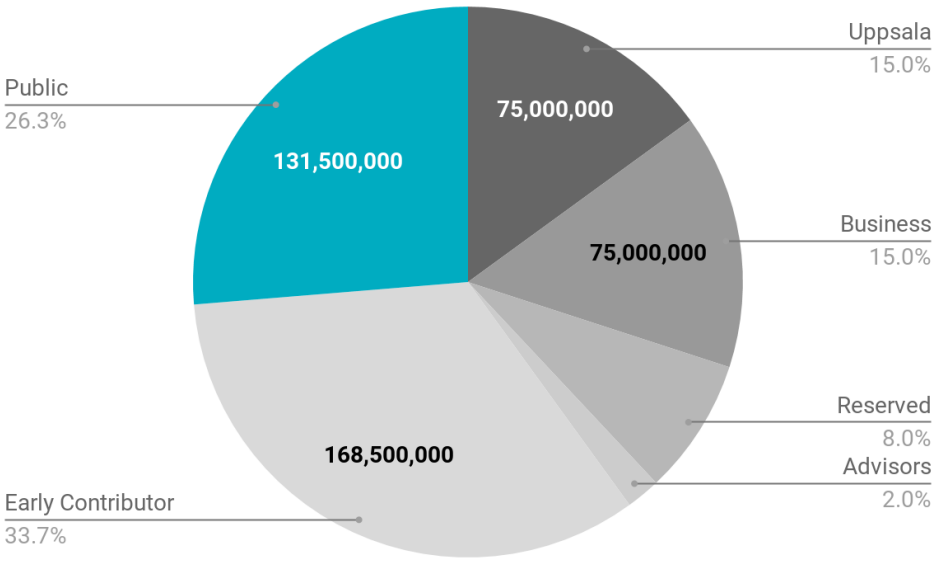
[Sentinel Point]

- Can only be acquired by PoP (Proof of Protection)
- Proof of Protection consists of various cybersecurity activities including: reporting a true scammer's address, IP, website, validating reports, resolving incident cases, etc.
- Legitimate report validation is done by The Sentinels
- S-Wallet holders can do PoP by D-Sandboxing computation
- Other indirect contribution for the Sentinel Protocol community includes: generating articles to enlighten the public on issues of cybersecurity or translating articles to other languages
- The Sentinels obtain Sentinel Points according to the report analysis and the user's reputation vote
- Sentinel Point holders will have the vesting benefit of UPP generation described above. Vesting amount will be proportional to the Sentinel Points each entity holds relative to the total Sentinel Points generated via Proof of Protection done for the community. Automated exchange process could be applied.

[Initial UPP Distribution Scheme]

Rounds	Number of UPP	Remark
Uppsala Foundation	75,000,000 (15% of Initial UPP)	-
Business Development	75,000,000 (15% of Initial UPP)	-
Reserved Allocation	40,000,000 (8% of Initial UPP)	-
Advisors	10,000,000 (2% of Initial UPP)	-
Early Contributor	168,500,000 (33.7% of Initial UPP)	-
Public Contributor	131,500,000 (26.3% of Initial UPP)	April ~ May 2018

[Initial UPP Allocation]



Chapter 12

Roadmap

At the same time as the establishment of the Uppsala Foundation, the following activities take place:

Phase 1 – Sentinel Protocol of The Cryptocurrency World

18 Jan	HQ R&D center open in Singapore, APAC
	HQ R&D center security researchers integrate cybercrime, scam information existing in history, indexing into blockchain scheme Threat Reputation Database (TRDB)
	Regional R&D center developing Interactive Cooperation Framework (ICF) interface
18 Feb	SIPB prototype beta test
18 Mar	SIPB testnet launch with token issuance

Phase 2 – Proof of Protection

18 Jun	Public SIPB best release : The Sentinel Protocols serviced by sentinel protocol collective portal
18 Jul	Mainnet launch (The manual report of TRDB feature enabled into mainnet)

Phase 3 – Self Purification

18 Nov	Machine learning engine beta test
18 Dec	Machine learning engine feature release (auto report applied) beta
	Distributed sandbox (D-sandbox) release

Phase 4 – Self Evolution

2019	Machine learning based Fraud Detection System (FDS) release into mainnet

Chapter 13

Conclusion

Sentinel Protocol is the most effective platform to help the current cybersecurity ecosystem, especially the cryptocurrency security industry, which suffers from inherent lack of oversight. The preemptive response to the new attack vectors has been proven to be effective through machine learning. However, the ambiguity of the threat based on probability is still a challenge. Utilizing the collective intelligence of the blockchain, Sentinel Protocol's Security Intelligence Platform for Blockchain provides the most efficient and rational solution to solve the cryptocurrency security problem. In addition, the cryptocurrency security industry, which was felt to have high entry barriers, could soon become a vehicle for many security vendors to enter, and thus have a greater positive effect of this convergence is for many people who are not currently protected by the legal system in collaboration with the cryptocurrency industry, such as exchanges, payments, and wallet companies. Sentinel Protocol opens up opportunities for individuals with the right skills to take part in this new platform for decentralized security on the blockchain.

References

[1] SANS Institute InfoSec Reading Room /IT Security Spending Trends
: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[2] Cyber security market report: https://cybersecurityventures.com/cybersecurity-market-report/
[3] Hard Fork Completed: https://blog.ethereum.org/2016/07/20/hard-fork-completed/
[4] bitcoin: https://bitcoin.org/bitcoin.pdf
[5] Rep on the block: A next generation reputation system based on the blockchain
: http://ieeexplore.ieee.org/document/7412073/
[6] BlockSci Traces Transactions Performed With Dash, ZCash, and Other Currencies
https://themerkle.com/blocksci-succesfully-traces-transactions-performed-with-dash-zcash-and-other-currencies/
[7] A behavioural-based approach to ransomware detection
:https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[8] Bitshares: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[9] Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[10] Practical Byzantine Fault Tolerance: http://pmg.csail.mit.edu/papers/osdi99.pdf