METEORA SYSTEM

Introduction of our intellectual property

METEORA SYSTEM Co., Ltd. (Isehara City, Kanagawa Prefecture, Japan; President: Eiji Watanabe) has been conducting research in information theory and developing implementation technologies since the 1970s. The following are two intellectual properties based on information-theoretic mathematics that are the result of these efforts. In the future, we will seek to provide our technology to companies developing zero-trust solutions. We look forward to hearing from you about partnership opportunities.

Contents

1. Introduction

Governments and the private sector struggle daily with the threat of cyber-terrorism. Two decades have passed without a solution to the problem, despite a flurry of products and services labeled as "security" and "solutions. As this history shows, countermeasures have not achieved cyber defense. This is an important lesson: countermeasure technologies cannot fundamentally solve problems. Shouldn't government and private sector resources be allocated to fundamental cyber defense technologies that do not rely on the word "countermeasure" and are not deceptive, i.e., technologies that can "solve" the problem?

Taking our company as an example, we have already completed two technologies that can solve the problem. As a small business, we did it all on our own, without relying on grants or outside funding. This is a testament to the voluntary, risk-taking cooperation of many of our brothers and sisters. Both of our technologies completed proof of concept prior to 2015. Unfortunately, Japan does not have a contact point to propose this to policy makers. We are looking to meet with anyone who can take advantage of our

technology. One of the IPs is "3-way handshake" and the other is "non-commutative algorithm" which is equivalent to post-quantum cryptography. These IPs include information-theoretic mathematics, implementation protocols, and patents that have gone through a PoC and will end the era of cyber terrorism.
The "Internetwork Transmission Control Program" of 1974 was a global civilization experiment. This was the first civilization experiment. We define the trend since 1974 as the 'age of cyber terrorism'. Our IP mission is to break the conventional wisdom that perfect cyber defense is impossible. In other words, the mission is to end the age of cyber terrorism. Our IP has the power to do so logically. If we don't do it, our sense of right and wrong will be paralyzed, and we will not leave a better world for future generations. That is why we must work on it from this very moment. This is the second civilization experiment.
To make the second civilization experiment a success, we need new encounters, and back in 1974 (the first civilization experiment), it was led by a U.S. government agency. Who will lead the second civilization experiment? In this context, the estimated $6 trillion in ransomware damage is a concrete indicator: in 1974, there was no such clear indicator. This indicator is the significance and rationale for government and private sector investment in 'problem-solving technology.

2. Our solutions

IP 1: Implementation technology to immediately and forcibly eliminate 3-way handshakes of backdoors and viruses

Feature:

Probability of a successful attempt to make an unauthorized communication connection = 0

IP 1 has the following feature: a 3-way handshake of a backdoor or virus will selectively and forcibly cause a "connection error", making the communication channel impassable. For example, by stealing the identifier of the communication channel (the third identity), one could normally hijack the communication channel, but this intellectual property causes such an attack to result in a "connection error. This algorithm and protocol can paralyze attackers, especially in DDoS attacks. Demonstration and testing of this technology was completed prior to 2011. At that time, it was implemented at Layer 5. Future implementations are expected to be at Layer 3 and Layer 4.

The patent specification does not mention the “hyper-fine time stamp” (the third identifier). The basis of the “hyper-fine time stamp” (updating the initial value) was claimed in the patent. NIST (in 2012) saw what this meant and asked us to register the "Figure 4 Matrix Expression" as a copyrighted work, to which we responded. Commercialization and dissemination of secondary products by forward-thinking vendors will enable a Net that guarantees the privacy of the Net while leaving no room for unauthorized attempts to establish connections. We call it CLEANNET.

IP 2: Implementation technology of cryptographic key (x1) knowledge split and dual control

Feature:

Probability of success of unauthorized user privilege takeover = $1/2^{256}$

Ransomware usually infiltrates a LAN, steals password files, hijacks users' job permissions, and accesses DBs. This behavior is neutralized by this IP. This technology achieves the key management (knowledge partitioning and dual control) required by PCI DSS v1.2. In 2013, we discovered a pair of one-way functions, which we call "separation of duties and consensus process", and as you already know, v1.2 did not find a way to implement this in the net. This is the implementation technology for knowledge partitioning and dual control (separation of duties and consensus process). Currently, a demo version implemented on a server is available for demonstration and loan as an actual example. In case you are wondering, applying this as a consensus algorithm to blockchain solves the trade-offs of privacy, finality, scalability, and so on. In other words, this IP will make it possible to create a digital currency that is fully compatible with paper currency.

The real value of IP 2 is that the service side does not manage accounts. Accounts are conventionally managed by the service, but in this implementation, the accounts are distributed across the net. The net can continue to provide the same service as before without requiring a password file for user authentication. For example, banknotes do not require personal information to be registered, do not require a password to be entered when paying, and do not record payment data. This can be attributed to a consensus algorithm between the banknote and the person. In short, paper money is a simple, mundane, but non-commutative algorithmic model; in 2014, we successfully demonstrated proof of concept, implementing an information-theoretic algorithm that is significantly superior to the PoW derived from Adam Back's Hashcash. With this IP, we can create a net that neutralizes viruses (ransomware), we can create signature chains for payments and signature chains for blocks.

3. Patents information

This paper is written using quotations and edited descriptions from our patent specifications. Detailed information, including patent numbers, will be disclosed in the course of specific discussions based on NDA.

4. Inquiries about this release

METEORA SYSTEM Co., Ltd

https://www.meteora-system.com

