Advanced TCP/IP

_ This is the foundation for ending the age of cyber terrorism _

Inheriting the promise of the Internet

...dramatically limit the freedom of cyber terrorism...

METEORA SYSTEM JAPAN
METEORA SYSTEM USA

Oct. 22, 2021

Advanced TCP/IP

This slide introduces a solution called "Advanced TCP / IP (post-BB84)" by citing recent topics on cyber terrorism. This slide includes the following topics.

This solution is positioned as an upgrade of the current "Internet Protocol Suit".

This solution is a universal technology derived from our intellectual property: that is a mathematical defense technology, not a patch technique.

This solution will dramatically limit the freedom of backdoors (including virus) and DDoS attacks.

It is impossible for a cyber attacker to enter a network through a gateway and to move freely through the advanced TCP/IP communication channel.

Note: we have also an implementation to neutralize ransomware. It is based on a different intellectual property.

February 21, 2000 Yahoo! Incident

More than 20 years after February 2000, cyber-terrorism is still gaining momentum. Why is this?

In the meantime, neither NIST nor international organizations have been slacking off. They have been engaged in various standardization activities, but cyber terrorism has only gained momentum. I wonder why?

You all have been asking the target to take action every time an incident occurs. We're still discussing the same thing. For example.

At this October's online international conference, you are always discussing the "visible" scope of the problem, calling for companies to strengthen their measures and building an international encirclement network etc.

A more in-depth discussion

There are two important points made in Chapter II (Monitoring and Visualization) of the U.S. Cyber Command 2020 Technical Challenge Problems Guidance. It is posted below.

· Cyber intruders may gain access to a network through gateway nodes and subsequently move laterally through the network over the course of many days, months, or even years.

· Detecting intruders, tracking their movements, estimating risk throughout the network, applying defensive countermeasures, and assessing damage and information exposure all present technical challenges.

There is an implementation technology that solves the above challenges. It is not a patching technique, nor is it a system that combines NIST standards. It is a defense technology based on the mathematics of C.E. SHANNON. We call it Advanced TCP/IP. A case study will be posted next.

Backdoor Killer

Backdoors exist even without proof

Characteristics of Cyber Terrorism

Backdoors use Internet Protocol Suit, so no matter how much you claim to have strengthened your security, it will have no effect. Strengthening key management and password management has nothing to do with backdoors.

Cyber terrorism can launch an operation at any time, at will: there is no warning of an attack. Backdoors are often planted during shipping or maintenance. No one has yet proved their existence. The reason?

The reason for this is simple: the Internet Protocol Suit (TCP/IP) itself is a backdoor. Realizing this, I invented the Backdoor Killer.

There is no comparison to this backdoor killer.

Because,

The TCP/IP has an identifier called IP address in the IP layer: an identifier called PORT number in the TCP layer. These are the only two identifiers.

Layer 5 of the OSI reference model is the virtual communication channel between ports. There is a technology that allows this virtual channel to have a third identifier: this is the backdoor killer. So we can say that there is no comparison.

What changes when a virtual communication channel is given an identifier? ➡ A backdoor will one day try to establish a communication channel, but the system of identifiers will selectively shutdown the backdoor's communication channel.

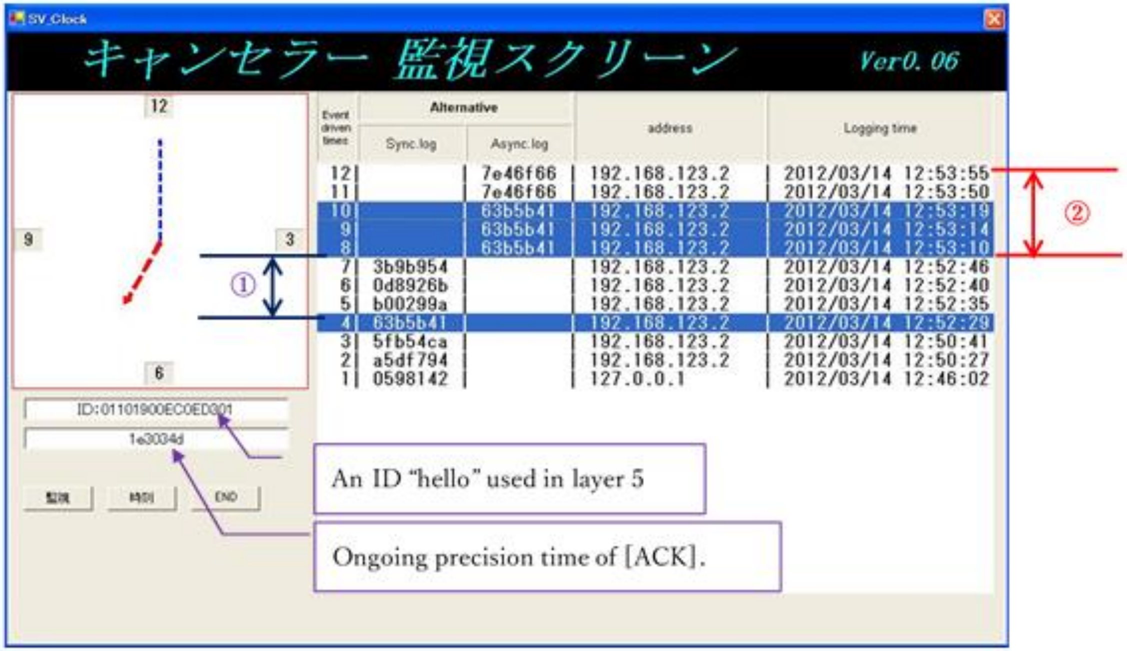
Hyperfine time stamping

This stamp selectively shutdowns a channel of the backdoor.

The new identifier system is a 256 [bit] random number that is synchronized to the computer's TOD (Time of Day). A visualization (log) of the hyperfine time stamp is posted below.

①"Synch. Log" indicates the time when there is no channel hijacking.

②"Asynch. Log" indicates the time when the channel hijacking was shutdown.



Event driven times	Alternative		address	Logging time
	Sync.log	Async.log		
12		7e46f66	192.168.123.2	2012/03/14 12:53:55
11		7e46f66	192.168.123.2	2012/03/14 12:53:50
10		63b5b41	192.168.123.2	2012/03/14 12:53:19
9		63b5b41	192.168.123.2	2012/03/14 12:53:14
8		63b5b41	192.168.123.2	2012/03/14 12:53:10
7	3b9b954		192.168.123.2	2012/03/14 12:52:46
6	0d8926b		192.168.123.2	2012/03/14 12:52:40
5	b00299a		192.168.123.2	2012/03/14 12:52:35
4	63b5b41		192.168.123.2	2012/03/14 12:52:29
3	5fb54ca		192.168.123.2	2012/03/14 12:50:41
2	a5df794		192.168.123.2	2012/03/14 12:50:27
1	0598142		127.0.0.1	2012/03/14 12:46:02

ID:01101900EC0ED001

1e3034d

An ID "hello" used in layer 5

Ongoing precision time of [ACK].

Why can only the backdoor channel be disconnected?

The parameters are set at the time of shipment and maintenance.

All these parameters are past tenses.

Even if you steal the hyper-fine time, the time will pass while the virus is hiding, and the backdoor tense will still be in the past. And.

When the backdoor tries to establish a connection, there will be two hyper-fine times for one ID.

So, the backdoor is immediately detected and its hyper-fine time is classified as ② "Asynchronous Log". The system can be designed in this way.

Cyberattacks

_ DoS attacks, DDoS attacks_

Cyberattacks, especially DoS attacks, use TCP/IP, so it doesn't matter how much you shout about strengthening security. An attacker can launch an operation at any time, at will: there is no declaration of war, but the country becomes the battlefield. Domestic targets will be "numbed" as if by magic.

But here's an invention that could reverse the situation. It is the Internet Protocol Suit (TCP/IP) with hyper-fine time. This will be referred to as Advanced TCP/IP.

Only the protocol logic is disclosed: the attacker throws [ACK] to the net, but [SYN+ACK] is not returned. In the meantime, the attacker's computers are forced to "wait". In other words, the attacker's computers are "numbed".

This proof of concept is already done!

_Advanced TCP/IP _

The hyper-fine time stamp on page 6 is the log of the virtual communication channel of layer 5. This demonstrates the concept of the advanced TCP/IP.

This is because the [ACK] thrown to the net by the DoS attacker will be classified as (2) "Asynchronous Log", and the net will not return [SYN+ACK].

For example, the hyper-fine time stamp will not reply to the DoS attack [ACK] even if the terrorist thinks no one will notice.

It is not today's TCP/IP that can counter DoS attacks but the advanced TCP/IP. Therefore, the advanced TCP/IP is the foundation to end the era of cyber terrorism.

Intellectual Property, Patents

Base intellectual property for hyper-fine time stamping

Patent	No. 5314240
Title of Invention	Communication channel system
Patentee	Eiji Watanabe METEORA SYSTEM
Application number	No. 2006-308164
Registration date	July 12, 2013

Attention:

There is no mention of hyper-fine time stamping in the specification. However, the patent does claim the basis for hyper-fine time stamping (updating the initial value): Figure 4 Matrix represents it. NIST (as of 2012) saw this context and asked to register Figure 4 as a copyrighted work. This history also played a role in the birth of the advanced TCP/IP.

The Promise of the Internet

...dramatically limit the freedom of cyber terrorism...

Who gave freedom to cyberterrorism? Let’s research this.

The Internet, after all, features openness and anonymity. This is because the technology that promises openness and anonymity is the Internet Protocol Suit (TCP/IP) .

For example, Bill Gates implemented the promise of openness, freedom, and universality to the world in 1995 by including TCP/IP in his operating system. That promise gave freedom to cyber terrorism. *But,*

The advanced TCP/IP dramatically limits the freedom of cyber terrorism, while inheriting the promise of the Internet.

The Promise of Democracy

An in-depth analysis of the weaknesses of democracy

The good thing about America is that if an external threat emerges, it will unite across parties. According to Dr. Limeng Yan, a virologist who went into exile in the United States, the CCP fueled the conflict and proceeded with the division of the United States every time an incident such as racism occurred. "It was the presidential election that this division will reach its climax, and that was the perfect opportunity to use biological weapons," she said. Cited from Magazine “The Liberty” November 2021 No.321

Dr. Leemon says, "That timing was the perfect opportunity to use a biological weapon. <u>Bioterrorism targets the timing when we don‘t realize that it is a war.</u>

We are so enamored with something so that we don’t even notice the bioterrorism. And so we give freedom to bioterrorism. The terrorist is calculating when their next move will be<u>.</u>

To limit the freedom of terro

It's not a divide, it's a clean net!

A hyper-fine time stamping guarantees the establishment of a connection to the person who is given a Clean Net ID. If terrorists steal this ID, it will not be useful for cyber terrorism. ☞page 6

Protocols like the one above are lacking in the US today. For example, there was an incident where Trump's account was deleted. This is an act of intense division, not unity. *Instead of this approach,* let's upgrade our current net to the advanced TCP/IP.

Then, each user will be given a Clean Net ID. (no personal information is required). <u>The net, with its hyper-fine time stamping, becomes a living thing!!</u> *Deleting this clean net account by a person is worthy of murder, because it is a living thing.*

Technology to End the Age of Terror

Cyber-terrorism in full swing and bioterrorism in its second phase. looming over our democracy, prepare for it!

Advanced TCP/IP has completed its proof of concept. I have the textbook for your discussion. This article refers to those notes. If you have any questions, please contact the provider of this slideshow or use the contact us link on the homepage. ☞http://www.meteora.co.jp

METEORA

METEORA SYSTEM
Eiji Watanabe

We also have _a DB account server that neutralizes ransomware_ although it is not posted here.