

Analysis and thought on quantum insert technology

ZHANG Xue-bo, WANG Si, ZOU Hong-xia

(Department of Information Equipment Aerospace Engineering University of PLA, Beijing 101416, China)

Abstract: Quantum insert (QI) is a technology that makes redirection attacks by injecting malicious content into certain sessions. A brief introduction of American “Quantum Insert” project was given and the connotation of this technology was discussed. It then looked into the application that quantum insert was put to in the Internet “Great Cannon” event. An open source QI tool made available by Fox IT, an IT security company, was then analyzed. An experimental verification environment was built using this tool and a verification was made. Finally, a thought was given on how to put QI to use in building network defense.

Key words: quantum insert, great cannon, FoxAcid, Fox IT

doi: 10.11959/j.issn.2096-109x.2017.00185

1 Introduction

“Quantum insert” project is part of and plays an instrumental role in “Quantum Plan”, a top-secret scheme under American National Security Agency (NSA)^[1]. “Quantum insert” project has by now developed a set of tools. Table 1 gives some of these tools and their application scenarios, including attack and defense scenarios.

QI is a technology that makes redirection attacks by injecting malicious content into certain sessions. QI is a kind of off-path attack, since it does not control a network node completely as in the case of man-in-the-middle attack. Instead, the

attacker accesses periodically the communication channels to read certain communications or insert additional messages without altering or deleting the user’s messages, that is not to insert into the messages but to insert additional messages in the session^[2].

The packets passing over the network nodes are captured by mirroring, without affecting the normal transmission of packets. Through the reconstruction of the mirror data packet, the data packet is restored to its original state. Then, according the informations of the four tuple and packet header, the packets are forged and sent to form a preemptive response to the client request and discard the normal

Table 1 Quantum insert tools and their application scenarios

Attack tools	Description
Quantum insert	Quantum insert. Brief hijack of connection to redirect target to exploit server
Quantumbot	Quantum bot. Capable of hijacking idle IRC bots and hijacking c2 communication from bots
Quantumbisquit	Quantum debris. Enhances QIs effectiveness against proxies and other hard to reach targets
Quantumdns	Quantum domain name. Targets single hosts or servers
Quantumhand	Quantum hand. Detects users’ sensitive information through social websites
Quantumsky	Quantum sky. Denies access to a website by injecting/spoofing a large number of packets
Quantumchopper	Quantum chopper. Interrupts or intercepts the uploading/downloading of files

Received Date: 2017-06-06, **Revised Date:** 2017-07-29. **Corresponding Author:** ZHANG Xuebo, 178140615@qq.com

Foundation Item: Basic Research Project of Information Security Laboratory for National Defense Research and Test

response packets after the arrival.

The process of a QI attack consists of monitoring TCP sessions and inserting spoofed data packets. When the spoofed packet reaches the target earlier than the original packet, we say there happens a successive “insert”. To make a data packet spoofing a success, the attacker needs to listen in on the network and acquire some session information: source IP & target IP, source port & target port, serial number and ACK number, all of them being retrievable from the TCP packets that contain http requests. In addition to this, the attacker’s spoofed data packets have to reach the target before the real network server responds, taking advantages of this speed difference and competitive edge to masquerade as the real network server. And the result is the website accessed by the user is redirected to the target server. The user may be unaware of being deceived if the false website, to which the user is redirected, masquerades well enough. If the user is redirected to, say, the FoxAcid server of the American Forces, he is utterly at the mercy of the forces. Fig. 1 presents the QI attack process.

2 Analysis of the “Great Cannon” event

QI technology attracted extensive attention after China’s “Great Cannon” event. GitHub, an America-based management platform of open source codes, suffered on March 26, 2015 the most massive denial of service (DoS) attack in its history. Some overseas users accessing a Baidu service script attacked instead two mirror image pages of GreatFire and the New York Times. This DDoS attack against GitHub was dubbed by international media as China’s “Great Cannon” event. Baidu, however, ruled out the possibility of security defect intrinsic to its product or the likelihood of hacker attacks.

This event was created by the attacker who, using QI technology, hijacked the sessions of overseas users when they attempted to access Baidu. It is Baidu’s statistics js code that was altered^[3,4]. Fig. 2 shows the altered code, whose function is to shut the cache and access every 2 seconds two of GitHub’s websites. The faked js file received by the user’s browser is used to make DDoS attack.

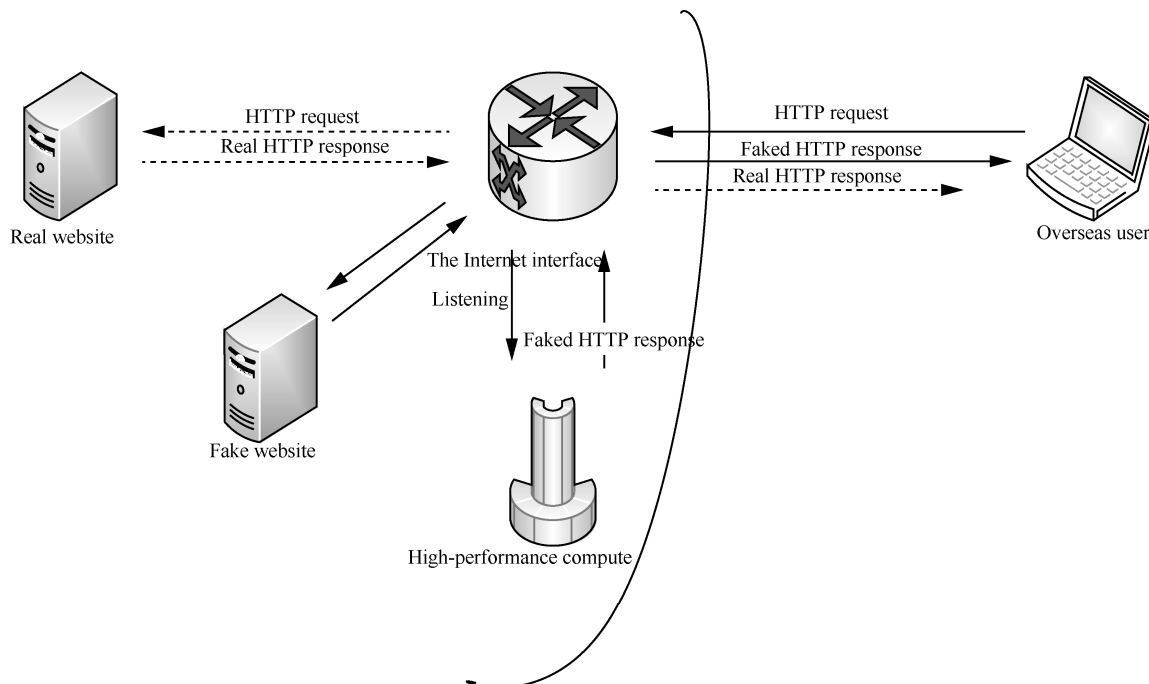


Fig. 1 The QI attack process

```

document.write("<script
src='http://libs.baidu.com/jquery/2.0.0/jquery.min.js'>\x3c/script>");
!window.jQuery && document.write("<script
src='http://code.jquery.com/jquery-latest.js'>\x3c/script>");
starttime = (new Date).getTime();
var count = 0;

function unixtime() {
    var a = new Date;
    return Date.UTC(a.getFullYear(), a.getMonth(), a.getDay(), a.
        getHours(), a.getMinutes(), a.getSeconds()) / 1E3
}

url_array = ["https://github.com/greatfire",
    "https://github.com/cn-nytimes"];
NUM = url_array.length;

function r_send2() {
    var a = unixtime() * NUM;
    get(url_array[a])
}

function get(a) {
    var b;
    $.ajax({
        url: a,
        dataType: "script",
        timeout: 1E4,
        cache: 10,
        beforeSend: function() {
            requestTime = (new Date).getTime()
        },
        complete: function() {
            responseTime = (new Date).getTime();
            b = Math.floor(responseTime - requestTime);
            3E5 > responseTime - starttime && (r_send2(b), count += 1)
        }
    })
}

```

Fig. 2 Hijacked statistics js code of Baidu

This QI attack process is illustrated in Fig. 3.

1) Http analysis: A data packet analysis tool, like Wireshark, was utilized to analyze the http data stream in normal Baidu website accessing.

2) Point of penetration of positioned attack:

The point after which data packets are to be faked, having regard to the designated js file. For instance, to which data packet shall a response be faked in order to substitute the m. js file.

3) Fake data packet: Fake the altered js file as data streams, and the data packet format shall be able to deceive the client side.

4) Stealthy substitution: Send the spoofed data packets to the client side before Baidu website does so.

3 Experimental analysis of QI technology

3.1 An open source quantum insert tool

Fox IT, an IT security company, develops a quantum insert tool and has released its source code on a website of an open source code: <https://github.com/fox-it/quantuminsert>. This open source quantum insert tool comes with a monitor (monitor. py), an attacker (shooter. py), and a test data packet. The monitor is a Python script, able to acquire the serial

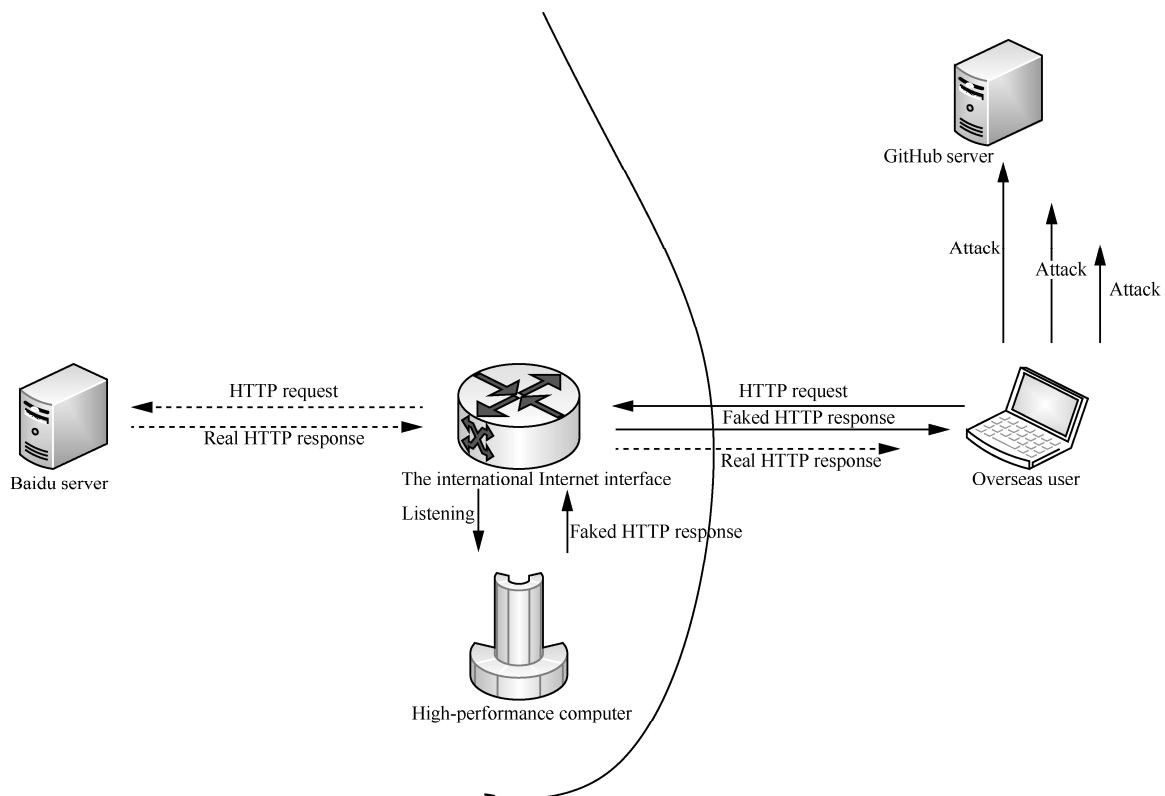


Fig. 3 The QI attack process

number (needed for Tcpdump and Tshark output), ACK number, TCP port, and IP address, and it permits to choose HTTP cookie value. The attack script is also written in Python, and the spoofed data packet is made and sent using Scapy, as shown in Fig.4^[5].

3.2 Designing a QI experiment

Using this open source QI tool and its test data packet, the authors constructed a QI experimental environment, as shown in Fig. 5, to investigate this technology and assess its effect. This environment consists of 2 nodal routers (C and D), 1 monitoring server, 1 insert server, 1 user host, and 1 target web-

site server B. QI was implemented on the nodal routers^[6].

The experimental QI process is as follows.

- 1) User host A accesses the target website server B via router nodes C and D.
- 2) The monitoring server sniffs the whole of the data packets that pass router node C.
- 3) The monitoring server screens out specific target addresses and access requests.
- 4) The monitoring server communicates to the insert server the access request data acquired in 3).
- 5) The insert server sends, via the router node C, faked data response to the user's host A, and this

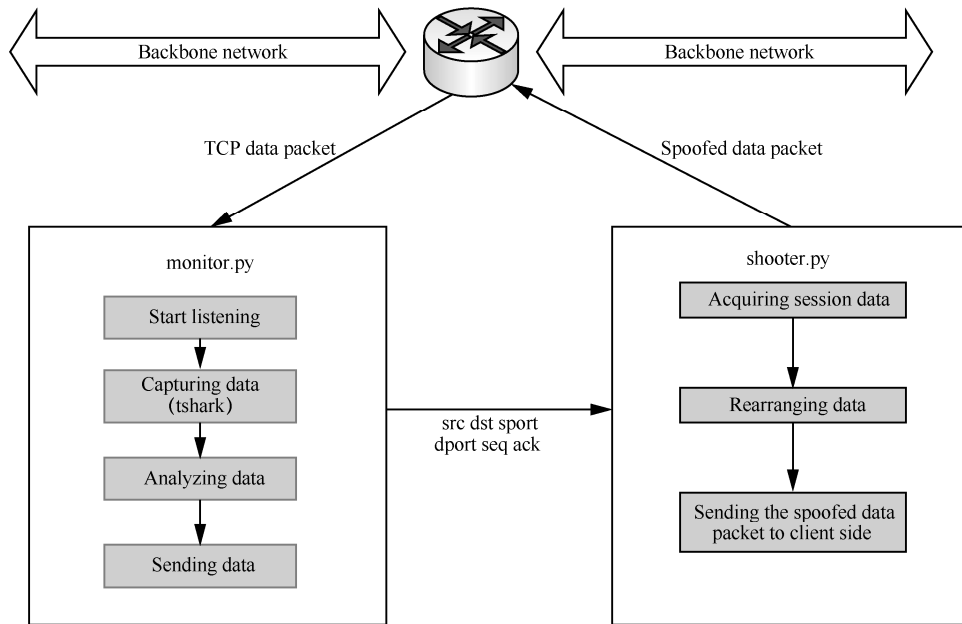


Fig. 4 An open source QI tool

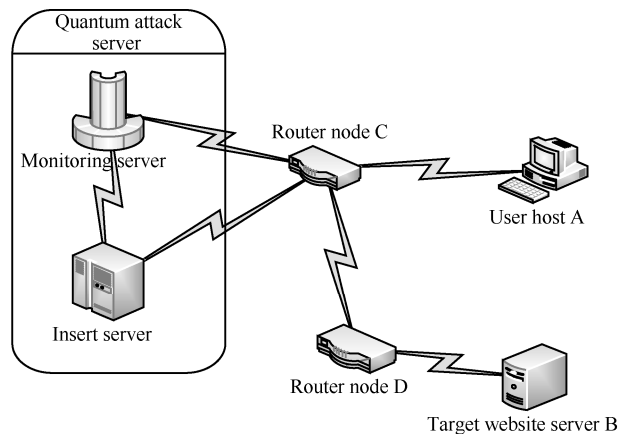


Fig. 5 A designed QI experiment

response reaches the user's host A earlier than the response of the real target website server B, hence achieving QI.

3.3 Analysis of the quantum insert experiment results

This experiment was performed in 2 groups to achieve QI, based on UDP and TCP respectively.

Experiment 1 UDP-based data packet insert. UDP does not need check, so to achieve QI we need only to run in the monitoring server a monitor program to listen in on the session information passing router node C, and let the insert server to alter the data sniffed and send via node C the spoofed data to host A. The spoofed and sent data is given in Fig. 6.

```
[root@localhost scapy]# python sniff_forge.py
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
WARNING: No route found for IPv6 destination :: (no default route?)
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
WARNING: No route found for IPv6 destination :: (no default route?)
('172.16.2.91', '21567')
...
Sent 3 packets.
('172.16.2.91', '21567')
...
Sent 3 packets.
('172.16.2.236', '61714')
...
Sent 3 packets.
('172.16.2.236', '61714')
...
Sent 3 packets.
```

Fig. 6 Sending a spoofed data packet

The spoofed data received on the user's host is as shown in Fig. 7.

```
Waiting for message...
Client('172.16.2.200', 12345) sent message: This is forge data.
Received from and returned to: ('172.16.2.200', 12345)
Waiting for message...
Client('172.16.2.200', 12345) sent message: This is forge data.
Received from and returned to: ('172.16.2.200', 12345)
Waiting for message...
Client('172.16.2.200', 12345) sent message: This is forge data.
Received from and returned to: ('172.16.2.200', 12345)
Waiting for message...
```

Fig. 7 Receiving a spoofed data packet

Experiment 2 TCP-based data packet insert.

TCP requires data check. For this reason, an additional check step is involved in TCP-based data packet insert. In the TCP header check computation, we need to clear the checksum field. Once the new checksum is found, it must be inserted into the field before sending the spoofed data packet; otherwise this spoofed packet will be discarded by host A. Fig. 8 shows the data packet received on host A, viewed using Wireshark.

Apparently, the user's host A receives, one after the other, two data packets (#3 and #5) coming from the source address and the target address respectively. The former, 60 in length, is the spoofed data packet sent by the insert server and contains TEST data; the latter, 54 in length, is the response data packet sent by the target website server, but is discarded by host A, and therefore QI is achieved.

4 A thought on QI's role in network defense building

4.1 An analysis of US forces "Turbine" plan

"Turbine" plan automatically inserts spyware, including malware and data collection ware, into target computers. "Turbine" plan relies primarily on QI tools, and also needs the coordination of "Chaos" and "FoxAcid" systems. First of all, "Chaos" system, by use of a series of "selectors", monitors and analyzes users' behavior, which helps

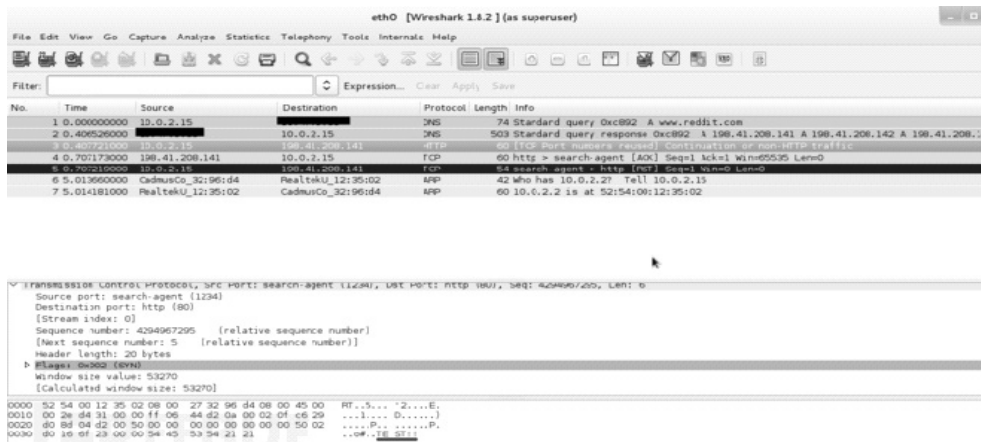


Fig. 8 Insert viewed on the user's host A

find worthy attack targets. Then, it informs “Turbine” system to hijack one target user’s session through QI technology, that is inserting a faked response command before the real one arrives and luring the target to access a “FoxAcid” server. The user then accesses the “FoxAcid” server unknowingly, downloads attack ware, and implants Trojan ware. The ultimate goal of putting the target under control is achieved. The whole of the attack process is shown in Figure 6^[7].

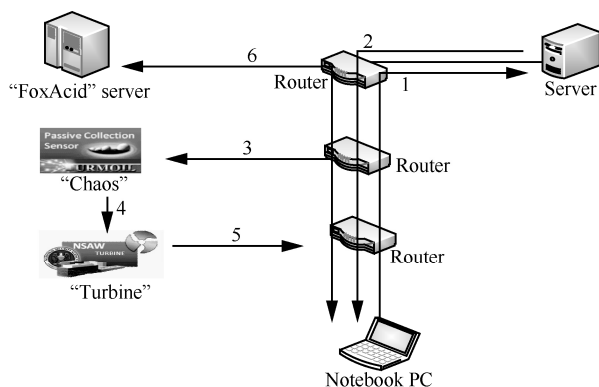


Fig. 9 The attack process of “Turbine” plan

4.2 An analysis of the QI system

Following the idea of NSA’s “Turbine” plan, a powerful network attack and defense weapon of huge deterrence can be created if QI technology is installed in the state trunk lines or the country border firewall.

1) QI technology is to play the following roles in building up network defense.

2) DDoS attack: Plants malicious code into a large number of user sessions making them to send countless data requests to the target server, thus mounting DDoS attack against the target server.

3) Pilferage and control of user data: Implants in the session returning to the user a redirection to the malicious website. This operation does not need webshell authority. When the user accesses this malicious website, this website scans the user’s system for any vulnerabilities and, by taking advantage of the vulnerabilities of the user’s system or its third-party software, infiltrates into and controls the

user’s host.

4) DNS hijack: Hijacks the user’s access to the DNS server so as to return a false IP address abducting users to access a faked website.

5) Gateway hijacking: Sends, before the gateway makes any response, a data packet to the source address claiming that the destination is not reachable, so making the source address host send request data packets repeatedly; and the result is that a large amount of the target host resources are wasted.

Network defense: Redirects an attacker to another address so that the target network or server is put under protection.

4.3 A thought on the design of a QI system

From the design perspective, a QI system involves three layers, as illustrated in Fig. 7. The bottom layer, called data operation layer, is for data acquisition and packet operation and also for providing the upper level with restored data and shielding such operation details as data acquisition, data packet restoration and reconstruction. The second is technical implementation layer. It is designed to provide functional modules to be used in the QI attack and includes data monitoring, insert, URL redirection, Trojan ware implanting, TCP half connection. The top layer is for functional application, and it is intended for mounting all types of network attacks: DDoS attack, user information pilferage and control, DNS hijack, gateway hijack, and network protection, etc^[8].

5 Conclusion

President Xi Jinping advocates for cyberspace sovereignty and safeguarding our network security. By taking advantage of the technical benefits specific to QI, a powerful network attack and defense weapon of great deterrence can be created if this technology is applied to China’s border route to the international Internet. This may provide an effective way to boost our cyberspace sovereignty and network security. Meanwhile, it is equally important for us to research into QI detection and protection

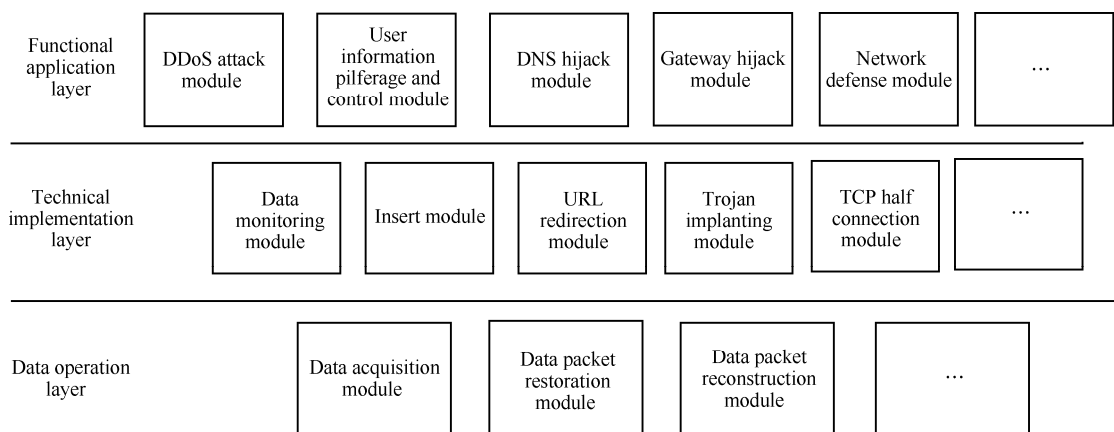


Fig. 10 A hierarchical breakdown of the QI system Concluding Remarks

technologies so that if our network suffering Cyber attacks, we can exploit QI technology to find and track it faster. We can use HTTPS and CDN acceleration to defense QI attacks.

References:

- [1] JIN Y. Elaboration on quantum: NSA's most power internet attack tool[EB/OL].(2014-3-17). <http://tech.qq.com/a/20140317/003378.htm>.
- [2] QING Y, CHEN Q. Emerging cyberspace security technologies [M]. CETGC 30th Institute, 2013.12.
- [3] Russell Brandom. GitHub was hit with massive denial-of-service attack from China[EB/OL]. <http://www.theverge.com/2015/3/27/8299555/github-china-ddos-censorship-great-firewall>.
- [4] BILL M, NICHOLAS W, et al. China's great Cannon[EB/OL]. <https://citizenlab.org/2015/04/chinas-great-cannon/>.
- [5] WANG J. Remote network based data packet monitoring and reconstruction technology[D]. Dalian: Dalian Jiaotong University, 2010.
- [6] CAI J J. HTTP Response splitting attack analysis and its detection method design[D]. Beijing: Beijing University of Posts and Tele-communications, 2012.
- [7] QING Y, ZHOU W. Discovery: America's network monitoring project [M]. CETGC 30th Institute, 2014.
- [8] LI N. IPv6-based intrusion detection system research and imple-mentation[M]. Petroleum Institute of Daqing, 2006.

About the authors:



ZHANG Xuebo(1977-), born in Jilin, Doctor's degree. He is a lecturer in department of information equipment aerospace engineering university of PLA. His main research interests include network security strategy, network attack and defense technology.



WANG Si(1985-), born in Jiangxi. He is a master in aerospace engineering university of PLA. His main research interest include network security.



ZOU Hongxia(1968-), born in Liaoning. She is an associate professor in department of information equipment Aerospace Engineering University of PLA. Her main research interest include network and information security.