International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

ENHANCED SECURE MD5 AND CRYPTOGRAPHIC PUZZLE HIDING SCHEME TO DEFEND DENIAL-OF SERVICE ATTACKS

V.Abirami[1], P.Manju Bala[2]
[1]*B.E Student ,Department of Computer Science And Engineering, IFET College of Engineering,Villupuram,India.*
Email Id:vabiramiecofriend@gmail.com
[2]*Associate Professor ,Department of Computer Science And Engineering, IFET College of Engineering,Villupuram,India.*
Email Id: pkmanju26@gmail.com

***Abstract*-This paper is an endeavor to improve the Software Puzzle with Secure MD5 and Cryptographic Puzzle Hiding Scheme. At the point when a password is encoded by a hash calculation, the resultant is called hashed password. This sort of transmission is dependably a subject of block attempt by the programmers. These hashed passwords are gone through the internet as information packets. TCP header is the most regular part of the information packets. In a TCP header, there are six reserved bits which remains constantly unused. We proposed another way to deal with improve the security of hashed passwords by utilizing the six reserved bits of a TCP header. Here we scramble the hashed secret key by an arbitrary key utilizing basic numerical function. The data expected to unscramble the scrambled hashed password is conveyed by the six bits of TCP header. In the Cryptographic Puzzle Hiding Scheme, A customer S has a packet m for transmission. The server chooses an irregular key k, of a padded length. S produces a puzzle (key, time), where puzzle () signifies the puzzle generator capacity, and t_p means the time required for the solution of the puzzles. Parameter is measured in units of time, and it is specifically reliant on the accepted computational capacity of the enemy, meant by N and measured in computational operations every second. Subsequent to creating the puzzles P, the server telecasts (C, P). At the customer side, any customer R illuminates the obtained puzzles to recoup the key and then computes. Experimental designs prove that how effectively we improvised the software puzzles using proposed scheme.**

Keywords: Software Puzzles, Secured MD5, Cryptographic puzzles, TCP header and Puzzle generator capacity.

I. INTRODUCTION

In the web serviceand network framework's, a vast number of computer machines are associated through geologically distributed system. Assaults and security is a noteworthy issue in computer systems. The web service or network security is a procedure of increasing unapproved access to the network. Furthermore, the assaults assume a noteworthy part in the security [1]. The assaults are characterized into two dynamic assaults and static assaults. The network interloper captures information going through the system is called as detached assaults. Wire tapping, unmoving scan and port scanner are the cases of detached assaults. Interloper starts the command to upset the systems through typical operation. This is called dynamic assaults. Denials of service assault, spoofing, Man-in-the middle assault, cradle over stream, load over stream arethe instances of dynamic assaults.

An "assault" is one of the exploitation blemishes in a system computingframework for purposes that are not known by the framework administrator and that are generally harmful [2]. Assaults are continually occurring on the web, at a rate at which the few assaults for each moment on each associated machine. These assaults are done naturally from contaminated machines (by Trojan horses, infections, worms, and so on.) client of the system does not think about it. Sometimes, these are propelled by computer aggressors or hackers. The attacks are executed on the system due to the following reasons:

- To obtain the access to the system.
- To embezzle the secret information like intellectual property.
- To obtain the information about the personal details of the user.
- To steal the bank account information.
- To steal data without the user's intervention.
- To utilize the user's of a system as bounce for an attack.

Computer frameworks utilize the assortment of segments [3], running from power to control the machinesby the software program executed by means of the

operating system and that uses the system. Assaults might happen at every connection of this chain from various clients. The DDoS or DoS is one sort of dynamic assaults. The DoS assault which implies that the aggressors send certain messages to the vulnerabilities, prompting the variation from the normal structure or it might send assault messages rapidly to any node to run out the system framework assets [4], bringing about business networks framework failures. A DDoS orDoS assault is small for Distributed Denial of Service assaults, which is created on the idea of DoS assault and the numerous disseminated assault sources. The attacker as a rule utilize a more number of controlled zombies which are circulated in various areas to advance an extensive number of denial of service attacks to a solitary target server or various target machines. With the quick advancement of aggressors as of late, the assault activity brought about by DDoS or DoS assaults has been developing.

II. RELATED WORK

A Rank Correlation Based Discovery against Distributed Reflection DoS Attacks[2], they recognized a DDoS by a procedure called rank connection based recognition which utilizes anestimation called spearman's rank relationship. In the event that there are no rehashed information values, an impeccable Spearman relationship of +1 or −1 happens when each of the variables is an impeccable monotone functionwhich recognize a DDoS by characterize all the bundle check in suspicious stream as indicated by time esteem. "A System for Denial-of-Service Assault Detection Based on Multivariate Correlation Analysis"[3], they proposed a methodology called as Macintosh which takes after a triangular territory to extricate the correlative component. This uses a threshold based peculiarity finder, which contains a traffic profile that is ordinary traffic profiles. At the point, when new packets are touches base in the system it produce the system traffic profile. This traffic profile is contrasted with the statistical data to identify the DDoS attack.

Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks [4],Adaptive Selective Verification (ASV), which is a circulated as an adaptive instrument for upsetting the aggressors endeavors to deny service to legitimate customers in view of particular verification. This plan utilizes data transfer capacity as cash, however the level of security utilized by the customers powerfully changes with the present level of DDoS assault. At a high level, the customers exponentially increase the quantity of demands in threshold limit. The server actualizes a reservoir based random testing strategy to successfully test from an arrangement of approaching packets utilizing limited space strategy. "Bandwidth Distributed Denial of Service: Attacks and Defense" [4],here, the bandwidth oriented distributed Denial of services which causes clog in the system which is completed by expansion of parcel or aggregate sum of traffic. BW DDoS assailant use diverse assaulting specialists and diverse sorts of networks. The agents incorporatethe three things puppets, zombies and root zombies.Filtering which just channels the congested parcels. Rate constraining which traces the packets labeling and booking based methodology. By utilizing an above component, we can ready to recognize and dodge the DDoS assaults.

Can a DDoS Attack Meltdown My Data Center?"A Simulation Study and DefenseTechniques[5],in cloud, the DDoS has been known to diminish the Cloud administrations, however would it be able to do more regrettable by causing damages to the network devices. Services are facilitated in information trots with a great many servers creating a substantial volume of heat in switches. Ventilation, heating and air conditioning (HVAC) frameworks which forestall the server downtime because of overheating as indicated by number of client access ascertain DDoS proportion and drop the packets. "Can we beat DDoS Attacks in Mists?" [6], the DDoS assault which causes the resources distribution in cloud. This utilizes an interruption counteractive action framework, which discovers DDoS assault. It is a device which emerge a message and an alert when DDoS assaults happen. On the off chance that it happens they take after a dynamic resources distribution with help of unmoving assets.

DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy [7] that distinguishes a DDoS by Chaos analysis and its entropy. The entropy has been utilized as a part of abnormality location of DDoS assaults. It portrays the level of focus and dispersal normal for traffics.But the entropy depends just on the qualities registered by every packets field [11], while the association data or the relationship between every field has been overlooked. In our methodology, the volume of traffic movement is pre-handled by entropy-based strategies. At that point, by utilizing chaotic examination on the entropy of source IPs and destination IPs, DDoS assaults are identified."Denial of-Service Attacks in bloom Filter-Based Forwarding" [8],Multicast empowers the sender to achieve an expansive number of recipients, despite the fact that it just sends every parcel once. The utilization of Bloom

channel makes a probabilistic component in packet sending which decrease the power of DDoS assault. It primarily concentrates on infusion assaults. Without giving numerous points of interest assailants can determine new channel and infuse the assaults. This can be dispensed with an additionally defenselessness is lessened.

Identifying Spam Zombies by Observing Outgoing Messages [9], the assaults incorporatespreading of a malware, DDoS and data fraud. Spam zombies location instrument named SPOT by observing active messages on system. SPOT is composed in view of an intense measurable device called Successive Probability Ratio Test, which has limited the error ratio, for example, false positive and false negative. The (content-based) spam channel is conveyed at the recognition framework so that an active message can be named either a spam or non-spam. "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" [10],the DDoS assault is distinguished by utilizing a comparability based calculation is utilized. Furthermore, they utilized a stream relationship and coefficient as a metric to discover a DDoS assault. Stream relationship[17-19] which characterizes a statistical relationship between two edge switches. The coefficient characterizes a particular property of assault. They execute programming on each switch to quantity of bundles for each stream and record this data for a fleeting at each switch. On the off chance that the bundle size is more prominent than the threshold level, it will drop[20].

III. SECURE MD5 AND CRYPTOGRAPHIC PUZZLE HIDING SCHEME

Firewalls are prudent to persistently reinforce and alter, so that interior system administrations were occupied to the external client. It is practical to set the analyzer of system activity; estimation of its parameters will permit so as to recognize at the beginning of the assaults. Our puzzle depends on rehashed squaring and utilizes the puzzles proposed as a part of its essential building block, however "outsources "a large portion of check of the puzzle's solution for the prover. This is accomplished without embedding so as to bargain the application reason by a secret which is just known to the verifier – inside of the trapdoor showed by the Euler capacity in a modular square. To affirm the customer's key, the verifier just needs to execute a minimal number of modular multiplications. An eminent countermeasure against DoS assaults issolving the client's puzzles. The malwared server trouble from the customers to confer the registering assets before it forms their necessities. To get administration, a customer must clarify a cryptographic puzzle and present the correct answer. If there should arise an occurrence of intuitive customer puzzles where the server represents the face of an aggressor may mount a counterattack on the customers by infusing fake packets containing false puzzle parameters.The proposed scheme is studied in four phases namely,

- GPU- inflated DoS attacks
- Framework of software puzzle
- Software puzzle generation
- Security analysis

i) GPU-inflated DoS attacks

A GPU-based system is typically composed in a way that takes the characteristically information parallel projects, (for example, matrix multiplications, simulations and so forth.). The GPU-based platform can run a system such that every string of the program works on a particular block of information. All of such strings can run at the same time on the stream processors as long as there are sufficient stream processors on the GPU. In case the information components are bigger than the quantity of stream processors, the Thread Dispatcher deals with the accessible processors for the strings.Once stacked, every stream processor will run at the same time and independently on a cut of the data, relating to the two information vectors and delivers the results.

ii) Framework of software puzzle

In order to vanquish the GPU-inflated DoS assault, we stretch out information puzzle to the software puzzle. At the server, the software puzzle plan has a code block stockroom W that stores different programming instruction blocks. Furthermore, it incorporates two modules: a) creating the puzzles C0x by arbitrarily gathering the code blocks removed from the stockroom; b) muddling the puzzle C0x for high security puzzles C1x. The code block distribution center W stores aggregated instruction blocks $\{b_1, b_2 \ldots b_m\}$, e.g., in Java byte code, or C binary code. The reason to store gathered codes as opposed to source codes is to spare server's time.Generally, the server needs to take additional time to arrange the source codes into assembled codes during the time spent software puzzles era.

iii) Generation of software puzzle

So as to build a software puzzle, the server needs to execute three modules: puzzle core era, puzzle challenge era, puzzle encoding/decoding. Once a software puzzle,

C1x is made at the server side and aggregated into the Java class record C1x.class, it will be conveyed to the customer who demands for services over an unreliable channel, for example, Internet, and keep running at the customer's side.

iv) Security analysis

Software puzzle expects to keep the GPU from being utilized as a part of the puzzle solving process in view of various instruction sets and constant situations in the middle of GPU and CPU. Alternately, an adversary might endeavor to damage the software puzzle plan by reenacting the host on GPU, cracking puzzle generation, re-creating GPU-rendition puzzle, or mishandling the access priority in puzzle solving. On the off chance that an aggressor can run a CPU test system over GPU environment; the software puzzle can be executed on GPU in direct manner. The MD5 generation is given as:

At the point, when a password is encoded by hashestimation, the resultant is called hashed password. In a server, client based communication framework, for example, Yahoo Messenger, AIM, passwords of customers are hashed by MD5 and went to the server for verification. This kind of transmission is dependably a subject of block attempt by the programmers. These hashed passwords are gone through the Internet as an information packet. TCP header is the most normal part of the information packet. In a TCP header, there are six reserved bits which remains dependably unused. Here, we incorporated the security of hashed passwords by using the six reserved bits of a TCP header. Then we encrypt the hashed password by a random key using simple mathematical function. The information needed to decrypt the encrypted hashed password is carried by the six bits of TCP header. The four steps are executed as follows:

Step 1: Append padding bits

The information message is "appended" (expanded) so that its length (in bits) equivalents to 448 mod 512. Padding is constantly performed, regardless of the fact that the length of the message is of 448 mod 512. Padding is executed as follows: a solitary "1" bit is annexed to the message, and afterward "0" bits are attached so that the length in bits of the padded message gets to be compatible to 448 mod 512. Not less than one bits and at most 512 bits are attached.

Step 2: Append Length

A 64-bit representation of the length of the message is added to the consequence of step1. On the off chance that the length of the message is more noteworthy than 2^64, just the low-arrangements of 64 bits will be utilized. The subsequent message has a length that is an accurate multiple levels of 512 bits. The data message will have a length that is a precisedlevel of 16 (32-bit) words.

Step 3: Initializing the MD buffer

A four-word padded (A, B, C, D) is utilized to register the message digest. Each of A, B, C, D is a 32-bit register. These registers are introduced to the accompanying qualities in hexadecimal, low-order bytes first):

Word A: 01 23 45 67
Word B: 89 ab cd ef
Word C: fe dc ba 98
Word D: 76 54 32 10

Step 4: Process message in 16 word blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z
G (X, Y, Z) = XZ or Y not (Z)
H (X, Y, Z) = X xor Y xor Z
I (X, Y, Z) = Y xor (X or not (Z))

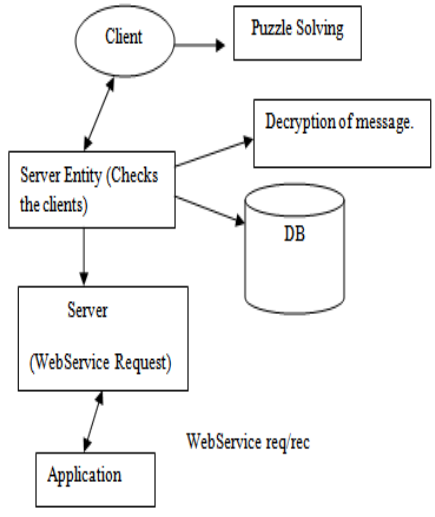

Fig.1. Workflow

IV. EXPERIMENTAL RESULTS

The study depicts in details how the study was directed including dependence of the volume of traffic on the sorts of assaults DoS/DDoS, proficiency of techniques of routing etc. It is practical to set the analyzer of system traffic estimation of its parameters will permit so as to recognize the starting of the assaults. Thusly, itis important that the ceaseless perception of over the router associated with the external network.The adequacy of routing strategies is directly subject to the topology of the system and its size. Multilevel routing generously relies on ideal allotment of a system on domains routing.

At the Physical layer, a packet m is encoded, interleaved and balanced before it is transmitted over the remote channel. At the beneficiary, the sign is demodulated, deinterleaved and decoded to recoup the first packet m. Hubs Aand B convey by means of a remote connection. Inside of the correspondence scope of both A and B there is a DoS hub J. At the point, when A transmits a packet m to B, hub J groups m by accepting the initial couple of bytes of m. J then defiles m recovery by meddling with its gathering at B. It is expedient to focus the parameters that regulate the packets transformation on each communication link and total packets transferred using the update of routing tables. The total volume of traffic is determined by:

$$V = \frac{T_{sys}}{\Delta t_{sys}} \sum_{i,j=1}^{N} P_i Q_j$$

(4.1)

Where t_{sys}= time of one clock period of system;

Q_j= Amount of information, transferred from one clock period on each certain system.

N= quantity of nodes on computer networks

Pi= degree of node is compromised

T_{sys}= Time of change of network nodes distribute the message of message on route restoration.

The analysis of the information gave research appears that in assaults. The time traffic volume in channels of a system immediately increments and the most part of traffic is utilized by assault like DoS/DDoS. It's essentially backs off the system. For the expansion of effectiveness of technique of routing in operation is offered to partition the information on the virtual communication. To counteract the assaults present in the system of extra locators of observing of traffic of a system. These locators educate the executing modules in various network fragments. Routes are chosen powerfully or statically, to utilize just the physical and security of the subnet, hubs of switching and channels. Transmission of information having security labels through certain subnet, switching hubs and channels fitting to disallow the security approach.And then, it is also shown in design view as follows:

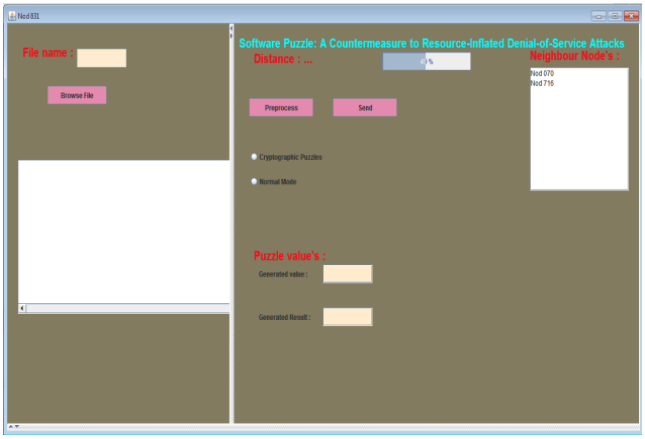

Fig.1. Allocation of nodes

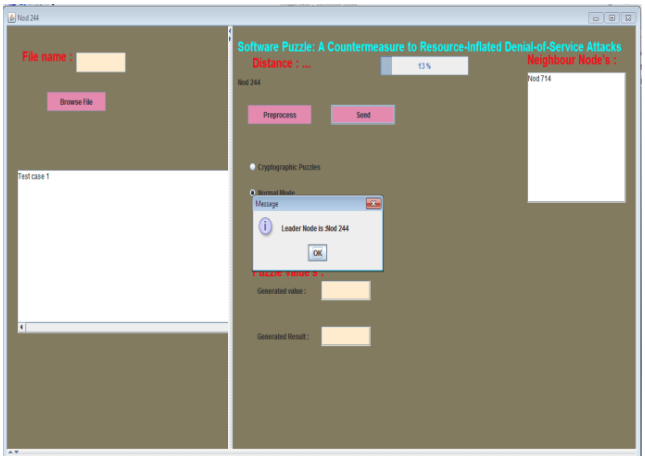

Fig.2. Obtaining the leader node details

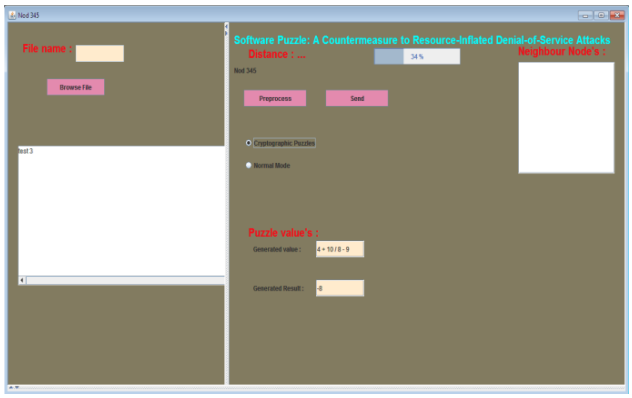

Fig.3. Message sending using cryptographic puzzles

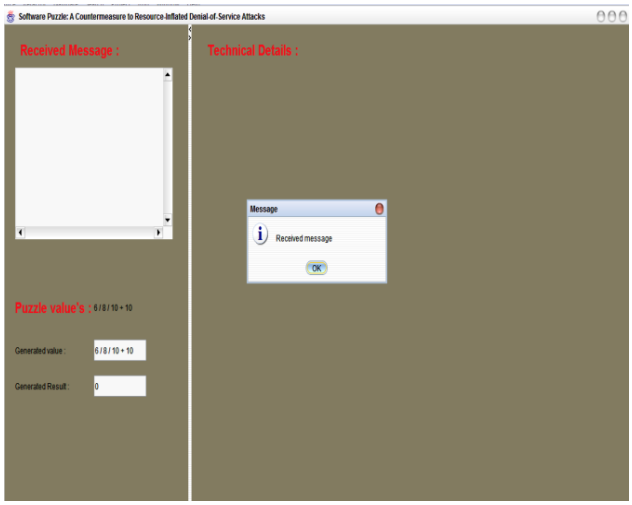

Fig.4. Successfully received the message

V. CONCLUSION

A novel effective customer puzzles taking into account of MD5 scheme. Our puzzle extends the time-lock puzzle that allows an extensively more productive operation of the puzzles arrangement that is accounted by provers. All the more particularly, our plan exchanges the puzzle check weight to the prover that executes the puzzles; we accomplish this by installing a verifier – as it were known not verifier – encompassed by the Euler trapdoor capacity that is utilized as a part of rehashed squaring puzzles. Given this, the improvement gain in the confirmation overhead of our puzzle when contrasted with the first rehashed squaring puzzle is just about 50 times for a 1024- bits modulus. Additionally, we also exhibited how our puzzle can be incorporated in various routing, counting those utilized for assurance against DoS assaults and for the remote verification of the computing performance devices.

REFERENCES

[1].Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng, "Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, January 2015.

[2]. Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks", IEEE Communications Letters, Vol. 17, No. 1, January, 2013.

[3]. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and RenPingLiu, Member, IEEE," A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis.", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[4]. Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM," Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks", IEEE/ACM Transactions On Networking, Vol. 20, No. 3, June 2012.

[5]. Moti Geva, Amir Herzberg, and Yehoshua Gev," Bandwidth Distributed Denial of Service: Attacks and Defenses", Co published by the IEEE Computer and Reliability Societies January/February 2014.

[6]. Zahid Anwar and Asad Waqar Malik," Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defense Strategies", IEEE Communications Letters, Vol. 18, No. 7, July 2014.

[7]. Shui Yu, Senior Member, IEEE, Yonghong Tian, Senior Member, IEEE, Song Guo, Senior Member, IEEE, and Dapeng Oliver Wu, Fellow, IEEE," Can We Beat DDoS Attacks in Clouds?", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 9, September 2014.

[8]. Xinlei Ma and Yonghong Chen," DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy", IEEE Communications Letters, Vol. 18, No. 1, January 2014.

[9]. Markku Antikainen, Tuomas Aura, and Mikko Särelä," Denial-of-Service Attacks in BloomFilter-Based Forwarding", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[10]. Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker," Detecting Spam Zombies by Monitoring Outgoing Messages", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[11]. Shui Yu, Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Weijia Jia, Senior Member, IEEE, Song Guo, Senior Member, IEEE, Yong Xiang, and Feilong Tang," Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient ", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.

[12]. E. Kaiser and W.-C. Feng, "mod_kaPoW: Mitigating DoS with transparentproof-of-work," in Proc. ACM CoNEXT Conf., 2007, p. 74.

[13]. NVIDIA CUDA. (Apr. 4, 2012). NVIDIA CUDA C Programming Guide, Version 4.2.Available: http://developer.download.nvidia.com/

[14]. X. Wang and M. K. Reiter, "Mitigating bandwidth-exhaustion attacks using congestion puzzles," in Proc. 11th ACM Conf. Comput. Commun.Secur., 2004, pp. 257–267.

[15] .M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols,"in Proc. IFIP TC6/TC11 Joint Working Conf. Secure Inf. Netw., Commun. Multimedia Secur., 1999, pp. 258–272.

[16]. D. Kahn, TheCodebreakers: The Story of Secret Writing, 2nd ed. New York, NY, USA: Scribners, 1996, p. 235.

[17].K. Iwai, N. Nishikawa, and T. Kurokawa, "Acceleration of AES encryption on CUDA GPU," Int. J. Netw. Comput., vol. 2, no. 1, pp. 131–145, 2012.

[18]. B. Barak et al., "On the Impossibility of obfuscating programs," in Advances in Cryptology (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 2001, pp. 1–18.

[19]. H.-Y. Tsai, Y.-L. Huang, and D. Wagner, "A graph approach to quantitative analysis of control-flow obfuscating transformations," IEEE Trans. Inf. Forensics Security,vol. 4, no. 2, pp. 257–267, 2009.

[20]. S. Wang. (Sep. 18, 2011). How to Create an Applet & C++Available: http://www.ehow.com/how_12074039_create- Applet-c.html#ixzz24Lsk0OJQ.