2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS)

Analysis and Comparison of the Network Security Protocol with DoS/DDoS Attack Resistance Performance

Linzhi Jiang
School of Computer
Science and Engineering
University of Electronic Science
and Technology of China
Chengdu 611731, China
School of Finance and Mathematics
West AnHui University
Lu An 237012,China
Email:linzhij1988@163.com

Chunxiang Xu
School of Computer
Science and Engineering
University of Electronic Science
and Technology of China
Chengdu 611731, China

Xiaofang Wang
School of Telecommunications Engineering
Xidian University
Xi'an 710071, China

Yanghong Zhou
School of Computer
Science and Engineering
University of Electronic Science
and Technology of China
Chengdu 611731, China

***Abstract*—Network security protocol design is important aspect of network security research. DoS/DDoS is very serious attack in wired and wireless network. DoS/DDoS attack depletes memory/cpu of service provider, so legitimate user can't gain normal service. According to anti-DoS attack strategy of network security protocols, we give and discuss three mechanisms (stateless connection, Fail-together and Subset Sum Client-Puzzle) on design of a key exchange protocol against denial of service attack for ISO/IEC1170-3 key exchange protocol. Subset Sum Client-Puzzle has simple structure, Non-Parallelizable speciality and fast verification. N Subset Sum Client-Puzzles' difficulties are sum of n Subset Sum Client-Puzzle's difficulty. Based on analysis of new key exchange protocol, we compare initiator and responder for computation resource, memory depletion and anti-DoS/DDoS. ISO/IEC1170-3 key exchange protocol on Subset Sum Client Puzzle, which is non-parallelizable, easy construction and verification, has the good property against DoS/DDoS attack. It provides a very good reference for network security protocol design with anti-DoS/DDoS attack.**

***Index Terms*—security protocol; DoS/DDoS; key exchange protocol;**

I. Introduction

Denial of service attack (DoS) is a common method of network attack. Malicious user attacks service provider in order to depleting it's memory/cpu resource by utilizing defects of protocol or system, making server is unable to provide service for authenticated user or making service delay. The distributed denial of service attack (DDoS) [11] is special form of DoS attack, in which malicious user destroys availability on service of network with a large number of puppet hosts. Malicious attacker can impersonate initiator of protocol to send a large number of authentication requests, if security protocol design do not consider threat of DoS/DDoS attack, then responder can easily run out of limited cpu and memory resource, and result in DoS/DDoS.

In network, DoS/DDoS attack is sponsored by malicious clients, whose target is server providing network service. Mirkovice et al. [36] provided three strategies on DoS/DDoS: (1) Protection. By modifying protocols, this strategy provides mechanisms to defend DoS/DDoS attack on server from adversaries. Protection strategy contains source validation, resource allocation, hiding, over-provisioning and proof of work. (2) Attack detection. In order to precaution DoS/DDoS attacks, server must detect such attack before protection strategy responding to them. Signature, anomaly, and misbehavior detection are three main methods for attack detection. (3) Attack response. This strategy is to reduce differentiation effect and maintain normal for legitimate users. Three prime methods are traffic policing, attack traceback and service differentiation. Direct object on DoS/DDoS is deplete responder's computation resource or memory depletion. In security protocol, endowing it with protection against DoS/DDoS is very important. According to above protection mechanism [36], three main ways defend DoS/DDoS: (1) stateless connection; (2) weak authentication; (3) increasing initiate cost. In state connection protocol, responder must save execution status of session, and provide authentication and key agreement service at the same time. When memory of responder is limited, DoS/DDoS attack of memory exhaustion is inevitable.

Aura et al. [5] put forward stateless connection. In the way of stateless connection, responder do not save information of session status about initiator, after it receives requests. The idea is to reduce memory consumption of responder. Aura et al. recommended that authentication protocol should remain stateless before validating initiator. After validating initiator about authentication information, responder can switch to stateful model. Weak authentication firstly referred to a lower computational validation, in order to authenticating identity of initiator; then beginning stronger authentication which

978-1-4799-8937-9/15 $31.00 © 2015 IEEE
DOI 10.1109/HPCC-CSS-ICESS.2015.148

exhausting more resource. The typical progressive authentication protocol is JFK protocol [19]. Kam and Simpson [12] proposed Cookie mechanism for security protocol. During the session, responder send a small piece of data (cookie) to initiator after receiving request; succedent information from initiator must include data block. The typical cookie consists of some special connection parameter, time-varying local secret, initial IP address, encrypted Hash and random number. Simpson [15] proved existence of attack about state exhaustion on cookie.

Matsuura and Imai [7] presented Fail-together mechanism against DoS attacks, and alternative IKE protocol. The main idea is to reduce computation resource consumption of responder, and increase cost of initiator. On condition of comparable computation resource between a sponsor and responder, calculation of sponsor is greater than or equal to responder's. So that attacker depletes its own computation resource, when it implements DoS attack.

Dwork and Naor [8] raised mechanism of proof of work. Basic idea is that client must prove that it has consumed certain cost to server, before it sends the mail; which makes cost of sending spam is high. Authentication protocol [13] has used this mechanism. Jakobsson and Juels [4] defined concept of reusable proof of work. To deal with the attacks on network, all kinds of client-puzzle construction had been presented. Client-puzzle is one of the easy implementation and effective method on anti-DoS/DDoS. Jules and Brainard [9] proposed the client-puzzle method to prevent SYN-flood attack. Aura et al. used it in the protocol. The idea of Client-puzzle mechanism is that the responser does not save any status, when it receives the authentication information, but only sending a puzzle based cryptography, such as initiator must solve the puzzle before continuing the protocol consuming for more resource. Frank A. Zdarsky, Matthias Wilhelm [21] implemented the client-puzzle in wireless network to help AP to defend DoS attack. Ellick M. Chan et al. [22] raised a cline-puzzle based on rhythmic nonces and cryptography. L. Chen et al. [20] firstly defined the security model about client-puzzle and the universal puzzle construction. Suratose Tritilanunt [23] provided an evaluation about authentication protocol for client-puzzle. Qiang Tang and Arjan Jeckmans [24] proved that RSW client-puzzle had the properties of parallel computation resistance and computation determinacy, and introduced the batch verification method. Antonis Michalas et al. [25] proposed an anti-DoS scheme based on the new client-puzzle for the ad hoc networks. Virendra Pal Singh et al. [26] used the short client puzzle to defend DoS attack for Wireless Sensor Networks. Mehran S. Fallah [27] took advantage of game theory to propose the optimal puzzle-based DoS defense strategies. R.Bestak et al. [28] presented a kind of secure client-puzzle architecture used in Lan, which was constructed through a random beacon. Sammy Chan et al. [29] described a scheme of anti-DoS based on client-puzzle for roaming authentication in wireless and mobile network. Bogdan Groza and Bogdan Warinschi[14] formalized the new difficulty and how to measure the difficulty bounds through the game on the client-puzzle for the theory and implementation. Lakshmi Kuppusamy et al. [30] stated how to construct the cryptographic client-puzzle for security in the standard model. Dr. Reena Dadhich et al. [31] showed the anti-DoS design based on puzzle for mobile Wimax with timestamp and nonce. Jing Yang Koh et al. [32] made use of repeated squaring and hash reversal client-puzzle with the leaky bucket algorithm to construct protocol for DoS attack. Santhosh K M and Elizabeth Isaac [33] described a method for preventing DDoS attack with stochastic model on client-puzzle. Robert H. Deng et al. [34] probed into the software puzzle to defend DDoS attack for server.

On the base of protection mechanism [36] and previous three main ways defending DoS/DDoS, stateless, Fail-together and Client-puzzle will be discussed. Discussion includes memory/cpu exhaustion, anti-DoS/DDoS attack and so on for ISO/IEC 1170-3 key exchange protocol. We propose a scheme with speciality of defending DoS/DDoS by client puzzle (Subset sum), which is Non-Parallelizable, controllable difficulty levels, easy construction and verification. The modified protocol maintains stateless.

II. ISO/IEC 1170-3 KEY EXCHANGE PROTOCOL AND ANTI-DOS TRANSFORMATION

The original ISO/IEC 1170-3 key exchange protocol: N_a are N_b Nounce, K_{ba} and K_{ab} are keys generated by each communication party. After finishing protocol, each subject gets his session key by Hash computation.

TABLE I
ISO/IEC1170-3 KEY EXCHANGE PROTOCOL

$Msg1:$	$A \longrightarrow B:$	A, N_a
$Msg2:$	$B \longrightarrow A:$	$\{N_b, N_a, A, \{B, K_{ba}\}K_a\}K_b^{-1}$
$Msg3:$	$A \longrightarrow B:$	$\{N_b, N_a, B, \{A, K_{ab}\}K_b\}K_a^{-1}$

According protocol, attacker can forge initiator to send Msg1, responder begin to generate K_{ba}, and carry on an encryption and signature computation. Cost of encryption and signature computation are high, because responder must store authentication message in memory at the same time. If a malicious user sends a large number of Msg1, responder of protocol suffers from DoS attack, which depletes computation and memory resource.

Before modification and analysis on security protocol, ability of attacker to assume: attacker can eavesdrop, tamper, forge and replay protocol information, and forge IP address; operation environment of protocol subject has enough network bandwidth and physical security countermeasure, which is main consideration of DoS attack on depletion of memory/cpu; subject of protocol can terminate process and release resource on memory/cpu, when it detects tempering, forgery and information that do not meet with running status for protocol.

Leiwo et al. [16] considered a protocol which having good ability of anti-DoS attack should include the following respects: (1) Resource should be released after sponsor is authenticated; (2) Attack detection should be completed during sponsor authentication phase; (3) Sponsor's workload should be higher than the responder to avoid Flooding-attacks; (4) Responder can adjust workload of sponsor according the requirement, so that it will ensure viability and flexibility for system. Meadows et al. [17] proposed a number of additional strategies and mechanism; (5) Reduce cost of protocol implementation about the potential defender; (6) Improve resource of defenders; (7) Introduce some authentication methods, so that defender can know source of attacks.

According above-mentioned requirements, we will modify ISO/IEC 1170-3 key exchange protocol, and analysis the anti-DoS/DDoS ability. We use three mechanisms to perfect protocol, which are stateless connection, Fail-together and Subset Sum Client-Puzzle. When server receives many session requests continuously, DoS/DDoS attacks are on. These mechanisms must be on work under attacks.

A. ISO/IEC1170-3 key exchange protocol based stateless connection

Key exchange protocol based stateless connection: A is sponsor, B is responder (server), $state_{b,i}$ stands for status information of B in interation of round i. In order to prevent an attacker from tampering with status information, responder must encrypt it's information and ensure integrity. $K_{b,e}$ and $K_{b,m}$ are security keys for responder on encryption and integrity.

TABLE II
ISO/IEC1170-3 KEY EXCHANGE PROTOCOL BASED STATELESS CONNECTION

$Msg1 : A \longrightarrow B :$	A, N_a
$Msg2 : B \longrightarrow A :$	$\{N_b, N_a, A, \{B, K_{ba}\}K_a\}K_b^{-1}, \{K_{ba}\}K_{be},$ $HMAC\{K_{bm}, \{A, N_a, N_b\{K_{ba}\}K_{be}\}\}$
$Msg3 : A \longrightarrow B :$	$\{N_a, N_b, B, \{A, K_{ab}\}K_b\}K_a^{-1}, A, N_a, N_b, \{K_{ba}\}K_{be},$ $HMAC\{K_{bm}, \{A, N_a, N_b\{K_{ba}\}K_{be}\}\}$

According above alternated protocol, responder B does not save current status, but sends back to A, after it receives request. After receiving Msg3, B firstly verifies correct of HMAC; if it is correct, protocol continue to execute. By the process of execution, we can see that responder does not store any status information in memory, so cost of memory is very low. However, duing to protecting confidentiality and integrity of protocol, there are cryptographic computation and HMAC operation, so consumption of computation resource is high. The protocol exist DoS attack by itself, if attackers send a great deal of key exchanging requests in short period.

B. ISO/IEC1170-3 key exchange protocol based Fail-together

Fail-together is based on a special signature verification algorithm. The algorithm has following characteristics:

(1) The computation of high cost can be carried out in advance on signature in advance contains in a material RF;

(2) Reconstitution of RF is required to verify signature;

(3) Matsuura and Imai [7] proposed Fail-together method, and used it in IKE protocol for anti-DoS.

ISO/IEC1170-3 key exchange protocol based Fail-together is showed in Table 3.

TABLE III
ISO/IEC1170-3 KEY EXCHANGE PROTOCOL BASED FAIL-TOGETHER

$Msg1 :$	$A \longrightarrow B :$	A, N_a
$Msg2 :$	$B \longrightarrow A :$	$N_b, N_a, A, \{B, K_{ba}\}K_a,$ $SIG_b, \{R_b, K_{ba}\}K_{be}$
$Msg3 :$	$A \longrightarrow B :$	$A, \{N_a, N_b, B, \{A, K_{ab}\}K_b\}K_a^{-1},$ $HASH_a, SIG_b, \{R_b, K_{ba}\}K_{be}$

$\{N_a, N_b, A, B, K_{ab}, B_b\}$, K_{be} is the B security key, $\{B_b, K_{ab}\}K_{be}$ make protocol stateless. $HASH_a$:

$$HASH_a = Hash\{A, \{N_a, N_b, B, \{A, K_{ab}\}K_b\}K_a^{-1}, B_b\}$$

B firstly computes B_b by decryption, after receiving Msg3, and verifies SIG_b through it. After verification, B verifies $HASH_a$ in order to ensure that A reliably makes the solution about B_b. Above-mentioned computation exhausts little resource. Computation of high cost begins with signature, after finishing above-mentioned computation. Protocol achieves the aim of stateless, and consumption of computation resource about sponsor and responder gets to a very high proportion, which significantly reduces risk of DoS attacks. But protocol only can prevent DoS attack, when attacker implement DDoS attack, protocol will lose utility.

C. ISO/IEC1170-3 key exchange protocol based Subset Sum Client-Puzzle

We use a technique called subset sum puzzle [18]. Predominant characteristic of this technology is not only a simple construction and verification as cheap as Hash-based puzzles, but also a non-parallelizable characteristic. Non-Parallelizable Client-puzzle can't be solved in parallel, so malicious attackers are unable to sponsor Dos/DDoS attack by puppet hosts to accelerate solution for puzzle. Non-Parallelizable Client-puzzle requires puzzle solving algorithm must be recursive. A subset sum system associates a given set of items, which have specifical weight, with a knapsack which can carry the number of items no more than a certain weight. Solver is required to search for a maximum value by picking many items , so the problem becomes knapsack with weight. To find whether a solution exists for a specifical weight, this becomes a decision problem, therefore knapsack falls into the NP-completeness category. This means no polynomial algorithm can break the knapsack problem within polynomial time as long as $D \neq NP$.

A famous tools used to successfully break subset sum crypt-system is lattice reduction. There are several lattice reduction algorithms, but the best method so far for breaking subset sum problem is LLL or L3 algorithm developed by lenstra et al [35]. The underlying lattice algorithm is recursive computation.

$puzzle = (w_1, W, k)$,
$w_n = H(w_{n-1})$, (pre-computed parameters set of random weight w_n),
Secret $s \in_R Z_n$ puzzle difficulty $K(25 \leq K \leq 100)$,
$c = LSB(H(ID_A, N_A, ID_B, s), K)_2$,
$W = \Sigma_1^K C_i w_i$,
ID_A is an identity of A,
ID_B is an identity of B,
N_A is nonce of A,
N_B is nonce of B.

To establish a security connection to B, A send a request containing an Identity (ID_A) along with a random nonce (N_A) to B. The B chooses a secret parameter s randomly in order to make output unique for each communication, and decides a puzzle difficulty k depending on workload . Value of k should be selected to be at least 25 to guarantee that brute-force search or bounding algorithm applied by adversary with puppet hosts approximates LLL lattice reduction algorithm applied by legitimate user. In order to construct a puzzle, B computes a Hash operation $(H(.))$, and computes $(LSB(.), K)_2$ to obtain K bits from output of Hash function. Finally, B forms a puzzle by computing a desired weight (W) that it wants a client to solve from a pre-computed set of random weight(w_n).

The weight can be generated on initial value of weight of the first item (w_1), desired weight (W), and puzzle difficulty(K). Construction of subset sum puzzle requires only one Hash operation and addition.

TABLE IV
ISO/IEC1170-3 KEY EXCHANGE PROTOCOL BASED SUBSET SUM CLIENT-PUZZLE

$Msg1:$	$A \longrightarrow B:$	A, N_a
$Msg2:$	$B \longrightarrow A:$	$\{N_b, N_a, A, \{B, K_{ba}\}K_a\}K_b^{-1}$, $Subsetsumpuzzle, \{solution, K_{ab}\}K_{be}$
$Msg3:$	$A \longrightarrow B:$	$A, \{N_a, N_b, B, \{A, K_{ab}\}K_b\}K_a^{-1}$, $solution, \{solution, K_{ab}\}K_{be}$

$HASH_a = Hash\{N_a, N_b, solution\}$. After B receives Msg3, it must decrypt information, compute and verify $Subsetsum\ puzzle$; after verification, B verifies $HASH_a$ in order to ensure that A reliably makes solution about $solution$. Above-mentioned computation exhausts little resource. Because of recursion about solving $Subsetsum\ puzzle$, it has a simple structure and difficulty for the brute force crack. So we can use it to achieve stateless about protocol. Non-Parallelizable speciality makes protocol with good nature of anti-DDoS . On account of B not saving protocol status during session, protocol is stateless. When DoS/DDoS attack becomes fierceness, we can easily adjust difficulty of puzzle by k. Improving puzzle difficulty lengthens time for solving puzzle and exhaust attackers' sources. So Subset sum possesses the linear granularity on the basis of LLL algorithm [35].

III. Security analysis

Attack model is adversaries can sponsor DoS/DDoS attack with puppet hosts. Sending a good deal of key exchange requests is representative attack. Adversaries have forging, precomputation and replay ability. They can forge identity and client-puzzle, precompute solution of client-puzzle and replay previous information and solutions.

The stateless connection is in a half open state, attacker may replay Msg3. Replaying a mass of previous information depletes memory/cpu. So stateless connection possesses certain anti-DoS ability, but it is subjected to replay attack. Fail-together makes computation comparable between the sponsor and responder, which realize stateless connection. Owing to computation of sponsor is lower than responder, Fail-together only defends DoS attack, but not for DDoS attack. Protocol is stateless, attackers may replay Msg3. So it can't be on guard replay attack. Protocol based Subset sum contains security of puzzle and anti-Dos/DDoS of protocol. Security of puzzle requires Subset sum is resistant to forge, and solution cannot be precomputed. Because puzzle based Subset sum requires responder choice different security parameter s randomly for each communication, the solution of it cannot be precomputed. Liqun Chen et al. [20] define the puzzle-unforgeability. According way of generating puzzle and parameters setting, adversaries cannot forge puzzle based subset sum. Interactive strong puzzle difficulty is defined by Douglas Stebila et al. [18], which enhances definition of puzzle-difficulty [20]. Puzzle based subset sum has non-parallelizable character. Solving n puzzles costs n times the cost of solving one puzzle, namely $\varepsilon_{d,k,n}(t) \leq \varepsilon_{d,k,1}(t/n)$. So puzzle based subset sum is unforgeable and strong difficult. Anti-DoS protocol is that the responder can execute n fresh sessions, when attacker initiates session with restricted time. Douglas Stebila et al. [18] describe Denial-of service-resistant protocol. Protocol based subset sum is stateless. Before returning correct solution of puzzle, responder only depletes very few resource. So key exchange protocol based subset sum satisfies this definition. Combining with definition of puzzle-difficulty and Theorem3 [18], the new constructive protocol has DoS-resistant speciality. Algorithm of solving Subset sum is based on lattice. LLL algorithm[35] is recursive, so parallelizable algorithm is invalid. Attacker with many puppet hosts can not solve the puzzle faster than independent. Key exchange protocol based subset sum is also DDoS-resistant.

IV. Performance comparison about Anti-DoS of the security protocol

We re-design ISO/IEC1170-3 key exchange protocol through three anti-DoS method. On analysis of the above transmission protocol, we will discuss cost about computation, memory and anti-DDoS ability.

Assumption is that three modifying key exchange protocol use same encryption algorithm, Hash function and Pseudo-Random Generation Algorithm (PRGA) during the whole protocol sessions. In order to analyze computation of sponsor and responder on every protocol session, computation cost is sum of all kinds of related computation on sponsor and responder. We compare their computation for the whole protocol. For comparison of memory cost, stored information in memory is norm. Algorithm for solving Subset sum refers to algorithm provided by Schnorr and Euchner [37].

A. Computation cost comparison about three new ISO/IEC 1170-3 key exchange protocol

ISO/IEC1170-3 key exchange protocol based stateless connection carrys out an encryption and HMAC, which in order to ensure confidentiality and integrity for information. But, in ISO/IEC1170-3 key exchange protocol based Fail-together, responder can get B_b through decryption, and verify SIG_b. In order to sure that A really makes solution about B_b, B must verify $HASH_a$. These computation has low resource exhaustion. ISO/IEC1170-3 key exchange protocol based Subset Sum Client-Puzzle needs n hash, one hash and look-up table about the hash value. But sponsor must solve puzzle based on LLL reduction algorithm [35]. So computation resource exhaustion of sponsor is much higher than responder.

TABLE V
COMPUTATION COST COMPARISON ON THREE NEW ISO/IEC1170-3 KEY EXCHANGE PROTOCOL

Computation cost	Sponsor	Responder
based stateless connection	1Decryption 1Hash(High)	1Encrypt1Hash (Low)
based Fail-together	Solve B_b 1Hash(High)	1Decryption1Hash (Low)
based Subset Sum Client-Puzzle	Solve Clint-puzzle based LLL algorithm(High)	1Hash (Low)

From Table 5, the minimum computation exhaustion is the transformed protocol based on Subset sum.

B. Memory cost comparison about three new ISO/IEC1170-3 key exchange protocol

From interactive process of above protocol, responder does not save information about protocol status, so memory exhaustion of sponsor is higher than responder.

TABLE VI
MEMORY COST COMPARISON ON THREE NEW ISO/IEC1170-3 KEY EXCHANGE PROTOCOL

Memory cost	Sponsor	Responder
based stateless connection	High	Low
based Fail-together	High	Low
based Subset Sum Client-Puzzle	High	Low

Stateless connection protocol requires sponsor A store A, $N_a, B, N_b, K_b, K_a^{-1}, K_{ab}, K_{ba}$ and running status of protocol , and responder B store K_a, K_{bm}, K_b^{-1} $and\ HMAC\{K_{bm},$ $\{A, N_a, N_b, \{K_{ba}\}K_{be}\}\}$. In Fail-together protocol, sponsor keeps $A, N_a, B, N_b, K_b, K_a^{-1}, K_{ab}, K_{ba}$ and running status of protocol in memory, responder only stores K_a, K_b^{-1}, K_{ba} and SIG_b. For protocol based on Subset sum, sponsor stores A, $N_a, B, N_b, K_b, K_a^{-1}, K_{ab}, K_{ba}$ and running status of protocol in memory, responder only stores K_a, K_b^{-1}, K_{ba} and solution.

C. Anti-DDoS comparison about three new ISO/IEC1170-3 key exchange protocol

ISO/IEC1170-3 key exchange protocol based stateless connection does not deliver anti-DDoS characteristic. Fail-together can only prevent DoS of signal attacker, but not anti-DDoS. Because of non-parallel characteristic, protocol based Subset Sum Client-Puzzle has the good ability against DDoS through puppet hosts.

TABLE VII
ANTI-DDOS COMPARISON ON THREE NEW ISO/IEC1170-3 KEY EXCHANGE PROTOCOL

Anti-DDoS	Sponsor	Responder
based stateless connection	——-	No
based Fail-together	——-	No
based Subset Sum Client-Puzzle	——-	Yes

V. CONCLUSION

Through analysis about dangers of DoS attack in the network, the beginning of design about network protocol needs to consider it's properties on anti-DoS/DDoS attack. On basis of above comparison and analysis about new ISO/IEC1170-3 key exchange protocol, we can conclude that protocol based Subset Sum Client-Puzzle has advantage of stateless, low resource exhaustion (memory/cpu) and anti-DDoS ability. In wired and wireless network, key exchange and authentication protocol exist threat, Subset sum technology can be widely used in protocol for anti-DoS/DDoS, which will introduce secure and robust network protocol.

ACKNOWLEDGMENT

The work described in this paper was supported by Lu'an commission directed city-level key research project, West Anhui University (2010LWA004), Lu'an commission directed city-level research project, West Anhui University (2012L-W022), Innovation Project of GUET Graduate Education (XJYC2012020). Author: Linzhi Jiang, male, Ph.D student, Lecturer. Research: Information security and cryptography, Email: linzhij1988@163.com.

REFERENCES

[1] Juels J, Brainard. Client puzzles: a cryptographic counter measure against connection deletion attacks. proceedings of the network and distributed security system(NDSS/99), IEEE computer society, 1999: P151-165.

[2] Cheng jianzhou. Research on Protecting Authentication Protocols against Denial of Service Attack and Implementation of Security Solution to Improve the Protocols. Nanjing,Nanjing University of Aeronautics and Astronautics, 2007 (Chinese).

[3] Gu Ye-hua, Zeng Xiao-yang, Han Jun, Zhang Zhan. A High-performance and Low-cost VLSI Implementation of the SHA-1 Hash Function. Journal of Chinese Computer Systems, Vol. 28, No.5 , pp940-943, May 2007.

[4] M.Jakobsson, A.Juels. Proofs of work and bread pudding protocols. In the IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security (CMS 99), Sep 1999.

[5] Aura T, Nikander P, Leiwo J. Resitant authentication with client puzzles. Security protocol, 2011: 170-177.

[6] Aura T, Nikander P, Leiwo J. Dos-resistant authentication with client puzzles. proc. 8th int workshop. on security protocols, Cambridge, UK, 2000.

[7] K.Matsuura, H.Imai. Protection of Authenticted Key-Agreement Protocol against a Denial of sevice Attack, Cientifica, Vol.2. No.11,1988:15-19.

[8] C.Dwork, M Noar. Pricing via processing or combatting junk mail. proc. CRYPTO"92, Calfornia USA, 1992:139-149.

[9] Aris Jules, John Brainard. Client puzzle:a cryptographic countermeasure against connection depletion attacks. In PROC. 1999 Network and Distributed system Security symposiumNDSS pages151-165,san Diego ,CA,February 1999.

[10] Russell Impaglia, Moni Naor. Efficient cryptographic Scheme Provably as sceurity as subset sum. Journal of cryptology-springer: pages 236-241,1989.

[11] J. Vijayan. Denial-of-service attacks still a threat. September 22, 2004.

[12] P. Karn , W. A. Experimental RFC 2522. http://www.ietf.org/rfc/rfc 2522.txt.

[13] T.Aura, P.Nikander, J.Leiwo. DoS-resistant authentication with client puzzles. Cambridge: Security Protocols Workshop 2000, Apr 2000: pages 170-181.

[14] Bogdan Groza1 and Bogdan Warinschi. Cryptographic Puzzles and DoS Resilience, Revisited. Information Security Lecture Notes in Computer Science Volume 7483, 2012, pp 39-54.

[15] W.A.Simpson. IKE/ISAKMP Considered Harmful. 1999.

[16] J.Leiwo, P.Nikander, T.Aura. Towards network denial of service resistant protocols. The 15th Annual Working Conference on Information Security (SEC2000). China : Aug 2000, volume 175.

[17] C.Meadows. A Cost-Based Framework for Analysis of DoS in Networks. Journal of Computer Security, Jan 2001,9(1/2):143-164.

[18] Douglas Stebila et al. Stronger difficulty notions for client puzzles and denial-of -service-resistant protocols. The Cryptographers' Track at the RSA Conference, LNCS, volume 6558, pp. 284-301. Springer, 2011. This is the full version.

[19] W. Aiello, et al. Efficient, DoS-resistant, secure key exchange for internet protocols. The 9th ACM Conference on Computer and Communications Security, 2002, pages 48-58.

[20] Liqun Chen, et al. Security notions and generic constructions forclient puzzles. ASIACRYPT 2009, LNCS, 2009,volume 5912, pp.505-523.

[21] Martinovic I, Zdarsky F A, Wilhelm M, et al. Wireless client puzzles in IEEE 802.11 networks: security by wireless. Acm Conference on Wireless Network Security, 2008:36–45.

[22] Chan E M, Gunter C A, Jahid S, et al. Using rhythmic nonces for puzzle-based DoS resistance. Csaw '08 Proceedings of Acm Workshop on Computer Security Architectures, 2008.

[23] Tritilanunt S. Performance Evaluation of Non-parallelizable Client Puzzles for Defeating DoS Attacks in Authentication Protocols. Lecture Notes in Computer Science, 2010, 6166.

[24] Tang Q, Jeckmans A. On Non-Parallelizable Deterministic Client Puzzle Scheme with Batch Verification Modes. Centre for Telematics and Information Technology University of Twente, 2010.

[25] Michalas A, Komninos N, Prasad N R, et al. New client puzzle approach for DoS resistance in ad hoc Networks. Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on. IEEE, 2010:568 - 573.

[26] Singh V P, Jain S, Singhai J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. International Journal of Computer Science Issues, 2010.

[27] Fallah M S. A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory. Dependable and Secure Computing IEEE Transactions on, 2010, 7(1):5-19.

[28] Jerschow Y I, Mauve M. Secure Client Puzzles Based on Random Beacons. Lecture Notes in Computer Science, 2012:184-197.

[29] He D, Chen C, Chan S, et al. Strong roaming authentication technique for wireless and mobile networks. International Journal of Communication Systems, 2013, 26(8):1028-1037.

[30] Kuppusamy L, Rangasamy J, Stebila D, et al. Practical client puzzles in the standard model. Proceedings of Acm Symposium on Information Computer and Communications Security, 2012.

[31] Dr. Reena Dadhich, Ms.Geetika Narang and Dr. D.M.Yadav. PUZZLE BASED APPROACH FOR SOLVING DENIAL OF SERVICE ATTACK IN MOBILE WIMAX. International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[32] Jing Y K, Ming J T C, Niyato D. Rate limiting client puzzle schemes for denial-of-service mitigation. Wireless Communications and Networking Conference (WCNC), 2013 IEEE. IEEE, 2013:1848 - 1853.

[33] M. S K, Isaac E. Defending DDoS Attack using Stochastic Model based Puzzle Controller. International Journal of Computer Science and Network Security, 2013.

[34] Wu Y, Zhao Z, Bao F, et al. Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks. IEEE Transactions on Information Forensics and Security, 2015, 10(1):168 - 177.

[35] Smeets I, Lenstra A, Lenstra H, et al. The History of the LLL-Algorithm: The LLL Algorithm. Springer Berlin Heidelberg, 2009:126-145.

[36] Mirkovic J, Dietrich S. et al. Internet Denial of Service: Attack and Defense Mechanisms. University of Pittsburgh, 2005.

[37] Schnorr C P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming, 1994, 66(1-3):181-199.