(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 4 월 18 일 (18.04.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/055091 A1

(51) 국제특허분류:
H04L 12/56 (2006.01) *H04L 1/16* (2006.01)

(21) 국제출원번호: PCT/KR2012/008194

(22) 국제출원일: 2012 년 10 월 10 일 (10.10.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0103135 2011 년 10 월 10 일 (10.10.2011) KR

(71) 출원인: **고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION)** [KR/KR]; 136-701 서울시 성북구 안암동 5 가 1, Seoul (KR).

(72) 발명자: **권신일 (KWON, Shin-il)**; 130-070 서울시 동대문구 용두동 751-8, 309 호, Seoul (KR). **차성덕 (CHA, Sungdeok)**; 136-729 서울시 성북구 종암동 삼성래미안 아파트 2 차 210-1401, Seoul (KR). **정세훈 (JUNG, Se-Hun)**; 136-072 서울시 성북구 안암동 2 가 155-5, 4 층, Seoul (KR). **김영갑 (KIM, Young-Gab)**; 427-708 경기도 과천시 별양동 주공아파트 614-303, Gyeonggi-do (KR).

(74) 대리인: **특허법인 충현 (CHUNG HYUN PATENT & LAW FIRM)**; 137-130 서울시 서초구 바우뫼로 225 한마음빌딩 4 층, Seoul (KR).

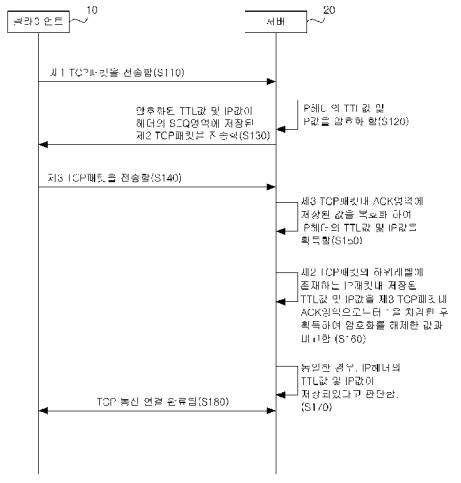
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) **Title**: METHOD AND SYSTEM FOR STORING INFORMATION BY USING TCP COMMUNICATION

(54) **발명의 명칭** : TCP 통신을 이용한 정보 저장방법 및 시스템



10 ... Client
20 ... Server
S110 ... Transmit a first TCP packet
S120 ... Encrypt a TTL value and IP value of an IP header
S130 ... Transmit a second TCP packet of which an encrypted TTL value and an IP value are stored in an SEQ region of its header
S140 ... Transmit a third TCP packet
S150 ... Decrypt a value stored in an ACK region of the third TCP packet to obtain a TTL value and an IP value of an IP header
S160 ... Compare a TTL value and an IP value, stored in an IP packet present on a lower level of the second TCP packet, with a decrypted value after subtracting 1 from the ACK region of the third TCP packet
S170 ... If equal, it is determined that a TTL value and an IP value of an IP header are stored
S180 ... TCP communication connection is completed

(57) **Abstract**: The present invention relates to a method and system for storing information by using TCP communication. The method of the present invention includes: activating, at a client, an SYN region of a header of a TCP packet to request a TCP communication connection with a server, generating a random number, and transmitting, to the server, a first TCP packet that includes the generated number in an SEQ region of the header of the TCP packet; encrypting, at the server, at least one piece of information to be stored in the first TCP packet; activating, at the server, the SYN region of the header of the TCP packet, storing encrypted information in the SEQ region of the header of the TCP packet, and transmitting, to the client, a second TCP packet storing, in an ACK region of the header of the TCP packet, a value derived by adding 1 to the random number in the SEQ region of the first TCP packet; activating, at the client, the ACK region of the header of the TCP packet, storing, in the SEQ region of the header of the TCP packet, a value that is derived by adding 1 to the random number stored in the SEQ region of the header of the first TCP packet, and transmitting, to the server, a third TCP packet that includes a value derived by adding 1 to the encrypted information in the ACK region of the header of the TCP packet; decrypting, at the server, the ACK region of the header of the third TCP packet to obtain encrypted information; and if it is determined through comparison that information stored in an IP packet present on a lower level of the second TCP packet is the same as a value that is derived by subtracting 1 from a value obtained from the ACK region of the header of the third TCP packet, determining that the information has been stored in the SEQ region of the second TCP packet and the ACK region of the third TCP packet.

(57) **요약서**:

[다음 쪽 계속]

WO 2013/055091 A1

본 발명은 TCP 통신을 이용한 정보 저장 방법 및 시스템에 관한 것으로, 클라이언트가 서버와의 TCP 통신 연결을 요청하기 위한 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제 1 TCP 패킷을 상기 서버로 전송하는 통신연결요청단계; 상기 서버가 상기 제 1 TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화하는 암호화단계; 상기 서버가 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, TCP 패킷의 헤더 중 SEQ 영역에 암호화된 정보를 저장하고, 상기 제 1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1 을 더한 값을 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제 2 TCP 패킷을 상기 클라이언트로 전송하는 통신연결확인단계; 상기 클라이언트가 TCP 패킷의 헤더 중 ACK 영역을 활성화하고, 상기 제 1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1 을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장하며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1 을 더한 값을 포함하는 제 3 TCP 패킷을 상기 서버로 전송하는 응답단계; 상기 서버가 상기 제 3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 암호화된 정보를 획득하는 복호화단계; 및 상기 서버가 상기 제 2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제 3 TCP 패킷의 헤더 중 ACK 영역으로부터 획득한 값에서 1 을 차감한 값을 비교하여 동일한 경우, 상기 정보가 제 2 TCP 패킷의 SEQ 영역과 제 3 TCP 패킷의 ACK 영역에 저장되었다고 판단하는 판단단계; 를 포함한다.

명세서

발명의 명칭: TCP통신을 이용한 정보 저장방법 및 시스템

기술분야

[1] 본 발명은 TCP통신을 이용한 정보 저장방법 및 시스템에 관한 것으로, 특히 서버와 클라이언트간 TCP통신의 연결과정을 수행함과 동시에, 상기 서버의 특정정보를 네트워크 패킷에 저장할 수 있는 TCP통신을 이용한 정보 저장방법 및 시스템에 관한 것이다.

[2]

배경기술

[3] 서버와 클라이언트 간에 이루어지는 TCP(Transmission Control Protocol)통신은 상대방의 IP주소와 포트를 알고 난 후에 통신연결을 요청하며, 이때, 상기 클라이언트로부터 통신연결을 요청받은 서버가 통신연결에 대한 응답을 받아주지 않으면 계속적으로 통신연결 요청을 수행한다. 이후, 통신연결이 되면, 서버와 클라이언트는 통신연결이 끊어지기 전까지 양방향 통신을 수행한다. 이러한 TCP통신은 특히, 전송하고자 하는 데이터가 정확히 전송되었는지를 확인할 수 있는 매카니즘을 포함하므로, 전송하고자 하는 데이터가 미수신 된 경우에는 상기 데이터를 재전송을 수행할 수 있어 데이터 전송에 신뢰성을 가질 수 있는 것이 특징이다.

[4] 이하, 도 1을 참조하여, 기본적인 TCP통신의 연결과정에 대하여 구체적으로 살펴보도록 한다.

[5] 도 1은 서버와 클라이언트간 TCP 통신의 기본적인 연결과정을 나타내는 순서도이다.

[6] 도 1에 도시된 바와 같이, TCP통신은 먼저, 클라이언트(10)가 서버(20)와의 TCP연결을 위해 TCP 패킷의 헤더 중 SYN영역의 플래그가 1로 설정된 제1 TCP 패킷을 상기 서버(20)로 전송한다(S11). 이때, 상기 SYN 영역의 플래그가 1인 것은 상기 클라이언트(10)가 상기 서버(20)로 TCP통신 연결을 요청하는 의미로 사용된다.

[7] *이에 따라, 상기 서버(20)는 수신한 제1 TCP 패킷에 응답하여, 상기 클라이언트(10)와의 TCP연결을 수행하기 위한 준비를 한다(S12).

[8] 이후, 상기 서버(20)는 상기 클라이언트(10)와의 TCP 연결을 위한 준비과정을 마치고, 수신한 제1 TCP 패킷에 대한 응답으로서, TCP 패킷의 헤더 중 ACK영역의 플래그가 1로 설정되고, SYN영역의 플래그 또한 1로 설정된 제2 TCP 패킷을 상기 클라이언트(10)로 전송한다(S13).

[9] 이때, 상기 서버(20)가 전송하는 제2 TCP 패킷의 헤더 중 SYN 영역의 플래그가 1로 설정되는 것은 상기 서버(20) 또한 상기 클라이언트(10)와의 통신연결을 원하고 있다는 의미로 전송된다.

[10] 이와 같이, 상기 서버(20)로부터 SYN영역 및 ACK 영역의 플래그가 각각 1로 설정된 제2 TCP 패킷을 수신한 상기 클라이언트(10)는 이에 응답하여 상기 서버(20)와의 TCP연결을 위한 준비를 수행한다(S14).

[11] 이후, 상기 클라이언트(10)는 상기 서버(20)와의 TCP연결을 위한 준비를 마치고, 수신한 상기 제2 TCP 패킷에 대한 응답으로서, TCP 패킷의 헤더 중 ACK 영역의 플래그가 1로 설정된 제3 TCP 패킷을 상기 서버(20)로 전송(S15)하여, 상기 서버(20)와 클라이언트(10)간에 TCP연결을 완료한다(S16).

[12] 이러한 서버(120)와 클라이언트(110)간 TCP통신 연결 시, 상호 전달되는 패킷을 통해 상기 서버(120)는 내부 메모리 공간에 접근한 클라이언트의 IP주소, 접근시간, SEQ번호, 윈도우 크기 등 다양한 종류의 정보를 저장하게 된다. 따라서, 상기 서버(120)는 클라이언트(110)의 IP주소, 접근 시간, SEQ번호, 윈도우 크기 등과 같은 다양하고 많은 양의 정보를 저장하기 위해, 상기 서버(120)가 별도의 메모리공간을 할애해야만 한다는 번거로움과, 이로 인해 DOS 공격 또는 DDOS 공격을 받는 비정상적인 상황에서 상기 서버(120)에 리소스가 소모되고, 많은 부하가 걸린다는 문제점이 발생했다.

[13] 상술한 바와 같이, 서버와 클라이언트간 TCP통신 연결에 대한 선행기술을 살펴보면 다음과 같다.

[14] 선행기술 1은 한국공개특허 제2011-0018528호(2011.02.24)로서, 네트워크 상에서 TCP SYN 플러딩 공격을 차단하는 장치 및 방법에 관한 것이다. 이러한 선행기술 1은 클라이언트로부터 상기 클라이언트와 서버의 연결 설정을 위한 SYN 패킷을 수신하면, 상기 클라이언트로 타임스탬프(Timestamp) 옵션을 적용한 SYN 패킷을 전송하고, 상기 클라이언트로부터 타임스탬프 옵션이 적용된 ACK 패킷을 수신하면, 상기 클라이언트와 서버 사이를 연결함으로써, 네트워크 상에서 악의적인 TCP SYN 플러딩 공격을 효율적으로 차단한다.

[15] 또한, 선행기술 2는 한국공개특허 제2011-0070750(2011.06.24)호로서, 안전한 TCP 연결 관리 장치 및 방법에 관한 것이다. 이러한 선행기술 2는 TCP 연결을 위해 수신한 SYN 패킷에 근거하여 검증키를 생성하여 사용자 단말기에 전달하고, 전달된 검증키에 대한 사용자 단말기로부터의 응답 신호를 분석한 결과와 SYN 패킷에 근거하여 유효한 TCP 연결인지를 판단하며, 유효한 TCP 연결인지에 대한 판단결과에 근거하여 사용자 단말기로부터 통신 서버로의 데이터 패킷의 송수신을 제어함으로써, TCP 연결에 대한 서비스 거부 공격을 효과적으로 차단한다.

[16]

발명의 상세한 설명

기술적 과제

[17] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 서버와 클라이언트간 TCP통신 연결 시, 상기 서버가 저장하고자 하는 특정정보를 TCP

통신 시 송수신되는 TCP 패킷의 헤더에 저장함으로써, 별도의 저장공간을 사용하지 않고도 특정정보를 저장할 수 있는 TCP통신을 이용한 정보 저장방법 및 시스템을 제공하고자 한다.

[18]

과제 해결 수단

[19] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 TCP통신을 이용한 정보 저장방법은 클라이언트가 서버와의 TCP 통신 연결을 요청하기 위한 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 상기 서버로 전송하는 통신연결요청단계; 상기 서버가 상기 제1 TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화하는 암호화단계; 상기 서버가 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, TCP 패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 상기 클라이언트로 전송하는 통신연결확인단계; 상기 클라이언트가 TCP 패킷의 헤더 중 ACK 영역을 활성화하고, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장하며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 포함하는 제3 TCP 패킷을 상기 서버로 전송하는 응답단계; 상기 서버가 상기 제3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 암호화된 정보를 획득하는 복호화단계; 및 상기 서버가 상기 제2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제3 TCP 패킷의 헤더 중 ACK 영역으로부터 1을 차감하고 획득하여 암호화를 해제한 값을 비교하여 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단하는 판단단계; 를 포함한다.

[20] 특히, TCP통신을 위해 사용되는 TCP헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화하는 암호화단계를 포함할 수 있다.

[21] 특히, 상기 서버가 상기 TTL값 및 IP값을 해시하고, 해시한 값을 상기 서버의 고유정보를 이용하여 암호화하는 암호화단계를 포함할 수 있다.

[22] 특히, 상기 서버가 기설정된 시간마다 상기 고유정보를 변경하는 암호화단계를 포함할 수 있다.

[23] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 TCP통신을 이용한 정보 저장시스템은 클라이언트로부터 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 전송받아, TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화하고, TCP 패킷의 헤더 중 SYN 영역 및 ACK영역을 활성화하고, TCP

패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 상기 제1 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 상기 클라이언트로 전송하며, 상기 클라이언트로부터 TCP 패킷의 헤더 중 ACK 영역이 활성화되고, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장되며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 저장하는 제3 TCP 패킷을 전송받아, 상기 제3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 암호화된 정보를 획득한 후, 상기 제2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제3 TCP 패킷의 헤더 중 ACK 영역으로부터 1을 차감하고 획득하여 암호화를 해제한 값을 비교하여 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단하는 서버를 포함하는 것을 특징으로 한다.

[24] 특히, TCP통신을 위해 사용되는 TCP 헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화하는 서버를 포함할 수 있다.

[25] 특히, 상기 TTL값 및 IP값을 해시하고, 해시한 값을 상기 서버의 고유정보를 이용하여 암호화하는 서버를 포함할 수 있다.

[26] 특히, 기설정된 시간마다 상기 고유정보를 변경시키는 서버를 포함할 수 있다.

[27]

발명의 효과

[28] 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버와 클라이언트간 TCP통신 연결 시, 상기 서버와 클라이언트간에 상호 송수신되는 TCP 패킷의 헤더 중 SEQ 영역 및 ACK 영역에 상기 서버가 저장하고자 하는 특정정보를 저장함으로써, 별도의 저장공간을 사용하지 않더라도 상기 특정정보를 용이하게 저장할 수 있는 효과가 있다.

[29] 또한, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버가 저장하고자 하는 특정정보를 별도의 저장공간에 저장하지 않고, TCP통신연결을 위해 클라이언트로 송수신되는 TCP 패킷의 헤더 중 SEQ 영역 및 ACK 영역에 상기 특정정보를 저장함에 따라, 상기 서버의 부하를 감소시킬 수 있는 효과가 있다.

[30] 더불어, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버가 저장하고자 하는 특정정보를 해시한 후, 해시한 값을 자신의 고유정보(key)를 이용하여 암호화하고, 이를 TCP 패킷의 헤더 중 SEQ 영역 및 ACK 영역에 저장하여 클라이언트로 전송하되, 상기 고유정보를 기설정된 시간마다 변경함으로써, 외부 공격자에 의해 공격을 받더라도 상기 고유정보의 복호화를 수행할 수 없도록 하여 상기 고유정보가 외부로 노출되거나 예측되는 것을 방지할 수 있는 효과가 있다.

[31] 이와 더불어, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 통신하고자 하는 클라이언트가 IP정보를 속이지 않는다고 판단하기 전까지 서버가 저장공간을 할애하지 않도록 함으로써, 클라이언트의 IP정보를 속이는 다양한 공격을 효과적으로 방어할 수 있는 효과가 있다.

[32] 또한, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 프로그램에 따라 다양한 방식이 사용되는 TCP 패킷의 데이터 영역이 아닌 정형화된 포맷이 존재하는 TCP 패킷의 헤더부분에 기록함에 따라 기존의 TCP통신을 위해 사용되는 클라이언트 부분에서 수정 또는 변경없이 용이하게 적용할 수 있는 효과가 있다.

[33]

도면의 간단한 설명

[34] 도 1은 서버와 클라이언트간 TCP통신의 기본적인 연결과정을 나타내는 순서도이다.

[35] 도 2는 서버와 클라이언트간의 TCP통신연결 시 수행되는 TCP 3방향 핸드쉐이크 과정을 나타낸 순서도이다.

[36] 도 3은 본 발명의 일 실시 예에 따른 TCP통신을 이용한 정보 저장방법을 나타낸 순서도이다.

발명의 실시를 위한 최선의 형태

[37] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[38] 먼저 본 발명에서 사용되는 서버와 클라이언트간의 TCP통신 연결은 상호간 인증을 위해, TCP헤더를 이용하여 TCP 3방향 핸드쉐이크 과정을 수행한다.

[39] 이하, 도 2를 참조하여, 서버와 클라이언트간의 TCP통신연결 시 수행되는 TCP 3방향 핸드쉐이크(3-way handshake) 과정에 대하여 살펴보도록 한다.

[40] 도 2는 서버와 클라이언트간의 TCP통신연결 시 수행되는 TCP 3방향 핸드쉐이크 과정을 나타낸 순서도이다.

[41] 도 2에 도시된 바와 같이, TCP 3방향 핸드쉐이크 과정은 먼저, 클라이언트(10)가 임의의 숫자를 생성하여, TCP 패킷의 헤더 중 SYN 영역의 플래그가 1로 활성화되고, 앞서 생성된 임의의 숫자를 SEQ영역에 포함하는 TCP 패킷을 서버(20)로 전송한다(S21).

[42] 이에 따라, 상기 서버(20)는 수신한 TCP 패킷에 응답하여 임의의 숫자를 생성한 후, TCP 패킷의 헤더 중 SYN 영역의 플래그가 1로 활성화되고, SEQ영역에 앞서 생성한 임의의 숫자를 저장하고, 상기 클라이언트로부터 수신한 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 ACK 영역에 포함시켜 상기 클라이언트(10)로 전송한다(S22).

[43] 이후, 상기 클라이언트(10)는 TCP 패킷의 헤더 중 SYN 영역의 플래그가 0으로 설정되어 비활성화되고 ACK 영역의 플래그가 1로 설정되어 활성화되며, SEQ 영역에 앞서 자신이 생성한 임의의 숫자에 1을 더한 값을 저장하며, ACK 영역에 상기 서버(20)로부터 수신한 TCP 패킷의 헤더 중 SEQ영역에 포함된 임의의 숫자에 1을 더한 값을 전송하여 상기 서버(20)로 전송한다(S23).

[44] 만약, 이러한 TCP 3방향 핸드쉐이크 과정에 있어서, 상기 클라이언트(10)가 자신의 IP주소를 속이고, 상기 서버(20)로 TCP 패킷의 헤더 중 SYN 영역의 플래그가 1이고, SEQ 영역에 임의로 생성한 숫자를 포함하는 TCP 패킷을 상기 서버(20)로 전송하는 경우, 상기 서버(20)는 상기 클라이언트(10)가 속인 위치로 해당 TCP 패킷을 전송하게 된다. 이에 따라, 상기 클라이언트(10)는 상기 서버(20)로부터 해당 TCP 패킷을 수신하지 못하게 되어, 해당 TCP 패킷 내 포함되는 임의의 숫자를 확인할 수 없게 되므로, 자신을 증명하지 못하게 된다.

[45] 이하, 도 3을 참조하여, 본 발명의 TCP 통신을 이용한 정보 저장방법에 대하여 자세히 살펴보도록 한다.

[46] 도 3은 본 발명의 일 실시 예에 따른 TCP통신을 이용한 정보 저장방법을 나타낸 순서도이다.

[47] 도 3에 도시된 바와 같이, 본 발명의 TCP 통신을 이용한 정보 저장방법은 클라이언트(110)가 서버(120)와의 TCP통신연결을 요청하기 위해, TCP 패킷의 헤더 중 SYN 영역의 플래그 1로 활성화하고, 임의의 숫자를 생성한 후, 생성된 임의의 숫자를 TCP 패킷의 해더 중 SEQ영역에 저장된 제1 TCP 패킷을 상기 서버(120)로 전송한다(S110).

[48] 상기 서버(120)는 상기 클라이언트로(110)부터 수신한 상기 제1 TCP 패킷에 응답하여 TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화한다(S120).

[49] 이러한 서버(120)는 TCP 패킷 내 저장하고자 하는 적어도 하나의 정보를 암호화하는 방법 외에도, 상기 정보를 해시한 후 암호화하거나, 상기 서버(120)의 고유정보 즉, 키 값을 갖는 해시(HMAC: Hash-based Message Authentication code)를 수행함으로써, 상기 정보를 암호화할 수 있다. 특히, 이러한 암호화과정을 상술한 방법 외에도 현재 사용되고 있는 다양한 암호화방법이 사용될 수 있음은 자명하다.

[50] 상기 서버(120)는 패킷을 받은 시간, 윈도우 크기 등의 정보를 복호화 시 필요한 정보 중에서 TCP헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화할 수 있으며, 특히 상기 TTL값 및 IP값을 해시하고, 해시한 값을 서버(120) 자신의 고유정보를 이용하여 암호화하는 것이 바람직하다. 특히 이때, 상기 서버(120)의 고유정보는 기설정된 시간마다 변경되도록 함으로써, 외부 공격자에 의한 해킹으로부터 저장하고자 하는 정보가 노출되지 않도록 보호할 수 있다.

[51] 이와 같이, 네트워크 패킷에 저장하고자 하는 TTL값 및 IP값을 포함하는 특정정보를 암호화한 상기 서버(120)는 TCP 패킷의 헤더 중 SYN 영역 및 ACK

영역의 플래그를 1로 각각 설정하여 활성화하고, TCP 패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 상기 클라이언트(110)로 전송한다(S130). 이때, 플래그가 1인 상태를 갖는 상기 제2 TCP 패킷의 SYN 영역은 상기 서버(120)가 상기 클라이언트(110)와의 통신연결을 원하고 있다는 의미를 포함한다. 또한, 상기 제2 TCP 패킷의 SEQ 영역은 앞서 S120과정을 통해 암호화된 상기 정보를 4Byte의 크기에 맞도록 저장한다.

[52] 이에 따라, 상기 클라이언트(110)는 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장하며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 포함하는 제3 TCP 패킷을 상기 서버(120)로 전송한다(S140).

[53] 이와 같이, 상기 제3 TCP 패킷을 수신한 상기 서버(120)는 상기 제3 TCP 패킷의 ACK 영역에 저장된 값 중 ACK number에서 1을 빼고난 후 이를 복호화하고, 자신의 고유정보를 이용하여 상기 해시한 값에 포함된 상기 서버(120)가 저장하고자 한 TTL값 및 IP값을 포함하는 특정정보를 획득한다(S150).

[54] 이외에도, 상기 서버(120)가 상기 제3 TCP 패킷의 ACK영역에 저장된 특정정보를 다시 해시하여 상기 특정정보를 확인할 수 있다.

[55] 이후, 상기 서버(120)는 제2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제3 TCP 패킷의 헤더 중 ACK 영역으로부터 1을 차감한 후 획득한 값에 대하여 암호화를 해제한 값을 상호 비교하여(S160) 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 상기 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단한다(S170).

[56] 따라서, 상기 서버(120)와 클라이언트(110) 간에 TCP 패킷의 송수신과정을 통해 상기 서버(120)와 클라이언트(110)간 TCP통신이 연결된다(S180).

[57] 상술한 바와 같이, 상기 서버(120)와 클라이언트(110) 간에 TCP통신을 위한 연결을 수행하는 과정에서, 별도의 저장공간을 사용하지 않더라도 상기 서버(120)가 저장하고자 하는 특정정보를 송수신되는 TCP 패킷의 헤더에 용이하게 저장할 수 있는 효과를 기대할 수 있다.

[58] 특히, 프로그램에 따라 다양한 방식이 사용되는 TCP 패킷의 내용부분이 아닌 정형화된 포맷이 존재하는 TCP 패킷의 헤더부분에 기록함에 따라 기존의 TCP통신을 위해 사용되는 클라이언트 부분에서 수정 또는 변경없이 용이하게 적용할 수 있는 효과가 있다.

[59] 또한, 이러한 TCP 통신을 이용한 정보 저장 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록

장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[60] 본 발명의 다른 실시 예에 따른 TCP통신을 이용한 정보 저장 시스템은 기본적으로 클라이언트(110)와 서버(120)를 상호 연결되어 있는 환경에서 구현된다.

[61] 이때, 상기 클라이언트(110)는 서버와의 TCP 통신 연결을 요청하기 위한 TCP 패킷의 헤더 중 SYN 영역을 1로 설정하여 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 상기 서버로 전송하고, TCP 패킷의 헤더 중 ACK 영역을 활성화하여 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장하며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 포함하는 제3 TCP 패킷을 상기 서버(120)로 전송한다.

[62] 서버(120)는 클라이언트(110)로부터 TCP 패킷의 헤더 중 SYN 영역이 1로 설정되어 활성화되고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 수신하여, TCP 패킷의 헤더에 저장하고자 하는 적어도 하나의 정보를 암호화하고, TCP 패킷의 헤더 중 SYN 영역 및 ACK 영역을 각각 1로 설정하여 활성화하고, TCP 패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 상기 제1 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 클라이언트(110)로 전송하며, 상기 클라이언트(110)로부터 TCP 패킷의 헤더 중 ACK영역이 1로 설정되어 활성화되며, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장되며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 저장하는 제3 TCP 패킷을 수신하여, 상기 제3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 상기 ACK영역으로부터 1을 차감한 후 획득하여 암호화를 해제한 값과 비교하여 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단한다.

[63] 이러한 서버(120)는 TCP통신을 위해 사용되는 TCP 헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화하되, 상기 TTL값 및 IP값을 해시하거나, 해시한 값을 자신의 고유정보를 이용하여 암호화하는 것이 바람직하다. 또한, 상기 서버(120)는 기설정된 시간마다 상기 고유정보를 변경한다. 특히, 상기 서버(120)는 외부 공격자에 의해 공격을 받는다고 판단하는 경우에는 일반적인 경우에 상기 고유정보를 변경하는 시간보다 빠르게 상기 고유정보를 변경하는 바와 같이, 상기 고유정보의 변경시간을 그 상황에 따라 가변할 수 있도록 함으로써, 저장하고자 하는 특정정보가 외부 공격자에 의해 외부로 노출되지 않도록 하는 효과를 기대할 수 있다.

[64] 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버와 클라이언트간 TCP통신 연결 시, 상기 서버와 클라이언트간에 상호 송수신되는 TCP 패킷의 헤더 중 SEQ영역 및 ACK 영역에 상기 서버가 저장하고자 하는 특정정보를 저장함으로써, 별도의 저장공간을 사용하지 않더라도 상기 특정정보를 용이하게 저장할 수 있는 효과가 있다.

[65] 또한, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버가 저장하고자 하는 특정정보를 별도의 저장공간에 저장하지 않고, TCP통신연결을 위해 클라이언트로 송수신되는 TCP 패킷의 헤더 중 SEQ 영역 및 ACK 영역에 상기 특정정보를 저장함에 따라, 상기 서버의 부하를 감소시킬 수 있는 효과가 있다.

[66] 더불어, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 서버가 저장하고자 하는 특정정보를 해시한 후, 해시한 값을 자신의 고유정보(key)를 이용하여 암호화하고, 이를 TCP 패킷의 헤더 중 SEQ 영역 및 ACK 영역에 저장하여 클라이언트로 전송하되, 상기 고유정보를 기설정된 시간마다 변경함으로써, 외부 공격자에 의해 공격을 받더라도 상기 고유정보의 복호화를 수행할 수 없도록 하여 상기 고유정보가 외부로 노출되거나 예측되는 것을 방지할 수 있는 효과가 있다.

[67] 이와 더불어, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 통신하고자 하는 클라이언트가 IP정보를 속이지 않는다고 판단하기 전까지 서버가 저장공간을 할애하지 않도록 함으로써, 클라이언트의 IP정보를 속이는 다양한 공격을 효과적으로 방어할 수 있는 효과가 있다.

[68] 또한, 본 발명의 TCP통신을 이용한 정보 저장방법 및 시스템은 프로그램에 따라 다양한 방식이 사용되는 TCP 패킷의 데이터 영역이 아닌 정형화된 포맷이 존재하는 TCP 패킷의 헤더부분에 기록함에 따라 기존의 TCP통신을 위해 사용되는 클라이언트 부분에서 수정 또는 변경없이 용이하게 적용할 수 있는 효과가 있다.

[69] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

[70]

청구범위

[청구항 1] 클라이언트가 서버와의 TCP 통신 연결을 요청하기 위한 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 상기 서버로 전송하는 통신연결요청단계;
상기 서버가 상기 제1 TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화하는 암호화단계;
상기 서버가 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, TCP 패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 상기 클라이언트로 전송하는 통신연결확인단계;
상기 클라이언트가 TCP 패킷의 헤더 중 ACK 영역을 활성화하고, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장하며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 포함하는 제3 TCP 패킷을 상기 서버로 전송하는 응답단계;
상기 서버가 상기 제3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 암호화된 정보를 획득하는 복호화단계; 및
상기 서버가 상기 제2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제3 TCP 패킷의 헤더 중 ACK 영역으로부터 1을 차감하고 획득하여 암호화를 해제한 값을 비교하여 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단하는 판단단계;
를 포함하는 TCP 통신을 이용한 정보 저장 방법.

[청구항 2] 제1항에 있어서,
상기 암호화단계는
TCP통신을 위해 사용되는 TCP헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화하는 것을 특징으로 하는 TCP통신을 이용한 정보 저장방법.

[청구항 3] 제2항에 있어서,
상기 암호화단계는
상기 서버가 상기 TTL값 및 IP값을 해시하고, 해시한 값을 상기 서버의 고유정보를 이용하여 암호화하는 것을 특징으로 하는 TCP통신을 이용한 정보 저장방법.

[청구항 4] 제3항에 있어서,

상기 암호화단계는
상기 서버가 기설정된 시간마다 상기 고유정보를 변경하는 것을
특징으로 하는 TCP통신을 이용한 정보 저장방법.

[청구항 5] 제1항 내지 제4항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

[청구항 6] 서버와 클라이언트간 TCP 통신을 수행하는 TCP통신을 이용한 정보 저장시스템에 있어서,
상기 서버는
클라이언트로부터 TCP 패킷의 헤더 중 SYN 영역을 활성화하고, 임의의 숫자를 생성하여 TCP 패킷의 헤더 중 SEQ 영역에 포함시킨 제1 TCP 패킷을 전송받아, TCP 패킷에 저장하고자 하는 적어도 하나의 정보를 암호화하고, TCP 패킷의 헤더 중 SYN 영역 및 ACK영역을 활성화하고, TCP 패킷의 헤더 중 SEQ영역에 암호화된 정보를 저장하고, 상기 제1 TCP 패킷의 SEQ 영역에 포함된 임의의 숫자에 1을 더한 값을 상기 제1 TCP 패킷의 헤더 중 ACK 영역에 저장하는 제2 TCP 패킷을 상기 클라이언트로 전송하며,
상기 클라이언트로부터 TCP 패킷의 헤더 중 ACK 영역이 활성화되고, 상기 제1 TCP 패킷의 헤더 중 SEQ 영역에 저장된 임의의 숫자에 1을 더한 값을 TCP 패킷의 헤더 중 SEQ 영역에 저장되며, TCP 패킷의 헤더 중 ACK 영역에 상기 암호화된 정보에 1을 더한 값을 저장하는 제3 TCP 패킷을 전송받아,
상기 제3 TCP 패킷의 헤더 중 ACK 영역을 복호화하여 암호화된 정보를 획득한 후, 상기 제2 TCP 패킷의 하위 레벨에 존재하는 IP 패킷 내 저장된 정보와 상기 제3 TCP 패킷의 헤더 중 ACK 영역으로부터 1을 차감하고 획득하여 암호화를 해제한 값을 비교하여 동일한 경우, 상기 정보가 제2 TCP 패킷의 SEQ 영역과 제3 TCP 패킷의 ACK 영역에 저장되었다고 판단하는 것을
특징으로 하는 TCP통신을 이용한 정보 저장시스템.

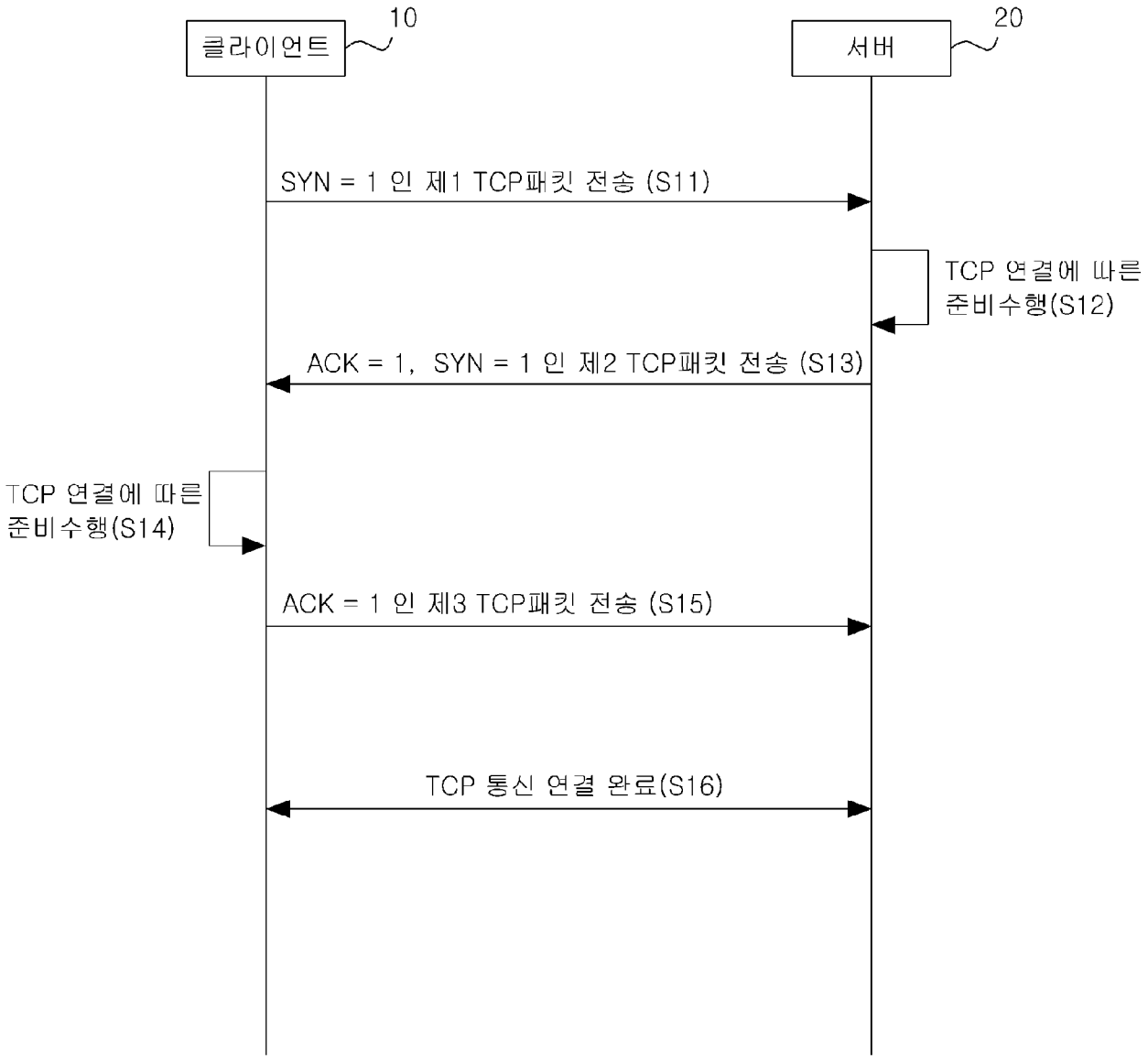
[청구항 7] 제6항에 있어서,
상기 서버는
TCP통신을 위해 사용되는 TCP 헤더와 쌍을 이루는 IP헤더에 포함된 TTL(Time To Live)값 및 IP값을 포함하는 정보를 암호화하는 것을 특징으로 하는 TCP통신을 이용한 정보 저장시스템.

[청구항 8] 제7항에 있어서,
상기 서버는
상기 TTL값 및 IP값을 해시하고, 해시한 값을 상기 서버의

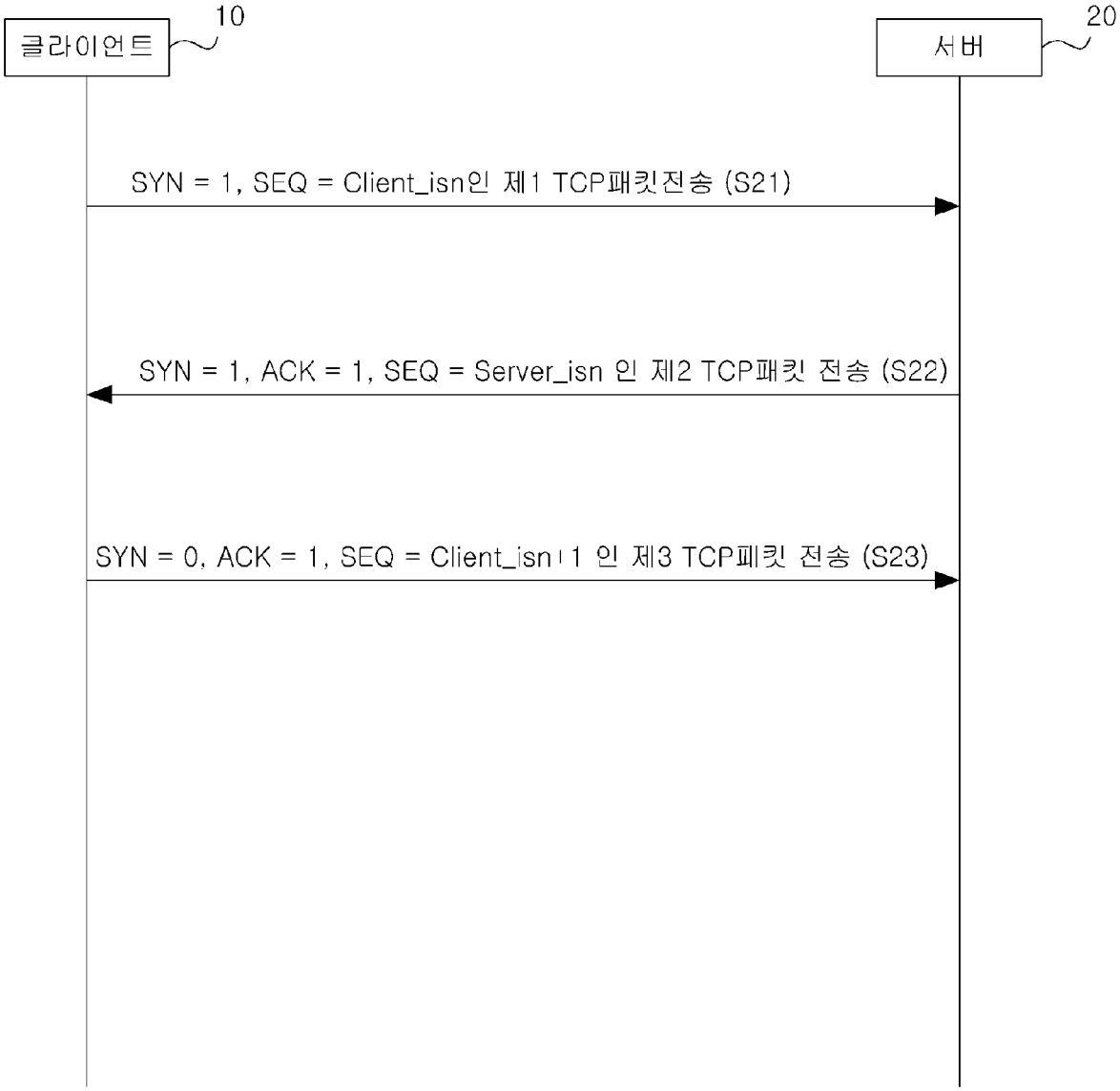
고유정보를 이용하여 암호화하는 것을 특징으로 하는 TCP통신을 이용한 정보 저장시스템.

[청구항 9] 제8항에 있어서,
상기 서버는
기설정된 시간마다 상기 고유정보를 변경시키는 것을 특징으로 하는 TCP통신을 이용한 정보 저장시스템.

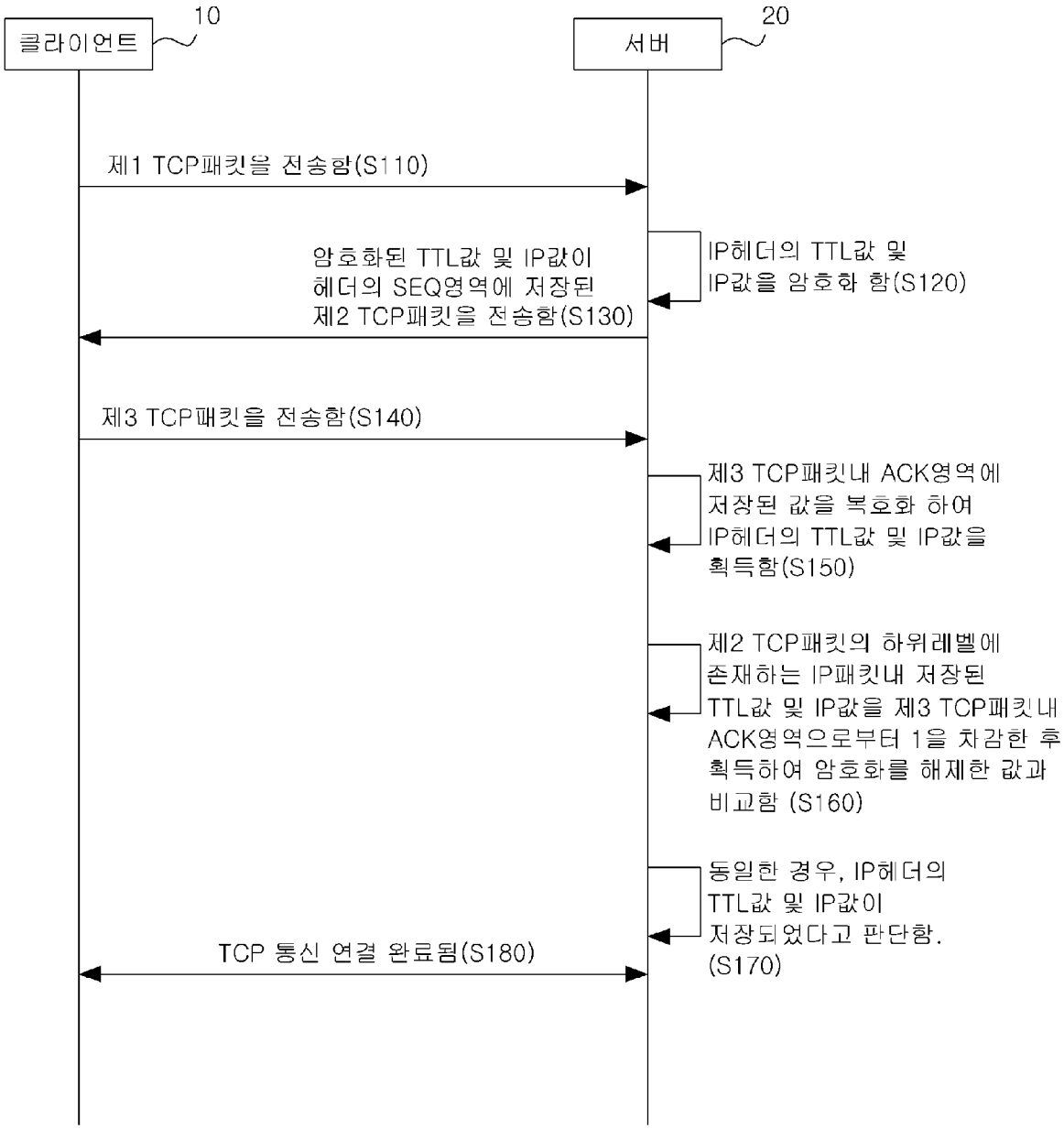
[Fig. 1]


클라이언트
10
서버
20
SYN = 1 인 제1 TCP패킷 전송 (S11)
TCP 연결에 따른 준비수행(S12)
ACK = 1, SYN = 1 인 제2 TCP패킷 전송 (S13)
TCP 연결에 따른 준비수행(S14)
ACK = 1 인 제3 TCP패킷 전송 (S15)
TCP 통신 연결 완료(S16)

[Fig. 2]


클라이언트
10
서버
20
SYN = 1, SEQ = Client_isn인 제1 TCP패킷전송 (S21)
SYN = 1, ACK = 1, SEQ = Server_isn 인 제2 TCP패킷 전송 (S22)
SYN = 0, ACK = 1, SEQ = Client_isn+1 인 제3 TCP패킷 전송 (S23)

[Fig. 3]


클라이언트
10
서버
20
제1 TCP패킷을 전송함(S110)
IP헤더의 TTL값 및
IP값을 암호화 함(S120)
암호화된 TTL값 및 IP값이
헤더의 SEQ영역에 저장된
제2 TCP패킷을 전송함(S130)
제3 TCP패킷을 전송함(S140)
제3 TCP패킷내 ACK영역에
저장된 값을 복호화 하여
IP헤더의 TTL값 및 IP값을
획득함(S150)
제2 TCP패킷의 하위레벨에
존재하는 IP패킷내 저장된
TTL값 및 IP값을 제3 TCP패킷내
ACK영역으로부터 1을 차감한 후
획득하여 암호화를 해제한 값과
비교함 (S160)
동일한 경우, IP헤더의
TTL값 및 IP값이
저장되었다고 판단함.
(S170)
TCP 통신 연결 완료됨(S180)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/008194

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/56(2006.01)i, H04L 1/16(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/56; H04L 9/08; H04L 29/08; H04L 12/66; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: TCP, encoding, random value, information storage and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-086597 A (TRINITY SECURITY SYSTEMS INC) 31 March 2005 See abstract, paragraph [0024] and claim 1.	1-9
A	KR 10-0431231 B1 (INTERNATIONAL BUSINESS MACHINES CORPORATION.) 12 May 2004 See abstract and claims 1,2,3,6,7.	1-9
A	JP 2005-073272 A (LUCENT TECHNOL INC) 17 March 2005 See abstract and claims 1,2,9.	1-9
A	KR 10-2010-0099109 A (ADOBE SYSTEMS INCORPORATED) 10 September 2010 See abstract and paragraphs [0004]-[0009].	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 DECEMBER 2012 (20.12.2012)	**21 DECEMBER 2012 (21.12.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

International application No.
PCT/KR2012/008194

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 2005-086597 A	31.03.2005	NONE	
KR 10-0431231 B1	12.05.2004	AU 2002-308250 A8	03.10.2002
		EP 1154610 A2	14.11.2001
		EP 1154610 A3	11.05.2005
		EP 1377955 A2	07.01.2004
		TW 518864 A	21.01.2003
		US 2001-0042200 A1	15.11.2001
		US 2004-0091842 A1	13.05.2004
		US 2008-0003548 A1	03.01.2008
		US 7316566 B2	08.01.2008
		US 7871271 B2	18.01.2011
		WO 02-075473 A2	26.09.2002
		WO 02-075473 A3	26.09.2002
JP 2005-073272 A	17.03.2005	JP 04-373306 B2	11.09.2009
		JP 4373306 B2	25.11.2009
		US 2005-0060557 A1	17.03.2005
		US 7404210 B2	22.07.2008
KR 10-2010-0099109 A	10.09.2010	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/008194

A. 발명이 속하는 기술분류(국제특허분류**(IPC)**)

H04L 12/56(2006.01)i, H04L 1/16(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 12/56; H04L 9/08; H04L 29/08; H04L 12/66; H04L 12/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: TCP, 암호화, 랜덤값, 정보저장 및 유사용어

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	JP 2005-086597 A (TRINITY SECURITY SYSTEMS INC) 2005.03.31 요약, 단락 [0024] 및 청구항 1 참조.	1-9
A	KR 10-0431231 B1 (인터내셔널 비지네스 머신즈 코포레이션) 2004.05.12 요약 및 청구항 1,2,3,6,7 참조.	1-9
A	JP 2005-073272 A (LUCENT TECHNOL INC) 2005.03.17 요약 및 청구항 1,2,9 참조.	1-9
A	KR 10-2010-0099109 A (어도비시스템즈인코오포레이티드) 2010.09.10 요약 및 단락 [0004]-[0009] 참조.	1-9

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2012년 12월 20일 (20.12.2012)	**2012년 12월 21일 (21.12.2012)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 82-42-472-7140

심사관
하은주
전화번호 82-42-481-5707

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/008194

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 2005-086597 A	2005.03.31	없음	
KR 10-0431231 B1	2004.05.12	AU 2002-308250 A8	2002.10.03
		EP 1154610 A2	2001.11.14
		EP 1154610 A3	2005.05.11
		EP 1377955 A2	2004.01.07
		TW 518864 A	2003.01.21
		US 2001-0042200 A1	2001.11.15
		US 2004-0091842 A1	2004.05.13
		US 2008-0003548 A1	2008.01.03
		US 7316566 B2	2008.01.08
		US 7871271 B2	2011.01.18
		WO 02-075473 A2	2002.09.26
		WO 02-075473 A3	2002.09.26
JP 2005-073272 A	2005.03.17	JP 04-373306 B2	2009.09.11
		JP 4373306 B2	2009.11.25
		US 2005-0060557 A1	2005.03.17
		US 7404210 B2	2008.07.22
KR 10-2010-0099109 A	2010.09.10	없음	