(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년07월16일
(11) 등록번호 10-2278808
(24) 등록일자 2021년07월13일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 63/166 (2013.01)
H04L 63/0838 (2013.01)
(21) 출원번호 10-2020-0003479
(22) 출원일자 2020년01월10일
심사청구일자 2020년01월10일
(56) 선행기술조사문헌
KR101503019 B1*
KR1020170074328 A*
KR1020170134657 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
남서울대학교 산학협력단
충청남도 천안시 서북구 성환읍 대학로 91 , 남서울대학교내
(72) 발명자
박승규
서울특별시 마포구 광성로 17, 신촌숲아이파크 104-2303
(74) 대리인
김견수

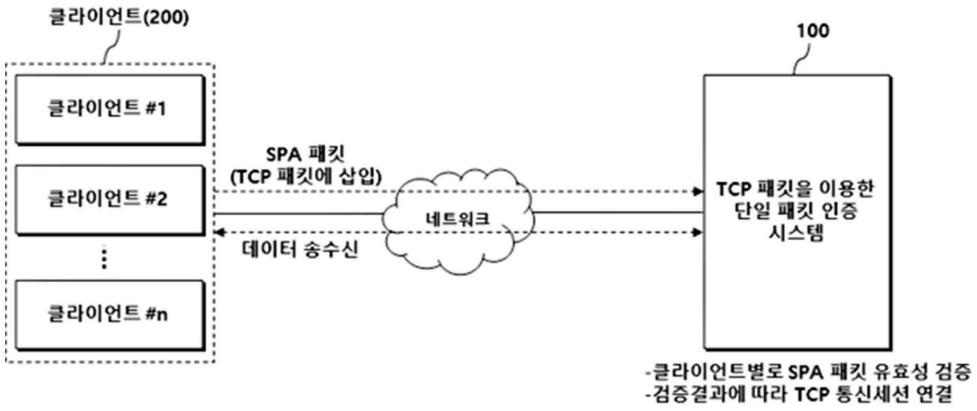
전체 청구항 수 : 총 7 항 심사관 : 홍기완

(54) 발명의 명칭 **TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법**

(57) 요 약

본 발명은 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법에 관한 것으로, 적어도 하나 이상의 클라이언트로부터 사용자 식별자, OTP(One Time Password), 디바이스 핑거프린트(Device Fingerprint) 등을 포함하는 SPA(Single Packet Authentication)패킷을 TCP 패킷을 통해 수신 받아, 상기 클라이언트별로 상기 SPA 패킷에 대한 유효성을 검증함과 동시에 통신세션을 연결함으로써, 상기 각 클라이언트에 대한 인증을 간소화하고, 제3의 클라이언트가 상기 클라이언트에 대한 사용자의 신분으로 상기 통신세션에 연결되는 것을 원천적으로 봉쇄하여 네트워크 보안을 극대화할 수 있도록 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 63/12 (2013.01)
H04L 9/0643 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 S2659705
부처명 중소벤처기업부
과제관리(전문)기관명 중소기업기술정보진흥원
연구사업명 산학연협력 기술개발사업
연구과제명 Cloud 및 IoT 시스템의 보안을 위한 소프트웨어 정의 방어선(Software Defined Perimeter) 기술 개발
기 여 율 1/1
과제수행기관명 주식회사 옥타솔루션
연구기간 2018.12.01 ~ 2019.11.30

명 세 서

청구범위

청구항 1

TCP 패킷을 이용한 단일 패킷 인증 시스템에 있어서,

적어도 하나 이상의 클라이언트로부터 TCP 패킷의 데이터 필드에 삽입한 SPA(Single Packet Authentication) 패킷을 수신하는 SPA 패킷 수신부;

상기 수신한 SPA 패킷의 유효성을 검증하여 상기 클라이언트를 인증하는 SPA 패킷 유효성 검증부; 및

상기 검증결과에 따라 상기 클라이언트와 TCP 통신세션을 연결하는 통신세션 연결부;를 포함하며,

상기 SPA 패킷은, 사용자 식별자, 디바이스 핑거프린트 및 상기 클라이언트가 생성한 OTP(One Time Password)를 포함하여 구성되고,

상기 디바이스 핑거프린트는 맥(MAC)주소, 식별정보 또는 이들의 조합을 포함하는 상기 클라이언트에 대한 디바이스 정보와 상기 클라이언트에 발급된 고유 암호키를 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 생성된 디바이스 인증코드를 포함하여 구성되며,

상기 SPA 패킷 유효성 검증부는,

상기 OTP 및 디바이스 인증코드의 유효여부를 동시에 판단하여 상기 SPA 패킷에 대한 유효성을 검증함으로써, 상기 클라이언트가 생성한 OTP가 폐기될 때까지의 유효시간 내에 해당 OTP를 해킹한 제3의 클라이언트 또는 상기 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 상기 클라이언트에 대한 정당한 사용자의 신분으로 상기 TCP 통신세션과 연결되는 것을 방지하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 SPA 패킷 유효성 검증부는,

사전에 등록된 상기 디바이스 정보와 상기 클라이언트의 고유 암호키를 상기 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 해당 클라이언트에 대한 디바이스 인증코드를 추출하고,

상기 추출한 디바이스 인증코드와 상기 수신한 SPA 패킷의 디바이스 핑거프린트로 구성된 디바이스 인증코드를 상호 비교함으로써, 상기 디바이스 핑거프린트에 대한 유효여부를 판단하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템.

청구항 5

청구항 1에 있어서,

상기 통신세션 연결부는,

상기 SPA 패킷이 유효하면, 상기 클라이언트와의 데이터 송수신을 위한 TLS(Transfer Layer Security)터널을 형성함으로써, 상기 TCP 통신세션을 연결하며,

상기 SPA 패킷이 유효하지 않으면, 해당 SPA 패킷을 포함하는 TCP 패킷을 드롭하여 상기 TCP 통신세션 연결을

수행하지 않는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템.

청구항 6

청구항 1에 있어서,

상기 SPA 패킷은, 상기 TCP 통신세션 연결을 위해 상기 인증을 요청하기 위한 사전에 설정한 인증요청코드, 상기 인증에 필요한 부가정보를 추가하기 위한 메타데이터 또는 이들의 조합을 더 포함하며,

상기 메타데이터는, 지문을 포함하는 상기 클라이언트에 대한 사용자의 생체정보, 성별, 나이, 주소, 이메일 정보, 전화번호 또는 이들의 조합을 포함하는 사용자 정보를 더 포함하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템.

청구항 7

TCP 패킷을 이용한 단일 패킷 인증 방법에 있어서,

적어도 하나 이상의 클라이언트로부터 TCP 패킷의 데이터 필드에 삽입한 SPA(Single Packet Authentication) 패킷을 수신하는 SPA 패킷 수신 단계;

상기 수신한 SPA 패킷의 유효성을 검증하여 상기 클라이언트를 인증하는 SPA 유효성 검증 단계; 및

상기 검증결과에 따라 상기 클라이언트와 TCP 통신세션을 연결하는 통신세션 연결 단계;를 포함하며,

상기 SPA 패킷은, 사용자 식별자, 디바이스 핑거프린트 및 상기 클라이언트가 생성한 OTP(One Time Password)를 포함하여 구성되고,

상기 디바이스 핑거프린트는 맥(MAC)주소, 식별정도 또는 이들의 조합을 포함하는 상기 클라이언트에 대한 디바이스 정보와 상기 클라이언트에 발급된 고유 암호키를 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 생성된 디바이스 인증코드를 포함하여 구성되며,

상기 SPA 패킷 유효성 검증 단계는,

상기 OTP 및 디바이스 인증코드의 유효여부를 동시에 판단하여 상기 SPA 패킷에 대한 유효성을 검증함으로써 상기 클라이언트가 생성한 OTP가 폐기될 때까지의 유효시간 내에 해당 OTP를 해킹한 제3의 클라이언트 또는 상기 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 상기 클라이언트에 대한 정당한 사용자의 신분으로 상기 TCP 통신세션과 연결되는 것을 방지하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 방법.

청구항 8

삭제

청구항 9

청구항 7에 있어서,

상기 SPA 패킷 유효성 검증 단계는,

사전에 등록된 상기 디바이스 정보와 상기 클라이언트의 고유 암호키를 상기 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 해당 클라이언트에 대한 디바이스 인증코드를 추출하고,

상기 추출한 디바이스 인증코드와 상기 수신한 SPA 패킷의 디바이스 핑거프린트로 구성되는 디바이스 인증코드를 상호 비교함으로써, 상기 디바이스 핑거프린트에 대한 유효여부를 판단하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 방법.

청구항 10

청구항 7에 있어서,

상기 통신세션 연결 단계는,

상기 SPA 패킷이 유효하면, 상기 클라이언트와의 데이터 송수신을 위한 TLS(Transfer Layer Security)터널을 형성함으로써, 상기 TCP 통신세션을 연결하고, 상기 SPA 패킷이 유효하지 않으면, 해당 SPA 패킷을 포함하는 TCP

패킷을 드롭하여 상기 TCP 통신세션 연결을 수행하지 않도록 하며,

상기 SPA 패킷은, 상기 TCP 통신세션 연결을 위해 상기 인증을 요청하기 위한 사전에 설정한 인증요청코드, 상기 인증에 필요한 부가정보를 추가하기 위한 메타데이터 또는 이들의 조합을 더 포함하며,

상기 메타데이터는, 지문을 포함하는 상기 클라이언트에 대한 사용자의 생체정보, 성별, 나이, 주소, 이메일 정보, 전화번호 또는 이들의 조합을 포함하는 사용자 정보를 더 포함하는 것을 특징으로 하는 TCP 패킷을 이용한 단일 패킷 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 적어도 하나 이상의 클라이언트로부터 사용자 식별자, OTP(One Time Password), 디바이스 핑거프린트(Device Fingerprint) 등을 포함하는 SPA(Single Packet Authentication)패킷을 TCP 패킷을 통해 수신 받아, 상기 클라이언트별로 상기 SPA 패킷에 대한 유효성을 검증함과 동시에 통신세션을 연결함으로써, 상기 각 클라이언트에 대한 인증을 간소화하고, 제3의 클라이언트가 상기 클라이언트에 대한 사용자의 신분으로 상기 통신세션에 연결되는 것을 원천적으로 봉쇄하여 네트워크 보안을 극대화할 수 있도록 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 산업기술과 정보통신 기술의 급격한 발전으로 인해, 현대 사회과 정보화 사회로 변화되고 있고, 유무선 통신을 기반으로 하는 네트워크 시스템이 급속도로 성장함에 따라 특정 서비스를 제공하기 위한 서버에 네트워크를 통해 접속하여 금융, 사용자 데이터 저장 및 처리 등과 같은 다양한 업무를 시간이나 장소에 상관없이 온라인상에서 처리할 수 있도록 하는 환경이 구축되고 있다.

[0003] 한편, 상기 서버에 접속하는 클라이언트에 대한 사용자의 신분을 악의적인 제3자가 해킹하여 도용하는 경우에는, 정당한 사용자에게 치명적인 피해를 초래할 수 있는 문제점이 있기 때문에, 상기 서버에서는 상기 해킹을 방지하기 위한 네트워크 보안 솔루션을 필수적으로 구비하여야 한다.

[0004] 상기 해킹을 방지하기 위해, 사전에 설정한 사용자의 사용자 ID와 패스워드를 입력하여 해당 사용자를 인증하는 로그인 방식이나, 공인인증서를 통한 사용자 인증방식을 통해 상기 클라이언트와 통신세션을 연결하는 방법을 채용하고 있다.

[0005] 그러나 상기 로그인 방식은, 사용자 ID와 패스워드가 쉽게 유출될 수 있고, 상기 공인인증서를 통한 사용자 인증방식은 대리사용이 가능하기 때문에 상기 해킹으로부터 완전히 자유롭지 못한 문제점이 있다.

[0006] 이러한 문제점을 해결과 최근에는 단일 패킷 인증(SPA, Single Packet Authentication)방법이 개발되어 상용화되고 있다.

[0007] 상기 단일 패킷 인증 방법은, 서버에 접속하고자 하는 클라이언트에서 OTP를 포함한 SPA 패킷을 생성하여, 상기 서버로 전송하면, 상기 SPA 패킷을 수신한 서버에서는, 해당 SPA 패킷에 대한 유효여부를 판단하는 SPA 패킷 유효성 판단 과정, 상기 SPA 패킷이 유효할 경우 상기 SPA 패킷에 포함된 클라이언트의 IP주소를 상기 서버의 ACL(Access Control List)에 등록하는 ACL 등록과정, 상기 등록한 IP주소에 대한 통신 허용 시간을 정의한 타이머를 세팅하는 타이머 세팅 과정, 상기 클라이언트에서 접속요청이 있는 경우, 상기 서버에서 해당 클라이언트의 IP주소가 상기 ACL에 등록되어 있는지를 확인하는 ACL 확인과정 및 상기 확인한 결과에 따라 해당 클라이언트의 IP주소가 상기 ACL에 등록되어 있으면 해당 클라이언트와의 통신세션을 수립하는 통신세션 수립과정을 포함하여 구성되며, 상기 서버에서, 통신 허용 시간이 종료되었을 경우, 해당 클라이언트의 IP주소를 상기 ACL에서 삭제함으로써, 네트워크에 대한 보안을 유지하도록 구현된다.

[0008] 즉, 종래의 단일 패킷 인증 방법은, 특정 클라이언트로부터 수신되는 SPA 패킷에 대한 유효성 판단 과정을 통과하면 해당 클라이언트의 IP주소를 ACL에 등록시킨 다음, 상기 통신 허용 시간 이내에 상기 클라이언트로부터 접속 요청이 있는 경우, ACL의 IP주소만을 참조하여 해당 클라이언트의 IP주소가 등록되어 있는 경우에 해당 클라이언트와의 통신세션을 수립한다.

[0009] 한편, 다수의 클라이언트가 하나의 공유기나 허브를 통해 상기 서버로 접속하는 경우, 상기 다수의 클라이언트

는 동일한 IP주소를 가지게 된다. 따라서 IP주소만을 참조하여 통신세션을 연결하는 종래의 단일 패킷 인증 방법은, 다수의 클라이언트가 하나의 공유기나 허브를 통해 상기 서버로의 접속 요청을 수행할 경우, 특정 하나의 클라이언트에서 상기 단일 패킷 인증 방법을 통해 인증을 수행하고, 상기 통신 허용 시간이 남은 상태에서 상기 인증을 수행하지 않은 제3의 클라이언트가 상기 서버로의 접속을 요청하더라도 상기 서버에서는 상기 제3의 클라이언트의 IP주소와 동일한 IP주소가 상기 ACL에 등록되어 있으므로 상기 제3의 클라이언트에 대한 접속을 허용하여 보안상의 문제점이 발생할 수 있다.

[0010] 또한 종래의 단일 패킷 인증 방법은, 상기 SPA 패킷 유효성 판단 과정, 상기 IP주소에 대한 ACL 확인과정, 상기 타이머 세팅 과정 및 통신세션 수립과정 등과 같이 복잡한 절차를 통해 상기 클라이언트에 대한 인증과정을 수행하기 때문에 시간지연으로 인한 서버의 응답속도가 저하되는 문제점이 있다.

[0011] 이에 따라 본 발명은, 클라이언트 인증을 위한 종래의 SPA 패킷을 재설계하여, 상기 SPA 패킷에 상기 클라이언트에 대한 사용자 식별자, 디바이스 핑거프린트, OTP를 포함하도록 구성하고, 상기 OPT 및 디바이스 핑거프린트에 대한 유효여부를 상기 클라이언트별로 동시에 판단하여, 해당 SPA 패킷에 대한 유효성을 검증함으로서, 상기 클라이언트에 대한 인증을 간소화함과 동시에 복수의 클라이언트가 동일한 IP주소를 가지더라도 상기 OTP 및 디바이스 핑거프린트가 동시에 유효하지 않는 경우에는 상기 각각의 클라이언트를 서로 다른 클라이언트로 판단하여 상기 인증을 수행함으로써, 네트워크 보안을 극대화할 수 있도록 하는 방안을 제안하고자 한다.

[0012] 다음으로 본 발명의 기술분야에 존재하는 선행기술에 대하여 간단하게 설명하고, 이어서 본 발명이 상기 선행기술에 비해서 차별적으로 이루고자 하는 기술적 사항에 대해서 기술하고자 한다.

[0013] 또한 한국공개특허 제2017-0074328호(2017.06.30.)는 티씨피 동기 패킷을 이용한 인증 시스템 및 방법 및 클라이언트 및 기록매체에 관한 것으로, 서버에 접속하고자 하는 클라이언트에서 OTP를 포함하는 SPA 패킷을 티씨피 동기 패킷에 포함시켜, 서버에 제공하고, 상기 서버에서는 해당 SPA 패킷의 OTP를 확인하여 상기 SAP 패킷에 대한 유요 여부를 판단하여, 해당 클라이언트와 상기 서버간의 통신이 가능하도록 하는 티씨피 동기 패킷을 이용한 인증 시스템 및 방법 및 클라이언트 및 기록매체에 관한 것이다.

[0014] 상기 선행기술은, 종래의 단일 패킷 인증 방법에서 사용되는 SPA 패킷을 그대로 이용하면서, 해당 SPA 패킷을 티씨피 동기 패킷을 통해 전송하여 클라이언트에 대한 인증을 수행하는 것이다.

[0015] 그러나 OTP를 이용하는 경우, 한번 사용한 OTP는 즉각적으로 폐기되지 않기 때문에 동일한 OTP를 유효시간 내에 사용하면 아무런 문제없이 상기 인증을 수행할 수 있어, 상기 OTP가 노출되는 경우, 정당한 사용자 이외에 제3자가 상기 정당한 사용자의 신분으로 상기 서버에 접속할 수 있는 보안상의 문제점을 내포하고 있다.

[0016] 반면에 본 발명은, 종래의 인증에 사용하는 SPA 패킷을 재설계하여, 상기 SPA 패킷이 사용자 식별자, 디바이스 핑거프린터 및 OTP를 포함하도록 함으로써, 상기 디바이스 핑거프린트와 OTP에 유효여부를 동시에 판단하여 상기 SPA 패킷의 유효성을 검증함으로서, 상기 클라이언트를 인증하고, 상기 인증된 클라이언트에 대해서만 TCP 통신세션이 연결되도록 하여, 네트워크 보안을 보장함과 동시에 인증절차를 간소화하도록 하는 것으로, 상기 선행기술은 이러한 본 발명의 기술적 특징을 기재하거나 시사하고 있지 않다.

[0017] 또한 정보통신망 정보보호 컨퍼런스(NETSEC-KR 2015)에서, 마크애니사는, 사용자 디바이스, 컨트롤러, 게이트웨이(또는 서버)로 구성되고, 상기 컨트롤러에서 단일 패킷 인증(SPA), 동적 방화벽, 상호인증방식의 TLS(Transfer Layer Security), 디바이스 인증, 사용자 인증, 소프트웨어 무결성 검증, 앱 바인딩 등 총 7단계의 보안정책을 적용한 네트워크 보안 솔루션인 블랙포트 기술을 공개했다.

[0018] 상기 블랙포트 기술은, 상기 사용자 디바이스에서 전송한 SPA 패킷을 상기 컨트롤러가 인증하면 해당 사용자 디바이스만을 위한 방화벽 핀홀을 생성하여, 상기 사용자 디바이스와 상기 컨트롤러 사이의 TLS를 형성한 후, 상기 사용자 디바이스와 사용자에 대한 인증을 수행한다. 이후, 상기 컨트롤러는 상기 사용자 디바이스에 사용할 수 있는 서비스와 접속할 게이트웨이에 대한 정보를 전송함과 동시에 상기 게이트웨이에 접속할 디바이스에 대한 디바이스 정보를 전송하면, 상기 디바이스는 상기 접속할 게이트웨이에 상기 SPA 패킷을 전송하며, 상기 게이트웨이는 상기 수신한 디바이스 정보와 상기 수신한 SPA 패킷에 대한 일치 여부를 검증하여, 검증결과에 따라 상기 사용자 디바이스와 데이터 통신용 TLS 터널을 생성함으로써, 해당 사용자 디바이스에 상기 서비스를 제공하도록 구현된다.

[0019] 즉, 상기 블랙포트 기술은, 컨트롤러에서 상기 단일 패킷 인증, 디바이스 인증을 포함하는 7단계 보안 정책을 개별적으로 수행하는 단계와 해당 보안 정책을 통과한 클라이언트에 대해서 또 다시 상기 게이트웨이나 서버에서 SPA 패킷에 대한 검증을 수행하는 단계로 구성되어 있다. 이는 클라이언트에 대한 인증 과정이 매우 복잡하

고, 상기 인증에 소요되는 시간이 오래 걸리는 단점이 있다.

[0020] 반면에 본 발명은, 클라이언트 인증에 필요한 사용자 식별자, 디바이스 핑거프린터 및 OTP 등을 하나의 SPA 패킷에 포함되도록 하고, 상기 SPA 패킷에 대한 유효성을 검증하여 상기 클라이언트별로 인증을 수행하도록 함으로써, 상기 인증을 수행한 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 존재하는 경우에도, 상기 제3의 클라이언트에 대한 새로운 통신세션을 수립하거나 인증을 거부하도록 함으로써, 정당한 사용자에 대한 해킹을 원천적으로 봉쇄하여 네트워크 보안을 극대화할 수 있도록 하는 것으로, 본 발명과 상기 블랙포트 기술은 현저한 차이점이 있음이 분명하다.

발명의 내용

해결하려는 과제

[0021] 본 발명은 상기와 같은 문제점을 해결하기 위해 창작된 것으로서, 적어도 하나 이상의 클라이언트로부터 수신되는 SPA 패킷에 대한 유효성을 클라이언트별로 검증하여, 검증결과에 따라 상기 클라이언트와 TCP 통신세션을 연결함으로서, IP주소 기반의 인증에서 발생할 수 있는 네트워크 보안의 허점을 방지할 수 있도록 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법을 제공하는 것을 그 목적으로 한다.

[0022] 또한 본 발명은, 종래의 SPA 패킷을 재설계하여, 상기 SPA 패킷에 클라이언트를 인증하기 위한 사용자 식별자, 일회성 비밀번호인 OTP, 디바이스 핑거프린트, 추가적인 인증에 필요한 부가정보를 추가하기 위한 메타데이터를 포함하도록 함으로써, 상기 OTP 및 디바이스 핑거프린트에 유효여부를 동시에 판단하여 검증하는 상기 SPA 패킷에 대한 유효성 검증과정을 통해, 상기 클라이언트에 대한 인증을 클라이언트별로 수행하여 상기 TCP 통신세션을 연결하도록 함으로써, 네트워크 보안을 보장하고, 인증절차를 간소화하여 즉각적인 TCP 통신이 수행될 수 있도록 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법을 제공하는 것을 그 목적으로 한다.

[0023] 또한 본 발명은, 상기 재설계한 SPA 패킷에 대한 유효성 검증을 통해 상기 클라이언트를 개별적으로 인증함으로써, 동일한 IP주소 가지는 제3의 클라이언트가 상기 SPA 패킷을 전송하는 경우에도, 상기 인증을 수행한 클라이언트와 제3의 클라이언트는 상이한 클라이언트로 판단하여, 상기 제3의 클라이언트에 대한 새로운 TCP 통신세션을 연결하거나, 상기 인증을 거부함으로써, 정당한 사용자가 상기 TCP 패킷을 이용한 단일 패킷 인증 시스템에 연결될 수 있도록 하는 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0024] 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템에 있어서, 적어도 하나 이상의 클라이언트로부터 SPA(Single Packet Authentication) 패킷을 수신하는 SPA 패킷 수신부, 상기 수신한 SPA 패킷의 유효성을 검증하여 상기 클라이언트를 인증하는 SPA 패킷 유효성 검증부 및 상기 검증결과에 따라 상기 클라이언트와 TCP 통신세션을 연결하는 통신세션 연결부를 포함하며, 상기 SPA 패킷은, TCP 패킷의 데이터 필드에 삽입되어 상기 SPA 패킷 수신부에 수신되며, 사용자 식별자, 디바이스 핑거프린트 및 OTP(One Time Password)를 포함하여 구성되는 것을 특징으로 한다.

[0025] 또한 상기 SPA 패킷 유효성 검증부는, 상기 수신한 SPA 패킷의 디바이스 핑거프린트와 OTP에 대한 유효여부를 동시에 판단하여, 상기 SPA 패킷에 대한 유효성을 검증함으로써, 상기 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 상기 클라이언트에 대한 사용자의 신분으로 상기 TCP 통신세션이 연결되는 것을 방지하는 것을 특징으로 한다.

[0026] 또한 상기 디바이스 핑거프린트는, 상기 클라이언트에 대한 디바이스 인증코드로 구성되며, 상기 디바이스 인증코드는, 상기 클라이언트에 대한 디바이스의 맥(MAC)주소, 식별정보 또는 이들의 조합을 포함하는 디바이스 정보와 상기 디바이스의 고유 암호키를 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 생성되는 것을 특징으로 한다.

[0027] 또한 상기 SPA 패킷 유효성 검증부는, 상기 사전에 등록된 상기 디바이스 정보와 상기 클라이언트의 고유 암호키를 상기 디바이스 인증코드 생성용 단방향 해시함수를 통해 해당 클라이언트에 대한 디바이스 인증코드를 추출하고, 상기 추출한 디바이스 인증코드와 상기 수신한 SPA 패킷의 디바이스 핑거프린트로 구성된 디바이스 인증코드를 상호 비교함으로써, 상기 디바이스 핑거프린트에 대한 유효여부를 판단하는 것을 특징으로 한다.

[0028] 또한 상기 통신세션 연결부는, 상기 SPA 패킷이 유효한 경우, 상기 클라이언트와 데이터 송수신을 위한

TLS(Transfer Layer Security)터널을 형성함으로써, 상기 TCP 통신세션을 연결하며, 상기 SPA 패킷이 유효하지 않은 경우에는, 해당 SPA 패킷을 포함하는 TCP 패킷을 드롭하여 상기 TCP 통신세션 연결을 수행하지 않는 것을 특징으로 한다.

[0029] 또한 상기 SPA 패킷은, 상기 TCP 통신세션 연결을 위해 상기 인증을 요청하기 위한 사전에 설정한 인증요청코드, 상기 인증에 필요한 부가정보를 추가하기 위한 메타데이터 또는 이들의 조합을 더 포함하며, 상기 메타데이터는, 지문을 포함하는 사용자의 생체정보, 성별, 나이, 주소, 이메일 정보, 전화번호 또는 이들의 조합을 포함하는 사용자 정보를 더 포함하는 것을 특징으로 한다.

[0030] 아울러 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 방법에 있어서, 적어도 하나 이상의 클라이언트로부터 SPA(Single Packet Authentication) 패킷을 수신하는 SPA 패킷 수신 단계, 상기 수신한 SPA 패킷의 유효성을 검증하여 상기 클라이언트를 인증하는 SPA 유효성 검증 단계 및 상기 검증결과에 따라 상기 클라이언트와 TCP 통신세션을 연결하는 통신세션 연결 단계를 포함하며, 상기 SPA 패킷은, TCP 패킷의 데이터 필드에 삽입되어 상기 SPA 패킷 수신단계를 통해 수신되며, 사용자 식별자, 디바이스 핑거프린트 및 OTP(One Time Password)를 포함하여 구성되는 것을 특징으로 한다.

[0031] 또한 상기 SPA 패킷 유효성 검증 단계는, 상기 수신한 SPA 패킷의 디바이스 핑거프린트와 OTP에 대한 유효여부를 판단하여, 상기 SPA 패킷에 대한 유효성을 검증함으로써, 상기 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 상기 클라이언트에 대한 사용자의 신분으로 상기 TCP 통신세션이 연결되는 것을 방지하는 것을 특징으로 한다.

[0032] 또한 상기 SPA 패킷 유효성 검증 단계는, 상기 사전에 등록된 상기 디바이스 정보와 상기 클라이언트의 고유 암호키를 상기 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 해당 클라이언트에 대한 디바이스 인증코드를 추출하고, 상기 추출한 디바이스 인증코드와 상기 수신한 SPA 패킷의 디바이스 핑거프린트로 구성되는 디바이스 인증코드를 상호 비교함으로써, 상기 디바이스 핑거프린트에 대한 유효여부를 판단하는 것을 특징으로 한다.

[0033] 또한 상기 통신세션 연결 단계는, 상기 SPA 패킷이 유효한 경우, 상기 클라이언트와의 데이터 송수신을 위한 TLS(Transfer Layer Security)터널을 형성함으로써, 상기 TCP 통신세션을 연결하고, 상기 SPA 패킷이 유효하지 않은 경우에는, 해당 SPA 패킷을 포함하는 TCP 패킷을 드롭하여 상기 TCP 통신세션 연결을 수행하지 않도록 하는 것을 특징으로 한다.

발명의 효과

[0034] 이상에서와 같이 본 발명의 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법은, 사용자 식별자, OTP, 디바이스 핑거프린트 및 메타정보를 포함하는 SPA 패킷을 삽입한 TCP 패킷을 적어도 하나 이상의 클라이언트로부터 수신하고, 상기 클라이언트별로 상기 수신한 SPA 패킷의 유효성을 판단하여 상기 클라이언트를 개별적으로 인증하고, 이와 동시에 상기 인증한 클라이언트와 TCP 통신세션을 연결하도록 함으로써, 상기 인증에 대한 절차를 간소화하여 상기 인증한 클라이언트와 즉각적인 통신이 수행될 수 있도록 함과 동시에 네트워크 보안을 극대화할 수 있도록 하는 효과가 있다.

[0035] 또한 본 발명은, 상기 인증을 수행한 클라이언트와 동일한 IP주소를 가지는 제3의 클라이언트가 존재하는 경우에도, 상기 SPA 패킷에 대한 유효성 검증을 통해 상기 제3의 클라이언트에 대한 새로운 TCP 통신세션을 연결하거나, 상기 제3의 클라이언트에 대한 인증을 거부함으로써, 정당한 사용자만이 상기 단일 패킷 인증 시스템에 접속하도록 하여, 상기 사용자에 대한 해킹을 원천적으로 봉쇄할 수 있도록 하는 효과가 있다.

도면의 간단한 설명

[0036] 도 1은 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법을 설명하기 위해 나타낸 개념도이다.

도 2는 본 발명의 일 실시예에 따른 SPA 패킷을 설명하기 위해 나타낸 도면이다.

도 3은 본 발명의 일 실시예에 따른 클라이언트의 구성을 나타낸 블록도이다.

도 4는 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템의 구성을 나타낸 블록도이다.

도 5는 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증을 수행하는 절차를 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0037] 이하, 첨부한 도면을 참조하여 본 발명의 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법 대한 바람직한 실시예를 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다. 또한 본 발명의 실시예들에 대해서 특정한 구조적 내지 기능적 설명들은 단지 본 발명에 따른 실시예를 설명하기 위한 목적으로 예시된 것으로, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는 것이 바람직하다. 본 발명에서는 데이터는 디지털 정보로 해석할 수 있다.

[0038] 도 1은 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법을 설명하기 위해 나타낸 개념도이다.

[0039] 도 1에 도시한 바와 같이, 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템(100)(이하, 단일 패킷 인증 시스템이라 칭함)은, 적어도 하나 이상의 클라이언트로부터 수신되는 SPA 패킷에 대한 유효성을 검증하여, 상기 클라이언트(200)를 인증하고, 상기 인증과 동시에 해당 클라이언트(200)와의 TCP 통신세션을 연결함으로써, 네트워크 보안이 보장된 상태에서 상기 클라이언트(200)와의 데이터를 송수신할 수 있도록 하는 기능을 수행한다.

[0040] 상기 클라이언트(200)는, 상기 사용자가 구비한 PC, 스마트폰 등과 같은 다양한 유무선 통신단말 또는 디바이스를 통칭하는 개념으로, 상기 사용자는 상기 클라이언트(200)를 통해 상기 단일 패킷 인증 시스템(100)에 온라인으로 접속하여, 상기 인증을 통해 상기 단일 패킷 인증 시스템(100)에서 제공하는 다양한 기능을 이용할 수 있다.

[0041] 이때, 상기 사용자는 상기 단일 패킷 인증 시스템(100)에서 제공하는 상기 인증을 위한 애플리케이션(application)이나 프로그램을, 상기 클라이언트(200)에 설치하여 이를 수행함으로서, 해당 클라이언트(200)를 인증 받아, 네트워크 보안이 보장된 상태에서 상기 단일 패킷 인증 시스템(100)과 연결되어 상기 단일 패킷 인증 시스템(100)에서 제공하는 다양한 기능을 이용할 수 있다.

[0042] 한편, 상기 단일 패킷 인증 시스템(100)은, 사용자의 업무에 관련된 사용자 데이터를 저장하거나, 상기 저장한 데이터를 해당 사용자에 의해 처리하도록 하는 기능을 제공하거나, 금융서비스 등과 같은 다양한 기능을 제공하며, 상기 인증을 통해 상기 기능을 정당한 사용자가 이용할 수 있도록 하는 것으로, 클라우드 서버와 같은 형태로 구현될 수 있다.

[0043] 즉, 단일 패킷 인증 시스템(100)은, 적어도 하나 이상의 클라이언트를 개별적으로 인증하고, 상기 인증한 클라이언트(200)에 대해서만 TCP 통신세션을 연결하도록 함으로써, 네트워크 보안이 보장된 상태에서, 상기 다양한 기능을 이용하기 위해 상기 클라이언트(200)와의 데이터를 송수신할 수 있도록 하는 것이다.

[0044] 이를 위해, 우선적으로 상기 클라이언트(200)는, 상기 단일 패킷 인증 시스템(100)에서 해당 클라이언트를 인증하기 위한 SPA(Single Packet Authentication) 패킷을 생성하여, 상기 단일 패킷 인증 시스템(100)으로 전송한다.

[0045] 이때, 상기 생성한 SPA 패킷은, 상기 클라이언트(200)에서 생성되는 TCP 패킷에 삽입되어 상기 단일 패킷 인증 시스템(100)으로 전송된다.

[0046] 또한 상기 SPA 패킷은, 상기 클라이언트에서 상기 인증을 요청하는 정보로써, 인증요청코드, 상기 클라이언트(200)에 대한 사용자를 식별하기 위한 사용자 식별자, OTP, 상기 클라이언트(200)에 대한 디바이스 정보를 토대로 생성되는 디바이스 핑거프린트, 상기 인증에 추가적으로 필요한 부가정보를 추가하기 위한 패킷 영역인 메타데이터 또는 이들의 조합을 포함하여 구성된다.

[0047] 이를 통해, 상기 단일 패킷 인증 시스템(100)은, 하나의 SPA 패킷, 즉 단일 패킷을 이용하여 상기 클라이언트(200)에 대한 인증을 수행하게 되며, 상기 SPA 패킷은 본 발명의 핵심적인 기술적 특징으로, 종래 기술의 SPA 패킷을 재설계하여 하나의 SPA 패킷을 통해 상기 OTP와 상기 디바이스 핑거프린트를 동시에 검증하여, 상기 클라이언트(200)를 인증할 수 있도록 하는 것으로, 상기 SPA 패킷은 도 2를 참조하여 상세히 설명하도록 한다.

[0048] 또한 상기 단일 패킷 인증 시스템(100)은, 적어도 하나 이상의 클라이언트(200)로부터 상기 TCP 통신세션 연결을 위한 TCP 패킷이 최초로 수신되는 경우, 상기 TCP 패킷에 포함된 SPA 패킷을 추출한다.

[0049] 이후, 상기 단일 패킷 인증 시스템(100)은, 상기 추출한 SPA 패킷에 대한 유효성을 검증하여, 해당 클라이언트(200)를 인증한다. 이때, 상기 SPA 패킷에 대한 유효성을 검증하는 것은, 상기 SPA 패킷에 포함된 OTP와 디바이스 핑거프린트에 대한 유효여부를 동시에 판단하여 검증함으로서, 수행된다.

[0050] 또한 상기 단일 패킷 인증 시스템(100)은, 상기 SPA 패킷에 대한 유효성을 검증한 결과, 상기 SPA 패킷이 유효한 경우, 해당 클라이언트(200)와의 TCP 통신세션을 연결하여, 상기 클라이언트(200)와 필요한 데이터를 송수신할 수 있도록 한다.

[0051] 또한 상기 단일 패킷 인증 시스템(100)은, 상기 SPA 패킷에 대한 유효성을 검증한 결과, 상기 SPA 패킷이 유효하지 않는 경우, 상기 SPA 패킷을 포함하는 상기 TCP 패킷을 드롭시켜, 해당 클라이언트(200)와의 통신을 종료함으로써, 해당 클라이언트(200)에 대한 인증을 거부하고, 해당 클라이언트(200)와의 TCP 통신세션을 연결하지 않는다.

[0052] 상기 단일 패킷 인증 시스템(100)은, IP주소를 기반으로 인증을 수행하는 종래기술과 달리, 상기 OTP 및 디바이스 핑거프린트를 동시에 검증하여 상기 클라이언트(200)별로 상기 인증을 수행하기 때문에, 상기 인증을 수행한 클라이언트(200)와 동일한 IP주소를 가지는 제3의 클라이언트(200)가 상기 클라이언트(200)에 대한 사용자의 신분으로 상기 TCP 통신세션이 연결되는 것을 원천적으로 방지하는 것이 가능하다. 즉, 두개의 클라이언트(200)가 동일한 IP주소를 가지더라도 상기 OTP, 상기 디바이스 핑거프린트 또는 이들의 조합 중 어느 하나라도 다른 경우에는, 서로 상이한 클라이언트(200)로 간주되기 때문에 상기 SPA 패킷의 검증결과에 따라 서로 다른 TCP 통신세션이 연결되는 것이다. 이를 통해 본 발명은, 상기 IP주소를 기반으로 인증을 수행하는 종래기술에서 발생할 수 있는 네트워크 보안에 대한 문제점을 극복하여, 제3자에 의한 해킹을 원천적으로 방지하여 네트워크 보안을 극대화할 수 있다.

[0053] 한편, 상기 TCP 통신세션을 연결하는 것은, 상기 인증을 완료한 상기 클라이언트(200)와 데이터 송수신을 위한 TLS(Transfer Layer Security)터널을 형성함으로써, 수행된다.

[0054] 도 2는 본 발명의 일 실시예에 따른 SPA 패킷을 설명하기 위해 나타낸 도면이다.

[0055] 도 2에 도시한 바와 같이, 본 발명의 일 실시예에 따른 SPA 패킷은 적어도 하나 이상의 클라이언트(200)에서 생성되어, TCP 패킷의 데이터 필드에 삽입된 후에 단일 패킷 인증 시스템(100)으로 전송된다.

[0056] 또한 상기 TCP 패킷은, TCP 헤더 및 데이터필드를 포함하여 구성된다.

[0057] 상기 TCP 헤더는, 상기 TCP 패킷을 전송하는 클라이언트(200)의 통신 포트번호, 해당 TCP 패킷을 수신하는 목적지(즉, 단일 패킷 인증 시스템)의 통신 포트번호, TCP 패킷의 순서에 대한 번호(sequence number), 예약 필드(reserved field), 상기 TCP 패킷을 어떠한 목적으로 전송할 것인지에 대한 값을 설정한 복수의 TCP 플래그, 체크섬(check sum)과 같은 다양한 정보가 포함된다.

[0058] 또한 상기 TCP 패킷의 데이터 필드는, 상기 클라이언트(200)에서 생성되는 SPA 패킷이 삽입되는 영역이다. 다만, 상기 인증을 통해 상기 클라이언트(200)에 대한 TCP 통신세션이 연결된 경우에는, 상기 단일 패킷 인증 시스템(100)과 송수신하기 위한 데이터가 삽입된다.

[0059] 또한 상기 SPA 패킷은, 상기 클라이언트(200)의 인증을 요청하기 위한 인증요청코드가 삽입되는 인증요청코드 필드, 상기 클라이언트(200)의 사용자에 대한 사용자 식별자가 삽입되는 사용자 식별자 필드, 상기 클라이언트를 인증하기 위해 검증의 대상이 되는 OTP와 디바이스 핑거프린트가 각각 삽입되는 OTP 필드와 디바이스 핑거프린트 필드 및 부가적인 정보를 삽입하기 위한 메타데이터 필드를 포함하여 구성된다.

[0060] 또한 상기 인증요청코드 필드는, 1바이트로 구성되며, 상기 인증요청코드는 상기 클라이언트(200)에서 상기 인증을 요청하기 위한 코드를 의미하는 것으로, 상기 단일 패킷 인증 시스템(100)에서 상기 클라이언트(200)별로 사전에 발급되어 설정된 코드를 의미한다.

[0061] 또한 상기 사용자 식별자 필드는, 총 8바이트로 구성되며, 상기 사용자 식별자는, 상기 단일 패킷 인증 시스템(100)에서 사용자별로 부여되는 고유의 식별자(ID)를 의미하며, 상기 단일 패킷 인증 시스템(100)에서 사용자별로 관리된다.

[0062] 또한 상기 OTP 필드는, 총 16바이트로 구성되며, 상기 OTP는, 사용자 패스워드를 기반으로 OTP 생성용 단방향

해시함수를 이용하여 생성되는 2차 암호를 의미한다. 또한 상기 사용자 패스워드, 별도의 사용자 고유 비밀값, 상기 OTP 누적횟수 또는 이들의 조합을 상기 단방향 해시함수에 입력하여 생성되는 해시값을 상기 OTP로 이용할 수 있다.

[0063] 한편, 상기 사용자 식별자 및 패스워드는, 상기 사용자가 상기 클라이언트(200) 인증을 위한 회원가입 절차를 통해 사용자가 설정함으로써, 상기 단일 패킷 인증 시스템(100)에서 발급되며, 상기 사용자 고유 비밀값 또한 상기 회원가입을 완료한 사용자에게 상기 단일 패킷 인증 시스템(100)에서 사용자에게 발급된다.

[0064] 또한 상기 OTP 생성용 단방향 해시함수 또한 상기 회원가입을 완료한 사용자의 클라이언트(200)별로 발급된다.

[0065] 이때, 상기 OTP는, 상기 단일 패킷 인증 시스템(100)에서, 해당 사용자의 클라이언트(200)로 발급한 동일한 OTP 생성용 해시함수를 이용하여 해시값을 추출하고, 상기 추출한 해시값과 상기 클라이언트(200)로부터 수신되는 SPA 패킷의 OTP를 비교함으로써, 해당 OTP를 검증하게 된다. 즉, 상기 OTP는 상기 클라이언트(200)에 대한 사용자를 인증하도록 함으로써, 해당 클라이언트(200)를 인증할 수 있도록 한다.

[0066] 또한 상기 디바이스 핑거프린트 필드는, 총 16바이트로 구성되며, 상기 디바이스 핑거프린트는, 상기 클라이언트(200)에 대한 디바이스 인증코드로 구성된다.

[0067] 상기 디바이스 인증코드는, 상기 맥(MAC)주소, 식별정보 또는 이들의 조합을 포함하는 상기 클라이언트(200)에 대한 디바이스 정보와 상기 클라이언트(200)에 대한 디바이스의 고유 암호키를 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 생성된다.

[0068] 이때, 상기 디바이스 정보는, 상기 회원절차 등을 통해 사전에 상기 단일 패킷 인증 시스템(100)에 등록되며, 상기 디바이스 고유 암호키는, 상기 단일 패킷 인증 시스템(100)에서 상기 클라이언트(200)별로 생성되어 등록되고, 상기 각 클라이언트(200)별로 발급된다.

[0069] 이후, 상기 단일 패킷 인증 시스템(100)은, 상기 클라이언트(200)로부터 SPA 패킷이 수신되는 경우, 상기 사전에 등록된 해당 클라이언트(200)의 디바이스 정보와 상기 클라이언트(200)에 대한 디바이스의 고유 암호키를 상기 클라이언트(200)에 발급한 디바이스 인증코드 생성용 단방향 해시함수에 입력하여, 해당 클라이언트(200)에 대한 디바이스 인증코드를 추출하고, 상기 추출한 디바이스 인증코드와 상기 SPA 패킷의 디바이스 핑거프린트로 구성된 디바이스 인증코드를 상호 비교함으로써, 상기 디바이스 핑거프린트에 대한 유효여부를 판단하여, 상기 비교한 결과가 일치한 경우에 상기 클라이언트(200)를 인증하게 된다. 즉, 상기 디바이스 핑거프린트는, 상기 클라이언트(200)에 대한 디바이스를 인증함으로써, 상기 클라이언트(200)를 인증할 수 있도록 한다.

[0070] 또한 상기 단일 패킷 인증 시스템(100)은, 상기 클라이언트에 대한 사용자의 사용자 식별자, 사용자 패스워드, 사용자 고유 비밀값, 상기 클라이언트(200)에 대한 디바이스 정보, 디바이스 고유 암호키, OTP 생성용 단방향 해시함수 및 디바이스 인증코드 생성용 단방향 해시함수를 포함하는 클라이언트 인증데이터를 상기 클라이언트(200)별로 관리하여, 상기 인증을 수행하게 된다.

[0071] 또한 상기 메타데이터 필드는, 총 16바이트로 구성되며, 상기 메타데이터는, 상기 클라이언트(200)의 구동을 위한 애플리케이션이나 프로그램의 버전정보나, 상기 인증에 필요한 부가정보를 추가하기 위한 것이다.

[0072] 예를 들어, 상기 인증에 필요한 부가정보를 포함하는 상기 메타데이터는, 지문을 포함하는 사용자의 생체정보, 상기 사용자의 이메일 정보, 성별, 나이, 주소, 전화번호 또는 이들이 조합을 포함하는 사용자 정보를 포함할 수 있다.

[0073] 이때, 상기 사용자 정보는 사전에 상기 단일 패킷 인증 시스템(100)에 사전에 등록되어 있으며, 상기 메타데이터에 상기 사용자 정보가 포함되어 있는 경우에는, 상기 단일 패킷 인증 시스템(100)은, 상기 OPT 및 디바이스 핑거프린트를 검증하는 것 이외에 상기 메타데이터의 사용자 정보와 상기 등록된 사용자 정보에 대한 일치 여부를 확인하여 상기 메타데이터를 추가적으로 더 검증함으로써, 상기 클라이언트(200)를 최종적으로 인증하게 된다.

[0074] 도 3은 본 발명의 일 실시예에 따른 클라이언트의 구성을 나타낸 블록도이다.

[0075] 도 3에 도시한 바와 같이, 본 발명의 일 실시예에 따른 클라이언트(200)는, OTP를 생성하는 OTP 생성부(210), 디바이스 핑거프린트를 생성하기 위한 디바이스 핑거프린트 생성부(220), 상기 생성한 OTP 및 디바이스 핑거프린트를 토대로 상기 클라이언트(200)의 인증을 위한 SPA 패킷을 생성하는 SPA 패킷 생성부(230), 상기 TCP 패킷에 상기 생성한 SPA 패킷을 삽입하여 상기 생성한 SPA 패킷을 상기 단일 패킷 인증 시스템(100)으로 전송하기

위한 TCP 패킷을 생성하는 TCP 패킷 생성부(240), 통신부(250) 및 메모리(260)를 포함하여 구성된다.

[0076] 상기 OTP 생성부(210)는, 일회성 비밀번호인 OTP를 생성하는 기능을 수행한다.

[0077] 상기 OTP는, OTP 생성용 단방향 해시함수에 사용자 패스워드, 사용자 고유 비밀값, 상기 OTP 생성 누적횟수 또는 이들의 조합을 입력하여 생성되는 해시값으로 구성된다.

[0078] 이때, 상기 OTP 생성용 단방향 해시함수와, 상기 사용자 패스워드, 사용자 고유 비밀값은, 상기 단일 패킷 인증 시스템(100)에서 회원 가입 등과 같은 절차를 통해 사전에 발급되어 상기 클라이언트(200)의 메모리(260)에 저장된다.

[0079] 또한 상기 OTP 생성 누적횟수는, 상기 OTP를 생성한 횟수를 의미하는 것으로, 상기 클라이언트(200) 및 상기 단일 패킷 인증 시스템(100)은, 상기 OTP를 생성할 때마다 그 횟수를 카운트하여 저장한다.

[0080] 또한 상기 디바이스 핑거프린트 생성부(220)는, 상기 클라이언트(200)에 대한 디바이스 정보와, 상기 클라이언트(200)에 대한 디바이스의 고유 암호키를 디바이스 인증코드 생성용 해시함수에 입력하여, 상기 클라이언트(200)에 대한 디바이스 인증코드를 생성함으로써, 상기 디바이스 핑거프린트를 생성하는 기능을 수행한다.

[0081] 이때, 상기 디바이스 정보는, MAC주소, 상기 단일 패킷 인증 시스템(100)에서 발급된 디바이스 식별정보 또는 이들의 조합을 포함하며, 상기 메모리(260)에 저장되어 있으며, 상기 단일 패킷 인증 시스템(100)에 사전에 등록되어 있다.

[0082] 또한 고유 암호키는, 상기 단일 패킷 인증 시스템(100)에서 상기 클라이언트(200)별로 사전에 발급된 고유한 암호키를 의미하는 것으로, 상기 메모리(260)에 저장되어 관리된다.

[0083] 또한 상기 SPA 패킷 생성부(230)는, 상기 생성한 OTP와 디바이스 핑거프린트를 토대로, 상기 단일 패킷 인증 시스템(100)에 해당 클라이언트(200)를 인증을 요청하기 위한 SPA 패킷을 생성하는 기능을 수행한다.

[0084] 여기서, 상기 SPA 패킷은, 상기 생성한 OTP 및 디바이스 핑거프린트 이외에 해당 클라이언트(200)에 대해 인증을 요청하기 위한 코드인 인증요청코드, 추가적인 정보를 포함하는 메타데이터를 더 포함함은 상술한 바와 같다.

[0085] 한편, 상기 SPA 패킷은, 도 2를 참조하여 설명하였으므로, 더 이상의 상세한 설명은 생략하도록 한다.

[0086] 또한 TCP 패킷 생성부(240)는, 상기 생성한 SPA 패킷을 TCP 패킷의 데이터 필드에 삽입함으로써, 상기 SPA 패킷을 전송하기 위한 TCP 패킷을 생성하고, 상기 통신부(250)를 통해 상기 단일 패킷 인증 시스템(100)으로 전송할 수 있도록 하는 기능을 수행한다.

[0087] 한편, 상기 SPA 패킷은, 상기 인증을 위해 상기 TCP 패킷에 삽입되는 것으로, 상기 단일 패킷 인증 시스템(100)에서 해당 클라이언트(200)를 인증하여 상기 클라이언트(200)와 상기 단일 패킷 인증 시스템(100)간의 TCP 통신세션이 연결된 경우에는, 상기 단일 패킷 인증 시스템(100)과의 데이터를 송수신하기 위한 TCP 패킷이 생성됨은 당연할 것이다.

[0088] 또한 상기 통신부(250)는, 상기 생성한 SAP 패킷을 포함하는 TCP 패킷을 상기 단일 패킷 인증 시스템(100)으로 전송하거나, 상기 단일 패킷 인증 시스템(100)과 TCP 통신세션이 연결된 경우에는, 상기 단일 패킷 인증 시스템(100)과 데이터를 송수신하기 위한 TCP 패킷을 송수신하는 기능을 수행한다.

[0089] 또한 상기 메모리(260)는, 상기 사용자 식별자, 사용자 고유의 비밀값, 패스워드, OTP 생성용 해시함수, 디바이스 정보, 디바이스 인증코드 생성용 해시함수, 디바이스 고유 암호키 등을 저장하는 기능을 수행한다.

[0090] 도 4는 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템의 구성을 나타낸 블록도이다.

[0091] 도 4에 도시한 바와 같이, 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증 시스템(100)은, 적어도 하나 이상의 클라이언트(200)로부터 SPA 패킷을 수신하는 SPA 패킷 수신부(110), 상기 수신한 SPA 패킷에 대한 유효성을 검증하여 상기 클라이언트(200)에 대한 인증을 수행하는 SPA 패킷 유효성 검증부(120), 상기 유효성을 검증한 결과에 따라 상기 클라이언트(200)와 TCP 통신세션을 연결하는 통신세션 연결부(130) 및 상기 클라이언트(200)별로 인증에 필요한 인증데이터를 관리하는 클라이언트 인증데이터 관리부(140)를 포함하여 구성된다.

[0092] 상기 SPA 패킷 수신부(110)는, 상기 적어도 하나 이상의 클라이언트(200)로부터 TCP 패킷에 삽입되어 수신되는 SPA 패킷을 수신하는 기능을 수행한다. 즉, 상기 SPA 패킷 수신부(110)는, 상기 적어도 하나 이상의 클라이언트

(200)로부터 수신되는 TCP 패킷에서 상기 SPA 패킷을 추출함으로써, 상기 SPA 패킷을 수신하게 된다.

[0093] 또한 상기 SPA 패킷 유효성 검증부(120)는, 상기 수신한 SPA 패킷의 유효성을 검증하여 상기 클라이언트(200)를 인증하기 위한 것으로, 상기 SPA 패킷의 OTP를 검증하는 OTP 검증부(121) 및 상기 수신한 SPA 패킷의 디바이스 핑거프린트를 검증하는 디바이스 핑거프린트 검증부(122)를 포함하여 구성된다.

[0094] 또한 상기 OTP 검증부(121)는, 상기 SPA 패킷의 사용자 식별자를 참조하여, 해당 클라이언트(200)에 대해 관리되는 사용자의 패스워드, 사용자 고유 비밀값과 해당 클라이언트(200)의 OTP 생성 누적횟수 또는 이들의 조합을 상기 클라이언트(200)에 발급한 OTP 생성용 단방향 해시함수에 입력하여, 상기 클라이언트(200)에 대한 OTP를 추출한다. 이때, 상기 OTP 생성용 단방향 해시함수에 입력되는 상기 조합은 상기 클라이언트(200)에서 상기 OTP를 생성하기 위해 입력한 조합과 동일함은 당연하다. 이는 사전에 미리 설정된다.

[0095] 또한 상기 OTP 검증부(121)는, 상기 추출한 OTP와 상기 수신한 SPA 패킷의 OTP를 상호 비교하여, 상기 SPA 패킷의 OTP에 대한 유효여부를 판단함으로써, 상기 SPA 패킷의 OTP를 검증한다.

[0096] 여기서, 상기 비교한 결과, 상기 추출한 OTP와 상기 SPA 패킷의 OTP가 일치하는 경우에는, 해당 OPT가 유효한 것으로 판단하며, 일치하지 않는 경우에는 해당 OTP가 유효하지 않는 것으로 판단한다.

[0097] 이때, 검증한 결과 상기 SAP 패킷에 포함된 OTP에 대한 유효성이 검증되지 않는 경우에는, 상기 SPA 패킷을 포함하여 수신한 TCP 패킷을 드롭하여 상기 클라이언트(200)와의 통신을 종료한다.

[0098] 또한 상기 디바이스 핑거프린트 검증부(122)는, 상기 SPA 패킷의 사용자 식별자를 참조하여, 해당 클라이언트(200)에 대해 관리되는 상기 클라이언트(200)에 대한 디바이스 정보, 디바이스에 대한 고유 암호키를 상기 클라이언트(200)에 발급한 디바이스 인증코드 생성용 단방향 해시함수에 입력하여 해당 클라이언트(200)에 대한 디바이스 인증코드를 추출한다.

[0099] 또한 상기 디바이스 핑거프린트 검증부(122)는, 상기 추출한 디바이스 인증코드와 상기 SPA 패킷의 디바이스 핑거프린트에 포함된 디바이스 인증코드를 상호 비교하여, 상기 SPA 패킷의 디바이스 핑거프린트에 대한 유효여부를 판단함으로써, 상기 SPA 패킷의 디바이스 핑거프린트를 검증한다.

[0100] 또한 상기 디바이스 핑거프린트 검증부(122)는, 상기 추출한 디바이스 인증코드와 상기 SPA 패킷의 디바이스 핑거프린트를 구성하는 디바이스 인증코드가 일치하는 경우에는, 해당 SPA 패킷의 디바이스 핑거프린트가 유효한 것으로 판단하며, 일치하지 않는 경우에는 해당 디바이스 핑거프린트가 유효하지 않는 것으로 판단한다.

[0101] 이때, 상기 검증한 결과, 상기 SPA 패킷의 디바이스 핑거프린트에 대한 유효성이 검증되지 않는 경우에는, 상기 SPA 패킷을 포함하여 상기 수신한 TCP 패킷을 드롭하여 상기 클라이언트(200)와의 통신을 종료한다.

[0102] 즉, 상기 SPA 패킷 유효성 검증부(120)는, 상기 SPA 패킷의 OTP와 디바이스 핑거프린트를 동시에 검증하여 상기 SPA 패킷에 대한 유효성을 검증함으로써, 상기 클라이언트(200)를 개별적으로 인증하는 것이다.

[0103] 한편, 상기 수신한 SPA 패킷에, 사용자의 지문이나, 성별, 주소 등과 같이 추가적인 인증을 위한 메타데이터가 포함되어 있는 경우에는, 상기 SPA 패킷 유효성 검증부(120)는, 상기 OTP, 디바이스 핑거프린트 이외에 해당 메타데이터에 대한 유효여부를 더 판단하여, 상기 클라이언트(200)를 인증함은 상술한 바와 같다.

[0104] 또한 상기 통신세션 연결부(130)는, 상기 SPA 패킷에 대한 유효성을 검증한 결과, 해당 SPA 패킷이 유효하여 상기 클라이언트(200)가 인증된 경우에는, 상기 인증한 클라이언트(200)와 TCP 통신세션을 연결하는 기능을 수행한다.

[0105] 상기 TCP 통신세션을 연결하는 것은, 상기 인증된 상기 클라이언트(200)와 데이터 송수신을 위한 TLS 터널을 형성함으로서, 수행된다.

[0106] 또한 상기 클라이언트 인증데이터 관리부(140)는, 상기 클라이언트를 인증하기 위한 관련 데이터를 클라이언트(200)별로 관리하는 기능을 수행한다.

[0107] 즉, 상기 클라이언트 인증데이터 관리부(140)는, 상기 사용자 식별자, 패스워드, 사용자 고유 비밀값, 상기 디바이스 정보, 상기 디바이스 고유 비밀키, OTP 생성용 단방향 해시함수, 디바이스 인증코드 생성용 단방향 해시함수 등을 데이터베이스(300)에 저장하여, 상기 클라이언트(200)의 인증에 필요한 데이터를 클라이언트(200)별로 분류하여 관리하는 기능을 수행하는 것이다.

[0108] 도 5는 본 발명의 일 실시예에 따른 TCP 패킷을 이용한 단일 패킷 인증을 수행하는 절차를 나타낸 흐름도이다.

[0109] 도 5에 도시한 바와 같이, 본 발명의 일 실시예에 따른 단일 패킷 인증 시스템(100)을 통해 단일 패킷 인증을 수행하여 적어도 하나 이상의 클라이언트(200)를 각각 인증하는 절차는 우선, 상기 적어도 하나 이상의 클라이언트(200)에서, 인증을 위한 SPA 패킷을 생성하여 TCP 패킷에 삽입한 후, 상기 단일 패킷 인증 시스템(100)으로 전송하는 단계를 수행한다(S110).

[0110] 이때, 상기 클라이언트(200)는, 상기 단일 패킷 인증 시스템(100)에 발급한 OTP 생성용 단방향 해시함수를 통해 OTP를 생성하는 OTP 생성단계를 수행하고, 상기 단일 패킷 인증 시스템(100)에서 발급한 디바이스 인증코드 생성용 단방향 해시함수를 통해 디바이스 인증코드를 생성하여 디바이스 핑거프린트를 생성하는 디바이스 핑거프린트 생성단계를 수행한다.

[0111] 또한 상기 클라이언트(200)는, 상기 생성한 OTP 및 디바이스 핑거프린트를 포함하는 SPA 패킷을 생성하는 SPA 패킷 생성 단계를 수행하고, 상기 생성한 SPA 패킷을 TCP 패킷의 데이터 필드에 삽입하여, 상기 SPA 패킷을 상기 단일 패킷 인증 시스템(100)으로 전송하기 위한 TCP 패킷을 생성하는 TCP 패킷 생성 단계를 수행한다.

[0112] 한편, 상기 SPA 패킷과 상기 TCP 패킷을 생성하는 것은 도 2 및 도 3을 참조하여 상세히 설명하였으므로, 더 이상의 상세한 설명은 생략하도록 한다.

[0113] 다음으로, 상기 단일 패킷 인증 시스템(100)에서 적어도 하나 이상의 클라이언트(200)로부터 SPA 패킷을 수신하는 SPA 패킷 수신 단계를 수행한다(S120).

[0114] 이때, 상기 SPA 패킷은 상기 적어도 하나 이상의 클라이언트(200)별로 수신되는 TCP 패킷의 데이터 필드로부터 SPA 패킷을 추출함으로써, 수신된다.

[0115] 다음으로, 상기 단일 패킷 인증 시스템(100)은, 상기 수신한 SPA 패킷에 포함된 OTP 및 디바이스 핑거프린트에 유효여부를 동시에 검증하여, 상기 SPA 패킷에 대한 유효성을 검증하는 SPA 패킷 유효성 검증 단계를 수행한다(S130).

[0116] 상기 OTP를 검증하는 것은, 상기 클라이언트(200)에 발급한 OTP 생성용 단방향 해시함수를 이용하여 상기 클라이언트(200)에 대한 OTP를 추출하고, 상기 추출한 OTP와 상기 수신한 SAP 패킷의 OTP를 비교함으로써, 수행됨은 상술한 바와 같다.

[0117] 또한 상기 디바이스 핑거프린트를 검증하는 것은, 상기 클라이언트(200)에 발급한 디바이스 인증코드 생성용 단방향 해시함수를 이용하여, 상기 클라이언트(200)에 대한 디바이스 인증코드를 추출하고, 상기 추출한 디바이스 인증코드와 상기 수신한 SPA 패킷의 디바이스 핑거프린트를 구성하는 디바이스 인증코드를 상호 비교함으로써, 수행됨은 상술한 바와 같다.

[0118] 한편, 상기 수신한 SPA 패킷에 사용자 지문 등과 같은 사용자 정보로 구성되는 메타데이터가 포함되어 있는 경우, 상기 단일 패킷 인증 시스템(100)은, 상기 메타데이터에 대한 유효성을 검증하는 것을 더 포함하여 상기 클라이언트(200)를 인증할 수 있음은 상술한 바와 같다.

[0119] 다음으로, 상기 단일 패킷 인증 시스템(100)은, 상기 수신한 SPA 패킷의 OTP와 디바이스 핑거프린트를 검증한 결과 상기 SPA 패킷의 유효성이 검증된 경우(S140), 상기 유효성이 검증되어 인증된 해당 클라이언트(200)와 TCP 통신세션을 연결하는 TCP 통신세션 연결 단계를 수행한다(S150).

[0120] 상기 TCP 통신세션 연결 단계는, 상기 인증된 상기 클라이언트(200)와 데이터 송수신을 위한 TLS 터널을 형성함으로써, 상기 TCP 통신세션을 연결하게 된다.

[0121] 한편, 상기 단일 패킷 인증 시스템(100)은, 상기 SPA 패킷의 유효성이 검증되지 않은 경우(S150)에는, 해당 클라이언트(200)로부터 수신된 TCP 패킷을 드롭하여 상기 클라이언트(200)와의 통신을 종료한다(S151).

[0122] 이상에서 설명한 바와 같이, 본 발명은 TCP 패킷을 이용한 단일 패킷 인증 시스템 및 그 방법에 관한 것으로, 적어도 하나 이상의 클라이언트로부터 사용자 식별자, OTP, 디바이스 핑거프린트 등을 포함하는 SPA 패킷을 TCP 패킷을 통해 수신하고, 상기 수신한 OPT와 디바이스 핑거프린트에 대한 유효여부를 판단하여 상기 클라이언트별 SPA 패킷에 대한 유효성을 검증하여, 검증한 결과에 따라 상기 클라이언트와 TCP 통신세션을 연결함으로써, 상기 클라이언트에 대한 인증과정을 간소화하고, 제3의 클라이언트가 상기 인증한 클라이언트에 대한 사용자 신분으로 상기 TCP 통신세션이 연결되는 것을 방지하여 네트워크 보안을 극대화할 수 있도록 하는 효과가 있다.

[0123] 상기에서는 본 발명에 따른 바람직한 실시예를 위주로 상술하였으나, 본 발명의 기술적 사상은 이에 한정되는 것은 아니며 본 발명의 각 구성요소는 동일한 목적 및 효과의 달성을 위하여 본 발명의 기술적 범위 내에서 변

경 또는 수정될 수 있을 것이다.

[0124] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형 실시가 가능한 것은 물론이고, 이러한 변형 실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안 될 것이다.

부호의 설명

[0125] 100: TCP 패킷을 이용한 단일 패킷 인증 시스템 110: SPA 패킷 수신부

120: SPA 패킷 유효성 검증부 121: OTP 검증부

122: 디바이스 핑거프린트 검증부 130: 통신세션 연결부

140: 클라이언트 인증데이터 관리부 200: 클라이언트

210: OTP 생성부 220: 디바이스 핑거프린트 생성부

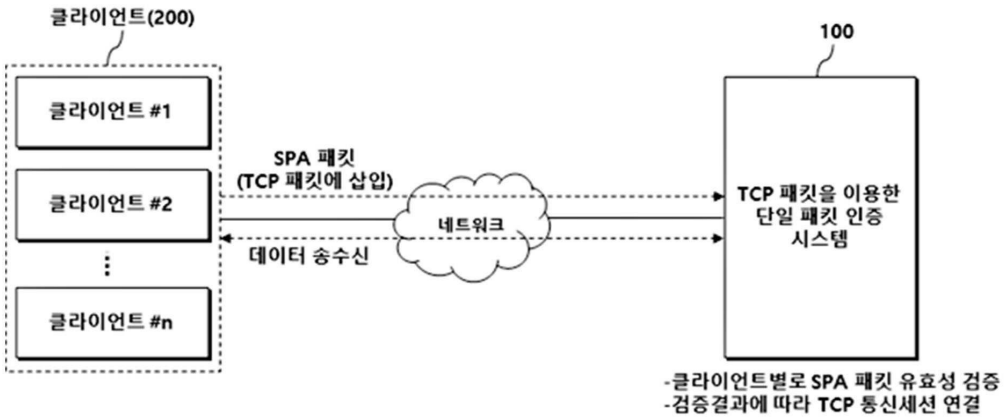
230: SPA 패킷 생성부 240: TCP 패킷 생성부

250: 통신부 260: 메모리

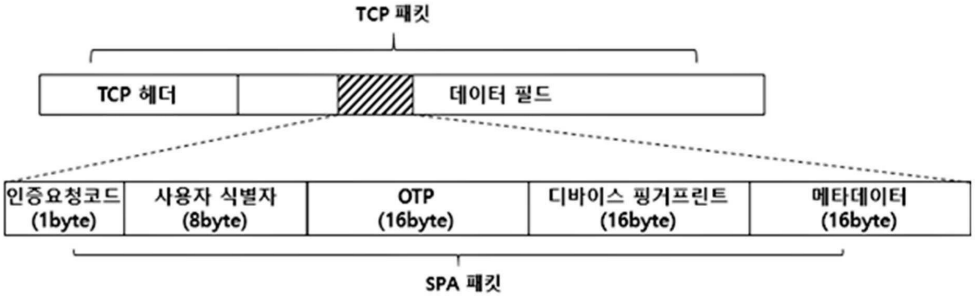
300: 데이터베이스

도면

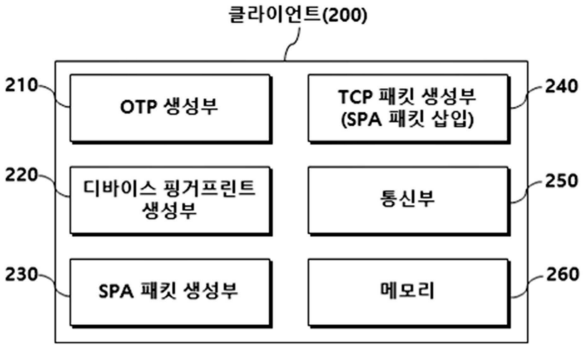
도면1



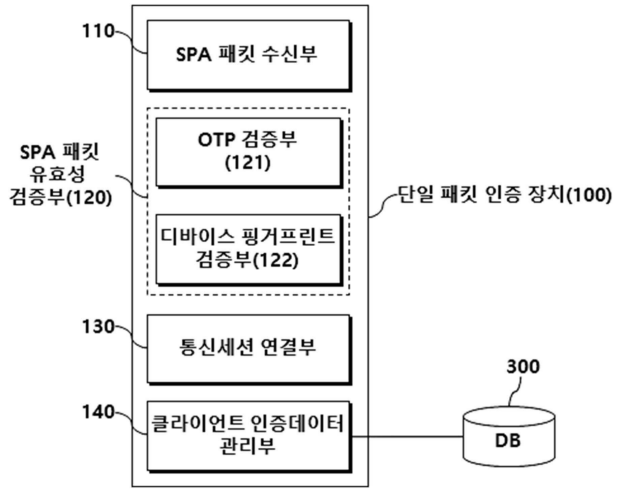
도면2



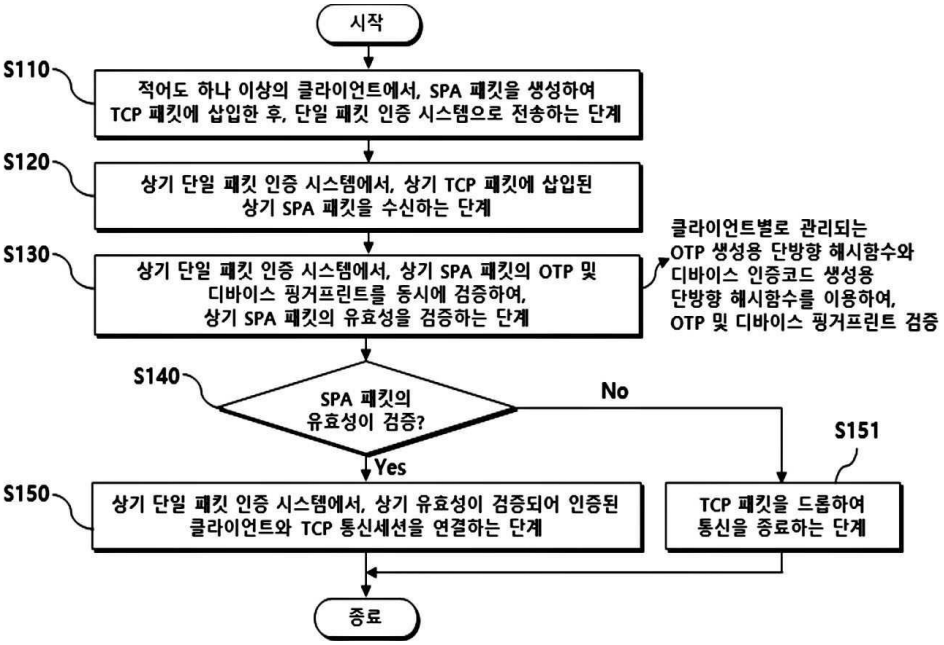
도면3


클라이언트(200)
210
OTP 생성부
TCP 패킷 생성부
(SPA 패킷 삽입)
240
220
디바이스 핑거프린트
생성부
통신부
250
230
SPA 패킷 생성부
메모리
260

도면4


110
SPA 패킷 수신부
SPA 패킷
유효성
검증부(120)
OTP 검증부
(121)
디바이스 핑거프린트
검증부(122)
단일 패킷 인증 장치(100)
130
통신세션 연결부
300
140
클라이언트 인증데이터
관리부
DB

도면5


시작
S110
적어도 하나 이상의 클라이언트에서, SPA 패킷을 생성하여
TCP 패킷에 삽입한 후, 단일 패킷 인증 시스템으로 전송하는 단계
S120
상기 단일 패킷 인증 시스템에서, 상기 TCP 패킷에 삽입된
상기 SPA 패킷을 수신하는 단계
S130
상기 단일 패킷 인증 시스템에서, 상기 SPA 패킷의 OTP 및
디바이스 핑거프린트를 동시에 검증하여,
상기 SPA 패킷의 유효성을 검증하는 단계
클라이언트별로 관리되는
OTP 생성용 단방향 해시함수와
디바이스 인증코드 생성용
단방향 해시함수를 이용하여,
OTP 및 디바이스 핑거프린트 검증
S140
SPA 패킷의
유효성이 검증?
No
S151
Yes
S150
상기 단일 패킷 인증 시스템에서, 상기 유효성이 검증되어 인증된
클라이언트와 TCP 통신세션을 연결하는 단계
TCP 패킷을 드롭하여
통신을 종료하는 단계
종료