(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월07일
(11) 등록번호 10-1575552
(24) 등록일자 2015년12월01일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/62* (2013.01)
G06Q 20/00 (2006.01) *H04L 29/08* (2006.01)
(21) 출원번호 10-2014-7018393
(22) 출원일자(국제) 2012년12월24일
심사청구일자 2014년07월02일
(85) 번역문제출일자 2014년07월02일
(65) 공개번호 10-2014-0098243
(43) 공개일자 2014년08월07일
(86) 국제출원번호 PCT/EP2012/076865
(87) 국제공개번호 WO 2013/102596
국제공개일자 2013년07월11일
(30) 우선권주장
1250043 2012년01월03일 프랑스(FR)
(56) 선행기술조사문헌
EP0889620 A2*
WO0128154 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
알까멜 루슨트
프랑스 92100 불론뉴-비영꾸르 루뜨 들 라 렌느 148/152
(72) 발명자
토우비아나 빈센트
프랑스 75020 파리 뤼 비슨 11
파필론 세르지
프랑스 91620 노자이 라우트 드 빌레저스트 센트레 드 빌라루소 알까뗄 루슨트 벨 랩스 프랑스
(74) 대리인
제일특허법인

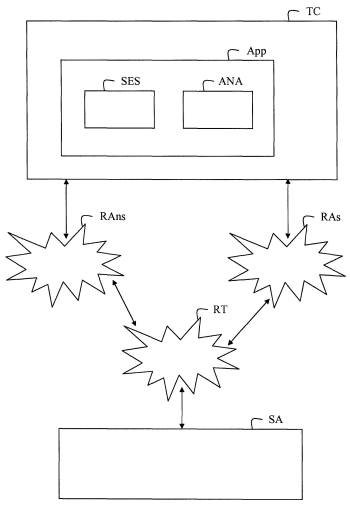
전체 청구항 수 : 총 9 항 심사관 : 문해진

(54) 발명의 명칭 **안전한 데이터 전송**

(57) 요 약

원격 통신 네트워크(RT)를 통해 통신 단말(TC)로부터 애플리케이션 서버(SA)로 데이터를 안전하게 전송하기 위해, - 통신 단말(TC)은 안전하지 않은 액세스 네트워크(RAns)를 통해 애플리케이션 서버(SA)에 접속되고, 적어도 하나의 안전한 액세스 네트워크(RAs)를 통해 애플리케이션 서버(SA)와 통신할 수 있음 - , 통신 단말(TC)은, 개인 데이터(DonP)가 사용자에 의해 입력될 가능성이 있거나 입력될 때, 애플리케이션 서버(SA)와의 접속을 안전하지 않은 액세스 네트워크(RAns)로부터 안전한 액세스 네트워크(RAs)로 스위칭하고, 안전한 액세스 네트워크(RAs)를 통해 개인 데이터(DonP)를 애플리케이션 서버(SA)로 전송하고, 애플리케이션 서버(SA)와의 접속을 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

원격 통신 네트워크(RT)를 통해 사용자의 통신 단말(TC)로부터 애플리케이션 서버(SA)로 안전한 방식으로 데이터를 전송하기 위한 방법으로서,

상기 통신 단말(TC)은 안전하지 않은 액세스 네트워크(RAns)를 통해 상기 애플리케이션 서버(SA)에 접속되고, 적어도 하나의 안전한 액세스 네트워크(RAs)를 통해 상기 애플리케이션 서버(SA)와 통신할 수 있고, 상기 방법은 상기 통신 단말(TC)에서,

개인 데이터(DonP)가 상기 사용자에 의해 입력되고 상기 애플리케이션 서버(SA)로 전송될 가능성이 있을 때, 상기 애플리케이션 서버(SA)와의 접속을 상기 안전하지 않은 액세스 네트워크(RAns)로부터 안전한 액세스 네트워크(RAs)로 스위칭하는 단계(E2)와,

상기 안전한 액세스 네트워크(RAs)를 통해 개인 데이터(DonP)를 상기 애플리케이션 서버(SA)로 전송하는 단계(E4)와,

상기 애플리케이션 서버(SA)와의 접속을 상기 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭하는 단계(E7)를 포함하되,

상기 애플리케이션 서버(SA)는 상기 통신 단말(TC)로부터 수신된 요청(Req)에 포함된 정보에 기초하여 세션 쿠키(Cs)를 생성하고, 상기 세션 쿠키(Cs)를 상기 통신 단말(TC)로 전송하고,

상기 세션 쿠키(Cs)는 세션 동안에 상기 애플리케이션 서버(SA)에 의해 제공되는 서비스의 사용에 대한 제한들을 포함하는

데이터 전송 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 애플리케이션 서버(SA)와의 접속은, 상기 통신 단말(TC)이 상기 세션 쿠키(Cs)를 수신한 후에, 상기 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭하는

데이터 전송 방법.

청구항 4

제 1 항 또는 제 3 항에 있어서,

상기 사용자에 의해 입력된 데이터는, 상기 애플리케이션 서버에 의해 호스팅되는 웹페이지가 상기 통신 단말(TC)의 웹 브라우저에 의해 액세스될 때, 및 상기 통신 단말(TC)이 안전하지 않은 액세스 네트워크(RAns)를 통해 상기 애플리케이션 서버(SA)에 접속될 때, 체크될 수 있는

데이터 전송 방법.

청구항 5

제 4 항에 있어서,

상기 사용자에 의해 입력된 데이터는, 상기 데이터의 입력 동안에, 또는 상기 애플리케이션 서버로 전송되는 것을 고려하여 상기 사용자에 의한 데이터의 확인 동안에 입력된 후, 체크될 수 있는

데이터 전송 방법.

청구항 6

제 1 항 또는 제 3 항에 있어서,

상기 통신 단말(TC)이 안전하지 않은 액세스 네트워크(RAns)를 통해 상기 애플리케이션 서버(SA)에 접속될 때, 개인 데이터로 완성될 수 있는, 상기 통신 단말(TC)의 웹 브라우저에 의해 액세스되는 웹페이지의 입력 필드들이 체크될 수 있는

데이터 전송 방법.

청구항 7

제 1 항 또는 제 3 항에 있어서,

안전하지 않은 액세스 네트워크는, 전송되는 데이터가 어떠한 기밀(confidentiality)도 갖지 않고 상기 데이터가 상기 데이터의 의도된 수신인이 아닌 엔티티에 의해 인터셉트될 수 있는 네트워크인

데이터 전송 방법.

청구항 8

제 1 항 또는 제 3 항에 있어서,

안전한 액세스 네트워크는, 전송되는 데이터가 기밀을 갖고 상기 데이터가 상기 데이터의 의도된 수신인이 아닌 엔티티에 의해 인터셉트될 수 없는 네트워크인

데이터 전송 방법.

청구항 9

원격 통신 네트워크(RT)를 통해 사용자의 통신 단말(TC)로부터 애플리케이션 서버(SA)로 안전한 방식으로 데이터를 전송하기 위한 통신 단말(TC)로서,

상기 통신 단말(TC)은 안전하지 않은 액세스 네트워크(RAns)를 통해 상기 애플리케이션 서버(SA)에 접속되고, 적어도 하나의 안전한 액세스 네트워크(RAs)를 통해 상기 애플리케이션 서버(SA)와 통신할 수 있고,

상기 통신 단말(TC)은,

개인 데이터(DonP)가 상기 사용자에 의해 입력되고 상기 애플리케이션 서버(SA)로 전송될 가능성이 있을 때, 상기 애플리케이션 서버(SA)와의 접속을 상기 안전하지 않은 액세스 네트워크(RAns)로부터 안전한 액세스 네트워크(RAs)로 스위칭하기 위한 수단(SES)과,

상기 안전한 액세스 네트워크(RAs)를 통해 개인 데이터(DonP)를 상기 애플리케이션 서버(SA)로 전송하기 위한 수단(SES)과,

상기 애플리케이션 서버(SA)와의 접속을 상기 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭하기 위한 수단(SES)을 포함하되,

상기 애플리케이션 서버(SA)는 상기 통신 단말(TC)로부터 수신된 요청(Req)에 포함된 정보에 기초하여 세션 쿠

키(Cs)를 생성하고, 상기 세션 쿠키(Cs)를 상기 통신 단말(TC)로 전송하고,

상기 세션 쿠키(Cs)는 세션 동안에 상기 애플리케이션 서버(SA)에 의해 제공되는 서비스의 사용에 대한 제한들을 포함하는

통신 단말.

청구항 10

원격 통신 네트워크(RT)를 통해 사용자의 통신 단말(TC)로부터 애플리케이션 서버(SA)로 안전한 방식으로 데이터를 전송하기 위해 통신 단말(TC)에서 구현될 수 있는 컴퓨터 프로그램으로서,

상기 통신 단말(TC)은 안전하지 않은 액세스 네트워크(RAns)를 통해 상기 애플리케이션 서버(SA)에 접속되고, 적어도 하나의 안전한 액세스 네트워크(RAs)를 통해 상기 애플리케이션 서버(SA)와 통신할 수 있고,

상기 컴퓨터 프로그램은, 상기 컴퓨터 프로그램이 상기 통신 단말(TC)에서 로딩 및 실행될 때,

개인 데이터(DonP)가 상기 사용자에 의해 입력되고 상기 애플리케이션 서버(SA)로 전송될 가능성이 있을 때, 상기 애플리케이션 서버(SA)와의 접속을 상기 안전하지 않은 액세스 네트워크(RAns)로부터 안전한 액세스 네트워크(RAs)로 스위칭하는 단계(E2)와,

상기 안전한 액세스 네트워크(RAs)를 통해 개인 데이터(DonP)를 상기 애플리케이션 서버(SA)로 전송하는 단계(E4)와,

상기 애플리케이션 서버(SA)와의 접속을 상기 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭하는 단계(E7)를 수행하되,

상기 애플리케이션 서버(SA)는 상기 통신 단말(TC)로부터 수신된 요청(Req)에 포함된 정보에 기초하여 세션 쿠키(Cs)를 생성하고, 상기 세션 쿠키(Cs)를 상기 통신 단말(TC)로 전송하고,

상기 세션 쿠키(Cs)는 세션 동안에 상기 애플리케이션 서버(SA)에 의해 제공되는 서비스의 사용에 대한 제한들을 포함하는

명령어들을 포함하는

컴퓨터 프로그램을 저장하는 컴퓨터 판독 가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 위험하다고 여겨지는 원격 통신 네트워크들을 통한 안전한 데이터 전송에 관한 것이다.

배 경 기 술

[0002] 사용자들이 안전하지 않은 네트워크들에 접속되고 안전하지 않은 서비스들에 로그인할 때, 사용자들은 다른 사용자들이 그들의 개인 데이터를 액세스하는 것을 가능하게 한다. 예를 들면, 사용자들이 공공 장소에서 공유된 액세스 포인트로부터 TLS(Transport Layer Security) 지원을 제공하지 않는 서비스에 접속될 때, 사용자들은 암호화(encryption) 없이 그들의 로그인들 및 패스워드들을 전송한다. 그러면, 악의적인 사용자는 그 데이터를 용이하게 인터셉트하고, 세션 식별자를 검색하고, 사용자 세션을 액세스할 수 있다.

발명의 내용

해결하려는 과제

[0003] 따라서, 사용자가 원격 통신 네트워크를 통해 서비스를 액세스할 때마다 그러한 위험성들을 감소시킬 필요성이

존재한다.

과제의 해결 수단

[0004] 상술된 문제점들을 해소하기 위해, 본 발명은 원격 통신 네트워크를 통해 사용자의 통신 단말로부터 애플리케이션 서버로 안전한 방식으로 데이터를 전송하기 위한 방법을 제공하고, 통신 단말은 안전하지 않은 액세스 네트워크를 통해 애플리케이션 서버에 접속되고, 적어도 하나의 안전한 액세스 네트워크를 통해 애플리케이션 서버와 통신할 수 있고, 상기 방법은 통신 단말에서, 다음의 단계들,

[0005] 개인 데이터가 사용자에 의해 입력되고 애플리케이션 서버로 전송될 가능성이 있을 때, 애플리케이션 서버와의 접속을 안전하지 않은 액세스 네트워크로부터 안전한 액세스 네트워크로 스위칭하는 단계와,

[0006] 안전한 액세스 네트워크를 통해 개인 데이터를 애플리케이션 서버로 전송하는 단계와,

[0007] 애플리케이션 서버와의 접속을 안전한 액세스 네트워크로부터 안전하지 않은 액세스 네트워크로 스위칭하는 단계를 포함한다.

[0008] 이롭게도, 상기 시스템은 안전하지 않은 액세스 네트워크를 통해, 로그인들 및 패스워드들과 같은 개인 데이터를 밝히지 않고, 세션을 수립하는 것을 가능하게 한다.

[0009] 본 발명의 또 다른 특성에 따라, 애플리케이션 서버는 통신 단말로부터 수신된 요청에 포함된 정보에 기초하여 세션 쿠키를 생성할 수 있고, 세션 쿠키를 통신 단말로 전송하고, 세션 쿠키는 세션 동안에 애플리케이션 서버)에 의해 제공되는 서비스의 사용에 대한 제한들을 포함한다.

[0010] 이로써, 사용자는 안전하지 않은 액세스 네트워크를 통해 서비스를 액세스하는데 나중에 사용될 수 있는 안전한 세션을 생성할 수 있다.

[0011] 본 발명의 또 다른 특성에 따라, 애플리케이션 서버와의 접속은, 통신 단말이 세션 쿠키를 수신한 후에, 안전한 액세스 네트워크로부터 안전하지 않은 액세스 네트워크로 스위칭할 수 있다.

[0012] 본 발명의 또 다른 특성에 따라, 사용자에 의해 입력된 데이터는, 애플리케이션 서버에 의해 호스팅되는 웹페이지가 통신 단말의 웹 브라우저에 의해 액세스될 때, 및 통신 단말이 안전하지 않은 액세스 네트워크를 통해 애플리케이션 서버에 접속될 때, 체크될 수 있다.

[0013] 본 발명의 또 다른 특성에 따라, 사용자에 의해 입력된 데이터는, 상기 데이터의 입력 동안에, 또는 애플리케이션 서버로 전송되는 것을 고려하여 사용자에 의한 데이터의 확인 동안에 입력된 후, 체크될 수 있다.

[0014] 본 발명의 또 다른 특성에 따라, 통신 단말이 안전하지 않은 액세스 네트워크를 통해 애플리케이션 서버에 접속될 때, 개인 데이터로 완성될 수 있는 통신 단말의 웹 브라우저에 의해 액세스되는 웹페이지의 입력 필드들이 체크될 수 있다.

[0015] 본 발명은 또한 원격 통신 네트워크를 통해 사용자의 통신 단말로부터 애플리케이션 서버로 안전한 방식으로 데이터를 전송하기 위한 통신 단말에 관한 것이며, 통신 단말은 안전하지 않은 액세스 네트워크를 통해 애플리케이션 서버에 접속되고, 적어도 하나의 안전한 액세스 네트워크를 통해 애플리케이션 서버와 통신할 수 있고, 통신 단말은,

[0016] 개인 데이터가 사용자에 의해 입력되고 애플리케이션 서버로 전송될 가능성이 있을 때, 애플리케이션 서버와의 접속을 안전하지 않은 액세스 네트워크로부터 안전한 액세스 네트워크로 스위칭하기 위한 수단과,

[0017] 안전한 액세스 네트워크를 통해 개인 데이터를 애플리케이션 서버로 전송하기 위한 수단과,

[0018] 애플리케이션 서버와의 접속을 안전한 액세스 네트워크로부터 안전하지 않은 액세스 네트워크로 스위칭하기 위한 수단을 포함한다.

[0019] 본 발명은 또한 단말에서 구현될 수 있는 컴퓨터 프로그램에 관한 것이며, 상기 프로그램은, 프로그램이 상기 단말에서 실행될 때마다, 본 발명의 방법에 따른 단계들을 수행하는 명령어들을 포함한다.

[0020] 본 발명 및 본 발명의 이점들은 첨부된 도면들을 참조하는 하기의 설명을 검토할 때 더 양호하게 이해되어야 한다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 통신 시스템의 간략한 블록도이다.

도 2는 본 발명의 일 실시예에 따른 안전한 데이터 전송을 위한 방법의 알고리즘이다.

발명을 실시하기 위한 구체적인 내용

[0022] 도 1을 참조하면, 통신 시스템은 원격 통신 네트워크(RT)를 통해 서로 통신할 수 있는 애플리케이션 서버(SA) 및 통신 단말(TC)을 포함한다.

[0023] 원격 통신 네트워크(RT)는, 애플리케이션 서버(SA)가 위치된 고속 IP 패킷 네트워크에 접속된 유선 또는 무선 네트워크들 또는 유선 및 무선 네트워크들의 조합을 포함할 수 있다.

[0024] 예를 들면, 통신 단말(TC)은 랩톱 개인용 컴퓨터, 태블릿 또는 모바일 셀룰러 무선 통신 단말일 수 있다. 또 다른 예를 들면, 통신 단말은, 사용자에게 개인적이고 통신 PDA(personal digital assistant) 또는 스마트폰일 수 있는 디바이스 또는 전자 원격 통신 오브젝트를 포함한다.

[0025] 원격 통신 단말은, 예를 들면, GMS("Global System for Mobile communications") 또는 UMTS("Universal Mobile Telecommunications System") 타입의 액세스 시스템, 및/또는 WLAN("Wireless Local Area Network") 타입의 단거리 공공 무선 네트워크, 또는 802.1x 표준들 중 하나를 준수하는 것, 또는 WIMAX 프로토콜("Worldwide Interoperability Microwave Access")에 따른 중거리 무선 네트워크를 통해 원격 통신 네트워크에 접속될 수 있다.

[0026] 통신 단말(TC)은 통신 단말(TC)이 애플리케이션 서버(SA)와 통신하게 하는 애플리케이션(App)을 포함한다. 일 예에 따라, 애플리케이션(App)이 웹 브라우저 내에 포함된다. 또 다른 예에 따라, 애플리케이션(App)은 백그라운드에서 실행되는 프로세스에서 프록시로서 실행된다. 또 다른 예에 따라, 애플리케이션(App)은 세션 수립을 관리할 수 있는 API(Application Programming Interface)이다.

[0027] 일 변형예에서, 애플리케이션(App)은, 예를 들면, 블루투쓰 접속을 통해 통신 단말(TC)에 접속된 또 다른 디바이스에 포함된다.

[0028] 애플리케이션(App)은 분석 모듈(ANA) 및 세션 모듈(SES)을 포함한다.

[0029] 원격 통신 네트워크가 안전하지 않은 것으로 불리는 하나 이상의 액세스 네트워크들(RAns), 및 안전한 것으로 불리는 하나 이상의 액세스 네트워크들(RAs)을 포함할 수 있다는 것이 믿어진다. 안전하지 않은 것으로 불리는 액세스 네트워크는, 전송되는 데이터가 어떠한 기밀도 없고, 데이터가 데이터의 의도된 수신인인 아닌 엔티티에 의해 인터셉트될 수 있는 네트워크이다. 반대로, 액세스 네트워크가, 전송되는 데이터가 비밀을 갖고, 데이터가 데이터의 의도된 수신인인 아닌 엔티티에 의해 인터셉트될 수 없는 네트워크인 경우에, 액세스 네트워크는 안전한 것으로 불린다. 일반적으로 말하면, 네트워크는 또한 안전하지 않다는 평판을 가질 수 있는데, 그 평판은 잠재적으로 사용자 자신에 의해, 또는 예를 들면, 네트워크에 접속된 다수의 사용자들의 평가를 통한 애플리케이션에 의해, 또는 애플리케이션과 통신하는 방화벽(firewall)에 의해 정의된다.

[0030] 예를 들면, 하나의 안전하지 않은 액세스 네트워크는 WLAN의 단거리 공공 무선 네트워크 또는 802.1x 표준들 중 하나를 준수하는 무선 네트워크, 또는 WIMAX 프로토콜에 기초한 중거리 무선 네트워크이다. 안전하지 않은 액세스 네트워크는 또한, 임의의 보안 프로토콜을 구현하지 않거나 (가령, 스위치를 사용하여 통신들을 차단시킴으로써) 통신의 인터셉션을 지연시키고 이로써 인터셉션을 방지하는 하드웨어를 사용하는 이더넷 네트워크일 수 있다.

[0031] 예를 들면, 안전한 액세스 네트워크는 GSM 또는 UMTS 셀룰러 네트워크이다. 안전하지 않은 액세스 네트워크는 또한 보안 프로토콜을 구현하는 이더넷 네트워크일 수 있다.

[0032] 안전한 액세스 네트워크가 안전하지 않은 액세스 네트워크보다 더 적은 대역폭을 갖거나, 사용자가 안전한 액세스 네트워크를 통해 전송할 수 있는 데이터의 양이 더 적다는 것이 또한 가정된다. 큰 대역폭을 갖는 안전하지 않은 액세스 네트워크를 통해 이미 접속된 사용자는, 그 네트워크가 제한된 대역폭을 가질지라도 안전하지 않은 액세스 네트워크를 통해 개인 데이터를 전송할 수 있고, 주어진 서비스를 사용하기 위해 안전하지 않은 액세스 네트워크를 다시 더 빠르게 사용할 수 있다.

[0033] 사용자가 사적, 비밀, 또는 기밀 데이터인 개인 데이터를 전송하고 한다고 또한 가정된다. 예를 들면, 개인 데

이터는 로그인, 패스워드, 또는 사용자의 이름, 메일링 어드레스, e-메일 어드레스들 또는 전화 번호와 같은 사용자에 관한 접속 정보를 포함한다.

[0034] 애플리케이션의 분석 모듈(ANA)은 원격 통신 네트워크를 통해 통신 단말(TC)로부터 전송되고 전송될 데이터의 타입을 모니터링한다. 단말이 안전하지 않은 네트워크를 통해 애플리케이션 서버(SA)에 접속될 때, 분석 모듈(ANA)은, 웹사이트가 패스워드와 같은 민감한 데이터의 전송을 요구할 때마다 경보를 전송한다. 예를 들면, 분석 모듈(ANA)은 개인 데이터 입력 필드들을 검출하기 위해 현재 웹 페이지의 코드를 탐사할 수 있거나, 그것이 확인되기 전에, 사용자에 의한 개인 데이터의 입력을 실시간으로 검출할 수 있다. 또한, 사용자는 그 또는 그녀가 개인 데이터로 간주하는 데이터의 세트를 애플리케이션에 스스로 표시할 수 있다.

[0035] 분석 모듈(ANA)이 개인 데이터가 안전하지 않은 네트워크를 통해 막 전송되려고 한다는 것을 검출하여 경보를 전송할 때마다, 분석 모듈(ANA)은 세션 모듈(SES)이 접속을 안전한 네트워크로 스위칭하도록 트리거링한다.

[0036] 일 실시예에 따라, 웹페이지가 로그인을 입력하는 것에 관련된 필드와 같이 개인 데이터에 관련될 가능성이 있는 입력 필드들을 포함하지만, 사용자가 거짓된 로그인과 같이, 사용자에 의해 이전에 정의된 개인 데이터를 입력하지 않았다고 분석 모듈(ANA)이 통지하면, 분석 모듈(ANA)은 세션 모듈(SES)이 네트워크를 변경하도록 트리거링하지 않을 수 있다.

[0037] 세션 모듈(SES)은 어떠한 타입의 세션이 수립되어야 하는지, 및 어떠한 허가들이 세션에 대해 승인되는지를 표시하도록 사용자에 의해 구성될 수 있다. 이로써, 세션은 애플리케이션 서버에 의해 제공되는 서비스에 대한 다음의 제한들을 가질 수 있다.

[0038] - 읽기 전용(세션은 사용자의 프로파일을 변경할 수 없음),

[0039] - 업데이트 전용(예를 들면, 아직 읽지 않은 최근 이메일들만을 읽기 위해, 마지막 업데이트 이래로 서비스에 의해 공개된 정보만을 읽음),

[0040] - 짧은 세션 수명,

[0041] - IP 어드레스에 링크된 세션(통신 단말이 그 자신의 공공 IP 어드레스를 인지한다고 가정함),

[0042] - 서비스에 특정된 다른 제한들(예를 들면, 제한된 수의 위치 업데이트들).

[0043] 일 실시예에 따라, 세션 모듈(SES)은 웹 브라우저가 안전한 접속을 통해 전송되지 않는 세션 쿠키를 수용하는 것을 방지할 수 있다.

[0044] 그러한 제한들은 세션 모듈(SES)로부터의 요청 시에 애플리케이션 서버(SA)에 의해 서비스에 관련된 세션 쿠키 또는 접속 표시자에 정의된다. 그러면, 통신 단말(TC)은 안전한 접속을 통해 쿠키를 수신하고, 세션 모듈(SES)은 접속을 다시 안전하지 않은 네트워크로 스위칭할 수 있다. 브라우저의 관점에서, 쿠키가 통신 단말의 접속성에 의해 영향을 받지 않기 때문에, 어떠한 부가적인 동작들도 요구되지 않는다.

[0045] 그러한 제한들을 갖는 세션 쿠키는 또한, 통신 단말(TC)과의 다음 교환들이 안전하지 않은 접속을 통해 수행될 것이라는 것을 애플리케이션 서버(SA)에 통지하는 것을 가능하게 한다.

[0046] 도 2를 참조하면, 본 발명의 일 실시예에 따른 안전한 데이터 전송을 위한 방법은 통신 시스템 내에서 실행되는 단계들(E1 내지 E6)을 포함한다.

[0047] 예비 단계(E01)에서, 사용자는 통신 단말(TC) 내에서 구현되는 애플리케이션(App)에 의해 개인 데이터(DonP)의 세트를 선택적으로 정의한다.

[0048] 그러면, 사용자는 통신 단말(TC1)을 통해 애플리케이션 서버(SA)에 접속한다. 통신 단말(TC)은 웹 브라우저가 애플리케이션 서버(SA)의 식별자를 저장하는 것을 가능하게 하는, 접속 쿠키라 불리는 제 1 쿠키를 수신한다. 통신 단말(TC)이 안전하지 않은 액세스 네트워크(RAns)를 통해 애플리케이션 서버(SA)에 접속된다고 가정된다.

[0049] 단계(E1)에서, 애플리케이션(App)의 분석 모듈(ANA)은, 애플리케이션 서버에 의해 호스팅되는 웹페이지가 통신 단말의 웹 브라우저에 의해 액세스될 때마다, 사용자에 의해 입력되거나 원격 통신 네트워크를 통해 통신 단말(TC)로부터 애플리케이션 서버(SA)로 전송될 데이터를 제어한다. 애플리케이션(App)의 분석 모듈(ANA)은, 애플리케이션 서버에 의해 호스팅되고 단말의 웹 브라우저에 의해 액세스되는 웹 페이지의 입력 필드들을 부가적으로 체크하고, 입력 필드들은 개인 데이터를 사용하여 완성될 가능성이 있다. 단말이 안전하지 않은 액세스 네트워크를 통해 애플리케이션 서버(SA)에 접속되기 때문에, 분석 모듈(ANA)은 개인 데이터(DonP)가 사용자에 의해

입력되고 애플리케이션 서버로 전송될 가능성이 있을 때 경보를 전송한다. 이러한 이유로, 경보는 3 개의 경우들에서 전송될 수 있다.

[0050] - 일단 애플리케이션이 웹페이지를 액세스하면, 개인 데이터(DonP)가 사용자에 의해 입력될 가능성이 있지만 아직 입력되지 않을 때,

[0051] - 사용자가 개인 데이터(DonP)를 입력할 때, 또는 일단 사용자가 이와 같이 식별된 개인 데이터(DonP)를 입력하는 것을 마친 경우에,

[0052] - 사용자가 전송하기 위해 입력한 개인 데이터(DonP)를 확인하고, 개인 데이터(DonP)가 애플리케이션 서버로 막 전송되려고 할 때,

[0053] 단계(E2)에서, 세션 모듈(SES)은, 안전한 네트워크(RAs)가 존재하면, 애플리케이션 서버(SA)와의 접속을 안전하지 않은 액세스 네트워크(RAns)로부터 안전한 네트워크(RAs)로 스위칭한다. 이를 위해, 분석 모듈(ANA)은 다양한 이용 가능한 안전한 액세스 네트워크들을 식별하고, 예를 들면, 사용자 선호도들 및 액세스 네트워크의 기술적 특성들에 기초하여 미리 정의된 기준에 따라 그들 중 하나를 선택한다. 애플리케이션 서버(SA)와의 접속은 사용자에 대해 방해되지 않는데, 왜냐하면 웹 브라우저가 애플리케이션 서버(SA)와 통신하기 위해 제 1 쿠키, 즉, 접속 쿠키를 사용할 수 있기 때문이다.

[0054] 단계(E3)에서, 세션 모듈(SES)은 사용자가 통신 단말(TC) 및 애플리케이션 서버(SA) 사이에서 하나 이상의 후속 세션들에 대한 제한들을 정의하도록 유도한다. 그러한 제한들은 상기 후속 세션들에 대해 승인된 허가들을 나타낸다.

[0055] 그러한 제한들은 요청 시에 세션 모듈(SES)로부터 애플리케이션 서버(SA)로 전송되어, 애플리케이션 서버(SA)가 그러한 제한들을 고려한 접속 표시자 또는 세션 쿠키(Cs)를 생성할 수 있게 한다.

[0056] 일 실시예에 따라, 단계들(E2 및 E3)의 순서는 반전될 수 있다.

[0057] 단계(E4)에서, 애플리케이션(App)은 안전한 액세스 네트워크(RAs)를 통한 애플리케이션 서버(SA)로의 개인 데이터(DonP)의 전송을 인증하고, 세션 쿠키에 대한 제한들을 포함하는 요청(Req)을 전송한다.

[0058] 단계(E5)에서, 애플리케이션 서버(SA)는 개인 데이터(DonP) 및 요청(Req)을 수신한다. 서버(SA)는 수신된 요청(Req)에 포함된 정보에 기초하여 세션 쿠키(Cs)를 생성한다.

[0059] 단계(E6)에서, 애플리케이션 서버(SA)는 세션 쿠키(Cs)를 통신 단말(TC)로 전송한다.

[0060] 단계(E7)에서, 세션 모듈(SES)은 세션 쿠키(Cs)의 수신을 검출하고, 애플리케이션 서버(SA)와의 접속을 안전한 액세스 네트워크(RAs)로부터 안전하지 않은 액세스 네트워크(RAns)로 스위칭하고, 안전하지 않은 액세스 네트워크는 초기의 안전하지 않은 액세스 네트워크일 수 있다.

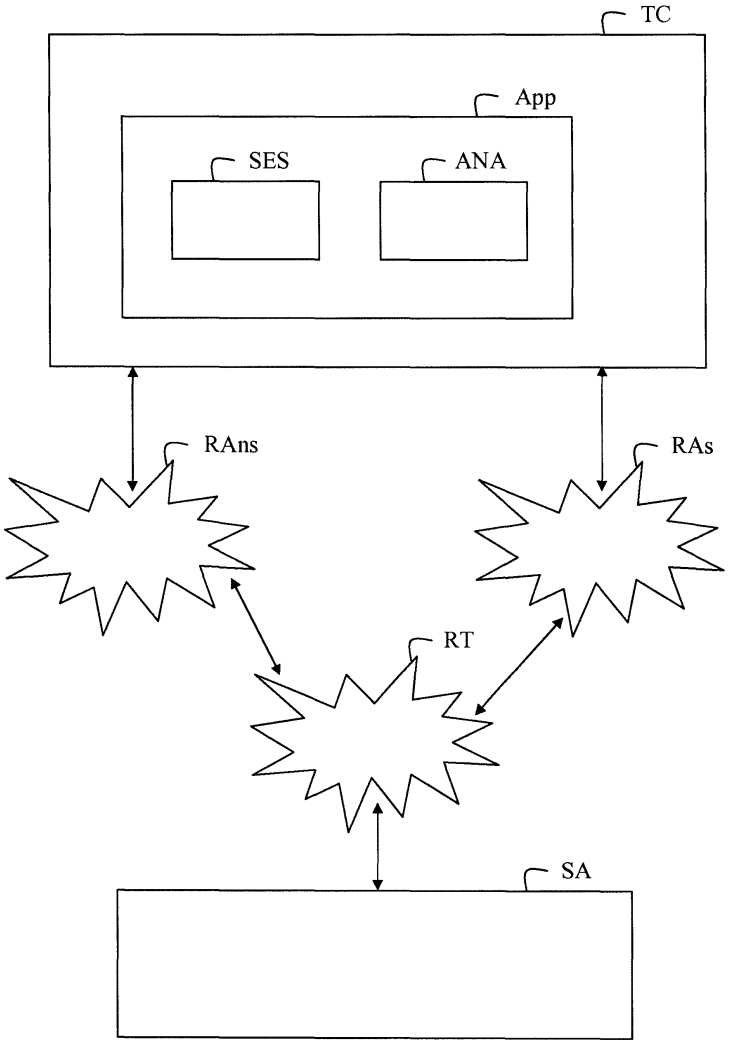
[0061] 단계들(E1 내지 E7)이 반복될 수 있다. 단계들의 제 1 반복 동안에, 개인 데이터(DonP)는 애플리케이션 서버(SA)에 의해 호스팅되는 웹사이트에서 사용자를 인증하는 것을 가능하게 하는 사용자 식별자 및 패스워드일 수 있다. 일단 인증되면, 애플리케이션(App)이 이름 또는 어드레스와 같은 사적 정보와 같이, 안전하지 않은 액세스 네트워크를 통해 전송될 가능성이 있는 개인 데이터를 여전히 모니터링하기 때문에, 사용자는 세션 쿠키에 포함된 허가들의 제한들 내에서 웹사이트와 상호 작용할 수 있다.

[0062] 여기에 기술된 본 발명은 안전한 데이터 전송을 위한 방법 및 단말에 관한 것이다. 본 발명의 일 실시예에 따라, 본 발명의 방법의 단계들은 통신 단말(TC)과 같은 단말에 통합된 컴퓨터 프로그램의 명령어들에 의해 결정되고, 프로그램은 애플리케이션(App)과 같은 적어도 하나의 소프트웨어 애플리케이션의 거동을 지시한다. 프로그램은, 상기 프로그램이 단말 내에서 로딩 및 실행될 때, 본 발명의 방법의 단계들을 수행하는 프로그램 명령어들을 포함한다.

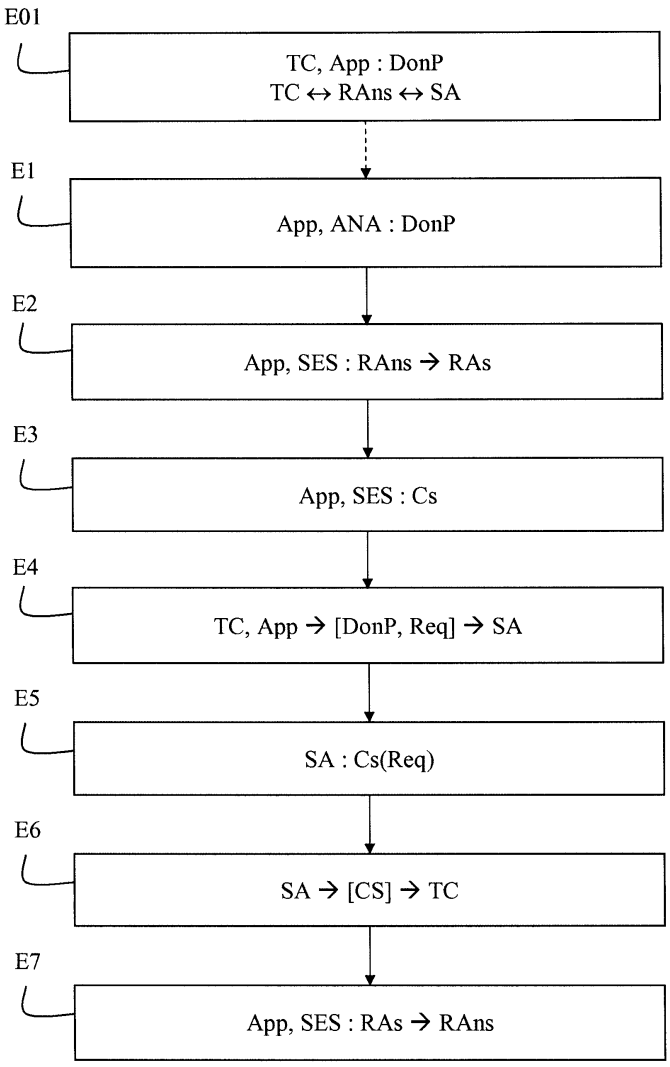
[0063] 결과적으로, 본 발명은 또한 컴퓨터 프로그램, 특히 본 발명을 구현하기에 적합한, 정보 매체 상의 또는 내의 컴퓨터 프로그램에 적용될 수 있다. 이러한 프로그램은 임의의 프로그래밍 언어를 사용하고, 소스 코드, 오브젝트 코드, 또는 소스 코드와 오브젝트 코드 사이의 중간 코드의 형태, 가령, 부분적으로 컴파일링된 형태, 또는 본 발명의 방법을 구현하기에 바람직한 임의의 다른 형태일 수 있다.

도면

도면1



도면2


E01
TC, App : DonP
TC ↔ RAns ↔ SA
E1
App, ANA : DonP
E2
App, SES : RAns → RAs
E3
App, SES : Cs
E4
TC, App → [DonP, Req] → SA
E5
SA : Cs(Req)
E6
SA → [CS] → TC
E7
App, SES : RAs → RAns