(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년02월09일
(11) 등록번호 10-1013268
(24) 등록일자 2011년01월28일

(51) Int. Cl.
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2006-7016526
(22) 출원일자(국제출원일자) 2005년03월01일
심사청구일자 2008년03월27일
(85) 번역문제출일자 2006년08월17일
(65) 공개번호 10-2007-0003862
(43) 공개일자 2007년01월05일
(86) 국제출원번호 PCT/EP2005/050895
(87) 국제공개번호 WO 2005/086452
국제공개일자 2005년09월15일
(30) 우선권주장
0405245.2 2004년03월09일 영국(GB)
(56) 선행기술조사문헌
EP01122930 A2*
EP00999673 A2
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
해랜, 리차드, 마이클, 웨인
영국, 사우스햄프톤 햄프셔 에스오15 2에이치제이, 2 윌튼애비뉴, 플랫 #3
호랜, 마이클
영국, 윈체스터 햄프셔 에스오22 4제이에이, 12 올리버스 배터리로드 노쓰
럼세이, 죠나단
영국, 윈체스터 햄프셔 에스오23 9디에이치, 트라팔가 스트리트,8웨스트게이트 하우스
(74) 대리인
신영무, 이용미

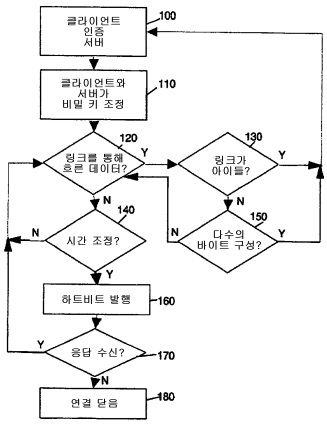
전체 청구항 수 : 총 10 항 심사관 : 유선중

(54) 키 기반 암호화

(57) 요 약

보안 데이터 통신을 촉진하기 위한 방법, 장치, 컴퓨터 프로그램 및 컴퓨터 프로그램 제품이 개시되고 있다. 보안 데이터 통신은 통신 링크를 통해 제1 및 제2 개체 사이에 흐르는 데이터를 암호화하기 위해 비밀 키를 이용해 실행된다. 먼저 통신 링크가 아이들 상태인 것이 결정된다. 이전의 아이들 통신 링크를 통해 흐른 데이터가 현재 있다고 결정되면, 새로운 비밀 키의 형성이 초기화된다. 이 새로운 비밀 키는 통신 링크를 통해 제1 및 제2 개체 사이에서 보내진 데이터를 암호화하기 위해 이용된다.

대 표 도 - 도1B



특허청구의 범위

청구항 1

프로세서와 메모리를 포함하는 제1 컴퓨팅 노드 및 제2 컴퓨팅 노드 사이의 통신 링크를 통해 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하는 보안 데이터 통신을 촉진하기 위한 방법에 있어서,

상기 통신 링크가 적어도 일정 시간 동안 아이들(idle)이었는지 결정하는 단계 -상기 통신 링크는 아이들과 비지(busy) 사이에서 변동하며, 아이들 통신 링크는 상기 적어도 일정 시간 동안 보안 데이터를 전송하지 않음-와,

상기 아이들 통신 링크를 통해 상기 제1 컴퓨팅 노드 및 상기 제2 컴퓨팅 노드 사이에서 흐를 보안 데이터가 존재하는지를 결정하는 단계와,

상기 통신 링크가 상기 적어도 일정 시간 동안 아이들이었으며, 상기 아이들 통신 링크를 통해 흐를 보안 데이터가 존재한다고 결정된 경우에만, 새로운 비밀 키를 생성하는 단계

를 포함하며,

상기 새로운 비밀 키는 상기 통신 링크를 통해 상기 제1 컴퓨팅 노드 및 상기 제2 컴퓨팅 노드 사이에서 보내지는 상기 보안 데이터를 암호화하는데 이용되는, 보안 데이터 통신 촉진 방법.

청구항 2

프로세서와 메모리를 포함하는 제1 컴퓨팅 노드 및 제2 컴퓨팅 노드 사이의 통신 링크를 통해 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하는 보안 데이터 통신을 촉진하기 위해 상기 제1 컴퓨팅 노드상에서 수행되는 방법에 있어서,

상기 방법은,

상기 통신 링크가 적어도 일정 시간 동안 아이들이었는지 결정하는 단계 -상기 통신 링크는 아이들과 비지 사이에서 변동하며, 아이들 통신 링크는 상기 적어도 일정 시간 동안 보안 데이터를 전송하지 않음- 와,

상기 아이들 통신 링크를 통해 상기 제1 컴퓨팅 노드 및 상기 제2 컴퓨팅 노드 사이에서 상기 보안 데이터가 흐를 수 있는지를 결정하는 단계와,

상기 통신 링크가 상기 적어도 일정 시간 동안 아이들이었다는 결정과 상기 보안 데이터가 흐를 수 있다는 결정에 응답하여, 상기 아이들 통신 링크를 통한 전송이 재개(recommence)되기 이전에 새로운 비밀 키를 생성하는 단계

를 포함하며,

상기 새로운 비밀 키는 상기 보안 데이터가 상기 통신 링크상에서 흐르기 이전에 상기 보안 데이터의 적어도 일부를 암호화하는데 이용되는, 보안 데이터 통신 촉진 방법.

청구항 3

제2항에 있어서,

가장 최근에 비밀 키가 생성된 이후부터 상기 통신 링크를 통해 보내진 상기 보안 데이터의 양이 임계치를 초과했는지 여부를 결정하는 단계와,

상기 보안 데이터의 양이 상기 임계치를 초과한 경우, 새로운 비밀 키의 생성을 시작하는 단계를 더 포함하는, 보안 데이터 통신 촉진 방법.

청구항 4

제2항에 있어서,

상기 통신 링크가 상기 적어도 일정 시간 동안 아이들이었으며 상기 통신 링크를 통해 흐를 수 있는 보안 데이터가 존재하지 않는 것으로 결정된 경우에만, 상기 제2 컴퓨팅 노드에 하트비트 메시지를 보내는 단계와,

상기 제2 컴퓨팅 노드로부터의 승인(acknowledgement)을 수신하기 위하여 상기 통신 링크를 모니터링하는 단계를 더 포함하는, 보안 데이터 통신 촉진 방법.

청구항 5

제4항에 있어서,

일정 시간 내에 상기 제2 컴퓨팅 노드로부터의 상기 승인이 수신되지 않는 경우, 상기 제2 컴퓨팅 노드와의 상기 통신 링크를 종료하는 단계를 더 포함하는, 보안 데이터 통신 촉진 방법.

청구항 6

통신 링크를 통해 장치와 원격 시스템 사이에 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하는 보안 데이터 통신을 촉진하는 장치에 있어서,

타이머를 이용하여 상기 통신 링크가 적어도 일정 시간 동안 아이들이었는지 여부를 결정하는 데이터 검출기 -상기 통신 링크는 아이들과 비지 사이에서 변동하며, 아이들 통신 링크는 상기 적어도 일정 시간 동안 보안 데이터를 전송하지 않으며, 상기 데이터 검출기는 상기 통신 링크를 통해 상기 원격 시스템으로 데이터가 흐를 수 있는지를 결정함- 와,

상기 통신 링크가 상기 적어도 일정 시간 동안 아이들이었다는 결정과 상기 보안 데이터가 상기 원격 시스템으로 흐를 수 있다는 결정에 응답하여, 새로운 비밀 키를 생성하는 키 생성 로직 -상기 새로운 비밀 키는 상기 보안 데이터가 상기 통신 링크상에서 흐르기 이전에 상기 보안 데이터의 적어도 일부를 암호화하는데 이용됨- 과,

가장 최근에 비밀 키가 생성된 이후부터 상기 통신 링크를 통해 보내진 상기 보안 데이터의 양이 임계치를 초과했는지 여부를 결정하는 바이트 측정기

를 포함하며,

상기 키 생성 로직은 상기 보안 데이터의 양이 상기 임계치를 초과한 경우, 새로운 비밀 키의 생성을 시작하는, 보안 데이터 통신 촉진 장치.

청구항 7

제6항에 있어서,

상기 통신 링크는 아이들이며 상기 통신 링크를 통해 상기 원격 시스템으로 흐를 수 있는 보안 데이터가 존재하지 않는 것으로 상기 데이터 검출기가 결정한 경우, 상기 원격 시스템으로 하트비트를 보내는 하트비트 발행기를 더 포함하는, 보안 데이터 통신 촉진 장치.

청구항 8

제7항에 있어서,

상기 하트비트에 대한 상기 원격 시스템으로부터의 승인을 위하여 상기 통신 링크를 모니터링하는 검출기를 더 포함하는, 보안 데이터 통신 촉진 장치.

청구항 9

제8항에 있어서,

상기 검출기가 일정 시간 내에 상기 원격 시스템으로부터의 상기 승인을 검출하는데 실패한 경우, 상기 통신 링크를 종료하기 위한 연결 종료기를 더 포함하는, 보안 데이터 통신 촉진 장치.

청구항 10

통신 링크를 통해 컴퓨터와 원격 시스템 사이에 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하는 보안 데이터 통신을 촉진시키는 프로그램 명령어들을 포함하는 컴퓨터 판독가능 매체에 있어서,

상기 프로그램 명령어들은,

상기 통신 링크가 적어도 일정 시간 동안 아이들이었는지 결정하는 단계 -상기 통신 링크는 아이들과 비지 사이

에서 변동하며, 아이들 통신 링크는 상기 적어도 일정 시간 동안 보안 데이터 통신 트래픽을 갖지 않음- 와,

상기 통신 링크가 상기 적어도 일정 시간 동안 아이들이었다는 결정 및 상기 통신 링크를 통해 흐를 수 있는 보안 데이터가 존재하지 않는 것으로 결정된 경우에만 상기 원격 시스템으로 하트비트 메시지를 보내는 단계와,

상기 원격 시스템으로부터의 승인을 수신하기 위하여 상기 통신 링크를 모니터링하는 단계와,

일정 시간 내에 상기 원격 시스템으로부터 상기 승인을 수신하는 단계와,

상기 아이들 통신 링크를 통해 상기 컴퓨터로부터 상기 원격 시스템으로 보안 데이터가 흐를 수 있는지를 결정하는 단계와,

상기 아이들 통신 링크를 거쳐 흐르는 하트비트를 검출하는 단계와,

상기 아이들 통신 링크를 통해 보안 데이터가 흐를 수 있으며, 상기 아이들 통신 링크를 거쳐 흐르는 상기 하트비트를 검출하고, 일정 시간 내에 상기 원격 시스템으로부터 상기 승인을 수신하는 경우에만 새로운 비밀 키를 생성하는 단계

를 포함하며,

상기 보안 데이터가 상기 아이들 통신 링크를 통해 흐를 수 있는 경우에만 상기 새로운 비밀 키를 생성하는 것이 발생하도록, 상기 새로운 비밀 키는 상기 보안 데이터가 상기 통신 링크상에서 흐르기 이전에 상기 보안 데이터의 적어도 일부를 암호화하는데 이용되는, 컴퓨터 판독가능 매체.

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 암호화에 관한 것으로, 더욱 특히는 암호화에 이용되는 키의 재조정에 관한 것이다.

배 경 기 술

[0002] 개인이나 사업체는 각종 데이터를 전송 및 수신하기 위해 컴퓨터를 이용한다. 이런 데이터의 합당한 비율은 민감하기 쉬으므로 데이터 비밀 보장은 중요한 사안이 되고 있다.

[0003] 데이터 비밀을 성취하는 데에 있어 한가지 대중적인 방법은 암호화 알고리즘을 이용하는 것이 있다. 이런 알고리즘은 보통 키 기반이며 대칭이나 비대칭으로 분류된다.

[0004] 대칭 암호화 알고리즘은 문제의 데이터의 송신기와 수신기에게만 알려진 비밀 키를 이용한다. 동일한 비밀 키는 수신기에 의해 수신될 때 데이터를 해독하는 데에 이용되는 바와 같이 송신기에서 데이터를 암호화하는 데에 이용된다.

[0005] 한편 비대칭 암호화 알고리즘은 공중 키와 비밀 키를 둘 다 이용한다. 공중키는 누구에게나 알려질 수 있는 반면 비밀 키는 제한된 존재에게만 알려지는 것이다. 하나의 키가 데이터를 암호화는 데에 이용되는 반면, 다른 키는 데이터의 해독을 가능하게 해준다.

[0006] 보안 소켓 레이어 (SSL)는 인터넷을 통해 보안 데이터 전송을 성취하기 위한 프로토콜이다. SSL은 비대칭과 대칭 암호화 기술 둘 다를 이용한다.

[0007] 한 쌍의 비대칭 키가 두 당사자 (예를 들어, 앨리스와 밥) 간의 초기 인증 핸드세이크에 이용되게 된다. 다음 예에서, 앨리스는 밥을 인증하길 원한다 (물론 밥은 또한 앨리스를 인증하길 원하고 - 이것이 바람직함). 밥은 공중-비밀 키 쌍을 갖는다. 밥의 공중 키가 앨리스에게 노출된다. 앨리스는 밥에게 메시지를 보내고 이때 밥은 그의 비밀 키로 암호화하여 앨리스에게 다시 보낸다. 앨리스는 밥이 전에 그녀에게 노출했던 공중 키를 이용하여 밥으로부터의 메시지를 해독한다. 이 해독된 메시지가 앨리스가 처음에 밥에게 보냈던 메시지와 일치하면, 앨리스는 밥이 그라는 것을 추측할 수 있다. 그러나 SSL은 또한 제 삼자가 앨리스의 원본 메시지를 취득하여 앨리스인척 하는 것을 방지하기 위해 디지털 신호를 이용한다. SSL은 또한 인증을 이용한다. 인증은 공중 키가 실제로 예를 들어, 밥으로부터 온 것임을 증명하는 데에 이용된다.

[0008] 밥을 인증하게 되면, 앨리스는 밥과 데이터를 교환할 준비가 된 것이다. 그러나 데이터 교환이 발생하기 전에, 앨리스와 밥이 대칭 (비밀) 키에 동의해야 한다. 교환될 데이터는 이 비밀 키로 먼저 암호화된다. 두 당사자가 비밀 키에 대해 동의한 이후에, 앨리스는 키를 이용하여 그녀의 데이터를 암호화하고 밥은 앨리스로부터 수신한 데이터를 해독할 수 있다.

[0009] 비밀 키가 비인가된 제 삼자에 의해 드러나게 된다면, 이것은 데이터를 해독하고 거짓 메시지를 암호화하고/데이터를 변경하는 데에 이용될 수 있다는 것이 이해될 것이다.

[0010] 이런 이유로 데이터를 교환하는 데에 앨리스 (클라이언트)와 밥 (서버)에 의해 이용되는 SSL 비밀 키를 주기적으로 재조정하는 것이 바람직하다. 비밀 키의 재조정은 클라이언트와 서버 둘다에 대해 CPU 집약적인 핸드세이크를 실행하는 것과 관련된다. 이것은 각 재조정이 비대칭 인가에 이어 대칭 비밀 키의 조정과 관련되면 특히 프로세서 집약적이다.

[0011] SSL의 상세한 개요는 http://developer.netscape.com/tech/security/ssl/howitworks.html에서 찾아볼 수 있다.

[0012] 현재의 해결책

[0013] 현재의 비밀 키 재조정 구현은 일반적으로 두 가지 방법 중 하나를 이용한다:

[0014] (ⅰ) 매 x 분마다 SSL 클라이언트에 의해 재조정이 개시되게 하는 정해진 시간의 리세트 (예를 들어, 웹 브라우저는 매 2분 마다 키 재조정을 개시할 수 있다); 또는

[0015] (ⅱ) 일정한 임계 바이트가 흐른 후에 개시.

[0016] 그러나 이들 해결책은 이런 환경에서 통신 링크가 통상 아이들과 비지 상태 사이에서 진동하기 때문에 메시징 환경에서는 효율적으로 작동하지 않는다. 상술한 해결책은 특히 통신 링크가 변동하는 시간에 아이들 또는 비지 상태인 경우 효율적이지 못하다 (메시징 환경에서 그런 것처럼).

[0017] 현재 해결책에서의 문제점

[0018] (ⅰ) 정해진 시간의 재조정 - 아이들 통신 링크

[0019] 데이터 (메시지)가 연장된 기간 동안 통신 링크를 통해 보내지지 않았을 때 불필요한 다수의 인증과 재조정이 있을 수 있다. 다시 말해, 클라이언트는 쓸데 없이 통신하길 원하는 서버를 인증한 다음에 그 서버와 비밀 키를 재조정할 수 있다. 따라서 성능이 불필요하게 떨어지게 된다.

[0020] (ⅱ) 바이트 임계 구현 - 아이들 통신 링크

[0021] 이 해결책은 비밀 키가 아이들 링크에 대해 유효한 기간을 늘리어 해커에게 비밀 키를 침투하고 '거짓' 메시지를 검출 없이 보내는 시간을 더 주게 된다.

[0022] (ⅲ) 정해진 시간의 재조정 - 비지 통신 링크

[0023] 비지 통신 링크는 동일한 비밀 키로 암호화된 대량의 데이터가 흐르게 된다. 해커가 정해진 시간의 재조정에 보통 이용되는 시간 동안 키를 차단할 가능성은 없지만, 문제는 그가 암호화된 데이터를 기록한 다음에 이를 여가 시간에 분석하게 된다는 것이다. 이것은 해커에게는 대량의 데이터가 동일한 비밀 키로 암호화되어 있는 경우 더 쉬우므로 대량의 데이터의 보안성은 통신 링크가 비지 상태일 때 이 해결책을 이용하여 해결될 수 있다.

[0024] (ⅳ) 바이트 임계 구현 - 비지 통신 링크

[0025] 비지 통신 링크 상에서 동일한 비밀 키로 암호화된 데이터 양은 최소화될 것이다. 따라서 이 해결책은 하나의 비밀 키로 암호화된 데이터 양을 최소화한다. 그러나 이 해결책은 링크가 주로 아이들 상태일 때는 양호하지 않다.

[0026] 따라서 비지와 아이들 상태 사이에서 진동하는 환경에서의 암호화는 이제까지 문제가 되고 있다

발명의 상세한 설명

[0027] 일 형태에 따르면, 통신 링크를 통해 제1 및 제2 개체 사이에서 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하여 보안 데이터 통신을 촉진하기 위한 방법을 제공하고 있으며, 이 방법은: 상기 통신 링크가 아이들 상태라고 결정하는 단계; 이전의 아이들 통신 링크를 통해 흐른 데이터가 있다고 결정하는 단계; 및 이전의 아이들 통신 링크를 통해 흐르는 데이터가 있다고 결정한 것에 응답하여, 새로운 비밀 키의 형성을 개시하는 단계를 포함하고, 상기 새로운 비밀 키는 통신 링크를 통해 제1 및 제2 개체 사이에서 보내진 데이터를 암호화하기 위한 것이다.

[0028] 이 방법에서, 키 형성은 아이들 통신 링크를 통한 전송이 다시 시작하려고 할 때만 발생하게 된다. 이는 키 형성이 시간에 기초하여 발생하는 종래의 기술과는 대조적이다.

[0029] 바람직하게, 미리 구성된 데이터 양이 상기 통신 링크를 통해 보내질 때를 결정할 수 있다. 미리 구성된 데이터 양이 상기 통신 링크를 통해 보내졌다고 결정하게 되면, 새로운 비밀 키의 형성이 개시된다.

[0030] 이는 통신 링크가 주로 아이들 상태가 아닌 상황의 요구를 채워준다. 따라서 비지 링크 상에서도, 키 형성은 자주 가능한 간격으로 발생한다.

[0031] 일 실시예에서, 통신 링크는 링크를 통해 흐른 데이터가 현재 있다고 결정한 결과 새로운 비밀 키의 형성이 개시되기 전에 적어도 미리 정해진 시간 동안 아이들 상태이어야 한다.

[0032] 이런 식으로, 단 주기의 아이들 상태는 즉시 새로운 비밀 키를 형성하기 위한 프로세스가 개시된다.

[0033] 링크가 적어도 x 초 동안 아이들 상태이고 현재 흐른 데이터가 있는 경우에 새로운 비밀 키가 형성되어야 하는

간단한 타임아웃 시스템이 이용되는 점에 유의해야 한다.

[0034] 바람직한 실시예에서, 통신 링크가 미리 정해진 주기 동안 아이들 상태라고 결정되면, 제1 개체가 하트비트를 통해 여전히 존재한다는 것을 제2 개체에게 알린다.

[0035] 이런 식으로, 제2 개체는 제1 개체가 현재 통신 링크를 통해 흐른 데이터를 갖고 있지 않아도 여전히 살아 있다는 것을 알게 된다. 제1 개체는 제2 개체에게 하나 이상의 하트비트를 보낼 수 있다는 점에 유의해야 한다(즉, 링크가 장기간 아이들인 경우).

[0036] 제2 개체는 제1 개체로부터의 하트비트 수신을 확인한다.

[0037] 일 실시예에서, 미리 정해진 시간 내에 하트비트의 수신 확인이 제1 개체에 의해 수신되지 않으면, 제1 개체에 의한 제2 개체와의 통신은 종료된다. 이것은 제2 개체에 이상이 있거나, 제3자가 하트비트를 소모하고 있거나 하트비트에 응답하기 때문이다.

[0038] 다른 실시예에서, 하트비트의 수신 확인이 미리 정해진 시간 내에 제1 개체에 의해 수신되지 않으면, 새로운 비밀 키의 형성은 제1 개체에 의해 제2 개체로 데이터가 전송되는 것을 허용하기 이전에 개시된다. 물론, 프로세스가 또한 인증을 포함하고 있지 않는 한, 제3자는 제2 개체인 척 하여 키 형성 프로세스에 연루될 수 있다.

[0039] 바람직한 실시예에서, 통신 링크가 제1 개체로 하여금 제2 개체에게 하트비트를 보낼 정도로 충분히 아이들 상태라고 결정할 수 있다. 바람직하게, 링크가 제1 개체로 하여금 제2 개체에게 하트비트를 보낼 정도로 충분히 아이들 상태라고 결정한 것에 응답하여, 새로운 비밀 키의 형성이 개시된다.

[0040] 바람직한 실시예에서, 적어도 제2 개체의 인증은 새로운 비밀 키의 형성 이전에 개시된다.

[0041] 새로운 비밀 키의 형성은 제1 및 제2 개체 사이에서 실행되는 조정 프로세스의 결과인 것이 바람직하다.

[0042] 다른 형태에 따르면, 통신 링크를 통해 상기 제1 및 상기 제2 개체 사이에 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하여 보안 데이터 통신을 촉진하기 위한 방법을 제공하고 있으며, 이 방법은 통신 링크가 아이들 상태라고 결정하는 단계; 및 통신 링크가 아이들 상태라고 결정한 것에 응답하여, 상기 비밀 키로 암호화된 데이터를 무시하는 단계를 포함한다.

[0043] 바람직하게 새로 형성된 비밀 키로 암호화된 후속 데이터만이 수용된다.

[0044] 바람직하게 통신 링크는 미리 정해진 시간 동안 아이들 상태이어야 한다. 바람직하게 이는 제1 개체로부터의 하트비트 수신을 통해 나타나게 된다.

[0045] 일 실시예에 따르면, 통신 링크가 미리 정해진 시간 동안 아이들 상태이고 하트비트가 제1 개체로부터 수신되지 않았다고 결정될 때, 제1 개체와의 통신이 종료된다.

[0046] 이는 제1 개체에 이상이 있거나 제3자가 하트비트를 소모하고 있기 때문이라고 가정된다.

[0047] 다른 실시예에서, 통신 링크가 적어도 미리 정해진 시간 동안 아이들 상태이고 하트비트가 제1 개체로부터 수신되지 않았다고 결정한 것에 응답하여, 새로 형성된 비밀 키로 암호화된 후속 데이터만을 수용한다.

[0048] 다른 형태에 따르면, 통신 링크를 통해 제1 개체와 제2 개체 간에 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하여 보안 데이터 통신을 촉진하기 위한 장치를 제공하고 있으며, 이 장치는: 통신 링크가 아이들 상태라고 결정하기 위한 수단; 이전의 아이들 통신 링크를 통해 흐른 데이터가 있다고 결정하기 위한 수단; 및 이전의 아이들 통신 링크를 통해 흐른 데이터가 있다고 결정한 것에 응답하여, 새로운 비밀 키의 형성을 개시하기 위한 수단을 포함하고, 새로운 비밀 키는 상기 통신 링크를 통해 상기 제1 및 제2 개체 간에 보내지는 데이터를 암호화하기 위한 것이다.

[0049] 다른 형태에 따르면, 통신 링크를 통해 상기 제1 및 상기 제2 개체 사이에 흐르는 데이터를 암호화하기 위한 비밀 키를 이용하여 보안 데이터 통신을 촉진하기 위한 장치를 제공하고 있으며, 이 장치는: 통신 링크가 아이들 상태라고 결정하기 위한 수단; 및 통신 링크가 아이들 상태인 것을 결정한 것에 응답하여, 비밀 키로 암호화된 데이터를 무시하기 위한 수단을 포함한다.

[0050] 바람직하게, 비밀 키로 암호화된 데이터는 데이터의 무결성을 신뢰하게 안전하게 생각되지 않는다는 관점에서 무시된다. 따라서 새로 형성된 비밀 키로 암호화된 데이터만이 신뢰할 만한 것으로 생각된다.

[0051] 본 발명은 컴퓨터 소프트웨어로 구현될 수 있다는 것이 이해될 것이다.

실 시 예

[0055] 본 발명의 바람직한 실시예는 도 1a 및 1b를 참조하여 이하 설명된다. 두 도면은 서로에 관련하여 이해되어야 한다.

[0056] SSL 클라이언트(5)는 데이터를 SSL 서버(6)에 전송하길 원한다. 먼저 SSL 클라이언트는 연결 초기화기(55)를 이용하여 통신 링크(90)를 통해 서버와의 연결을 개시한다. 클라이언트(5)는 서버 상에서 등가의 구성 요소(10')와 통신하는 인증기(10)를 이용하여 서버(6)를 인증한다 (단계 100).

[0057] 서버(6)를 인증하게 되면, 클라이언트와 서버는 키 조정기 구성 요소(20, 20')에 의해 대칭 비밀 키를 조정한다 (단계 110). 이 비밀 키는 이어서 클라이언트가 통신 링크(90)를 통해 흐르게 하는 메시지를 암호화 및 해독하는 데에 이용되게 된다.

[0058] 클라이언트 상에서의 데이터 검출기(70)는 클라이언트(5)가 통신 링크(90)를 통해 흐르는 데이터를 가지고 있는지를 검출하도록 작동한다 (단계 120). 링크를 통해 흐르는 데이터가 있다면, 단계 130에서 링크는 이전에 클라이언트가 서버로 하트비트를 보낼 정도로 충분히 아이들 상태인지가 검출된다 (후에 참조).

[0059] 그 경우가 아니라고 가정하면 이 데이터는 현재 비밀 키로 암호화되어 보내진다 (도시 생략). 바이트 측정기(40)에 의해 미리 구성된 다수의 바이트가 보내졌는지가 결정된다 (단계 150). 응답이 아니오라면, 프로세스 루프는 단계 120로 돌아가 또 다른 데이터가 흐르는지의 여부를 판단한다.

[0060] 미리 구성된 다수의 바이트가 보내지면 (바이트 측정기(40)로 검출된 바와 같이), 이 때가 구성 요소 (10, 10', 20, 20')를 이용하여 키를 재인증하고 재조정할 때이다 (단계 100, 110). 이 시점에서 바이트 측정기(40)에 의해 값이 고정되어 보내진 다수의 바이트가 제로로 리세트된다.

[0061] 재구성 가능한 바이트 임계는 바이트 임계가 만족된 결과 비밀 키가 정규적으로 재조정되게 되기 때문에 동일한 비밀 키로 비지 통신 리크상에서 보내진 데이터 양이 제한되는 것을 보장한다.

[0062] 적당한 바이트 임계의 세팅은 트레이드-오프란 점에 유의해야 한다:

[0063] 임계를 낮출수록, 재조정은 자주 실행되고 비밀 키도 자주 변경되게 되므로 - 더 많은 처리력도 요구되게 된다. 그러나 자주 재조정이 실행되고 비밀 키가 변경되면, 통신 링크를 통해 흐르는 데이터는 더욱 보안적이 된다;

[0064] 임계를 높일수록, 성능은 더욱 좋아진다 (재조정과 비밀키 재조정을 덜 하게 되므로). 물론 통신 링크를 통해 흐르는 데이터는 임계가 낮은 환경에서 보다 덜 보안적이 된다.

[0065] 타이머(30)는 데이터 검출기 구성 요소(70)에 의해 이용되어 통신 링크(90)가 재구성 가능한 주기 동안 아이들 상태일 때를 결정한다. 그런 경우라면, 특수 "하트비트" 메시지를 (하트비트 발행기(50)를 통해) 발하여 SSL 서버(6)에게 여전히 존재한다는 것을 확인시켜 준다 (단계 160). (타이머는 제로로 리세트되고 - 타이머는 또한 재인증이 개시될 때 제로로 세트되는 것이 바람직하다는 것에 유의해야 한다). 클라이언트는 서버 (하트비트 수신기(75), 하트비트 응답 형성기(80))로부터 하트비트에 대한 응답을 대기한다 (단계 170) - 나중 참조.

[0066] 재구성 가능한 주기는 너무 짧지 않은 게 바람직한데 (예를 들어, 10초), 왜냐하면 이것은 수많은 하트비트를 초래할 수 있기 때문이다 (즉, 불필요한 트래픽이 너무 많아짐). 선택된 시간은 환경에 좌우되며 - 예를 들어 5분의 주기가 적당할 수 있다.

[0067] SSL 서버는 하나 이상의 '하트비트' 메시지를 수신한 후에 동일한 비밀 키로 암호화된 어플리케이션 데이터를 포함하는 다른 메시지를 '거짓'으로 거절하게 된다 (데이터 거절기 구성 요소(95)). 거짓 데이터의 검출시 이것을 관리기로 로깅하거나 클라이언트와의 연결을 닫는 등의 적당한 동작이 취해져야 한다.

[0068] SSL 클라이언트가 (통신 링크가 이전에 아이들 상태인 것을 나타내는 하트비트를 수신한) SSL 서버에게 새로운 메시지를 보내기 위해서 먼저 메시지를 보내기 전에 새로운 비밀 키를 재조정하여 SSL 서버가 이를 '거짓'으로 거절하는 것을 막아야 한다 (단계 120, 130, 100 및 110). 따라서 일정 주기의 아이들 상태 후에 비밀 노출이 없어야 한다.

[0069] 상술된 바와 같이, 일정 주기의 아이들 이후 보내진 거짓 데이터는 서버가 클라이언트와의 연결을 종료하게 하는 것이 바람직하다. 다음에 클라이언트는 서버와의 연결 재시작을 선택할 수 있으며 서버에 더 많은 데이터

를 보내기 이전에 재인가 및 재조정해야 한다.

[0070] 하트비트가 유용한 데이터를 포함하지 않기 때문에, 이들은 암호화될 필요가 없다.

[0071] SSL 서버가 링크가 재구성 가능한 주기 (즉, 클라이언트(5)에 의해 이용되는 것과 동일한 주기) 보다 더 오래 동안 아이들 상태라고 (데이터 검출기 구성 요소(70') 및 타이머 구성 요소(30')를 통해) 검출할 때 '하트비트'를 수신하지 않으면, SSL 서버는 연결 종료기(85)를 통해 연결 상태를 끝낸다. 이것은 비밀 키 재조정을 방지하기 위해 해커가 '하트비트' 메시지를 소모하지 않도록 하여 비밀키 수명을 연장시킨다.

[0072] 거짓 하트비트는 어떤 어플리케이션 데이터와도 타협하지 않기 때문에 이를 검출할 필요가 없다는 점에 유의해야 한다.

[0073] SSL 서버(6)가 존재하여 클라이언트로부터 하트비트를 수신하면 서버는 특수 '하트비트' 메시지에 응답하여 하트비트가 통신 링크를 통해 흐를 정도로 충분히 긴 동안 아이들 상태라는 것을 기억한다. SSL 클라이언트는 여전히 존재한다는 것을 확인하기 위해 임의 수의 '하트비트' 메시지를 보낼 수 있다.

[0074] '하트비트' 메시지는 비밀 키가 바이트 임계로 트리거되어야 할 때를 연산하는 데에 이용되는 총 바이트에 기여하지 않은다는 것에 유의해야 한다.

[0075] 클라이언트가 서버로부터 응답을 수신하면, 도 1b의 프로세스는 단계 120으로 돌아간다. 링크를 통해 데이터가 흐르고 있다고 결정되면, 단계 130에서 링크가 하트비트의 형성을 초래할 정도로 충분히 아이들 상태인지가 테스트된다. 응답이 예이면, 비밀 키는 재조정되어야 한다. 따라서 클라이언트는 재조정과 키 조정이 이루어질 때 까지 서버에 더 이상의 데이터를 보내지 않을 것이다.

[0076] 이것은 해커가 통신 링크가 아이들 상태인 연장된 기간으로 인해 비밀 키를 억지로 파손한 경우에도, 그 키는 이제 이들에게 쓸모가 없다.

[0077] 응답이 수신되지 않았다면 클라이언트는 연결 종료기(55)를 이용하여 연결을 닫는다 (단계 180). 왜냐하면 응답의 실패는 서버가 더이상 존재하지 않거나 누군가 서버의 응답을 소모하고 있다는 것을 나타내기 때문이다.

[0078] 다른 실시예로, 클라이언트는 연결을 종료하기 전에 서버에 추가 회수 접촉을 시도할 수 있다. 이것은 서버로부터의 응답 결여가 단지 일시적인 문제일 수 있기 때문이다. 안전 측에 있기 위해서, 재인증/키 조정이 개시될 수 있다.

[0079] (하나 이상이 아이들 링크 상에서 보내질 때) 하트비트 간의 타이밍은 일정한 것이 바람직하다. 임의의 타이밍이 각 하트비트 메시지 간에 이용되는 경우, 하트비트가 과도 (해커에 의해 소모될 가능성이 꽤 됨) 할 때를 예측하기가 불가능한다.

[0080] 물론 하트비트가 먼저 보내지기 전의 시간 및 (및 하트비트 간의 간격) 바이트플로우 계수는 동일한 비밀키가 연장된 기간 동안 계속해서 이용되지 않도록 선택되는 것이 바람직하다는 것이 이해될 것이다. 이 선택된 값이 해커에게 비밀 키를 캡쳐하여 발견해 낼 시간을 제공할 정도로 충분히 크다면 '거짓' 메시지는 여전히 취득 가능할 수 있다는 점에 유의해야 한다. 그러나 하트비트 트리거된 비밀 키 재조정이 발생하게 되면, 해커는 서버를 더 이상 속일 수가 없게 될 것이다. 이런 이유로, 데이터 송신측이 새로운 키의 조정을 개시하는 것이 바람직하다. 그렇지 않으면, 서버가 정확히 암호화된 거짓 메시지를 수신하고 있으면, 서버의 시점에서는 재조정이 필요하지 않다.

[0081] 이제까지 기재한 해결책을 이용하게 되면 다음 네 가지 주요한 장점이 있게 된다:

[0082] (ⅰ) 이 제안은 비밀 키의 재인증 및 재조정이 보안을 유지하면서 최적의 성능을 성취하도록 아이들 통신 링크 상에서 절대적으로 필요할 때에만 발해지는 것을 확실히 한다.

[0083] (ⅱ) 정확한 비밀 키로 암호화된 경우에도 '거짓' 메시지를 검출하는 능력이 '하트비트' 메시지의 이용으로 제공된다 - 비밀 키는 데이터 통신이 재개될 때 재조정되기 때문이다.

[0084] (ⅲ) 이 제안은 비밀 키가 타협된 비밀 키로 해커에 의해 판독될 수 있는 어플리케이션 데이터 양을 제한하도록 비지 통신 링크 상에서 정규적으로 변경되는 것을 확실히 한다.

[0085] (ⅳ) 특수 '하트비트' 메시지는 어플리케이션 데이터를 포함하고 있지 않으므로 데이터를 암호화 및 해독하는 데에 이용되는 비밀 키가 폭력적으로 발견되는 경우에도 해커에게 쓸모 없어진다.

[0086] 이 프로토콜은 인증 및 키 조정이 항상 하나 이상의 하트비트가 링크를 통해 흐를 정도로 충분히 긴 기간 동안

통신 링크가 아이들 상태였던 후에 그리고 특정한 수의 바이트가 통신 링크를 통해 흐를 때 실행되는 것을 확실히 한다.

[0087] '거짓' 메시지를 보낸 해커는 현재 합의된 비밀 키를 발견해 낸 경우에도 (클라이언트의) 재인증 및 키 재조정을 개시하기 위한 비대칭 비밀 키를 소유하고 있지 않기 (또한 재인증을 위한 인증서를 가지고 있지 않기) 때문에 합의된 프로토콜을 따를 수 없다. 또한 구 대칭 비밀 키는 서버가 클라이언트로부터 하트비트를 보는 순간부터 무효가 된다.

[0088] 이 해결책은 재인증, 키 조정을 불필요하게 실행할 필요 없이 아이들 통신 링크 상에서 해커가 '거짓' 메시지를 보내는 것을 효과적으로 방지한다. 이 해결책은 또한 비지 통신 링크에 대처한다.

[0089] SSL 클라이언트가 성공적인 재인증이 발생하게 하기 위해서 SSL 서버에 인증 정보를 제시할 필요가 없도록 SSL를 구성하는 것이 가능하다 - 이 경우 서버는 클라이언트에게 인증되고, 반대의 경우는 아니다. 그러나, 이것은 제 삼자가 클라이언트인 척하여 서버와 통신하는 것을 가능하게 하기 때문에, 보안 피어-투-피어 환경에서는 적당하지가 않다.

[0090] 본 발명이 특히 메시징 환경에 적용 가능한 것으로 기재되고 있지만, 이에만 제한되는 것은 아님에 유의해야 한다. 본 발명은 아이들과 비지 상태 주기 사이에 진동하는 환경에도 적용 가능하다.

[0091] 또한, 본 발명은 SSL 암호화 프로토콜에 있어서 기재되었지만, 또한 이에만 제한하는 것은 아니다. 본 발명은 인증 및 키 조정이 프로세서 집약적인 환경에 특히 적용 가능하다. 다른 예로 TLS가 있다.

[0092] 예시의 실시예에서, 데이터는 클라이언트로부터 서버에 흐르고 있다. 이는 꼭 그럴 필요는 없고 - 반대의 방향으로도 흐를 수 있다. 데이터를 보내고 있는 누구라도 인증과 키 조정을 개시하고 또한 하트비트를 보내는 것이 바람직하다.

[0093] 다른 실시예에서는, 인증과 키 재조정은 항상 SSL 클라이언트에 의해 개시된다. 따라서 SSL 서버가 보낼 데이터를 가지고 있는 경우, 서버는 SSL 클라이언트에게 먼저 인증 및 재조정하길 요청한다. 반대도 또한 그렇다.

[0094] 바람직한 실시예가 각 경우 초기 풀 핸드세이크 (비대칭 인증)를 다음에 비밀 키의 조정을 실행한다는 관점에서 기재되고 있지만, 이는 반드시 그런 것은 아니다. 본 발명은 인증에 이어 키 조정이 특히 프로세서 집약적이기 때문에 이 경우에 특히 적용 가능한 것이다. 그러나 본 발명은 또한 세션 캐싱 (덜 프로세서 집약적)을 이용하는 환경에도 또한 적용 가능하다. 이는 예를 들어, SSL v3.0 및 TLS에서 이용 가능한 특성이다.

[0095] 세션 캐싱이 초기 핸드세이크 동안 실행될 수 있다. 클라이언트 및 서버는 공통의 세션 ID, 마스터 비밀 키 및 약간의 인증 체인을 세이브한다. 이 정보는 보통 구성 가능한 주기 동안 캐시에 유지된다.

[0096] 후속의 핸드세이크가 요청되고 (즉, 클라이언트가 새로운 비밀 키를 요청할 때) 이 정보가 캐시로부터 만료되지 않은 경우, 양 측은 서로 그들의 세션 ID를 제시한다. 세션 ID가 일치하면 캐시된 정보는 핸드세이크 동안 실행되는 처리를 감소하게 이용되게 되고 - 이는 풀 핸드세이크와 반대로 보통 축약 핸드세이크로 불린다.

[0097] 세션 캐싱을 이용하는 점에 있어서의 결점은 핸드세이크에 응답할 때 원래의 세션 ID를 제시할 필요가 있다는 것이다 (인증서는 교환되지 않고 공중 키 연산도 발생하지 않는다). 세션 ID는 클라이언트 "헬로우" 플로우에 포함된다.

[0098] 데이터가 한 방향으로만 흐를 필요가 없다는 점에 유의해야 한다 - 데이터는 양 방향으로 흐른다. 이 시나리오에서는, 비밀 키 재조정이 필요해질 때 마다 보낼 데이터를 갖고 있는 누구나 하트비트를 보낼 책임이 있는 것으로 특정되는 것이 바람직하다 (즉, 적어도 미리 결정된 시간 동안 데이터가 양 방향으로 전혀 흐르지 않은 후에). 따라서 하트비트와 이의 응답은 양 단부의 존재를 결정하는 데에 이용된다. 이용된 바이트 계수는 특정 주기 동안 통신 링크를 통해 보내진 모든 데이터의 총 합인 것이 바람직하다 - 즉, 양 단부에 의해 보내진 데이터를 포함한다. 일 실시예에서, 일 단부는 바이트 계수 및 링크의 아이들 상태를 추적하여 다른 단부에 두 임계가 맞을 때를 알려준다.

도면의 간단한 설명

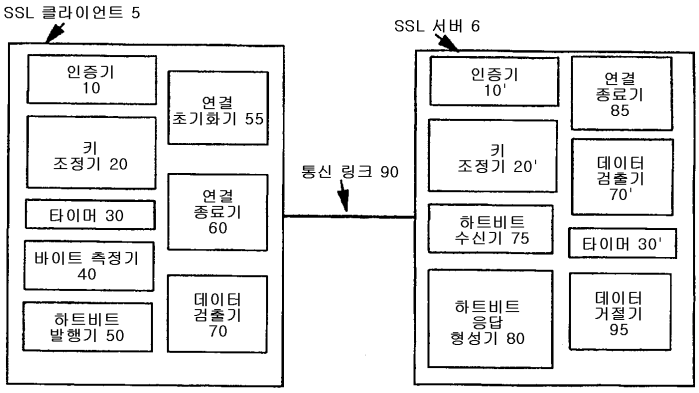
[0052] 본 발명의 바람직한 실시예를 오직 예시적으로만 첨부한 도면을 참조하여 이하 기재될 것이다.

[0053] 도 1a는 본 발명의 바람직한 실시예에 따른 클라이언트-서버 구성 요소의 도면이다.

[0054] 도 1b는 본 발명의 바람직한 실시예에 따라서 클라이언트에 의해 실행되는 처리의 플로우 챠트이다.

도면

도면1A



도면1B