



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0099898
(43) 공개일자 2019년08월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) G06F 21/12 (2013.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 63/12 (2013.01)
G06F 21/128 (2013.01)
(21) 출원번호 10-2018-0019945
(22) 출원일자 2018년02월20일
심사청구일자 2018년02월20일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준범
경기도 용인시 기흥구 보정로 30, 119동 201호(보정동, 동아솔레시티아파트)
남현재
서울특별시 강동구 천호대로168길 25, 101동 901
(74) 대리인
김홍석

전체 청구항 수 : 총 4 항

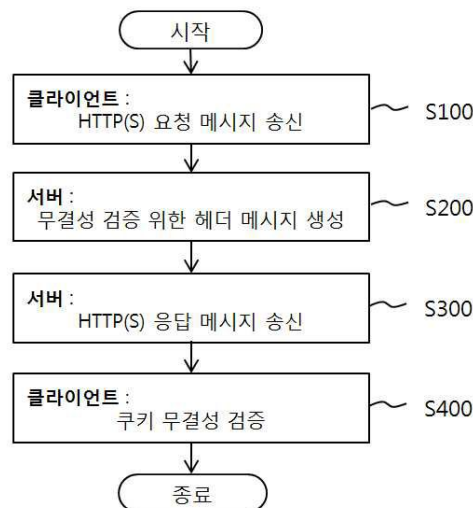
(54) 발명의 명칭 HTTPS에서의 쿠키 무결성 검증 방법

(57) 요약

사용자 장치, 포그 디바이스, 및 클라우드 서버를 포함하는 포그 컴퓨팅 환경에서의 하이브리드 데이터 중복제거 방법이 개시된다. 하이브리드 데이터 중복제거 방법은

클라이언트 및 서버를 포함하는 HTTPS 환경에서의 쿠키 무결성 검증 방법이 개시된다. HTTPS 환경에서의 쿠키 무결성 검증 방법은 클라이언트가 서버에 HTTPS 요청 메시지를 송신하는 단계, 서버가 Header-MD5 옵션을 추가하여 쿠키 탈취 공격에 대하여 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 생성하는 단계, 서버가 클라이언트에 상기 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 포함하는 HTTPS 응답 메시지를 송신하는 단계, 및 클라이언트가 상기 HTTPS 응답 메시지의 무결성을 검증하는 단계;를 포함한다.

대표도 - 도3



(52) CPC특허분류

H04L 63/1433 (2013.01)

H04L 63/166 (2013.01)

H04L 9/0643 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2017045199

부처명 과학기술정보통신부

연구관리전문기관 한국연구재단

연구사업명 (이공)중견연구자-핵심(후속)

연구과제명 분산 클라우드컴퓨팅을 위한 보안 및 프라이버시 계층 연구 및 개발

기 여 율 1/2

주관기관 고려대학교 산학협력단

연구기간 2017.06.01 ~ 2018.03.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711055304

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발

연구과제명 자기학습형 사이버면역 기술개발

기 여 율 1/2

주관기관 한국인터넷진흥원

연구기간 2017.03.01 ~ 2020.12.31

명세서

청구범위

청구항 1

클라이언트 및 서버를 포함하는 HTTPS 환경에서의 쿠키 무결성 검증 방법은,

클라이언트가 서버에 HTTPS 요청 메시지를 송신하는 단계;

상기 서버가 Header-MD5 옵션을 추가하여 쿠키 탈취 공격에 대하여 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 생성하는 단계;

상기 서버가 상기 클라이언트에 상기 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 포함하는 HTTPS 응답 메시지를 송신하는 단계; 및

상기 클라이언트가 상기 서버로부터 수신한 Header-MD5 값 및 HTTPS 헤더 메시지에서 생성한 Header-MD5 값을 비교하여 상기 HTTPS 응답 메시지의 무결성을 검증하는 단계;를 포함하는

쿠키 무결성 검증 방법.

청구항 2

제1항에 있어서,

상기 쿠키 탈취 공격은 쿠키 플래그 변경을 통한 쿠키 탈취 공격인,

쿠키 무결성 검증 방법.

청구항 3

제1항에 있어서,

상기 쿠키 탈취 공격은

GCM을 사용하는 서버에 대해서 공격자가 쿠키 플래그를 임의로 수정하여 유효한 태그를 생성하여 클라이언트가 쿠키 플래그 없이 쿠키 값을 저장하고 HTTPS가 아닌 HTTP 프로토콜로 쿠키 값을 전송 가능하게 함으로써 공격자가 쿠키 탈취 가능하도록 하는 제1 공격을 포함하는,

쿠키 무결성 검증 방법.

청구항 4

제1항에 있어서,

상기 쿠키 탈취 공격은

같은 키를 사용하는 연결을 만들어 클라이언트로 가는 메시지를 조작하는 공격으로, 클라이언트가 쿠키 플래그 없이 쿠키 값을 저장하고 HTTPS가 아닌 HTTP 프로토콜로 쿠키 값을 전송 가능하게 함으로써 공격자가 쿠키 탈취 가능하도록 하는 제2 공격을 포함하는,

쿠키 무결성 검증 방법.

발명의 설명

기술분야

- [0001] 본 발명은 HTTPS에서의 쿠키 무결성 검증 방법에 관한 것으로, 특히 암호 통신 프로토콜인 SSL/TLS와 웹 프로토콜인 HTTP에서 사용자의 비밀정보를 담고있는 HTTP 쿠키를 탈취할 수 있는 공격 유형 제시하고 이를 해결하기 위해 새로운 HTTP 옵션을 추가하여 HTTP 쿠키의 무결성을 검증할 수 있는 방법에 관한 것이다.

배경기술

- [0002] 본 발명은 HTTPS에서의 쿠키 무결성 검증 기법을 제안한다.
- [0003] SSL/TLS 프로토콜은 전 세계적으로 가장 많이 사용되는 네트워크 보안 프로토콜로써 클라이언트와 서버간의 안전한 메시지 교환을 목적으로 상호인증, 키 교환, 데이터암호화, 데이터 무결성 체크 등의 기능을 수행한다. 하지만 아직까지도 그 취약점이 발표되고 있고 낮은 버전의 프로토콜을 사용하는 경우나 취약점이 존재하는 라이브러리를 사용하는 경우 공격자는 다양한 공격을 수행할 수 있다.
- [0004] 대표적인 웹 프로토콜인 HTTP에서 클라이언트의 정보를 저장하기 위해 사용되는 cookie는 다양한 정보를 담을 수 있다. 쿠키(cookie)란 인터넷 사용자가 어떠한 웹사이트를 방문할 경우 그 사이트가 사용하고 있는 서버를 통해 인터넷 사용자의 컴퓨터에 설치되는 작은 기록 정보 파일로, HTTP 쿠키, 웹 쿠키, 또는 브라우저 쿠키라고도 한다. 쿠키에 담긴 정보는 인터넷 사용자가 같은 웹사이트를 방문할 때마다 읽히고 수시로 새로운 정보로 바뀐다. 쿠키는 컴퓨터내에서 프로그램처럼 실행될 수 없으며 바이러스를 옮길 수도, 악성코드를 설치할 수도 없지만 스파이웨어를 통해 유저의 브라우징 행동을 추적하는데에 사용될 수 있고, 누군가의 쿠키를 훔쳐서 해당 사용자의 웹 계정 접근권한을 획득할 수도 있다.
- [0005] 쿠키가 사용자 계정의 로그인 정보 또는 기밀 정보를 담고 사용자에게 대한 인증의 기능을 수행하는 경우, 이러한 쿠키는 공격자로부터 보호되어야 하며 이를 위해 HTTPS에서의 쿠키 무결성 검증 방법이 필요하다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) US 8448233 B2
(특허문헌 0002) KR 2010-0108132 A
(특허문헌 0003) US 8286225 B2

발명의 내용

해결하려는 과제

- [0007] 본 발명이 이루고자 하는 기술적인 과제는 암호 통신 프로토콜인 SSL/TLS와 웹 프로토콜인 HTTP에서 사용자의 비밀정보를 담고있는 HTTP 쿠키를 탈취할 수 있는 공격 유형 제시하고 이를 방어함으로써 HTTP 쿠키의 무결성을 검증할 수 있는 방법을 제공하는 것이다.

과제의 해결 수단

- [0008] 본 발명의 실시 예에 따른 클라이언트 및 서버를 포함하는 HTTPS 환경에서의 쿠키 무결성 검증 방법은
- [0009] 클라이언트가 서버에 HTTPS 요청 메시지를 송신하는 단계, 서버가 Header-MD5 옵션을 추가하여 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 생성하는 단계, 서버가 클라이언트에 상기 쿠키 무결성 검증이 가능한 HTTPS 헤더 메시지를 포함하는 HTTPS 응답 메시지를 송신하는 단계, 및 클라이언트가 쿠키 무결성을 검증하는 단계를 포함한다.

발명의 효과

- [0010] 본 발명의 실시 예에 따른 HTTPS에서의 쿠키 무결성 검증 방법에 의한 경우, HTTPS상의 쿠키 탈취 공격으로부터 Set-Cookie 메시지를 보호할 수 있으며, 또한 SSL/TLS의 암호화를 통해 Header-MD5 값을 보호할 수 있다.

도면의 간단한 설명

- [0011] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 본 발명의 실시 예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 시스템의 개략도이다.
- 도 2a 내지 도 2b는 도 1에 도시된 브라우저의 취약점을 나타낸 도면이다.
- 도 3은 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법을 설명하기 위한 흐름도이다.
- 도 4 내지 도 5는 본 발명의 일 실시예에 따른 쿠키 무결성 검증 방법을 통해 방어할 수 있는 예시적인 공격 유형을 도시한다.
- 도 6은 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법이 적용된 예시적인 HTTP 쿠키 헤더 메시지이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0013] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0014] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0015] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0016] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0017] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.
- [0018] 먼저, 도 1 내지 도 2를 참조하여, 본 발명의 일 실시예에 HTTPS에서의 쿠키 무결성 검증 시스템에 대해 상술한

다.

- [0019] 도 1은 본 발명의 실시 예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 시스템(10)을 도시하고, 도 2는 도 1에 도시된 브라우저의 취약점을 도시한다.
- [0020] 도 1을 참조하면, HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 시스템(10)은 브라우저(110)을 포함하는 클라이언트 장치(100) 및 웹 서버(200)를 포함한다.
- [0021] 클라이언트 장치(100)는 네트워크 망을 통하여 웹 서버(200)와 통신할 수 있다. 일 실시예에 따른 네트워크 망은, 개방형 인터넷, 폐쇄형 인트라넷을 포함한 유선 인터넷망, 이동 통신망과 연동된 무선 인터넷 통신망뿐만 아니라, 각종 데이터 통신이 가능한 컴퓨터 네트워크 등의 가능한 통신 수단을 포함하는 넓은 개념이다.
- [0022] 클라이언트 장치(100)는 브라우저(110)를 포함한다. 도 2를 참조하면 브라우저(110)가 HTTP 메시지를 받아드리는데 있어서 메시지에 대한 포맷이나 무결성에 대해 검증하지 않으며 해석가능한 부분만 받아드리는 취약점이 존재한다.
- [0023] 브라우저(110)는 서버(200) 설정의 오류나 네트워크 오류로 발생할 수 있는 잘못된 메시지를 받아드리고 Secure 플래그가 없이 쿠키를 저장할 수 있다(도 2a). 마찬가지로 HTTP 프로토콜의 상태를 나타내는 Status line이 두 개 이상의 메시지로 잘못된 포맷이더라도 정상적으로 쿠키 값을 저장할 수 있다(도 2b).
- [0024] 이하, 도 3 내지 도 6을 참조하여, 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법에 대하여 자세히 살펴보도록 한다.
- [0025] 도 3은 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법을 설명하기 위한 흐름도이고, 도 4 내지 도 5는 본 발명의 일 실시예에 따른 쿠키 무결성 검증 방법을 통해 방어할 수 있는 예시적인 공격 유형을 도시한다.
- [0026] 도 6은 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법이 적용된 예시적인 HTTP 쿠키 헤더 메시지이다.
- [0027] 후술하는 HTTP 관련 용어들은, 하이퍼텍스트 전송 규약(Hypertext Transfer Protocol, HTTP)에 근거한다.
- [0028] 이하, 도 4 내지 도 5를 참조하여, 상기 브라우저 및 SSL/TLS의 취약점에 따른 예시적인 공격 유형을 설명한다.
- [0029] 제1 공격 유형은 취약한 GCM을 사용하는 서버에 대해서 중간공격자가 쿠키 플래그를 임의로 수정하여 유효한 태그를 생성하는 방법이다(도 4). 클라이언트는 쿠키 플래그 없이 쿠키 값을 저장하며 이는 나중에 암호화통신인 HTTPS가 아닌 HTTP 프로토콜로 쿠키 값을 전송할 수 있어 공격자는 쿠키 값을 탈취할 수 있다.
- [0030] 제2 공격 유형은 같은 키를 사용하는 연결을 만들어 클라이언트로 가는 메시지를 조작하는 방법이다(도 5). 0-RTT 메시지의 경우 키 생성에 사용되는 랜덤 값을 클라이언트만 생성하여 사용하기 때문에 키를 생성할 때 사용되는 0-RTT 요청 메시지를 복사하여 전송하게 될 경우 같은 키를 사용하는 연결을 생성할 수 있다. 마찬가지로 클라이언트는 쿠키 플래그 없이 쿠키를 저장하기 때문에 후에 HTTP 프로토콜을 사용하여 쿠키 값을 탈취할 수 있다.
- [0031] 이하 도 3을 참조하여 본 발명의 일 실시예에 따른 HTTPS 컴퓨팅 환경에서의 쿠키 무결성 검증 방법을 설명한다.
- [0032] 먼저, 클라이언트(100)는 서버(200)에 HTTPS(HTTP??) 요청 메시지를 송신한다(S100).
- [0033] 다음, 서버(200)는 Header-MD5 옵션을 추가하여 HTTP 헤더 메시지를 생성한다(S200). 다시 말해, 상기 브라우저 및 SSL/TLS의 취약점에 따른 공격을 방어하기 위하여 서버(200)가 클라이언트(100)에 쿠키 값을 보낼 때 사용되는 HTTPS 헤더 메시지에 대해서 무결성을 검증하기 위한 헤더 옵션을 추가한다. Header-MD5 옵션을 추가함으로써 헤더 부분의 메시지에 대한 무결성 검증을 가능하게 한다.

[0034] 이를 통해 Set-Cookie 메시지를 보호할 수 있으며 또한 SSL/TLS의 암호화를 통해 Header-MD5 값을 보호할 수 있기 때문에 앞서 제시한 공격 시나리오에 대해 안전하게 설계 가능하다.

[0035] 다음, 서버(200)는 클라이언트(100)에 무결성 검증이 가능한 HTTPS 헤더를 포함하는 HTTPS 응답 메시지를 송신한다(S300).

[0036] 다음, 클라이언트(100)는 수신한 HTTPS 응답 메시지에 포함되어 있는 HTTPS 헤더로부터 Header-MD5 값을 얻는다. Header-MD5 값을 제외한 HTTP 헤더 메시지로부터 상기 서버와 동일한 방식으로 Header-MD5 값을 생성한다. 2개의 Header-MD5 값을 비교하여 HTTPS 헤더 메시지에 대한 무결성을 검증한다(S400). 다시 말해, 2개의 Header-MD5 값이 동일하다면 HTTPS 응답 메시지를 받아드리고 그렇지 않다면 재요청 메시지를 송신한다.

[0037] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0038] 100 : 클라이언트 110 : 브라우저

200 : 서버

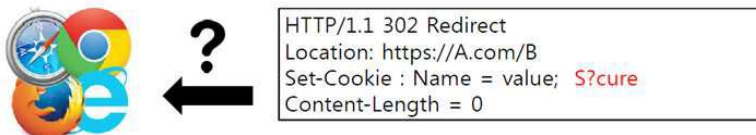
도면

도면1

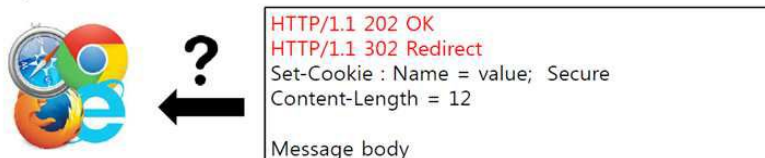


도면2

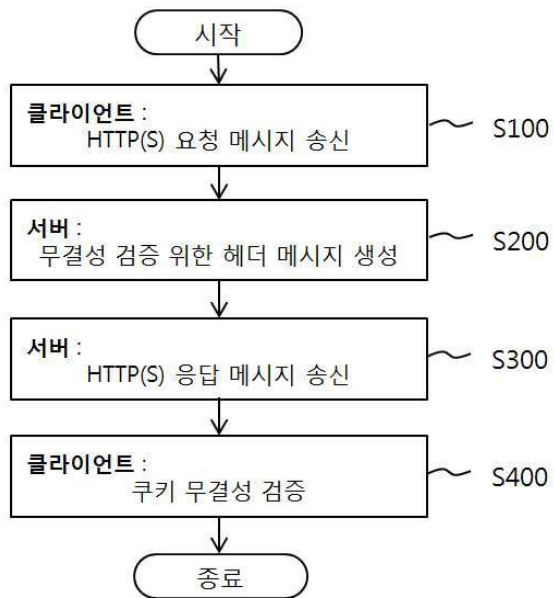
2a)



2b)

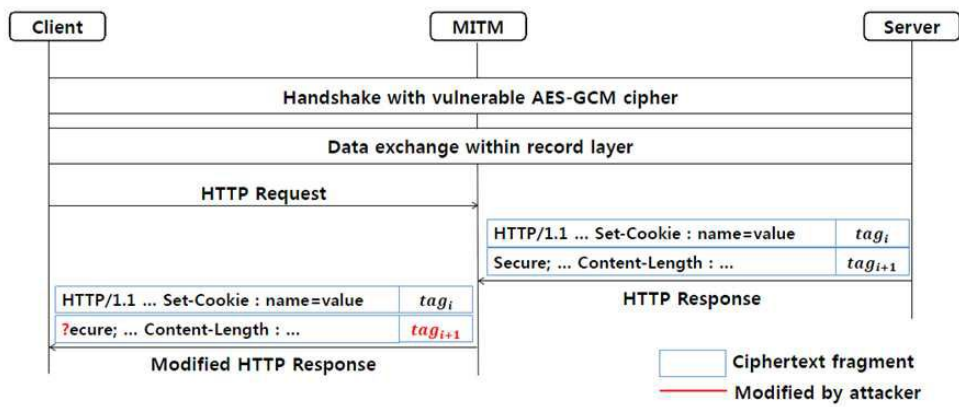


도면3



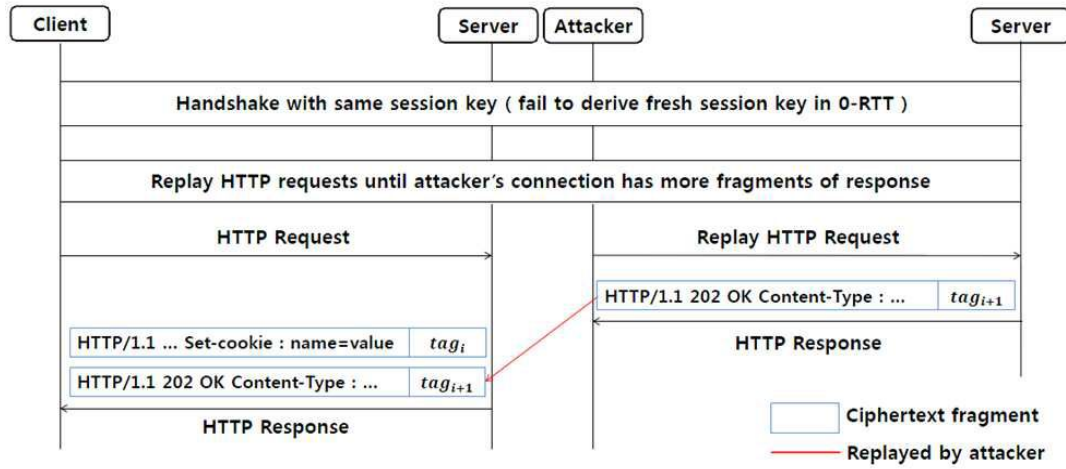
도면4

- Based on vulnerable GCM server



도면5

- Based on vulnerable 0-RTT server



도면6

```
HTTP/1.1 202 OK
Date: Sun, 10 Oct 2017 23:26:07 GMT
Set-Cookie: Name=value;Secure;HttpOnly
Content-Type: text/html
Content-Length: 20
Header-MD5 : Yzg4ZjgxMjQzOTc0NGVhMD...
HTTP content message
```