The Journal of Digital Policy & Management 2013 May; 11(5): 291-298

방문자의 프라이버시를 보호하는 측정 방식

박춘식*
서울여자대학교 정보보호학과

Metering scheme for client privacy protection

Choon-Sik Park*
Dept. of Information Security, Seoul Women's University

요 약 방문 측정 방식은 많은 방문자, 서버들 그리고 서버들에 의해 처리되는 방문자의 정보를 수집하는 감사 기관으로 구성된다. 많은 효율적이고 안전한 방문 측정 방식들이 문헌상에 제안되어 있지만, 이들은 방문자의 프라이버시 문제를 고려하고 있지 않다. 관련 연구에서의 이러한 제약을 완화하기 위하여, 인터넷상의 방문자의 프라이버시를 보호하는 방문 측정 방식을 제안하고자 한다. 좀 더 구체적으로, 방문자와의 감사 기관 사이에 RSA 기반 blind signature를 적용하였다. 만일 방문자가 2회 이상의 방문 정보를 서버에 보내게 되는 경우, 서버나 감사 기관에 의해 방문자의 신분은 드러나게 된다.

주제어 : 방문측정방식, 프라이버시, 시큐리티, 블라인드 서명, 해시 함수

Abstract Metering scheme is composed of servers, clients, and an audit agency who collects the information for the clients which have been processed by servers. Although many efficient and secure metering schemes have been proposed in the literature, they do not consider the client privacy issue. To mitigate this limitation of the related work, we propose a metering scheme to protect the privacy of clients in internet. More specifically, we apply RSA based blind signature to the interaction between client and audit agency. If a client spends metering information to the server more than twice, the identity of the client is revealed by the server or audit agency.

Key Words : metering scheme, privacy, security, blind signature, Hash Function

1. 서론

온라인 광고는 인터넷과 웹 브라우저를 이용하여, 검색 엔진 결과 페이지, 웹 배너, 블로그, 리치 미디어 광고, 소셜 네트워크 광고, 전자 우편 광고 등에 온라인 광고를 넣어, 고객들을 끌어들이기 위한 마케팅 메시지를 전달하는 것이다. 온라인 광고는 배너 광고, 텍스트 형 광고, 키 워드 검색 광고 등으로 형태별로 분류되고 있으며 비용대비 광고효과, 부정 클릭 등에 따라서 각각 활용되고 있다. 구글이나 오버츄어[1] 등이 서비스하고 있으며 인터넷 광고로 주로 대표되고 있는 키 워드 검색 광고는, 사용자가 포털 등의 검색 창에 원하는 단어를 검색한 뒤

* 본 논문은 2013학년도 서울여자대학교 컴퓨터과학연구소 교내학술연구비의 지원을 받았음
Received 11 March 2013, Revised 5 April 2013
Accepted 20 May 2013
Corresponding Author: Choon-Sik Park(Seoul Women's University)
Email: csp@swu..ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.otg/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

출력된 결과 페이지의 사이트를 클릭하면 사이트에 노출된 광고에 대한 광고주와 사이트를 게시해 준 포털 등의 관계에서 클릭에 해당되는 광고료가 제공되게 된다. 이러한 형태의 검색광고가 포털의 가장 큰 수익원이 되는 비즈니스 모델이 되어 있으며 이를 이용하는 광고주들은 대부분 영세하거나 인터넷상의 광고에 의존하게 되는 많은 인터넷 비즈니스 중소기업체들이 해당되고 있다는 것은 주지의 사실이다.

또한 온 라인 광고를 과금 형태로 분류할 때는 1000번의 노출에 대한 광고비 지급 방식인 CPM(Cost Per Millennium), 클릭 횟 수당 광고비 지급 방식인 CPC(Cost Per Click), 클릭을 한 후 실제로 구매 등의 행위를 했을 때 광고비를 지급하는 방식인 CPA(Cost Per Action)방식으로 크게 나누어지며 통상적으로 키워드 검색이며 CPC 클릭 방식의 과금 방식이 인터넷 광고로 많이 통용되고 있다.

인터넷 광고는 광고 측면에서 많은 이점이 있지만 부정 클릭에 의한 부당한 광고비 청구, 정확한 클릭 확인을 위한 투명한 절차 부재, 포털과 광고주 사이의 끊임없는 분쟁 등 부정 클릭에 의한 사회적 문제가 제기된 지 오래된 사실이다[2]. 대부분의 부정 클릭은, 포털사 등이 부당하게 클릭(방문)한 횟수를 늘려 광고비를 수령하는 공격과 쿠키를 제거하거나 IP를 변환하면서 클릭을 자동으로 하는 부정클릭 프로그램을 이용한 부정 클릭 방문객(경쟁사, 경쟁사와 결탁한 방문객, 부정 방문객 등)에 의한 공격이 크게 이루어진다[3].

연속적인 클릭에 대한 과금 제외, 접속자 IP 추적, 유동 접속자 IP 추적, 쿠키를 제거하고 IP를 변동하는 접속자 등에 대한 부정 클릭 접속자에 대해서는 접속자(방문자)화면에 클릭한 사이트, 클릭한 키워드, 클릭 시간, IP 주소 등을 팝업창 제공 및 부정 접속자 추적 등을 통하여 부정 클릭에 의한 공격을 사전에 예방하는 기존의 각종 도구(프로그램)들이 많이 제공되고 있어, 경쟁사나 부정 방문객 등에 의한 단순한 부정 클릭에 대해서는 방지할 수 있다. 본 논문에서는 연속 클릭, 유동 IP 사용 등 단순한 부정 클릭에 대한 것은 이러한 도구를 사용하여 방지 가능한 상황이라고 가정하고, 단순한 부정 클릭이 아닌 감사기관(광고대행사) 으로부터 수령한 동일한 방문 정보를 부당하게 사용하는 공격 등 보다 고도화된 연속 방문(클릭) 등에 대한 안전한 인터넷 광고 방문 측정 방식을 연구하고자 한다.

본 논문에서는 단순한 부정 클릭에 의한 방지 도구가 설치되어 있는 상황에서, 클릭, 노출, 히트 등의 측정에 관한 내용보다는 방문객이 조회한 즉 측정된 값이 얼마나 정확하고 안전하게 측정되었는지를 중점적으로 연구하고자 한다. 기존의 대부분의 방식들은 측정과정에서 발생한 정보를 이용하여 방문객의 프라이버시를 침해할 수가 있지만 제안 방식에서는 이러한 방문객의 프라이버시를 고려한 안전한 인터넷 광고 방문 측정 방식을 제안하고자 한다.

본 논문의 2장에서는 안전한 인터넷 측정 방식에 대한 기존 연구 동향을 살펴보고, 3장에서는 인터넷 광고 방문 측정 모델 및 요구사항을 설명하고, 4장에서는 프라이버시가 제공되는 새로운 측정 방법을 제안하고, 5장에서 결론 및 향후 연구에 대해 논하고자 한다.

2. 관련 연구 현황

인터넷 상에서 광고를 게재하고 있는 웹서버 방문 고객의 클릭들을 일정 기간 지난 후 측정하여 광고주로부터 해당 금액을 수령하는 방식을 인터넷 측정 방식(Metering Scheme)이라 부르며 주로 광고대행사인 감사기관(Audit Agency)과 방문객인 고객(Client) 그리고 포털 등 웹 사이트 제공자인 서버(Server)로 기본적인 모델을 구성하고 있다. 광고 클릭 측정 방식에서 고객이 광고가 게재되어 있는 웹 사이트 서버를 방문 또는 클릭한 횟수만큼만 즉 서버가 방문 횟수를 허위로 부풀리지 않도록 하는 것이 가장 중요하다.

서버의 방문 횟수 부정 조작과 고객의 측정 방해 행위를 막아내는 안전한 인터넷 광고 방문 측정 방식(Secure Metering Scheme)으로 기존에 여러 방식들이 제안되어 왔다. 가장 기본적으로 생각할 수 있는 방식으로 디지털 서명을 이용하여 광고 방문 측정 방식을 구현할 수 있다. 디지털 서명을 이용한 광고 측정 방식은 먼저 감사기관이 향후 방문할 고객에게 디지털 서명키를 제공하고, 고객은 서버를 방문할 때 디지털 서명키를 이용하여 생성한 디지털 서명을 서버에 제공하게 된다. 서버는 고객들의 서명을 광고주에게 제출하여 해당 금액을 수령하게 된다. 디지털 서명을 이용한 광고 방문 측정 방식은 서버의 방문 회수 부정을 막고 정확하게 방문 고객을 측정할 수 있는 장점이 있는 반면, 사전에 고객들에게 서명키를

안전하게 제공하여야 하며, 증거로 활용되는 정보량이나 검증에 사용되는 계산량으로 인하여 비효율적인 방식이며 방문자 개인의 디지털 서명을 확인하므로 방문자의 광고 선호도 취향 등 개인의 프라이버시가 침해되는 부작용이 있다[4][5].

디지털 서명에 의한 광고 방문 측정 방식과는 별도로 안전하고, 시스템의 부하를 줄이면서 그리고 효율적인 광고 방문 측정을 위한 새로운 많은 방식들이 제안되어 왔다. Franklin과 Malkhi[6]방식, Naor와 Pinkas[7]방식, Masucci와 Stinson방식[8], Ogata와 Kurosawa방식[5], 김순석 등 방식[4], Kuo 등 방식[9], Wang 등 방식[10] 등[11][12] 효율적이고 안전한 많은 방식들이 제안되었다.

Franklin과 Malkhi[6]방식은 방문객이 웹 사이트를 방문했을 때 일정 시간동안 계산을 한 후 그 결과 값으로 측정할 수 있는 시간함수(timming function)라는 개념을 도입하여 사전 등록 단계를 수행하지 않으면서 방문자의 프라이버시를 제공하는 방식이다. 그러나 인터넷 광고 측정보다 방문자와 서버간의 1:1 측정에 유용한 방식이다[4].

Naor와 Pinkas[10]방식은 서버와 방문자와의 결탁에 의한 부정에도 안전한 인터넷 광고 방문 측정의 대표적인 방식으로 비밀공유(Secret Sharing)방식에 의하여 최종 증거를 제시하는 효율적인 방식이나 방문한 횟수 그 자체를 측정하는 방법이라기 보다는 미리 결정된 방문 횟수에 도달할 경우에만 사용 가능한 단점이 있으며 2명의 공격자(고객)에 의해 서버의 정확한 집계를 방해할 수 있는 Ogata와 Kurosawa[5] 공격이 가능하여 기본적으로 안전하지 못한 방식이다.

김순석 등[4]은 Naor와 Pinkas[7] 방식이 방문자 집계수가 미리 정해진 임계치에 정확히 도달해야만 증거를 확보할 수 있는 단점이 있는 반면 이를 해결하기 위하여 해쉬 함수와 일종의 MASK 테이블을 이용하여 방문자 집계 수에 대한 자유로운 측정이 가능한 방식을 제안하였다. 그러나 이 방식은 방문자의 프라이버시가 서버에 의해 제공되지 못하는 즉 익명성이 보장되지 못하고 있다. 특히 이 방법은 방문자에 의한 서버의 올바른 측정 방해 공격을 방지하기 위하여 특정 서버와 특정 기간에만 방문을 하도록 하여 비효율적임은 물론 용도가 극히 제한되는 방식이다.

비밀공유방식에 기반을 둔 Naor와 Pinkas[7] 방식 등에서는 방문자 측정이 1회 완료되면 비밀공유방식에 의한 증거(비밀정보)가 노출되게 되어 재활용이 불가능하여 단발성 측정 방식으로 밖에 사용할 수 없는 공통된 문제점이 있다. Kuo 등 방식[9]은 증거가 노출되지 않으면서도 연속하여 사용할 수 있는 방식을 제안하였으나 여전히 Naor와 Pinkas 류의 방식들이 갖고 있는 방문자의 방해 공격에 취약하며 방문자 집계수가 미리 정해진 임계치에 정확히 도달해야만 증거를 확보할 수 있는 면에서도 문제가 있는 방식이다.

해시 함수와 배타적 논리 합 연산에 의한 효율적인 방식인 김순석 등[4]의 방식은 안전성을 위해 특정 서버와 특정 기간으로 서버를 한정하는 제약이 있어 실용적이지 못한 면이 있다. 이러한 서버의 제약을 해결하기 위해서 해시함수와 비밀공유방식을 이용한 개선된 인터넷 광고 측정 방식을 Wang 등[10]이 제안하였다. 그러나 이 방식 역시 비밀공유 방식에 의한 문제점인 방문자 집계수가 미리 정해진 임계치에 정확히 도달해야만 증거를 확보할 수 있는 면에서 유연성이 결여된 방식이며 방문자의 프라이버시 여전히 문제가 되는 방식이다.

지금까지 제안된 많은 효율적인 인터넷 광고 측정 방식은 주로 비밀공유방식과 해시 함수 방식에 의한 변형된 방식들이다. 기존 제안 방식들은 비밀공유방식에 의한 문제점인 유연성면이나 해시 함수 방식에 의한 특정 서버 한정이나 프라이버시 문제를 안고 있다. 또한 감사기관(Audit Agency)과 방문객(Client) 그리고 서버(Server)간의 사전 비밀 정보 공유에 의한 가정은 실질적인 환경에서 인터넷 광고 방문 측정을 행할 경우 실용적이지 못하며 이를 구현하고자 할 경우에는 즉 비밀 채널을 제공하고자 할 경우에는 보다 복잡한 방식이 될 수 밖에 없다.

따라서 많은 단말들의 계산 능력이 향상되고 그리고 기존의 많은 단말들은 암호 구현 능력을 갖추고 있는 것이 많으며 실용적인 인터넷 광고 방문 측정을 이루기 위해서는 유연성이 있고 서버 제한이 없으며 프라이버시 문제나 사전 비밀 정보 공유와 같은 가정이 필요하지 않은 방식이 필요하다.

3. 인터넷 광고 방문 측정 모델 및 요구사항

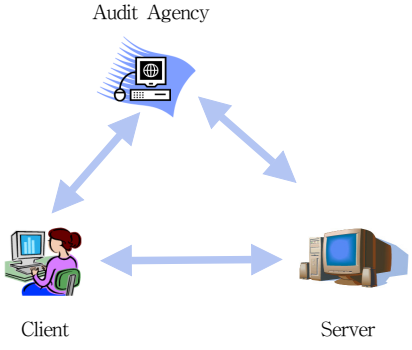
3.1 인터넷 광고 방문 측정 기본 모델

광고를 의뢰한 광고 회사가 인터넷상의 웹 사이트 광

고를 제공한 웹서버에게 지불하는 광고 비용은 광고가 게재되어 있는 웹 서버를 클릭 방문한 방문객의 수에 의존하게 된다. 이러한 방문객의 클릭 수를 측정하는 프로토콜이 인터넷 광고 방문 측정 방식이다.

인터넷 광고 방문 측정 기본 모델은 인터넷을 통하여 행하여지는 광고와 광고가 게시된 웹사이트를 방문한 방문자를 측정하여 광고대행사에 제시하는 Fig. 1과 같은 구조로 주로 이루어진다. 본 논문에서 가정하는 방문 측정 기본 모델은 복수의 방문자와 복수의 서버 그리고 하나의 감사 기관으로 구성되는 것으로 가장 일반적인 모델이라고 생각된다. 먼저, 자사의 제품 등의 인터넷 광고를 원하는 광고주가 광고 대행사(감사 기관)에게 광고를 의뢰하면, 광고 대행사인 감사 기관은 광고 제공 웹 사이트(서버)에게 일정 기간 동안의 광고 게재관련 계약을 맺게 된다. 다음으로, 서버는 일정 기간 동안 방문한(광고를 클릭한) 조회 횟수를 측정하여 측정된 모든 결과값을 광고대행사에게 제공한다. 광고 대행사는 서버가 제출한 측정값 중 정확하게 방문한 값만을 확인한 후 서버에게는 해당 광고비를 제공하며 광고주에게도 방문한 값을 전달한다.

서버는 일정 기간 동안 서버를 방문한 정확한 값만을 측정하여 감사 기간에 제공해야 하며 방문객은 측정 프로세서에 대한 어떠한 방해를 하지 않아야만 성립되는 모델로 안전한 인터넷 광고 방문 측정 방식은 서버나 방문객의 이러한 공격에 견디어내어야만 안전하다할 수 있다. 여기서 광고대행사인 감사기관은 서버가 보낸 특정 값을 정확한지 판단해야 하는 기능을 가지므로 신뢰할만한 제3의 기관(Trusted Third Party)이라고 가정한다.



[Fig. 1] Metering Scheme Basic Model

3.2 안전한 인터넷 광고 방문 측정 요구사항

안전한 인터넷 광고 방문 측정을 위해서는 방문객이나 서버에 의한 부정 행위에 무관하게 광고대행사인 감사기관이 서버가 보낸 측정값을 정확하게 판단해야 한다. 방문객에 의한 공격, 서버에 의한 공격, 제3의 부정 공격(경쟁사간의 의도적인 공격 등) 등에 대하여 안전한 인터넷 광고 방문 측정이 이루어지기 위해서는 다음과 같은 요구사항들이 고려되어야 한다. 본 논문에서 제안하게 되는 방문객의 프라이버시 보호는 빅 데이터 시대를 맞이하여 인터넷 광고 방문 측정을 위해 서버와 감사기관이 수집한 정보나 측정 관련 정보에 의해서 방문객의 프라이버시가 보호되지 않을 위협이 있어 추가적으로 요구사항에 언급하였다.

- ○ 안전성:
  - 부정 서버에 대한 안전: 서버는 방문자 수를 임의로 증가시키지 못하며 정확한 방문자 수를 입증하여야 한다.
  - 부정 클라이언트에 대한 안전: 방문자(클라이언트)는 서버의 방문자 수 측정을 방해하지 않아야 한다. 즉, 방문자, 방문자들간의 결탁, 방문자와 서버간의 결탁 등에 의하여 위조 방문을 하거나 서버의 위조된 방문 측정이 되지 못하도록 하여야 한다.
- ○ 정확성: 방문자의 정확한 수 만큼 측정되어야 한다.
- ○ 유연성: 방문자 집계수가 미리 정해진 임계치에 정확히 도달해야만 증거를 확보할 수 있는 방식이 아니라 자유로운 집계 방식이 되어야 한다.
- ○ 효율성: 감사기관, 서버 그리고 방문자간의 사전 비밀 통신이 최소한으로 국한되어야 하며(가능하면 사전비밀통신 없는 것이 바람직함) 방문자와 서버간 통신이 효율적이며 방문자와 서버의 계산량이 최소화되어야 한다. 그리고 인터넷 방문 광고 측정을 위해 특정 서버나 특정 기간으로 한정되지 않아야 한다.
- ○ 프라이버시: 감사기관과 서버를 방문한 방문자로부터 얻은 정보를 이용하여 방문자에 대한 최소한의 정보도 유출되지 않아 방문자의 프라이버시가 보호되어야 한다.

4. 새로운 방식 제안

기존의 방식에 있어서는 방문자가 어떤 인터넷 광고를 방문하였는 지 방문자의 선호도, 취미 등 프라이버시가 감사 기관이나 서버 그리고 제3자에게 노출될 수 있는 반면, 본 논문에서 제안하는 방식은 이러한 방문자의 프라이버시를 보호할 수 있다. 제안 방식을 개괄적으로 설명하면 기존 방식들의 일반적인 모델을 기준으로 하고 있다. 즉, 광고 대행사인 감사기관(A), 포털과 같이 광고를 게재하여 방문객의 클릭 수를 측정하여 감사기관에 제출하는 서버(S), 그리고 방문자 Ui로 구성되며 Fig. 2와 같다.

웹 사이트 광고를 희망하는 각 방문자는 감사기관에 Blind Signature[13]를 받기 위한 관련 정보를 제공하고 또한 경우에 따라서는 ZKIP(Zero Knowledge Interactive)에 의한 방법으로 자신의 ID 정보는 제공하지 않으면서 자신의 ID가 정당함을 입증한다. 이러한 절차가 완료되면 감사기관은 방문자가 보내온 정보에 대해서 감사 기관이 발행한 증명으로 수단으로 디지털서명된 값을 방문자에게 되돌려준다. 방문자는 수신한 서명값을 이용하여 감사 기관도 방문자의 정보를 알 수 없도록 해주는 Blind Signature 정보를 얻게 된다.

일정한 시간이 되어 방문객이 서버를 방문하게 될 경우, 감사기관으로부터 수령한 Blind Signature 정보와 이 정보를 이용하여 생성된 값을 방문 행위의 차원에서 서버에게 제공하게 된다. 서버는 각 방문자들이 보내 온 측정값들에 대한 정당성을 확인한 후, 일정기간 동안의 확인된 모든 방문자들의 정보를 감사기관에 제출하게 된다. 감사기관은 서버로부터 전달 받은 정보를 모두 검사하고 정당성을 확인하게 된다.

A는 신뢰할만한 감사기관이며 S는 서버이며 IDS_i 는 서버의 ID 값이며 복수개의 서버도 가정될 수 있다. 그리고 IDU_i는 방문자 U_i의 ID 값으로 복수명의 방문자라고 가정한다. 그리고 T_i 는 타임스탬프값으로 재전송 공격 방지를 위해서 방문자가 서버에 정보를 보낼 때 사용하며 서버가 일치 여부를 확인한다. 사용된 함수 H는 collision free oneway hash function이며 연산은 mod N 상에서 행하여지며, 지수부의 연산이나 랜덤 수 등의 파라미터들은 mod e상에서 연산되거나 생성된다. 감사기관은 Blind Signature와 서버의 검증에 필요한 RSA 암호 시스템의 개인키 d와 공개키 e를 준비되어 있는 것으로 가정한다.

4.1 Blind Signature 방식 이용한 방문 측정 방식

<단계 1> Initialization

감사 기관(A)이 방문자 U_i 의 행동을 판단할 수 있는 프라이버시 문제를 해결하고자 방문자 U_i 와 감사 기관 A 사이에 Blind Signature 방식을 적용한다.

(step 1) 먼저 방문자 U_i는 랜덤 값 r_1과 r_2 그리고 k를 각각 발생하여 $(r_1)^e(V^{IDU_i} \times W)$와 $(r_2)^e(V^k)$을 계산한다. 여기서 e는 감사 기관 A의 공개 키, IDU_i는 방문자 U_i의 ID 값, V=H(v), W=H(w)이다. H는 one way hash function이며 v와 w는 랜덤 값이다.

방문자 U_i는 임의의 시간에 서버(S)를 방문하기 위한 준비 단계로 자신의 계산한 값 $(r_1)^e(V^{IDU_i} \times W)$와 $(r_2)^e(V^k)$을 감사 기관 A에게 전송한다.

(step 2) 감사 기관 A는 방문자 U_i가 보낸 정보를 기반으로 인터넷 광고 방문을 희망하는 것으로 판단하고 감사 기관의 확인인 개인 키(=d)로 디지털 서명을 행하여 되돌려주게 된다. 이때 전송되는 정보는 다음과 같다.

$$r_1 \times (V^{IDU_i} \times W)^d \ , \ r_2 \times (V^k)^d$$

(step 3) 방문자 U_i는 감사 기관 A로부터 받은 값들로부터 간단하게 $(V^{IDU_i} \times W)^d$ 와 $(V^k)^d$를 계산할 수 있다. 이 두 값은 감사기관으로부터 받은 두 개의 RSA signature이다.

<단계 2> Interaction between client Ui and Server S

(step 1) 방문자 Ui는 기간 T_i에 서버 S를 방문하려면 서버 S의 IDS_i 값을 이용하여 $X = H(v, w, IDS_i, T_i)$를 계산한 후, 감사기관으로부터 받은 두 개의 RSA signatures를 이용하여 계산한 $R = ((V^{IDU_i} \times W)^d)^X \times (V^k)^d$ 과 $r = IDU_i \times X + k$을 포함한 (v, w, r, R)를 서버에게 전송한다. 여기서 k는 임의의 랜덤 값이다.

(step 2) 서버 S는 수신한 이 값들을 이용하여 $X' = H(v, w, IDS_i, T_i)$ 그리고 V와 W를 계산하고 다음 식이 성립하는 지 확인한다.

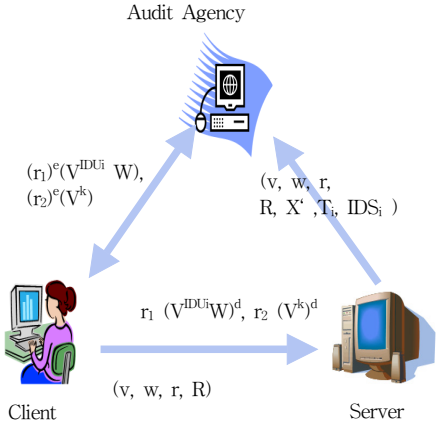
$$R^e \stackrel{?}{=} V^r \times W^{X'} \ (\mathrm{mod}\ N) \quad (1)$$

<단계 3> Proof Transmission

일정한 측정 기간이 만료되면, 서버 S는 (1) 식을 만족한 방문자 U_i에 해당하는 (v, w, r, R, X', T_i, IDS_i)을 모두 감사 기관 A에게 보낸다.

<단계 4> Verification

감사 기관 A는 서버 S로부터 받은 정보를 이용하여 동일한 (v, w, r, R, X', T_i, IDS_i) 들이 중복되어 있지 않는 지 확인한 후 각 방문자에 대해 식(1)이 만족하는 지가 모두 확인되면 증거로 받아들인다. 중복된 것이 있거나 식(1)이 만족하지 않는 경우에는 이를 증거에서 제외하도록 하며 중복된 것이 있을 경우에는 어떤 방문자가 이중 방문을 하였는 지 확인할 수 있다. 이는 방문자 또는 서버가 이중 방문하여 불법으로 증거를 제시하는 행위를 사전에 막을 수 있는 효과가 있다.



[Fig. 2] Proposed Metering Scheme

4.2 제안 방식의 분석

<정확성>

만일 방문자 U_i와 서버 S가 모두 honest하면, 서버가 측정하여 감사 기관에 제출한 측정값은 정확한 방문자 값이다. 방문자 U_i가 honest하기 때문에 단 1회의 정보 전송(방문)과 프로토콜에 따라 행동하고 서버 또한 honest하여 식(1)에 의한 검사와 프로토콜에 따라 행동하게 된다.따라서, $R^e \stackrel{?}{=} V^r \times W^{X'} \ (\mathrm{mod}\ N)$에서 $R^e = (((V^{IDU_i} \times W)^d)^X \times (V^k)^d)^e = (V^{IDU_i} \times W)^X \times (V^k) = V^r \times W^X \ (\mathrm{mod}\ N)$이 성립하게 된다. ($\because r = IDU_i \times X + k$)

<안전성>

<방문자 U_i의 이중 공격>

부정 방문자 U_i는 동일 서버에 2회 이상 방문하여 서버의 증거를 조작하게 할 수 있다. 이는 부정 방문자 단독 공격도 가능하지만 부정 방문자와 서버와의 결탁에 의한 공격도 가능하다.

먼저 예상되는 공격으로 부정 방문자가 기간 정보 T_i만을 변경하면서 동일 값들을 2회 이상 서버에 보내어서 공격할 수 있다. 즉, 부정 방문자(dishonest client)는 T_i 시각에 (v, w, r, R)를 서버에 전송한 후, 일정 시간이 경과한 T_j 에 다시 (v, w, r', R')를 전송할 수 있다. 여기서 서버는 Honest하다고 가정한다. 물론 서버가 dishonest할지라도 감사기관에서 동일한 검증 절차가 이루어지게 되므로 서버 입장에서는 감사 기관으로부터 부정으로 판단되는 것보다 서버 측에서 사전에 이러한 검증 절차를 제대로 수행하는 것이 효율적이다.

부정 방문자가 T_i 시각에 (v, w, r, R)를, T_j 에 다시 (v, w, r', R')를 서버에 전송한 경우에는 서버는 식(1)이 성립되는 지 검사한 후 성립되면 증거로 보존해두게 된다. 일정한 측정 시간이 완료되면 서버 S는 감사 기관에 증거를 모두 전송하기 전에 보존되어 있는 증거에 대해서 동일 값들이 존재하는 지 검사하게 된다. 이 경우, (v, w, r, R)와 (v, w, r', R')의 경우에는 동일한 v, w를 사용하였으므로 r과 r′를 이용하여 어떠한 방문자가 이중 방문을 하였는지 찾아낼 수가 있다. 즉, $r = IDU_i \times X + k$와 $r' = IDU_i \times X' + k$ 를 이용하여 $IDU_i = r - r'/ X' - X$, 즉 방문자의 ID 정보를 알게 된다. 물론 부정 방문자가 랜덤 값 k를 변경하여 전송할 수 있으나 이는 Blind Signature 방식에 의해서 감사 기관으로 서명된 정보가 아니기 때문에 서버에 의한 식(1)에 의한 검사를 통과할 수 없게 된다.

두 번째로 가능한 공격(v≠v')은 (v, w, r, R)와 (v', w, r', R')의 전송에 의한 공격을 가정해 볼 수 있다.

첫 번째 서버에 보내는 전송 정보인 (v, w, r, R)에 값에 대해서는 정당한 v와 w값을 이용하여 생성된 r과 R이기 때문에 서버 S가 식(1)에 의한 검증을 하여도 정당한 방문으로 판단된다. 그러나 두 번째 보내어진 (v', w, r', R') 방문에 대해서는 식 (1)인 $(R')^e \stackrel{?}{=} (V')^{r'} \times W^{X'}$

(modN)에서 $(R')^e = (((V^{IDUj} \times W)^d)^{X'} \times (V^k)^d)^e = (V^{IDUj} \times W)^{X'} \times (V^k) = V^{r'} \times W^{X'}$ (mod N)이 되어 식(1)이 성립하지 않는다. 왜냐하면 $V \neq V'$이기 때문이다. 이러한 공격을 성공하기 위해서는 (H(v)=H(v'))을 만족하는 해시 함수의 충돌 쌍 (v,v')를 찾으면 된다. 그러나 H: collision free oneway hash function이므로 안전하다.

<방문자 Ui의 허위 ID 값 제공>

initialization 단계에서 방문자는 허위 ID를 감사 기관에 제공하고 blind signature를 만들 수 있다. 이를 경우, 방문자 U_i의 이중 공격 시, 감사 기관이나 서버가 이중 제공에 대한 dishonest 방문자 ID를 찾아낸다 하더라도 이는 허위 ID값이므로 dishonest 방문자의 신분을 확인할 수 없다. 그러나 신분을 확인할 수 없다하더라도 감사기관은 측정값에서 이를 제거할 수는 있다. 다소 프로토콜이 복잡해질 수 있는 점이 있지만 ZKIP를 사용하면 허위 ID값에 의한 blind signature를 방지할 수 있다.

<dishonest 서버 S에 의한 공격>

dishonest 서버 S가 할 수 있는 공격으로 방문자 Ui가 보내지 않은 정보를 무작위로 추가하여 서버가 특정이 완료된 후에 감사기관에 제공하는 경우를 생각해 볼 수 있다. 이는 방문자 Ui가 보낸 정보를 이용하여 추가 정보를 생성하거나 또는 무작위로 추가 정보를 생성할 수 있다. 그러나 서버 S가 이러한 추가 정보를 계산하려고 하면 반드시 감사 기관으로부터의 blind signature 값이 있어야 한다. 따라서 dishonest 서버 S가 이러한 공격에 성공하려면 blind signature를 공격하여야 하며 이는 RSA 암호 알고리즘에 의한 공격과 동일하게 된다.

<dishonest 서버 S와 dishonest 방문자 Ui에 의한 결탁 공격>

방문자 Ui와 서버 S가 서로 결탁하여 방문 측정한 정보 외에 추가적으로 정보를 생성하여 감사 기관에 실지 방문한 정보보다 허위로 추가된 방문 정보를 제공할 수 있다. 그러나 이러한 결탁에 공격은 감사 기관으로부터 blind singature를 받지 않는 정보를 이용하여 생성된 방문 정보들은 모두 감사 기관의 식(1)에 의한 검사에 의하여 모두 부정한 정보로 판단되어 받아들이지 않게 되며 dishonest 서버 S는 감사기관으로부터 신뢰를 잃게 된다.

<방문자의 프라이버시>

기존의 모든 방식들은 방문자가 어떠한 서버 S를 방문하였는지를 쉽게 알 수 있다. 본 제안 방식에서는 방문자가 감사 기관으로부터 blind signature 특성 때문에 감사 기관 또는 감사 기관과 서버가 결탁하여도 방문자가 이용한 랜덤 값들을 알 수 없는 한 방문자의 방문 여부를 알 수가 없다. 물론 방문자가 2회 이상 부정하게 방문한 경우에는 방문자의 ID 정보가 계산되어 프라이버시가 지켜질 수 없게 된다. blind signature가 암호학적으로 안전하다면 방문자의 프라이버시는 유지될 수 있다.

5. 결 론

본 논문에서는 방문자의 프라이버시를 전혀 고려하지 않는 기존의 방식에 비해서 방문자의 프라이버시가 보장되는 안전한 인터넷 광고 방문 측정 방식에 대하여 제안하였다. 방문자의 프라이버시를 보장하기 위하여 방문자와 감사 기관 간에 Blind Signature 방식을 적용하여 정상적인 방문을 한 경우에는 방문자의 프라이버시가 보장되나 방문자가 방문 측정 방식을 방해하거나 동일 방문자가 2회 이상 방문 정보를 보내는 등의 불법 행위를 하는 경우에는 방문자의 신분이 확인되는 방식을 제안하였다. 그러나 프라이버시를 제공하기 위한 기능 추가로 인하여 본 제안 방식은 기존의 방식들에 비하여 방문자나 서버의 계산량이나 전송량이 증가하여 기존 제안 방식들과 비교할 때 효율적이지 못하는 문제점이 존재한다. 프라이버시 기능을 제공하면서도 보다 효율적인 방식 연구는 추가적인 연구를 통하여 계속할 예정이다.

ACKNOWLEDGMENTS

This work was supported by a research grant from Seoul Women's University(2013).

REFERENCES

[1] http://www.overture.co.kr
[2]www.kisa.or.kr/jsp/common/libraryDown.jsp?folder=017284

[3] http://www.ipwatch.co.kr/click-fraud/10-what-is-click-fraud

[4] S,S, Kim, J.Y.Shin and S.K Kim, A Secure and Efficient Metering Scheme for Internet Advertising, Journal of KIISE : Computer Systems and Theory, Vol. 29, No. 3, pp. 153 -160. 2002.

[5] W. Ogata, and K. Kurosawa, Provably Secure Metering Scheme, In Proceedings of ASIACRYPT, 1976, pp. 388-398, 2000.

[6] M.K. Franklin. and D. Malkhi, Auditable Metering with Lightweight Security, Financial Cryptography' 97, 1318, pp. 151-160, 1997.

[7] M. Naor. and B. Pinkas, Secure and Efficient Metering, In Proceedings of EUROCRYPT'98, 1403, pp. 576-590, 1998.

[8] B. Masucci. and D.R. Stinson, Metering Schemes for General Access Structures, ESORICS, 1985, pp. 72-87, 2000.

[9] W.C. Kuo, C.J. Fu, and C.S. Laih, Design a Secure and Practical Metering Scheme, Int'l Conference on Internet Computing, pp. 443-447, 2006.

[10] B.C. Wang, W.S. Juang. and C.L. Lei, A Web Metering Scheme for Fair Advertisement Transactions, Int'l Conference on Information Security and Assurance, pp. 453-456, 2008.

[11] C. Blund, S. Cimato, and B. Masucci, Information Processing Letters, 84, pp. 319-326, 2002.

[12] W. Shin. and R.H. Rhee, A WWW Metering Secure using a Secure Primitive, Proceedings of WISA, pp. 182-191, 2000.

[13] N. Ferguson, single term off-line coins, Proceedings of Eurocrypt, pp. 318-328, 1993.

박 춘 식(Park, Choon Sik)

- 1995년 3월 : 동경공업대학교(공학박사)
- 1982년 12월 : 한국전자통신연구원(책임연구원)
- 2000년 1월 : 국가보안기술연구소(책임연구원)
- 2009년 3월 ~ 현재 : 서울여자대학교 정보보호학과 교수
- 관심분야 : 클라우드컴퓨팅, 개인정보보호, 사이버보안
- E-Mail : csp@swu.ac..kr