웹페이지의 전자서명 핑거프린팅 기법

박수빈, 조동섭
이화여자대학교 컴퓨터공학과

Digital Signature Using Fingerprinting for Web Page

Su-Bin Park, Dong-Sub Cho
Dept of Computer Science Engineering, Ewha Womans University

Abstract - 새로운 유비쿼터스 컴퓨터 환경 하에서 다양한 응용 서비스들은 사용자들의 편의성과 정보의 접근성을 향상시키고 있다. 그러나 정보의 고도화에 따른 역기능이 사회적 문제로 지적되고 있다. 특히 개방형 환경에서의 인가되지 않는 제 3자에 의한 공격은 사용자의 프라이버시 문제뿐만 아니라, 국가적 문제로 대두되고 있다. 따라서 안전한 유비쿼터스 컴퓨팅 환경에서의 사회·경제활동을 위한 정보보호의 연구가 활발히 진행되고 있으며 이 중 전자서명은 개인의 프라이버시 보호뿐만 아니라 사회 경제활동의 근간을 제공할 수 있다.

따라서 본 논문에서는 안전한 유비쿼터스 환경의 구현을 위한 전자서명 핑거프린팅 기법을 제안한다. 제안된 방식은 기존의 전자서명 방식의 제한성을 보완하여 이를 웹 페이지에 적용하고 HTML로 표현된 문서에 대한 안정성 향상을 제공할 수 있다.

1. 서 론

급속한 인터넷의 발전과 사용자의 정보에 대한 욕구의 증대성은 물리적 공간의 발전을 가져왔으며 이와 더불어 가상공간에서의 또다른 사회를 창출하였다. 유비쿼터스 환경은 물리적 공간과 가상공간의 결합으로 새로운 형태의 사이버 사회를 구축하여 유비쿼터스 혁명 시대로 진입하는데 성공하였다.

새로운 유비쿼터스 컴퓨터 환경 하에서 다양한 응용 서비스들은 사용자들의 편의성과 정보의 접근성을 향상시키고 있다 원하던 원하지 않던 공기를 마시듯 네트워크로 연결되고, 사무실이 아닌 어느 곳에서든지 정보교환이 가능하다. 그러나 유비쿼터스 시대와 함께 웹에 대한 의존도가 커져감에 따라 정보의 고도화에 따른 역기능이 사회적 문제로 지적되고 있다. 개인정보나 구매 내역이 기업들 사이에서 상업적인 목적으로 공유되고, 언제 어디서나 접속되는 네트워크는 수많은 감시카메라의 역할을 할지 모른다. 정보 오류, 유출, 해킹, 스팸 등으로 인한 피해는 규모와 파급력 면에서 현재와는 비교도 안 될 정도로 심각해지고 있다. 이런 우려에도 불구하고 현재 정부와 민간 차원에서 준비되는 유비쿼터스 전략은 지나치게 기술과 사업에만 초점이 맞춰져 있다. 자칫 우리 사회를 마비시킬 수도 있는 사이버 역기능 문제에 대해서는 아직 연구가 미흡한 시점이다. 본 논문에서는 이러한 유비쿼터스 컴퓨팅 환경에서의 전자문서의 안정성에 대하여 논한다.

전자문서를 교환하는 과정에서 상대방의 신원과 문서내용의 변조여부가 확인되지 않는 경우에는 사용자 위장의 문제가 있을 수 있으며 스니핑이나 가로채기 공격 등 여러 가지 문제점이 발생할 수도 있다. 따라서 전자상거래에 있어서 전자문서와 관련하여 존재하는 보안상의 위험을 제거하기 위해서는 인증, 무결성, 기밀성, 부인방지의 기능을 가지는 전자서명이라는 안전장치를 필요로 하게 된다. 이는 전자문서, 전자영수증, 대금결제 서명 및 상호인증 등 전자 상거래의 거의 모든 영역에서 주로 사용되는 안전한 상거래와 전자문서 사용에 필수적이 되었다. 본 논문에서는 워터마킹 기술의 한 분야인 핑거프린팅 기법을 이용하여 전자서명을 웹페이지에 적용하여, HTML 문서로 표현된 전자문서의 안정성을 위한 알고리즘을 제안한다.

2장에서는 핑거프린팅과 전자서명 기술의 개요에 대해 기술하고 3장에서는 보다 안전하고 효율적인 HTML 웹 문서 핑거프린팅을 위한 방법을 제안한 뒤 마지막으로 4장에서 결론과 향후 연구방향을 기술한다.

2. 기 술 개 요

본 장에서는 핑거프린팅 기법을 사용한 웹페이지의 전자서명을 위한 기술인 디지털 핑거프린팅(Digital Fingerprinting)과 전자서명(Digital Signature)에 대하여 기술한다.

2.1 디지털 핑거프린팅

핑거프린팅(fingerprinting) 기술은 콘텐츠의 상거래 시 구매자의 정보도 포함하는 핑거프린팅 정보를 콘텐츠에 삽입하여 후에 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 저작권 보호 기술이다. 콘텐츠에 저작권 정보를 삽입할 때 워터마킹 기법을 이용한다. 워터마킹 기술은 디지털 콘텐츠에 원래의 소유주를 표시하는 저작권 정보, 즉 워터마크를 넣어 배포하고 불법복제 후의 콘텐츠에 대해 워터마크를 다시 추출함으로써 원소유주를 증명한다. 따라서 모든 판매된 콘텐츠들은 모두 동일한 워터마크가 삽입되어 있다. 이와는 달리, 핑거프린팅 기법은 판매되는 콘텐츠마다 서로 다른 구매자 정보를 삽입하기 때문에 핑거프린팅 된 콘텐츠는 서로 조금씩 다르게 된다.

2.2 전자서명

컴퓨터 네트워크를 통한 비대면 방식의 전자적 거래는 기존 거래 방식에서 시간적, 공간적 제약의 문제점을 해결해줌으로써 새로운 거래 문화로서 자리 잡아 가고 있다. 그러나 전자적 거래는 많은 순기능이 있음에도 불구하고, 사용자에게 역기능을 제공할 수 있다는 문제점 때문에 보안 요구사항이 선결되어야만 전자적 거래의 활성화를 기대할 수 있을 것이다. 정보보호 역기능을 방지하기 위하여 필요한 대표적인 정보보호 서비스는 <표 1>과 같다. 전자서명은 상기의 보안 요구사항 중 인증, 무결성, 부인방지에 대한 보안 기능을 제공해 주며, 이것은 결국 비대면 방식의 전자적 거래 환경 구축 시 전자서명 기술이 필요하다는 것을 의미하는 것이다.

<표 1> 정보보호 서비스

기능	내용
인증 (Authentication)	어떠한 행위 또는 문서의 성립·기재가 정당한 절차로 이루어졌음을 공적 기관이 증명
무결성 (Integrity)	메시지의 진정성 확인
기밀성 (Confidentiality)	인가된 사용자가 아닌 경우 메시지 확인 불가
부인방지 (Non-repudiation)	메시지의 송수신이나 교환 후 교환 사실 부인 시 그 사실을 증명함으로써 사실 부인을 방지

3. 제 안 방 식

본 장에서는 핑거프린팅 기법을 사용한 웹페이지의 전자서명의 동작원리에 대해 논하고 웹 페이지에 정보를 삽입하는 알고리즘을 제안한다.

3.1 시나리오

유비쿼터스 컴퓨팅 환경에서 사용자가 생성한 정보가 비인가된 제 3자에 의해 불법적인 침해에 대해 안전성을 제공받고자한다. 따라서 본 논문에서는 일반적인 웹 환경에서 핑거프린팅 기법을 웹 문서에 적용시키는 기능을 서버에 추가하여 기존의 전자상거래나 인터넷뱅킹 등에 적용하던 전자서명 기법을 이용하였다. 특히 웹페이지에 전자서명을 첨부하여 웹 페이지 작성자가 전자문서를 작성하였다는 사실과 작성내용이 송·수신과정에서 위조·변조되지 않았다는 사실을 증명하고, 작성자가 웹페이지 작성 사실에 대해 부인봉쇄 서비스를 제공받도록 하였다.

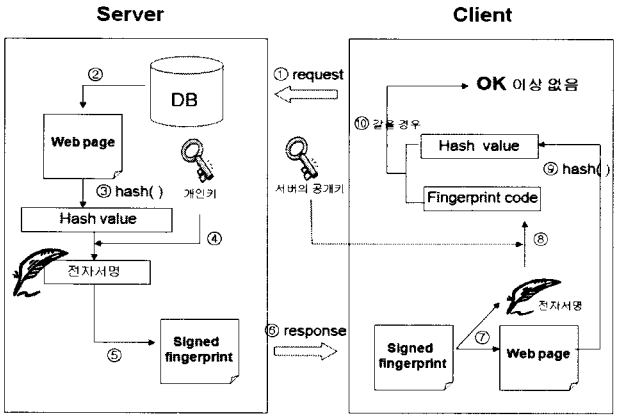
<표 2> 구현 환경

	장비	사양
Web Server	Web server	HttpSvr Version 2.0
	OS	Microsoft Windows XP Professional Version 2002 Service Pack 2
	CPU	Intel Pentium 4 CPU 3.20GHz
	RAM	504MB
Client	OS	Microsoft Windows XP Professional Version 2002 Service Pack 2
	CPU	Intel Pentium 4 CPU 3.20GHz
	RAM	504MB

본 시스템의 구현 환경은 위의 <표 2>와 같다. 미니 웹서버 HttpSvr Version 2.0에 기능을 추가하여 구현되었다. 대부분의 웹 서버와 마찬가지로 HttpSvr Version 2.0의 언어는 C++인데 이는 웹 페이지에 주로 사용되는 언어인 HTML과는 다른 특징을 가지고 있다. HTML 문서의 소스는

대·소문자의 구분이 없다. 또한 공백문자는 인정하지 않고 태그로만 인식된다. 이와는 반대로 C++로 이루어진 서버의 경우 대·소문자를 구별할 뿐만 아니라 공백문자를 인식한다. 본 논문에서는 이 차이점을 이용한 삽입 알고리즘을 제안한다.

3.2 웹페이지 전자서명



<그림 1> 웹 페이지 전자서명 프로세스

위의 (그림 1)의 처리과정은 다음과 같다.

- Server측 -
  ① 사용자는 서버에 특정 웹 페이지를 요청한다.
  ② 서버는 DB에 저장되어 있는 웹 페이지를 찾아온다.
  ③ 사용자에게 전송할 특정 웹 페이지의 소스코드를 기반으로 해쉬하여 해쉬 값을 생성한다.
  ④ 생성된 해쉬 값을 서버의 개인키를 사용하여 서명한다.
  ⑤ 암호화된 코드(서명 값)를 웹 페이지에 첨부한다.
  ⑥ 사용자에게 서명된 웹페이지를 전달한다.

- Client측 -
  ⑦ 받은 웹 페이지에서 전자서명과 본래의 웹페이지를 분리한다.
  ⑧ 서버의 공개키를 이용, 전자서명을 복호화하여 해쉬 값(1)을 얻는다.
  ⑨ 분리된 본래의 웹페이지를 해쉬하여 해쉬 값(2)을 얻는다.
  ⑩ 해쉬 값(1)과 해쉬 값(2)를 비교하여 같을 경우 웹페이지에 제 3자의 관여 없이 제대로 전달받았음을 확인한다.

서버는 전자서명 삽입을 위하여 사용자의 요청을 받은 후 요청받은 웹 페이지를 사용자에게 전달하기 전 단계에서 서명을 실행한다. 전처리과정으로 웹 페이지의 '=' 문자 좌우의 공백을 제거한 후 해쉬하여 해쉬 값을 얻는다. 이 때 얻은 해쉬 값은 그 페이지 고유의 값으로 하나의 웹 페이지는 다른 사용자가 접속했을 때에도 같은 해쉬 값을 갖지만 각각의 웹 페이지마다 가지는 해쉬 값은 모두 다르게 나타난다. 이렇게 해쉬되어 나타난 메시지 요약(Message Digest)은 서명자 즉 웹페이지 작성자의 공개키로 암호화되고 암호화된 코드는 이진수로 변환되어 웹 문서에 첨부된다. 이 때 전자서명이 된 사실을 비가시적으로 핑거프린팅 기법을 사용하여 웹 페이지에 첨부를 해주기 위해서(그림 1의 ⑤) 사용자에게 전송할 웹문서의 HTML 소스 코드에서 제일 처음 읽어 들인 '='부터 순차적으로 2자리씩 삽입하여준다. 이 때 이용될 수 있는 본 논문에서는 공백 삽입 시 별다른 영향이 없고, 등장 빈도수가 높은 문자인 '=' 문자를 사용하였는데 이 외에도 다른 문자를 택할 수 있다. 여기서 사용된 공백의 유무에 따른 두 자리의 이진수를 표현하는 코드는 다음에 제시된 <표 3>과 같다.

<표 3> 표현코드에 따른 소스코드

소스코드	00	01	10	11
표현코드	A=B	A= B	A =B	A = B

다음 코드를 삽입하기 전처리 과정으로 기존의 웹문서에서 '=' 양쪽의 공백을 제거 후 코드에 따른 공백의 삽입을 해주어야한다. 그 후 변환된 이진수를 웹 페이지 소스코드의 맨 위에서부터 '='을 만날 경우 공백을 삽입한다. 이 때 유의할 점은 수식의 '='은 포함시키지 않아야한다는 것이다. '!=' 나 '==', '>=', '<='와 같은 경우에는 공백문자를 포함시키는 경우 제대로 동작하지 않으므로 위와 같은 문자열을 만날 경우에는 코드 삽입을 수행하지 않고 넘어가는 알고리즘을 추가한다(그림 2).

```
InsertInform(signature)
        read HTML source sequentially
            while (uninserting signature exists)
                find character '='
                then check before and after char
                                    //서명 삽입 전처리과정
                if that is '<', '>', '!' of '='
                    skip        // 수식의 '='은 pass
                else if that is ' '
                    delete      // 공백문자 제거
                else
                    switch(signature)   // 공백문자 삽입
                        case 00:
                            break
                        case 01:
                            insert ' ' right of '='
                            break
                        case 10:
                            insert ' ' left of '='
                            break
                        case 11:
                            insert ' ' both side of '='
                            break
        return
```

<그림 2> 웹페이지 전자서명 삽입 알고리즘

이렇게 변환된 웹 페이지는 최종적으로 사용자에게 전송된다. 사용자는 변환 전 웹 페이지와 같은 화면의 웹 페이지를 받아볼 수 있고 전자서명의 확인을 필요로 할 경우 변환된 코드를 추출하여 복호화한 후 기존의 해쉬 코드와 비교하여 알 수 있다.

3.3 시스템 요약 및 활용방안

웹페이지 전자서명은 서버 상에서 전자서명을 코드로 변환, 웹 페이지에 추가하여 주는 방식으로 모델링하여 향후 웹페이지의 거래 내용의 변경 여부확인과 작성자의 부인방지 기능을 확보할 수 있다. 필요 시 전자서명 코드를 복호화하여 기존 웹 페이지의 해쉬 값과 비교함으로써 메시지의 무결성을 확인할 수 있고, 작성자가 메시지 전달 사실을 부인할 시 서버는 전자서명된 웹 페이지에서 서버의 개인키를 추출, 증명함으로써 부인방지 기능을 확보할 수 있게되는 것이다. 웹 서버의 발전과 함께 서버의 부하는 커다란 문제가 되지 않게 되었으므로 진정성이 필요한 웹 페이지의 경우 이 시스템은 기존에서의 웹 페이지에서 확인하지 못한 것들을 확인할 수 있다. 웹 페이지에 제 3자의 개입이 있어 페이지의 변화가 있었는지 무결성을 확인할 수 있고 서버의 서명이 찍혀있기 때문에 페이지를 작성한 사실이 없다고 부인할 경우 서버의 공개키를 통한 서명의 복호화로 부인방지 기능을 할 수도 있다.

4. 결 론

지금까지 웹 페이지에 전자서명을 첨부하는 방법에 대하여 살펴보았다. 수신자 확인이나 서명의 진정성, 무결성, 기밀성 및 부인방지 기능을 확보할 수 있는 전자서명을 공개키 기반 방식으로 암호화한 후 웹 페이지 안에 공백의 유무에 따른 코드의 할당으로 핑거프린팅 하여 웹 페이지의 내용에 따른 도장과도 같은 역할을 하는 두 가지 기술이 삽입되어 기존의 웹 페이지보다 좀 더 신뢰성 높은 웹 페이지를 받도록 하였다.

기존의 전자서명은 공인인증서를 통해 인증기관에서 인증하는 방식으로 쓰였다면 이 방식은 검증방법을 좀 더 간략화하여 평문의 무결성에 초점을 두어 구현하였다. 웹 페이지의 전자서명은 암호화 시간의 단축과 가정 사항으로 두었던 키 관리 문제 등 기술적으로 더욱 안정적인 개발이 필요하다.

[참 고 문 헌]

[1] J. Camenish, "Efficient anonymous fingerprinting with group signature," Asisacrypt 2000, LNCS 1976, pp. 415-428, 2000.
[2] R. Wagner, "Fingerprinting," IEEE Symposium on Security and Privacy, Oakland, pp. 18-22, 1983
[3] R. Wagner, "Fingerprinting," IEEE Symposium on Security and Privacy, Oakland, pp. 18-22, 1983.
[4] S. Katzenveisser and F. Petitcolas, Information Hiding, "Techniques for steganography and digital watermarking," Artech House, 2000.
[5] American Bar Association, "Digital Signature Guidelines : Legal Infrastructure for Certification Authorities and Secure Electronic Commerce", August 1, 1996.