情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

프라이버시 보호를 위한 익명성 및 익명성 제어 모델 분석

박 해 룡*, 김 지 연*, 천 동 현*, 전 길 수*, 이 재 일*

요 약

인터넷의 급속한 발전과 유비쿼터스 컴퓨팅 능력이 발전됨에 따라 이러한 정보 인프라에서의 프라이버시 보호에 대한 요구가 더욱 증가하고 있다. 프라이버시 보호를 위한 핵심 기술로서 익명성 기술이 사용하고 있으며, 익명성 기술의 역기능을 방지하기 위해서 익명성 제어 기술을 사용하고 있다. 국외에서는 이미 익명성 및 익명성 제어 기술을 다양한 분야에서 연구·적용하고 있으나 국내에서는 전자투표 시스템 이외의 분야에서는 연구가 미진한 실정이다. 이에 본고에서는 국외 익명성 및 익명성 제어 모델인 익명 이메일 시스템, 익명 출판 시스템, 전자투표 시스템 및 익명 브라우징 시스템을 소개하고 분석하였다. 또한, 각 시스템별로 시스템 구성객체, 익명성 제공과 관련 없는 요구사항, 익명성 제공 서비스의 요구사항, 익명성 제어 서비스를 위한 요구사항을 기술하여 국내 익명성 및 익명성 제어 시스템 개발에 도움이 되고자 한다.

Ⅰ. 서 론

인터넷의 급속한 발전과 유비쿼터스 컴퓨팅 능력이 발전됨에 따라 이러한 정보 인프라에서의 프라이버시 보호에 대한 요구가 더욱 증가하고 있다. 프라이버시 보호를 위한 핵심 기술로서 익명성 기술이 사용되고 있다. 익명성(Anonymity)이란 특정 집단에 있는 사람들 중에서 어떤 구성원이 특정한 행위를 한 것에 대해 다른 구성원들이 특정한 행위를 한 구성원이 누구인지 모르게 하는 성질을 의미한다. 익명성에는 저자의 영속적인 익명성, 위치의 영속적인 익명성, 저자의 일회용 익명성, 위치의 일회용 익명성 등이 있다. 다음은 각각의 익명성에 대해서 설명하고 있다.

- 저자의 영속적인 익명성 : 저자가 문서나 글을 작성할 때 동일한 가명을 사용하므로, 다른 사람들은 동일한 가명을 사용하여 작성된 문서나 글이 서로 연관성이 있음을 인지할 수 있다.
- 위치의 영속적인 익명성 : 이용자가 익명 위치나 서버에서 여러 개의 문서나 글을 검색하기 원할 때 해당 문서나 글을 동일한 위치탐색장치를 이용해서 검색할 수 있다.
- 저자의 일회용 익명성 : 저자가 문서나 글을 작성할 때 다른 가명을 사용하므로, 다른 사람들은 저자가 동일한 문서나 글을 보고 동일한 저자가 작성했는지 판단할 수 없다.
- 위치의 일회용 익명성 : 이용자가 익명 위치나 서버에서 여러 개의 문서나 글을 검색하기 원할 때 해당 문서나 글을 다른 위치탐색장치를 이용해서 검색하도록 하여 각각의 문서나 글이 서로 다른 위치나 서버에 있는 것처럼 할 수 있다.

하지만, 익명성 기술의 남용은 역기능을 유발할 수 있으며, 익명성 기술의 역기능을 방지하기 위해서 익명성 제어 기술을 사용하고 있다. 국외에서는 이미 익명성 및 익명성 제어 기술을 다양한 분야에서 연구·적용하고 있으나 국내에서는 전자투표 시스템 이외의 분야에서는 연구가 미진한 실정이다. 이에 본고에서는 국외 익명성 및 익명성 제어 모델인 익명 이메일 시스템, 익명 출판 시스템, 전자투표 시스템 및 익명 브라우징 시스템을 소개하고 분석하였다. 또한, 각 시스템별로 시스템 구성객체, 익명성 제공과 관련 없는 요구사항, 익명성 제공 서비스

* 한국정보보호진흥원({hrpark, jykim, dhcheon, kschun, jilee}@kisa.or.kr)

의 요구사항, 익명성 제어 서비스를 위한 요구사항을 기술하여 국내 익명성 및 익명성 제어 시스템 개발에 도움이 되고자 한다.

II. 익명성 및 익명성 제어 모델

1. 익명 이메일 시스템(Anonymous e-mail)

익명 이메일 시스템을 사용자는 자신의 신원을 드러내지 않고 메시지를 전송할 수 있어야 한다. 또한, 응답자는 그 메시지의 송신자의 신원을 모르는 상태에서 해당 사용자에게 회신을 보낼 수 있어야 한다. 메일 시스템은 다음과 같이 3가지 단계로 구성된다.

- 등록 단계(선택) : 익명 이메일 시스템에서 사용자는 해당 시스템을 이용하기 전에 등록 단계를 수행해야 한다. 이러한 등록 단계에서, 사용자는 시스템에 접근할 수 있는 토큰(패스워드, 증명서 등)을 수신한 후, 시스템 이용시(예: 전송단계) 수신한 접근 토큰의 소유를 증명해야 한다.
- 전송 단계 : 사용자는 수신자에게 이메일을 전송한다. 익명 이메일 시스템에서 송시자의 신원은 수신자에게는 숨겨진다. 전송단계에서 사용자는 유효한 토큰을 제시 (또는 소유 여부를 증명)를 요구받을 수도 있고 요구받지 않을 수도 있다. 또한 이 단계에서 시스템 (또는 신뢰 객체)은 메시지 송신자의 실제 신원을 알아낼 수도 있고 그렇지 않을 수도 있게 설계할 수 있다.
- 회신 단계(선택) : 이 단계에서 수신자는 메시지 송신자의 신원을 모르고 메일을 회신한다. 원래 메시지에는 시스템이 메시지를 해당 송신자에게 전달할 수 있도록 충분한 정보를 포함해야 한다.

1.1 역할 및 객체

익명 이메일 시스템의 역할 및 객체에 대해서는 두 부분으로 구분하여 설명하도록 한다. 첫 번째 부분에서는 익명성을 고려하지 않은 이메일 응용 구성객체들에 대해 설명하고, 두 번째 부분에서는 이메일 응용에 익명성을 고려하는 경우에 추가되는 객체들에 대해 논의하도록 한다.

1.1.1 일반적인 이메일 시스템의 구성객체

일반적인 이메일 시스템의 구성객체는 송신자의 메일 클라이언트, 송신자의 메일 서버, 수신자의 메일 클라이언트로 구성된다. 다음은 각각의 구성객체에 대한 설명이다.

- 송신자의 메일 클라이언트: 사용자(송신자)는 이메일 메시지를 작성하고 "전송(send)" 버튼을 누른다. 메일 클라이언트는 이메일 메시지를 특정 포맷으로 변환하고 그것을 클라이언트쪽의 메일 서버로 전송함으로써 메시지를 핸들링한다. 변경된 메시지는 메시지의 내용, 송신자의 이메일 주소, 수신자의 이메일 주소 등으로 구성된다. 결국, 메일 클라이언트는 메시지의 물리적 송신자와 매우 관련 있는 이메일 시스템의 구성요소이다. 다시 말하면, 메일 클라이언트는 메시지의 개시자이다. 수신자가 해당 메시지에 대해 회신을 할 때, 송신자측은 수신자가 된다.
- 송신자의 메일 서버 : 메일 서버는 이메일 메시지를 네트워크를 통해 메시지 수신자의 메일 서버로 전송하는 역할을 수행한다. 이러한 메일 서버는 메시지의 실제 송신자가 된다. 이것은 회신 메시지의 수신자이기도 하다.
- 수신자의 메일 서버 : 메일 서버는 이메일 메시지를 네트워크를 통해 메시지 송신자의 메일 서버로부터 수신하는 역할을 수행한다. 이러한 메일서버는 사용자(수신자)의 메일 클라이언트가 요청할 때까지 이메일을 보관·관리한다. 이러한 메일 서버는 회신의 송신자가 된다.
- 수신자의 메일 클라이언트: 사용자(수신자)는 자신의 이메일을 읽고 싶을 때 응용 프로그램을 가동한다. 메일 클라이언트는 수신자의 메일 서버에 연결하여 이메일 메시지를 검색해서 가지고 온다. 수신자는 특정 메시지에 대해 회신할 수도 있다. 사용자가 자신의 이메일을 읽었을 때, 메일 클라이언트는 수동상태로 있다. 사용자가 특정 메시지에 대해 회신하고자 할 때, 메일 클라이언트는 원래 메시지의 응답자로 행동한다. 결국, 메일 클라이언트는 회신 메시지의 개시자가 된다.

1.1.2 익명 이메일 시스템의 구성객체

익명 이메일 시스템의 구성객체는 송신자의 메일 클라이언트, 중앙 재우송자, 재우송자의 체인으로 구성된다. 다음은 각각의 구성객체에 대한 설명이다.

- 송신자의 메일 클라이언트 : 앞에서 언급하였듯이 메일 클라이언트는 메일 서버에 메시지를 개시한다. 익명 메일 환경에서는 메일 클라이언트 기능은 어느 정도의 익명성과 프라이버시를 제공하도록 확장된다. 이 경우, 메일 클라이언트 역시 익명성 기능을 갖는다. 익명 서비스의 목적은 개시자가 수신자에게

익명으로 남고 전송되는 동안 개시자와 수신자를 연결할 수 없도록 하는 것이다.

- 중앙 재우송자 : 익명 메일 시스템에서 이메일은, 익명성 기능을 제공하고 수신자의 메일 서버에 이메일을 전송할 수 있는 충분한 정보를 갖는 중앙의 재우송자에게 전송될 수 있다. 중앙의 재우송자는 메시지의 개시자와 수신자를 연결할 수 있다. 이러한 재우송자는 정보를 갖는 제공자라 한다.
- 재우송자의 체인 : 또다른 선택으로 이메일을 재우송자의 체인에 전송하는 것이다. 체인의 각 재우송자는 메시지를 다음의 재우송자에게 전송한다. 메시지의 개시자는 첫 번째 재우송자만이 알 수 있고 체인의 마지막 재우송자만 이메일의 수신자를 안다. 이렇게 함으로써 개시자와 수신자는 서로 연결될 수 있다. 이러한 스킴에서 각 재우송자는 정보를 갖지 않는 제공자로 생각한다.

1.2 익명성 제공 및 익명성 제어 서비스를 위한 시스템의 요구사항 및 특성

1.2.1 익명성 제공과 관련 없는 요구사항

- 양방향 통신(선택) : 이메일 시스템에서 메시지 수신자는 해당 메시지에 대해 회신하도록 요구 받을 수도 있다. 이것은 익명 이메일 시스템에 대해서도 마찬가지이다. 익명 이메일 메시지는 충분한 정보를 (신뢰하는 헤더 필드에) 포함할 필요가 있다. 그래서 메일 시스템이 회신 메시지를 원 메시지의 개시자에게 전송할 수 있다. 이것은 수신자에게 송신자의 실제 신원을 알리지 않고 구현되어야 한다. 비록 이러한 요구사항이 이상적이긴 하나 모든 기존의 시스템은 양방향이 아니다. 단방향 메일 시스템은 긴급 통신선을 통한 익명 보고의 목적으로 이용될 수도 있다.
- 실시간이 아님 : 이메일은 실시간 응용이 아니다. 익명 이메일 시스템은 익명성 서비스를 구현했을 때 이러한 특성으로부터 장점을 가질 수 있다. 예를 들어, 재우송자는 메시지를 전송하는 것을 지연시켜 도청자가 타이밍 공격(timing attack)을 통해 입력되는 메시지와 출력되는 메시지를 연결할 수 없도록 할 수 있다. 결국, 글로벌 도청자는 개시자로부터 수신자로의 경로를 알수 없게 된다.

1.2.2 익명성 제공 서비스를 위한 요구사항

- **일회용 익명성 (One time anonymity)** : 수신자 및 공격자에 대해, 개시자의 일회용 익명성 보장은 이메일 응용에서 매우 유용하다. 특히, 긴급 통신선을 통한 사용자가 범죄나 피해를 보고하는 응용에서 사용자는 자신의 이메일의 연속적인 사용이 연결되지 않는 것을 선호한다.
- **영속적인 익명성 (Persistent anonymity)** : 익명성을 갖는 개시자는 각 메시지에 대해 동일한 가명을 사용한다. 그러므로 동일 개시자에 의해 전송된 모든 이메일 메시지는 연결된다. 이 특성은 수신자가 여러 개의 다른 메시지로부터 정보를 모아 전체적인 상황을 파악할 필요가 있는 경우(예: 사용자/환자 컨설팅 등)에 좋다. 익명성을 갖는 수신자는 만약 그 수신자가 특별한 서비스의 제공자라면 영속적인 가명을 사용할 것이다. 이러한 가명은 업종별 번호란(yellow pages)에 기록될 것이다.
- **회신 익명성 (Reply anonymity)** : 만약 수신자가 익명 메시지에 대해 응답을 할 수 있기를 원한다면, 메시지에 충분한 정보(예: 신뢰 헤더 필드에)가 포함되도록 하여, 수신자가 회신 메시지를 원 메시지의 개시자에게 전송할 수 있도록 할 필요가 있다.

1.2.3 익명성 제어 서비스를 위한 요구사항

익명 이메일 시스템에서의 익명성 제어는 스팸과 같은 메일시스템의 오·남용을 방지하고 심각한 범죄 발생시 사용자(개시자 또는 수신자)의 익명성을 취소하는 데 유용하다.

1.2.3.1 무조건적인 익명성 제어

- **접근 제어** : 접근제어는 개시자가 등록 단계에서 획득한 유효한 접근 토큰을 제시(또는 소유를 증명)해야만 하는 경우 가능하다. 즉, 유효한 토큰이 없는 사용자 또는 토큰이 무효화된 사용자는 더 이상 시스템을 이용할 수 없도록 한다.
- **특정 조건에 해당하는 이메일 메시지 전송을 막음 (Block sending e-mail messages)**
  - 수신자의 주소에 기반 : 수신자는 자신에게로 전송되는 모든 익명 이메일 메시지를 막아달라고 요청할 수 있다.
  - 시스템 용도에 기반 : 임의의 시간 간격동안 동일한 메시지가 전송될 수 있는 횟수의 최대치를 셋팅함으로써, 개시자가 스팸 메일을 전송하는 것을 방지할 수 있다. 또한 시스템은 개시자가 전송할 수 있는 볼륨(메시지의 개수 또는 메시지의 총 크기)을 제한할 수 있다.

1.2.3.2 사용자 제어의 조건적 익명성

- **이메일시스템의 과용 방지(Discourage overuse of the mail system)**: 이메일 시스템은 사용자가 전송할 수 있는 이메일 메시지의 최대 수를 설정한다. 만약 사용자가 해당 최대치를 초과하면, 해당 사용자의 신원이 드러나도록 설계한다. 이러한 제어를 위해서는 등록 단계가 필요하며 등록단계에서 시스템은 사용자에게 제한된 수만큼만 사용될 수 있는 증명서를 제공한다. 증명서의 연속적인 사용이 불연결성을 보장한다 할지라도 설정된 수 이상의 사용하면 시스템에게 송신자의 신원을 알 수 있도록 하는 충분한 정보가 제공된다. 결국, 사용자가 시스템을 남용할 때, 익명성 취소가 가능하도록 한다.

1.2.3.3 신뢰 객체 제어의 조건적 익명성

익명 이메일 시스템에서 신뢰객체의 도움을 받을 경우 이메일 메시지의 개시자 또는 수신자의 신원을 취소할 수 있도록 할 수 있다.

- **익명 송신자의 신원 확인(Revealing the identity of an anonymous originator)** : 만약 개시자가 불법적인 문서를 전송하거나 수신자를 괴롭히거나 또는 다른 불법적인 행위를 수행하는 혐의가 발견되는 경우 유용하다.
- **익명 수신자의 신원 확인(Revealing the identity of an anonymous recipient)** : 수신자가 범죄에의 공범자인 혐의가 있을 경우 유용하다.

1.3. 기술 동향

현재의 익명 이메일 시스템에는 익명성 제어 메커니즘이 탑재되어 있지 않으나, 제어 메커니즘을 추가하는 작업은 그리 어려운 일이 아니라고 학계에서는 판단하고 있다.

1.3.1 Type 0 Re-mailer : Penet

Type 0 Re-mailer 시스템[1] 에서 개시자는 중앙의 재우송자에게 메시지를 전송한다. 재우송자는 개시자의 신원을 없애고 그 자리에 일회용 신원 또는 가명을 놓는다. 그러고 난 후, 재우송자는 메시지를 수신자에게 메시지를 전송한다. 그러나 중앙 재우송자에 대한 공격은 전체 시스템의 안전성을 위협한다. 그래서 중앙의 재우송자는 신뢰 객체여야 한다. 중앙 재우송자는 개시자의 익명성을 제어하고 필요시 익명성을 취소할 수 있다. 중앙의 재우송자는 필요하지 않을 때 개시자의 익명성을 취소하지 않을 것이라고 신뢰한다.

penet.fi 사이트를 운영했던 Johan Helsingius는 한 고객이 교회의 비밀을 네트워크상에 올린 것을 교회측이 사이트에 항의를 했고 핀란드 법정이 그에게 고객의 이메일 주소를 알려주라고 종용하자 그는 사이트를 폐쇄했다. 현재 사이트는 폐쇄된 상태이다.

1.3.2 Type 1 Re-mailer : CypherPunk

이메일의 개시자는 암호화된 메시지의 집합을 생성한다[2,3]. 각 계층에서 암호화된 메시지는 일련의 명령(instruction)과 또 다른 암호화된 메시지로 구성된다. 체인의 각 재우송자는 우선 메시지를 복호화해서 명령어를 수행한 후, 다음 재우송자에게 메시지를 전송한다. 수신한 메시지를 복호화하면 다음 재우송자를 알 수 있다. 각 재우송자는 암호화의 하나의 계층만을 제거하기 때문에 지역 도청자 또는 체인의 재우송자는 개시자와 수신자를 연결할 수 없다.

재우송자들은 서로 협력하지 않는다고 신뢰하지만, 만약 그렇지 않다면 통신 객체의 신원이 드러난다.

1.3.3 Type 2 Re-mailer : MixMaster

Type 2 재우송자 시스템[2,3] 은 주로 Type 1 재우송자 시스템과 동일한 구성요소로 구성된다. 게다가 Type 2 재우송자 시스템은 글로벌 도청자에 의한 공격에 대한 대응 기술을 제공한다. 이러한 기술은 각 홉에서 메시지를 재배열하는 것이다. CypherPunk에서와 마찬가지로 재우송자들은 서로 협력하지 않는다고 신뢰한다.

1.3.4 Type 3 Remailer : MixMinion

Mixminion[4] 은 안전한 단일 사용의 회신 블록(secure single-use reply blocks)을 갖는 메시지 기반의 익명 재우송자 프로토콜이다. 믹스 노드는 Mixminion 전송 메시지와 회신 메시지를 구분할 수 없어서 전송과 회신 메시지가 같은 익명 집합을 공유해야 한다. 이 재우송자 시스템에서는 사용자가 참여하는 재우송자의 공개키와 성능을 알 수 있도록 디렉토리 서버를 추가해야 한다. 또한, 프리미티브로 단일 사용의 회신 블록을 이용하는 긴 주기동안의 가명을 제공하는 nymservers를 기술하고 있으며, 전송 익명성을 제공하기 위해 재우송자간의 링크 암호화를 수행하도록 설계하고 있다. CypherPunk에서와 마찬가지로 재우송자들이 서로 협력하지 않는다고 신뢰한다.

2. 익명 출판 시스템

출판 시스템의 목적은 사용자가 문서를 출판할 수 있도록 하는 것이다. 출판 시스템에서 문서는 하나 이상의 서버에 저장되며 사용자가 나중에 이러한 문서들을 검색할 수 있도록 한다. 출판 시스템은 다음과 같이 3가지 단계로 구성된다.

- 등록 단계(선택) : 등록 단계에서 사용자는 출판 시스템에 대한 접근권한을 획득할 수 있다. 예를 들어, 사용자는 출판시스템을 오용하지 않겠다는 계약서에 서명을 한 후 문서를 출판할 수 있는 증명서를 획득한다. 이 단계는 선택사항이다.
- 출판 단계 : 출판 단계에서 출판자는 시스템에 익명으로 문서를 저장한다. 익명 문서가 불법적이거나 누군가를 위협하는 것이라면 익명성을 제어하는 단계가 필요하다.
- 검색 단계 : 검색 단계에서 사용자는 문서를 검색하기를 원한다. 이 단계는 웹 브라우징 단계와 매우 관련이 있다.

익명 브라우징과 대등한 익명 출판에 대해 초점을 둔다. 즉, 본 절에서는 익명성 관점에서 문서가 저장되어 있는 서버의 신원/위치를 숨기는 문제를 주로 살펴볼 것이다. 검열에 견디는 출판(censorship-resistant publishing)은 두 번째 중요한 사항이다. 문서는 여러 서버들로 분산·저장되기 때문에 (단일) 서버의 신원/위치를 숨기는 것은 본 절에서 설명과는 연관성이 적다.

2.1 역할 및 객체

2.1.1 일반적인 출판 시스템의 구성객체

- 출판자(Publisher) : 출판자는 하나 이상의 서버에 문서를 온라인으로 출판한다. 출판자는 출판 시스템의 첫 번째 단계의 개시자이다.
- 클라이언트 검색 응용(Client retrieval application) : 특정 사용자가 온라인 문서를 참고하려고 할 때, 사용자는 자신의 검색 응용에서 위치를 입력한다. 응용(예, 웹 브라우저 응용)은 해당 요청을 받아들여 문서를 다운로드받을 수 있는 서버와 연결한다. 요청의 결과로 클라이언트 응용은 요구된 문서를 수신하고 그것을 스크린에 보여준다. 결국, 클라이언트 응용은 요청의 개시자이며 송신자이다.
- 서버(Server(s)) : 문서를 보관·저장하는 서버들이다. 서버들은 출판 요청의 수신자이다. 게다가 검색요청의 수신자이기도 하다. 검색요청에 대해 서버는 원하는 문서를 보내준다.

2.1.2 익명 웹 출판 시스템의 구성객체

- 출판자(Publisher) : 출판자는 다른 서버에 자신의 문서를 출판할 때, 출판자는 익명으로 남기를 원한다. 그러므로 출판자의 요청은 익명 요청으로 전환되어야 한다. 예를 들어, 출판자는 익명 이메일 메시지에 문서를 포함해서 출판 서버에게 전송할 수 있다.
- 위치 제공자(Location provider) : 위치 제공자는 "nested 암호화된 위치"와 해당 "nested 암호화된 위치"로부터 요청될 수 있는 문서의 스펙을 함께 공개한다. 이러한 위치 탐색 장치(locator)는 충분한 정보를 포함하여 올바른 서버와 연결되도록 할 수 있으나, 개시자가 정보로부터 해당 서버를 알아내는 것은 불가능하도록 한다. 즉, 서버와 바로 연결되지 않고, rewebber 네트워크 내의 임의의 rewebber에게 위치가 보내진다. 위치 제공자는 단지 공개 데이터베이스일 뿐이기 때문에 정보를 갖지 않는 제공자이다.
- rewebber의 체인(Chain of rewebbers) : 공개된 nested 암호화된 위치 탐색 장치는 체인의 첫 번째 rewebber를 포함한다. 요청은 이 첫번째 rewebber에게 전송된다. 이 rewebber가 nested 암호화된 위치탐색장치의 첫 번째 계층을 없애면 두 번째 rewebber가 나타난다. 요청은 두 번째 rewebber에게 보내진다. 이 과정은 요청이 체인의 마지막 rewebber에게 전달될 때까지 계속된다. 마지막 rewebber는 문서가 저장된 서버의 위치를 알지만 원래 요청의 전송자는 누구인지 모른다. 결국 네트워크의 rewebber 역시 정보를 갖지 않는 제공자이다.

본 절에서는 문서가 단일 위치에 저장되면서 익명을 유지하는 시스템에 초점을 둔다. 검열에 견디는 출판 시스템을 위해서 문서는 여러 서버로 분산/저장된다. 이러한 시스템에 문서가 일단 출판되면 서버에서 문서를 제거하는 것이 매우 어렵거나 불가능하다. 그러나 문서 자체가 저자의 신원을 드러내지 않기 때문에 서버의 익명성은 덜 중요하다고 할 수 있다.

2.2 익명성 제공 및 익명성 제어 서비스를 위한 시스템의 요구사항 및 특성

2.2.1 익명성 제공 서비스를 위한 요구사항

- **영속적인 익명성(Persistent anonymity)**
  - 출판자(저자)의 영속적인 익명성 : 출판자는 다른

문서를 출판하기 위해 동일한 가명을 사용하므로 동일한 출판자가 출판한 문서는 서로 연결성을 갖는다.

- 서버(위치)의 영속적인 익명성 : 이 경우 같은 서버의 문서는 연결될 수 있다. 같은 익명 서버에서 여러 개의 문서를 검색하길 원하는 사람은 해당 문서를 검색하기 위해 동일한 위치탐색장치를 이용할 수 있다.

· 일회용 익명성(One time anonymity)

- 출판자(저자)의 일회용 익명성 : 이 경우 동일한 출판자의 문서가 서로 연결되지 않는다. 만약 사용자가 자신의 다양한 관심 분야에 관해 여러 개의 문서를 출판할 경우 유용하다. 만약 외부자(outsider)가 이러한 주제들을 연결할 수 있다면 이것은 출판자의 신원을 위협하게 될 것이다.
- 서버(위치)의 일회용 익명성 : 동일한 서버의 각 문서에 대해 다른 위치탐색장치를 사용하도록 하여 해당 서버의 여러 문서에 대한 위치를 서로 연결할 수 없도록 한다. 이것은 경우에 따라 유용할 수 있다. 만약 임의의 서버에 저장된 문서가 불법이라면 해당 문서의 위치탐색장치만을 이용하지 못하도록 할 수 있다. 해당 서버의 다른 문서는 여전히 탐색될 수 있도록 할 수 있다.

2.2.2 익명성 제어 서비스를 위한 요구사항

출판자는 익명 출판 시스템을 오용하여 불법 문서나 잘못된 정보를 출판할 수 있다. 익명성 제어는 매우 유용한 기법으로 익명성 제어를 위해 다음을 수행한다.

- 문서의 제거 : 이 행위는 철회가 가능하여 문서를 다시 만들어 낼 수 있다. 그리고 검열에 견디는 시스템에 대해서는 이러한 제어 방법은 매우 어렵다는 것을 유의해야 한다.
- (출판자/위치의) 신원 노출 : 신원이 한번 노출되면 철회가 불가능하다.

2.2.2.1. 무조건적인 익명성을 제공하는 제어

- **접근 제어** : 등록 단계 후에 사용자는 출판 시스템에 접근을 획득할 수 있다. 예를 들어, 사용자는 웹 출판 시스템을 오용하지 않겠다고 계약서에 서명한 후, 사용자는 문서를 출판할 수 있는 증명서를 획득한다. 사용자는 출판 시스템으로부터 문서를 검색할 수 있다. 만약 시스템이 사용자가 불법적 문서를 출판한다는 것을 알아내면, 해당 사용자를 추방한다.
- **출판물의 차단/출판물의 제거** : 어떤 사람이 시스템에 문서를 제공할 때, 경우에 따라 문서는 차단되거나 이후 제거될 수 있다. 문서의 차단 또는 제거는 다음을 기반으로 수행된다.
  - 문서의 크기 및 내용 기반 : 예를 들어, 문서가 불법적인 내용이나 잘못된 정보 또는 어떤 사람을 모함하거나 비난하는 내용을 포함한다면, 해당 문서를 이용할 수 없도록 해야 한다. 이 경우, 문서를 제거하여 이용할 수 없도록 한다.
  - 문서의 저자 기반 : 시스템은 악의적인 저자(예를 들어, 이전에 바이러스를 공개한 적인 있는 저자)로부터 전송된 문서를 차단할 수 있다. 이 기법은 저자에 대해 영속적인 익명성을 보장했을 경우에만 가능하다.
  - 문서의 위치 기반 : 이 기법 역시 웹 서버에 대해 영속적인 익명성을 보장한 경우에만 가능하다.
- **출판 여부의 제어(Control presence of publications)** : 만약 문서를 제거/차단할 아무런 이유가 없다면, 시스템이 문서의 이용 여부를 확인할 수 있도록 설계할 수 있다.

2.2.2.2 사용자 제어의 조건적 익명성

- 출판 서비스의 과적 방지(Prevent overloading publication servers) : 시스템의 사용자는 수많은 익명 출판물에 대해 비용을 지불할 수 있다. 만약 사용자가 출판물의 수를 초과하였다면, 사용자의 신원이 드러나게 할 수 있다.

2.2.2.3 신뢰객체 제어의 조건적 익명성

익명 출판 시스템은 신뢰객체의 도움을 받아 출판자의 신원이나 웹서버의 위치를 드러나게 할 수 있다. 출판자의 익명성을 취소하기 위해서는 신뢰객체의 도움을 받아야만 알아볼 수 있는 정보가 출판물에 부가(예. 신뢰하는 헤더 필드)되어야 한다. 웹서버의 익명성을 취소하기 위해서는 신뢰객체의 도움을 받아야만 알아볼 수 있는 정보가 익명 url에 포함되어 있어야 한다.

- **출판자의 신원 노출** : 만약 출판자가 불법적인 내용이나 어떤 사람을 귀찮게 하거나 불법적인 행위를 수행하는 혐의가 발견되는 경우 유용하다.
- **서버로부터 문서의 제거** : 만약 서버가 불법적인 문서를 포함하고 있다면 해당서버의 신원을 밝히고 해당 서버로부터 문서를 제거한다. 그러나 이것은

검열에 견디는 시스템에 대해서는 매우 어렵다. 그러한 시스템에서는 여러 서버에 문서가 분산/저장되어 있기 때문이다.

2.3 기술 동향

2.3.1 Eternity

Eternity [5] 시스템에서 익명성은 출판 단계에서 보장된다. 출판자는 Eternity 서버에 익명으로 문서를 전송한다. Eternity 서버는 문서를 여러 서버에 복사하여 모든 서버로부터 문서를 제거하는 것을 실질적으로 불가능하게 한다. 공개된 문서를 요청하는 사용자는 출판자의 신원을 알아낼 수 없다. 리던던시(redundancy)로 인해 출판자는 문서가 이용가능하고 온라인 상태라는 것을 확신한다. 문서의 내용은 키워드를 제어함으로써 출판 단계에서 제어된다. 게다가 사용자의 익명성은 취소될 수 있고, 사용자는 더 이상 출판 시스템에 접근할 수 없어야 한다. 출판 단계 후의 취소는 보다 더 힘들 것이다. 그리고 Eternity 시스템에서는 모든 서버로부터 문서를 제거하는 것은 실질적으로 불가능하다.

2.3.2 Publius

Publius [6] 는 Eternity와 기본사항이 동일하다. Publius는 외부자가 문서를 갱신하는 것을 불가능하게 하는 메커니즘을 제공한다. 즉, 오직 출판자만이 문서를 갱신할 수 있다. 출판자는 문서의 복사와 문서 복호화에 필요한 키를 여러 서버에 분배하는 것에 책임을 진다. Publius는 Eternity와 기본사항이 동일하기 때문에, 익명서 제어방법도 비슷하다.

2.3.3 TAZ 서버 시스템

TAZ 서버 시스템 [7] 에서 출판자는 웹서버에 문서를 공개한다. 이 웹서버는 자신의 웹서버일수도 있고 아닐 수도 있다. 익명성이 문서를 공개하는 단계가 아닌 웹 브라우징 단계에서 가능하다. TAZ 시스템은 TAZ 서버와 rewebber의 네트워크로 구성된다. TAZ 서버는 공개 데이터베이스를 제공한다. 공개 데이터베이스는 실질적인 호스트이름을 해당 호스트이름을 포함한 암호화된 URL 이름으로 대응시킨다. 실질적인 호스트이름 다음에 (저자의) 가명이 추가될 수 있다. 개시자는 rewebber의 체인을 통해 여러 계층으로 암호화된 url을 전송한다. 중간의 각 rewebber는 여러 계층으로 암호화된 URL을 복호화함으로써, 계층을 하나씩 없애 나간다. 문서 자체는 탐색엔진의 공격을 막기 위해 웹서버에 암호화되어 있다.

신뢰객체는 문서에 연결된 가명을 제어할 수 있다. 만약 불법적인 문서가 공개되면, 신뢰객체는 사용자의 익명성을 취소하고 해당 사용자에게 웹서버로부터 문서를 제거하라고 요청할 수 있다. 만약 신뢰객체가 없으면, 문서의 내용은 암호화된 URL이 TAZ 서버에 저장되기 전에 제어될 수 있다. 만약 문서가 불법적인 데이터를 포함하였다면, url은 TAZ 서버에서 사용할 수 없다. rewebber가 서로 협력하지 않는다고 신뢰한다. 만약 그렇지 않으면 시스템의 안전성을 신뢰할 수 없기 때문이다.

3. 전자투표 시스템(Electronic voting)

민주 국가에서는 투표를 실시하는데, 투표자가 물리적으로 투표소에 가는 것이 항상 편한 것은 아니다. 인터넷을 통한 투표가 참여를 증가할 수 있고 투표를 보다 편하게 할 수 있고 특히 시내에서 먼데 살거나 노약자나 장애인에게는 편리할 수 있다.

민주주의 투표에서는 익명투표의 요구가 매우 강하다. 임의의 객체가 투표자에 의한 투표를 추적할 수 있거나 해당 투표를 한 투표자를 추적할 수 있다면 전자투표는 이용되지 않을 것이다. 이러한 익명성은 영속성을 가지고 무조건적이어야 한다. 분산 신뢰 기술은 전통적인 종이 기반의 투표를 실현하고 감시자(observers)가 투표 결과를 검증할 수 있도록 구현되어야 한다. 전자 투표는 다음의 단계로 구성된다.

- 등록 단계(Registration phase) : 첫 번째 단계 동안, 특정 투표 기관(voting authority)은 선거인 명부(electoral roll)를 생성하고 그것을 네트워크에 공개한다. 특정 기간동안 투표자가 반대를 공표할 수 있도록 해야 한다. 그 기간이 지난 후에, 투표 기관은 최종 선거인 명단을 공개한다. 이 단계동안, 투표자는 투표 단계에 이용될 암호 요소들(키, 패스워드 등)을 얻어야 한다. 구현 및 투표 시스템에 따라 등록은 사용자 인증 후(예., 민주적 선거) 또는 가명으로(예., Yahoo 사용자는 가명으로 메일 주소를 이용하여, 새로운 Yahoo 메일 특성에 대해 투표할 수 있다.) 수행될 수 있다.
- 투표 단계(Voting phase) : 투표 단계동안 투표자는 네트워크의 통신 시설을 이용하여 투표를 할 수 있다. 투표 절차는 투표 수집 기관(ballot collection authority)과의 단일 세션을 필요하다. (투표 수집 기관은 선거인 명부에 책임을 지는 기관과 동일한 기관일 수 있다) 몇몇 투표 시스템은 단일 세션이상을 요구할 수 있다. 투표 단계에서 하나 이상

의 투표 기관이 관여하는 것은 이상한 것은 아니다.

- 집계 단계(Counting phase) : 투표 단계 끝에, 투표 수집 기관은 투표 수신을 멈추면서, 집계단계가 개시된다. 또한, 집계가 공개되고 네트워크를 통해 공개된다. 그 결과는 투표자 또는 다른 제 3 객체에 의해 검증되어야 한다.

3.1 객체 및 역할

- 투표자(voter) : 투표자는 개시자에 대응될 수 있다. 투표자는 투표 서버에게 투표를 요청한다.
- 검증기관 및 집계기관 : 대부분의 시스템에서, 하나의 검증 기관과 하나의 분리된 집계 기관이 있다.
- 응답자 : 응답자는 투표를 수신한다. 몇몇 시스템에서는 게시판(bulletin board)으로 구현된다. 이것은 모든 객체에 의해 감시되고 읽을 수 있는 메모리를 갖는 방송 채널(broadcast channel)로 구성된다. 각 객체는 보드내의 자신의 부분을 제어한다. 각 객체는 자신이 맡은 부분에만 메시지를 게시할 수 있으나 이전 메시지를 지우거나 다시 쓰는 것은 할 수 없다.
- 공격자 : 시스템에 대한 공격자가 투표 단계에 관여할 수도 있고 아닐 수도 있다. 도청자는 시스템에 관여하지 않는 공격자이고 지역적 또는 글로벌하게 통신을 도청하려고 시도할 수 있다. 또 다른 좀 더 위협한 형태의 공격자는 손상된 기관이다. 그러므로 손상된 기관이 투표 결과를 조작하거나 투표자의 프라이버시를 침해하는 것을 피하기 위해 신뢰는 분산되어야 한다.

3.2 익명성 제공 및 제어 서비스를 위한 시스템의 요구사항

3.2.1 익명성 제공과 무관한 요구사항 및 특성

- 정확성(correctness) : 만약 이미 만들어진 투표를 변경하는 것이 불가능하다면 해당 시스템은 정확하다. 최종 결과를 계산하는 동안 유효한 투표를 무시하는 것이 불가능하고 무효한 투표를 집계하는 것이 불가능하다.
- 공정성(fairness) : 모든 투표는 투표 단계가 끝날 때까지 비밀이어야 한다.
- 공개 검증성(universal verifiability) : 수동적 감시자를 포함한 모든 객체가 자기 자신에게도 투표가 정확했음을 보장한다.
- 적임성(eligibility) : 자격 있는 투표자만 투표를 할 수 있다.
- 유일성(uniqueness) : 어떠한 투표자도 한번 이상 투표할 수 없다.
- 강제불가능성(Non-coercibility)(receipt-freeness: 영수 방지성) : 어떠한 투표자도 투표 결과 수행의 결과로 자신이 어떻게 투표했음을 증명하는 영수증을 획득할 수 없음을 보장한다. (투표 매표 및 다른 투표 회유 전술을 방지하기 위함이다.) 어떠한 투표자도 자신이 투표했음을 증명할 수 없어야 한다.
- 교정성(Revisability) : 투표자는 주어진 기간 내에 자신의 투표를 변경할 수 있다. 이 요구사항은 선택사항이다.
- null 투표 제공(provide for null ballots) : 투표자는 null값의 투표를 제공할 수 있다. (예, 강제에 대응하기 위해, 투표 선택상의 부족에 항의하기 위해)
- 사전투표(under-voting) 수용성 : 투표자는 사전투표에 대한 경고를 받을 수 있다. 그러나 그러한 경고는 공개되어서는 안되고 사전투표를 방지해서는 안 된다.
- 인증된 투표 스타일(authenticated ballot styles) : 각 투표자에 의해 이용되는 투표 스타일과 투표 순환(rotation)은 인증되어야 하며 다른 제어 구조 없이 제공되어야 한다. 그러나 투표자에 의해 인증 절차 자체가 주어진다.
- 투표복사 방지(No vote duplication) : 다른 투표를 복사하는 것이 불가능해야 한다.

3.2.2 익명성 제공을 위한 요구사항 및 특성

투표 스킴에서 프라이버시는 공개된 투표에 대한 불추적성을 의미한다. 프로토콜은 정직한 사용자에 의해 투표된 투표에 대해 어떠한 정보도 노출해서는 안 된다. 즉, 투표자로부터 해당 투표를 추적할 수 없으며 투표로부터 투표자를 추적할 수 없다. "투표자 프라이버시"와 "투표 비밀성"은 다음과 같이 나뉘어진다.

- **투표자 익명성(voter anonymity)** : 투표가 주어졌거나 투표 과정으로부터 획득된 어떠한 정보가 주어졌을 때, 시스템은 투표자의 신원에 대한 정보를 노출해서는 안된다. 즉, 투표자는 신원이 드러나지 않고 추적될 수 없어야 한다.
- **투표 비밀성(vote secrecy)** : 임의의 투표자에 대해 시스템은 투표자가 투표한 투표에 대해 비밀을

유지해야 한다. 투표자로부터 투표가 추적되어서는 안 된다.

- **투표 불연결성(vote unlinkability)** : 한 투표자의 서로 다른 투표 용지는 서로 연결될 수 없어야 한다. 즉, 시스템의 어떠한 객체도 서로 다른 투표가 동일한 투표자에 의한 것임을 알 수 없어야 한다.
- **영속성(durability)** : 익명성은 영속성을 가져야 한다.

3.2.3 익명 제어 서비스를 위한 요구사항 및 특성

전자투표 시스템에는 어떤 형태의 조건적 익명성이 없어야 한다. 만약, 신뢰객체에 의한 조건적 익명성이 구현된다면, 임의의 집합의 악의 있는 기관은 투표자의 신원 및 투표자들의 투표 결과를 노출할 수 있고 이것은 민주적 투표에서는 수용될 수 없다. 만약, 신뢰객체 없는 조건적 익명성이 구현된다면, 투표자는 자신이 특별한 투표를 수행했음을 증명할 수 있어, 이것은 매표방지(receipt-freeness) 요구사항을 위반한다.

그럼에도 불구하고 이중 투표 및 다른 형태의 남용을 방지하기 위해 제어되는 무조건적인 익명성은 구현되어야 한다. 이상적으로 전자투표 시스템은 어떠한 신뢰도 요구해서는 안 된다. 왜냐하면 어떠한 객체의 협력이 투표자와 투표를 연결해서는 안되기 때문이다. 투표자와 투표를 연결하기 위해 객체들이 서로 협력하지 않는다고 신뢰되어야 한다.

3.3 기술동향

1981년이후, Chaum의 믹스넷을 이용한 기법 외의 다양한 기법을 이용하는 전자투표 시스템이 제안되었다. 이러한 전자투표 시스템은 사용하는 기술에 따라 크게 세 가지로 분류할 수 있다[8].

- 준동형 암호화를 이용한 전자투표 시스템[9,10,11,12,13]
- 믹스넷을 이용한 전자투표 시스템[8,14,15,16]
- 은닉서명을 이용한 전자투표 시스템[17,18,19,20]

그리고, 1994년 Benaloh와 Tuinstra가 최초로 전자투표 시스템의 매표방지 기능과 1995년 Sako와 Kilian이 전체검증 기능을 제안한 이후에는, 매표방지 기능 및 전체검증 기능을 제공하면서 효율적인 전자투표 시스템에 대한 연구가 중점적으로 진행되고 있다. 본 절에서는 1994년 이후의 연구 동향을 중심으로 살펴보도록 한다.

3.3.1 준동형 암호화를 이용한 전자투표 시스템

Benaloh와 Tuinstra는 선거관리자와 투표자 사이의 비밀통신을 물리적으로 보장하는 선거부스(voting booth)와 준동형 암호화 기법을 이용한 두 가지 전자투표 시스템을 제안하였다[BT1994]. 첫 번째 시스템에서는 단일 선거관리자를 이용하여 매표방지를 제공하였지만 투표자의 투표내용이 노출되는 단점이 있다. 두 번째 시스템에서 다중 선거관리자를 두어 투표자의 투표내용의 노출을 방지하였지만, 투표자가 cut-and-choose 기법으로 투표지의 유효성을 증명할 때, 임의의 문자열을 선택하여 해쉬한 값을 사용하면, 매표행위가 가능하다는 문제점이 이후에 제기되었다[8].

이병천 박사와 김광조 교수는 정직한 확인자(HV: Honest Verifier)라고하는 신뢰할 수 있는 제3자를 이용하여 매표방지와 전체검증을 제공하는 전자투표 시스템을 제안하였다[13]. 이 전자투표 시스템에서, 투표자는 자신이 구성한 첫 번째 투표지와 HV가 생성하는 임의의 쌍을 곱하여 최종 투표지를 구성하여 투표하게 된다. 투표자는 도청 불가능한 채널을 통해 HV에게 첫 번째 투표지를 전달하고, HV도 도청 불가능한 채널을 통해 임의의 쌍을 투표자에게 전달하기 때문에 투표자는 구매자에게 가짜 트랜스크립트를 제시할 수 있게 된다. 따라서 구매자는 투표자를 신뢰할 수 없게되어, 매표행위를 방지할 수 있다. Hirt는 HV3가 임의의 쌍에 대해서 유효성을 증명할 때 투표자가 선택하는 임의의 도전값을 특정값으로 고정하면 투표자가 가짜 트랜스크립트를 생성할 수 없게 되어, 매표행위를 막을 수 없다는 것을 증명하였다[12]. 그러나 HV가 투표자에게 임의의 쌍에 대해서 유효성을 증명할 때 일반적인 영지식 증명을 이용하지 않고 지정된 확인자 증명으로 증명하면 매표행위를 방지할 수 있다.

Hirt는 이병천박사와 김광조교수의 기법을 확장한 새로운 전자투표 시스템을 제안하였다[12]. 이 기법은 이병천 박사와 김광조교수의 시스템의 HV와 비슷한 역할을 하는 HR(Honest Randomizer)를 이용한다. 그러나 Hirt의 전자투표 시스템은 전체검증기능을 제공하지 못한다.

3.3.2 믹스넷을 이용한 전자투표 시스템

Sako와 Killian은 밋스넷을 이용하여 처음으로 매표방지와 전체검증 기능을 제공하는 전자투표 시스템을 제안하였다[16]. 여기에서는 일방향 도청 불가능한 채널을 가정한다. 그러나 믹스넷을 이용하여 투표자의 익명성을 보장하고 단일표를 일일이 해독하여 집계하기 때문에 시간이 많이 걸리고 계산량이 많은 단점이 있다.

2000년에 Hirt와 Sako는 Sako와 Kilian이 제안한 전자투표 시스템보다 효율성을 개선한 전자투표 시스템을 제안하였다[8]. 그러나, 이 시스템 역시 각각의 믹스서버가 계산해야 하는 증명이 너무 많아 후보자가 여럿인 투표에는 적합하지 않다.

3.3.3 은닉서명을 이용한 전자투표 시스템

Okamoto는 은닉서명과 트랩도어 비트위임(trap-door bit-commitment)을 이용하여 매표방지를 제공하는 전자투표 시스템을 제안하였다[18]. 그러나 이 시스템은 투표자가 비트위임에 사용되는 개인키를 모르는 상태에서 투표를 하면 매표행위가 가능해지는 단점이 있다.

Okamoto는 이 단점을 보완한 새로운 두 가지 전자투표 시스템을 제안하였다[19]. 첫 번째 기법에서는 PRC (Parameter Registration Committee)를 가정하고 PRC를 통해 투표자가 개인키를 알도록 한다. 두 번째 시스템에서는 양방향 도청 불가능한 채널인 선거부스를 가정하고, 투표자가 개인키를 알고 있다는 것을 선거부스를 통해 선거관리자에게 증명한다. 그러나, 이 기법은 매표방지는 가능하지만 전체검증을 제공하지 못한다.

4. 익명 브라우징(Anonymous browing)

웹 브라우징 시스템의 목적은 사용자에게 익명의 웹 브라우징 환경을 제공하는 것이다. 이런 형태의 응용에서 웹 브라우저의 개시자는 익명인 상태로 남는다. 웹 브라우징 시스템은 두 단계로 구성된다.

- 등록 단계(선택 사항) : 이 단계에서 사용자는 웹 브라우징 시스템에 등록한다. 등록이 성공된 후, 사용자는 웹 브라우징 요청을 전송할 수 있다.
- 웹 브라우징 단계 : 사용자는 웹 서버에 웹 문서에 대해 익명으로 요청을 전송한다. 시스템은 사용자의 익명성을 제어할 수 있다.

4.1 객체 및 역할

4.1.1 일반적인 웹 브라우징 시스템의 구성 객체

- 클라이언트 웹 브라우저 응용 : 특정 사용자가 온라인 문서를 검색할 때, 사용자는 웹 브라우저에 적당한 url을 입력한다. 웹 브라우저는 문서를 다운로드 받을 수 있는 웹 서버에 연결함으로써 해당 요청을 처리한다. 요청의 결과로 클라이언트 웹 브라우저는 원하는 문서를 받고 그것을 스크린에 보여준다. 클라이언트 웹 브라우저는 요청의 개시자이며 전송자이다.
- 웹 서버(들) : 문서가 공개되어 있는 서버(들)로 웹 서버는 웹 공개 요청의 수신자이다. 또한, 웹 서버는 웹 브라우저 요청의 수신자이고 응답자이다. 요청을 받은 웹 서버는 원하는 문서를 전송한다.

4.1.2 익명 웹 브라우징 시스템과 관련된 객체

- 클라이언트 웹 브라우저 응용 : 익명 웹 브라우징 시스템을 제공하기 위해 클라이언트 웹 브라우저는 어느 정도의 익명 기능까지는 확장되어야 한다. 웹 서버에 요청을 즉각적으로 보내는 대신, 요청은 다른 서버(들)에게 전송되어 요청의 수신자로부터 클라이언트를 숨길 수 있도록 한다.
- 중앙 서버 : 익명 웹 브라우징 시스템에서 중앙 서버는 익명성 서비스를 제공할 수 있다. 웹 브라우저의 요청은 중앙 서버로 보내진다. 이 서버는 개시자의 신원을 지우고 해당 요청을 수신자에게 전송한다. 수신자는 중앙 서버에게 요청에 대해 응답한다. 이러한 솔루션에서는 익명 메일 시스템에서의 하나의 중앙 재우송자의 시스템과 비슷한 상황이 존재한다. 중앙 서버는 요청의 개시자 신원에 관한 모든 정보를 알고 있기 때문에 정보를 갖는 제공자이다.
- 믹스의 체인 : 요청을 하나의 중앙 서버에 보내는 대신, 믹스의 체인을 사용할 수 있다. 믹스의 체인는 오직 자신과 연결된 다음 믹스만을 알고 있다. 그러므로 체인내의 어떠한 믹스도 요청의 개시자와 수신자간의 완전한 경로를 알 수 없다. 체인의 첫 번째 믹스는 개시자와 다음 믹스를 알고 있을 뿐 요청의 수신자에 관해서는 모른다. 비슷하게 마지막 믹스는 체인의 이전 믹스와 요청의 수신자를 알고 있을 뿐 요청의 개시자에 대해서는 모른다. 그래서 만약 믹스들간 협력하지 않는다면, 개시자와 수신자는 연결될 수 없다. 결국, 체인의 믹스는 정보를 갖지 않는 제공자이다. 이러한 시스템은 "재우송자의 체인"과 비슷하다.
- 참여자 그룹(Group of participants) : 웹 브라우저 요청을 믹스 체인에 보내는 대신 요청을 다른 웹 브라우저 요청의 또 다른 개시자에게 보낼 수 있다. 이것이 반복되어 요청이 실제 웹 서버에 전송되기 전에, 랜덤하게 선택되는 개시자의 체인에 전송된다. 그러한 솔루션에서 체인의 첫 번째 개시자는 요청의 실제 개시자이다. 그러나 체인의 두 번째 개시자는 이전 개시자가 실제 개시자인지 아닌지를 모

른다. 웹 서버는 체인의 마지막 개시자로부터 그 요청이 왔다고 생각할 수 있다. 즉 웹 서버는 요청의 실제 개시자는 모른다. 모든 개시자는 인가 서버(authority server)에 등록한다.

- 인가 서버(신뢰객체) : 개시자 체인의 시스템은 손상되지 않는 개시자가 등록되는 경우에만 올바르게 작동한다. 그러므로 등록 서버는 인가 서버로 동작한다. 이런 형태의 서버는 실제 웹 브라우저 요청에 대해 모르므로 정보를 갖지 않는 서버이다. 인가 서버는 새로운 사용자를 승인하거나 거절하고 승인한 경우 다른 사용자에게 해당 정보를 알려준다.

4.2 익명성 제공 및 익명성 제어 서비스를 위한 시스템의 요구사항 및 특성

4.2.1 익명 서비스와 관련 없는 요구사항

- 양방향 : 웹 브라우징 요청은 웹 브라우저로부터 웹 서버로 요청이 보내지고 웹 서버가 해당 요청에 응답하기 때문에 양방향이다. 응답은 원래 요청과 동일한 연결에 따라 발생한다. 왜냐하면 요청 후에 응답이 즉각적으로 수행되기 때문이다. 웹 서버는 이후 개시자와 연결하기 위한 충분한 정보를 가질 필요가 없다.(즉, 웹 서버는 개시자에 익명 연결을 할 필요가 없다.) 응답자가 메시지의 개시자에 응답하기 위해 개시자에 대한 충분한 정보를 가져야 하는 메일시스템과는 다르다.
- 실시간 : 이메일 시스템과 대조적으로 웹 브라우징 요청은 실시간으로 처리된다. 요청을 받은 즉시 응답이 즉각적으로 일어난다. 그러므로, 네트워크의 믹스는 보안 메커니즘으로서 지연(latency)을 이용할 수 없다.

4.2.2 익명 서비스를 위한 요구사항

- **일회용 익명성** : 익명 웹 브라우징 시스템에서 개시자는 웹 브라우징 과정동안 익명인 상태로 남는다. 그러므로 개시자의 신원은 드러나서는 안되고 서로 다른 웹 요청이 서로 연결되어서도 안 된다.
- **영속적 익명성** : 만약 개시자가 여러 웹 브라우징 세션동안 같은 가명을 갖길 원한다면, 영속적 익명성이 요구된다. 만약 사용자가 같은 사이트에 여러 번 같은 가명으로 로그인하길 원할때에 유용하다. 이런 형태의 익명성은 익명 이메일 시스템과 비슷하다. 익명 이메일 시스템에서도 이메일 개시자는 다른 객체(수신자와 공격자)에게 익명이다. 응답에 대한 익명성 보장은 익명 웹 브라우징 시스템의 특성이다. 웹 브라우저 요청에 대한 응답은 요청 자체와 같은 연결에 따라 주어진다. 웹 서버는 개시자에 나중에 어떻게 응답을 해야하는지를 알 필요가 없다.

4.2.3 익명성 제어 서비스를 위한 요구사항

익명성 제어는 웹 브라우징 시스템에서 유용하다. 익명성 제어는 사용자 제어와 요청 제어의 두 가지 형태로 구분된다.

- **사용자 제어** : 시스템의 사용자를 제어하는 것은 유용하다. 예를 들어, 등록된 사용자만이 웹 브라우징 시스템에 접근할 수 있으며 악의 있는 사용자는 시스템에서 제거된다.
- **요청 제어** : 웹 브라우징 시스템은 웹 요청을 제어할 수 있다. 만약 악의 있는 웹사이트에 대한 웹 요청이 있으면 시스템은 해당 요청을 거절한다.

사용자 제어와 요청 제어는 구분하기 어렵다. 만약 시스템이 (웹 요청을 제어함으로써) 악의 있는 웹사이트에 대한 웹 요청을 발견했다면, 해당 요청자의 개시자의 신원이 (사용자 익명성을 제어함으로써) 드러나게 할 수 있다.

4.2.3.1 무조건적인 익명성을 제공하는 제어

만약 웹 브라우저를 제어하는 환경에서 웹 브라우저 요청뿐만 아니라 시스템에의 접근도 제어될 수 있다.

- **접근 제어** : 악의 있는 사용자가 웹 브라우저 시스템에 접근하는 것을 방지하기 위해서는 접근 제어가 유용하다. 접근제어는 개시자가 유효한 접근 토큰을 제시(또는, 소유를 증명하거나)해야 하는 경우에만 가능하다. 유효한 토큰이 없거나 소유한 토큰이 무효화(취소)된 사용자는 더 이상 시스템을 사용할 수 없다. 만약 사용자가 불법적인 웹사이트를 방문하였다면 토큰은 취소될 수 있다. 결국 접근 제어는 미래의 오용을 방지할 수 있다. 그러나 모든 시스템이 등록 단계를 제공하지 않음을 유의해야 한다.
- **웹 요청의 차단**
  - 수신자 주소(즉, 웹 서버)에 기반 : 수신자는 웹 서버로 보내지는 모든 익명의 웹 요청을 차단해 달라고 요청할 수 있다. 이를 통해 웹 브라우징 시스템은 사용자가 악의 있는 정보를 요청하는 것

을 방지할 수 있다. 시스템은 악의 있는 웹 서버의 목록을 만들어 각각의 서버로의 요청을 거절할 수 있다.

- 시스템 이전 사용에 기반 : 만약 한 사용자가 네트워크를 과용하는 것을 원하지 않는다면, 시스템은 그것을 방지하기 위해 제어할 수 있다. 예를 들어, 시스템은 일정 시간 기간 동안 한 사용자에 대한 웹 요청 수에 대해 최대치를 정할 수 있다. 시스템은 설정된 최대치를 초과하는 웹 요청을 거절한다. 이를 위해서는 시스템이 동일 사용자에 의한 모든 요청을 연결할 수 있어야 한다.

4.2.3.2 사용자 제어의 조건적 익명성

- **웹 브라우징 시스템의 과용 방지** : 웹 요청의 수를 제한함으로써 가능하다. 웹 브라우저 시스템은 사용자가 전송할 수 있는 웹 요청의 수에 대한 최대치를 설정한다. 만약 사용자가 이 수를 초과하면, 신원이 드러나게 한다. 이를 위해 시스템은 사용자에게 제한된 수만큼만 사용될 수 있는 증명서를 제공하는 등록 단계가 필요하다. 서로 다르게 사용된 증명서가 연결될 수 없다 할지라도 설정된 수를 초과해서 사용하는 경우 시스템에 송신자의 신원을 알아낼 수 있는 충분한 정보가 제공되도록 설계해야 할 것이다.

4.2.3.3 신뢰객체 제어의 조건적 익명성

익명 웹 브라우징 시스템은 신뢰객체의 도움을 받아 개시자의 신원을 취소할 수 있다. 이를 위해서는 웹 요청은 별도의 정보(즉, 신뢰하는 헤더 필드)를 포함해야 한다. 이러한 정보는 신뢰객체의 도움으로만 알아볼 수 있다.

- **익명 개시자의 익명성 취소** : 만약 개시자가 불법적인 웹 서버(불법 음악, 아동 포르노 등)에게 요청을 전송하였을 경우 개시자의 신원이 밝혀지도록 할 수 있다. 즉 신뢰 객체는 해당 사용자가 악의 있는 행위를 수행한 경우에만 해당 사용자의 익명성을 취소할 수 있도록 한다.

4.3 기술 동향

현재의 익명 웹 브라우징 솔루션은 익명성 제어를 제공하지 않는다. 본 절에서는 현재의 솔루션을 기술하고 어떻게 익명성 제어를 추가할 수 있는지를 살펴보도록 한다.

4.3.1 LPWA

LPWA 웹 브라우징 시스템 [21] 은 하나의 중앙서버로 구성된다. 중앙 서버는 사용자 이름과 패스워드와 전자메일 주소를 가명으로 대응한다. 결국, 요청의 수신자는 개시자의 신원을 알 수 없다. 개시자와 LPWA 서버간의 지역적 도청자는 개시자와 웹 브라우저 요청의 수신자를 연결할 수 있는 문제가 있어 LPWA 프록시와 파이어월을 가진 LPWA 서버를 이용하는 두 가지 방법을 제안하였다.

중앙의 LPWA 서버(신뢰객체)는 모든 입력되는 요청을 수신하고 mapping을 만든다. 이 서버의 기능은 쉽게 확장될 수 있어 익명성을 제어할 수 있다. 만약 개시자가 불법적인 웹사이트를 브라우징한다면 중앙 서버는 이것을 알아내어 적절한 대응을 할 수 있다. 개시자의 익명성은 취소되거나 개시자는 익명 웹 브라우징 시스템에서 제거된다.

4.3.2 Web Mixes

웹믹스(Web mixes) [22] 는 요청이 전송되는 믹스의 체인으로 구성된다. 이것은 기본적으로 onion 라우팅과 같은 기술을 이용한다. 각 웹믹스는 계층화되어 암호화된 요청의 계층을 없앤다. 그러나 이 시스템은 onion 라우팅과는 달리 응용 계층에 탑재된다. 웹믹스들이 서로 협력하지 않는다고 신뢰한다. 웹믹스들이 협력할 경우 통신 객체들의 신원이 밝혀질 수 있기 때문이다.

Ⅲ. 결 론

지금까지 익명성 및 익명성 제어 서비스에서 사용되는 기술이나 요구사항을 비교·분석하였다. 이를 기반으로 국내 실정에 맞는 익명성 및 익명성 제어 서비스를 개발하는 것이 가능할 것으로 보인다. 앞에서 살펴보았듯이 익명성과 익명성 제어 기술은 동전의 양면과 같이 따로 생각할 수 없는 관계인 것은 분명하다. 그러므로 익명성 및 익명성 제어 기술은 동시에 고려해야 한다. 현재 KISA에서는 전자거래에서 본격적으로 공개키 인증서가 사용되면서 실명 인증을 통한 개인정보유출이 심각성을 인지하여, 실명 인증서의 단점을 보완할 수 있는 익명인증서에 대한 연구를 진행하고 있다. 이러한, 익명인증서의 필요성은 전자거래뿐만 아니라 실명 유비쿼터스 컴퓨팅 환경과 같은 미래의 정보 인프라에서는 그 요구가 더욱 증가할 것으로 보인다. 특히, 익명인증서는 웹사이트에서의 사용자 인증, 익명 게시판에서의 사용자 인증(추적가능 익명인증서), 전자투표 시스템에서의 사용자 인증

(자기은닉 익명인증서), 의약처방전에서의 사용자 인증 (일회사용 추적가능 익명인증서) 등 다양한 분야에서 사용될 것으로 예측하고 있다. 끝으로, 본고의 연구결과는 향후 익명성 및 익명성 제어 기술을 기반으로 익명 이메일 시스템, 익명 출판 시스템, 전자투표 시스템 및 익명 브라우징 시스템을 설계할 경우, 이러한 서비스에 대한 최소한의 요구사항을 제시할 것으로 기대된다.

참 고 문 헌

[1] Type 0 re-mailer, http://www.penet.fi/.

[2] Lance Cottrell. Mixmaster & Remailer Attacks, http://www.obscura.com/~loki/remailer/remailer-essay.html, http://www.inf.tudresden.de/~hf2/anon/mixmaster/remailer-essay. html.

[3] Type 1 and 2 re-mailers, http://anon.efga.org/.

[4] George Danezis, Roger Dingledine, Nick Mathewson, "Mixminion : Design of a type iii anonymous remailer protocol", the 9th ACM conference on Computer and Communications Security, 2003.

[5] R. J. Anderson, The eternity service. Pragocrypt 1996.

[6] Marc Waldman, Aviel D. Rubin, Lorrie Faith Cranor, "Publius : A robust, tamper-evident, censorship-resistant web publishing system", the 9th USENIX Security Symposium, August 2000.

[7] Ian Goldberg, David Wagner, "TAZ Servers and the Rewebber Network : Enabling Anonymous Publishing on the World Wide Web", First Monday 3(4), April 1998.

[8] M. Hirt, K. Sako, "Efficient Receipt-Free Voting Based on Homomorphic Encryption", Advances in Cryptology, Eurocrypt '00, LNCS 1807, pp. 539~556, 2000.

[9] J. Benaloh, D. Tuinstra, "Receipt-free Secret-ballot Elections," the 26th ACM Symposium on Theory of Computing, pp. 544~553, 1994

[10] J. D. Cohen, M. J. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", the 26th IEEE Symposium on Foundations of Computer Science, pp. 372~382, October 1985

[11] R. Cramer, R. Gennaro, B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology, Eurocrypt '97, LNCS 1233, pp. 103~118, 1997

[12] M. Hirt, "Receipt-free Voting with Randomizers", the Workshop on Tustworthy Eletions, Aug. 2001.

[13] B. Lee, K. Kim, "Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier", the JWISC 2000, pp. 101~108, 2000.

[14] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24 (2): pp. 84-88, February 1981.

[15] M. Jakobsson, "A Practical Mix", Advances in Cryptology, Eurocrypt '98, LNCS 1403, pp. 448~461, Springer, 1998.

[16] K. Sako, J. Kilian, "Receipt-free Mix-Type Voting Scheme: APractical Solution to the Implementation of a Voting Booth", Advances in Cryptology, Eurocrypt'95, LNCS 921, pp. 393~403, Springer, 1995

[17] Eiichiro Fujisaki, Tatsuaki Okamoto, "Practical Escrow Cash System", the 4th Security Protocols Workshop, LNCS 1189, pp 33-48, April 1996.

[18] T. Okamoto, "An Electronic Voting Scheme," IFIP '96, Advanced IT Tools, pp. 21~30, 1996.

[19] T. Okamoto, "Receipt-Free Electronic Voting Scheme for Large Scale Elections", Workshop on Security Protocols '97, LNCS 1361, pp. 25~35, 1998.

[20] K. Sako, "Electronic Voting Scheme allowing Open Objection tothe Tally", IEICE Trans. on Fundamentals, Vol E77-A, No. 1, Jan. 1994.

[21] LPWA, the Lucent Personalized Web Assistant website, http://www.bell-labs.

com/project/lpwa/.
[22] Oliver Berthold, Hannes Federrath, Stefan Kopsell, "Web MIXes : A system for anonymous and unobservable Internet access", Designing Privacy Enhancing Technologies, the Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, pp 115-129, July 2000.
[23] Anonymity and Privacy in Electronic Services, https://www.cosic.esat.kuleuven.ac.be/apes/.

〈著 者 紹 介〉

박 해 룡 (Haeryong Park)
종신회원

1999년 2월 : 전남대학교 수학과 학사
2001년 2월 : 서울대학교 수학과 석사
2000년 12월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 : 암호프로토콜, 키관리, 정보보호

김 지 연(Jeeyeon Kim)
종신회원

1995년2월 : 성균관대학교 정보공학과 공학사
1997년2월 : 성균관대학교 대학원 정보공학과 공학석사
1996년12월~현재 : 한국정보보호진흥원(KISA) 연구원
〈관심분야〉 암호프로토콜, 키관리

천 동 현(Donghyeon Cheon)
종신회원

1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사
2001년 9월~현재 : 한국정보보호진흥원 암호인증기술팀 선임연구원
〈관심분야〉 암호학, 정보보호

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호인증기술팀장
〈관심분야〉 암호학, 정보보호, RFID/USN 정보보호

이 재 일 (Jae-il Lee)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호진흥원 전자거래보호단장
〈관심분야〉 : 정보보호, 유·무선PKI, 유비쿼터스 보안