情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

e-privacy와 정보보호기술

박 춘 식*

요 약

인터넷과 정보통신기술의 발달로 인하여 e-privacy 문제가 최근 많이 거론되고 있다. 많은 내용들이 제도나 법 차원에서 논의되고 있으나 기술적인 관점에서의 논의는 다소 부족한 실정이다. 본 논문에서는 e-privacy와 정보보호 기술과의 관계를 검토하여 보고, privacy 침해 기술과 privacy 보호 기술 그리고 privacy 보호 기술의 중심이 되는 익명성과 익명성 구현 기술, 익명성이 가지는 역기능과 고려사항 등에 대하여 논의해보고자 한다. e-privacy는 정보보호 기술과 밀접한 관계를 가지고 있으며, 법이나 제도 등과 함께 고려될 때 보다 나은 e-privacy가 제공될 것으로 생각된다.

Ⅰ. 서 론

프라이버시에 대한 정의는 1890년 S.D. Warren 박사 등이 Harvard Law Review에서 밝힌 "the right to be alone"이 최초라고 생각되며, 1967년 컬럼비아대학의 Alan Westin 교수의 "the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"라는 정의[1]에 이어, 2000년 UC 버클리대학의 Ian A. Goldberg박사가 자신의 학위논문[2]에서, "the ability of the individuals to control the distribution of information about himself"라고 인터넷 시대를 고려한 프라이버시를 정의하여, 시대에 따라 변화되어 가는 프라이버시의 모습을 볼 수 있다.

이러한 프라이버시 문제는 독일 등의 유럽을 중심으로 활발하게 논의되어 왔으며, 1970년대부터 법제화가 이루어지고, 다른 나라나 국제기구에 영향을 미쳐 OECD 프라이버시 8원칙[3]이나 EU나 UN 등의 가이드라인 제정[1]에 이르게 하였다. 프라이버시 문제는 정보화와 인터넷 시대를 맞이하여 보다 더 중요한 이슈[4]가 되어 왔으며 최근에는 각종 시민단체[5]나 연구 모임 등이 등장하게 되었다. 우리나라에서도, 최근 교육행정정보시스템(NEIS)의 문제로 e-privacy 문제가 크게 대두되고 있다. 정보화에 대한 관심 못지않게 정보화로 인한 역기능(security, privacy, 정보격차 등) 문제를 해결하지 않으면 성공적인 정보화를 이룰 수 없음을 점점 인식하고 있는 느낌이다.

인터넷상의 e-privacy 위협은 크게 비인가된 모니터링과 수 년 후의 접근을 위한 정보의 logging과 보존으로 대별할 수 있다. 이러한 위협은 정보통신 기술의 발달로 인하여 프라이버시 관련 정보를 보다 쉽게 수집 저장할 수 있는 신분 확인 기술, 스파이웨어 등 해킹 기술, 쿠키, 로봇 기술 등의 정보 수집 저장 기술의 발달도 함께 이루어져 더욱 가속화되고 있는 실정이다. 또한, Data/Text 마이닝 기술과 같은 수집 정보의 가공 분석 기술도 발달하여 정보 통신 기술의 발전에 의한 e-privacy 침해 가능성도 보다 증가하게 되었다. 또한, 최근 많은 스마트 태그의 활성화로 인한 RFID 기술의 프라이버시[6] 그리고 유비쿼터스 시대로 인한 프라이버시 문제[7]는 새로운 기술의 등장과 새로운 사회의 전개 시 수반되는 것으로 해결해야할 많은 과제들을 던져주고 있다.

한편, e-privacy의 침해 가능성은 이러한 기술 발전의 문제보다도 e-privacy에 대한 사회적 인식 부족이 보다 더 많은 영향을 끼쳐온 것도 사실이다. 일반적으로 인터넷상의 쇼핑몰에서 개인 정보를 요청할 경우 자신의 정보를 쉽게 제공하는 경우나 자신의 비밀번호를 동료나 관련자에게 쉽게 알려주는 행동들은 우

* 국가보안기술연구소(csp@etri.re.kr)

리 주변에서 쉽게 볼 수 있는 현상이다. 또한, 자신의 주민등록번호나 전화번호 등의 개인 정보가 어떻게 활용되고 어디에 사용되어 심각한 문제를 제기하는 지는 자신의 문제로 대두되기 전에는 쉽게 인식하지 못하고 있는 실정이다.

일반적으로 e-privacy 문제는 사회적 인식 제고를 위한 법적 제도적 문제이며 정보 윤리 교육이나 홍보를 통하여 개선해 나가야 할 것으로 많이 생각하고 있다. 그러나, 이러한 해결 방법으로는 한계가 있다. 즉, 교육이나 법에 의한 사회적 장치로는 급변하고 있는 기술의 발전과 정보의 가치 향상에 따른 정보화의 흐름을 멈출 수가 없기 때문이다. 그리고 이러한 정보화의 발달은 새로운 역기능을 창출하거나 프라이버시에 부정적인 요소들을 만들어내며 e-privacy 침해 가능성과 위험성을 계속해서 증대시켜 나가기 때문에 적절한 대책이 될 수 없다고 생각한다.

따라서, 본 논문에서는 정보화 기술로 인하여 발생한 정보화의 역기능인 e-privacy 문제를 기술적인 관점에서 접근하여 해결하고자 하는 일환으로 관련 정보보호 기술들을 분석 소개하고자 한다.

e-privacy 관련한 기술로는 크게 e-privacy를 침해하는 기술(PITs:Privacy Invading Technologies)과 이를 보호하려는 e-privacy 보호 기술(PETs: Privacy Enhancing Technologies)로 대별할 수 있다[8,9]. IT 기술은 e-privacy 침해 기술이나 e-privacy 보호 기술 모두에 활용될 수 있어 IT 기술의 발달과 함께 필연적으로 역기능중의 하나인 e-privacy 침해는 발생할 수밖에 없으며, 보호 기술과 함께 서로 경쟁하듯 발전 변모해 나갈 수밖에 없다고 생각한다.

II. 프라이버시 침해 기술(PIT)와 프라이버시 보호 기술(PET)

1. 프라이버시 침해 기술(Privacy Invading Technologies)

많은 기술들은 순기능적인 측면과 역기능적인 측면을 가지고 있는 경우가 많다. 역기능적인 측면으로 프라이버시에 부정적인 영향을 주는 기술들도 있다. 익명성 위협, ITS(Intelligent Transportation Systems)나 GPS(Global Positioning System), U-LBS (Ubiquitous Location Based Service)와 같이 사용자 위치 정보 추적, 쿠키, 스파이웨어, 웹로봇 또는 사이버로봇, 웹버그 등 정보수집 기술을 통한 신원확인 및 사용자 정보 수집, 데이터 또는 텍스트 마이닝 등 정보 분석 기술을 통한 수집된 정보의 극대화, 백 오리피스 등의 토로이안 목마나 트랩도어 등을 이용한 해킹 기술 그리고 정보보호기술과 인터넷 감시 기술 등은 이러한 기술 분류에 속할 수 있다.

1.1 익명성 위협 기술적 요소

익명성을 위협할 수 있는 인터넷 관련 기술적 요소로는 TCP/IP 주소, 이메일 도메인명, PSN(Processor Serial Number), IPv6 등이 있다[10].

TCP/IP 주소는 http://www.whois.co.kr 을 이용하여 인터넷상의 TCP/IP 주소로 주소를 할당해 준 기관을 추적할 수 있다. 또한, TCP/IP 주소를 할당받은 ISP(Internet Service Provider)를 알려주며, ISP의 고객 정보 DB를 통하여 이용자의 신원확인도 가능하게 해 준다. 이메일의 주소를 통하여 ISP 정보와 이메일 이용자의 ID를 알 수 있으며, 법집행기관 등은 ISP에게 이용자의 개인정보를 요구하여 신원 확인을 행할 수 있다.

PSN은 인텔사의 팬티엄 III 칩에 프로세서 고유 PSN을 부여하여 인터넷 접속 컴퓨터의 신원을 인증할 수 있으며, 휴대폰의 ESN을 이용하여 이용자의 신원을 확인할 수 있다.

IETF가 개발한 IPv6는 인터넷상의 모든 장치에 고정된 주소를 할당하여, 즉 모든 패킷에 변경이 곤란하도록 하여 특정 패킷의 출처를 확인할 수 있도록 하여 인터넷상의 익명성을 잃게 되어 익명성 자체를 부인하고 있다. 다가올 유비쿼터스 컴퓨팅에서는 PSN,IPv6 등의 기술은 핵심 기술이 될 것으로 전망되어 e-privacy 문제는 보다 심각해 질 것으로 예상된다.

1.2 정보 수집 기술

1.2.1 쿠키(Cookies)

쿠키는 사용자가 웹서버에 접속할 때, 웹서버가 사용자의 하드디스크에 자동적으로 집어넣는 작은 텍스트 파일로, 웹서버쪽에서 사용자쪽으로 정보를 전송, 저장하고 다시 그 정보를 필요시 뽑아내어 사용하는 시스템이라 말할 수 있다. 웹서버에 대한 사용자 각각의 요구와 다른 요구들 간의 상관 관계가 없는 웹 프로토콜인 HTTP의 stateless한 특징 때문에 웹서버에서 제공하는 서비스의 불편이 존재하여, 지속적인 사용자 상태 정보(이름, 주소, 비밀번호, 소비정보, 방문여부, 횟수 등)를, 즉 쿠키를 이용하여 사용자에 대

한 서비스를 제공하고자 하는 기술이다.

그러나, 사용자 정보가 하드웨어에 저장되어 각 개인의 활동이나 선호도가 쉽게 노출될 수 있으며 e-privacy에 심각한 문제점을 줄 수 있다. 웹 브라우저상에서 쿠키를 받아들이지 않도록 선택할 수 있는 기능은 있으나 대부분의 사용자들은 이러한 사실도 모른 채 자신의 하드디스크에 쿠키를 저장하고 있는 실정이다.

1.2.2 스파이웨어(Spyware)

스파이웨어는 무료로 배포되는 공개 소프트웨어에 들어있는 일종의 프로그램 모듈을 통칭하는 것으로 광고 효과 모니터링을 위하여 컴퓨터 이용자의 이름이나 IP 주소, 방문한 웹사이트 목록, 클릭한 배너 광고 등의 프로그램 이용자에 대한 개인정보를 미리 설정된 특정 서버로 보냄으로써 외부에서 인터넷을 통해 특정 이용자의 개인정보를 확인할 수 있도록 해주는 소프트웨어를 의미한다. 스파이웨어는 단지 개인정보를 유출하는 기능을 할 뿐이므로 백오리피스 등의 해킹 도구와는 구별된다[11].

웹사이트에서 사용자가 알지 못하는 범위까지 그 사용자에 대한 정보를 쿠키에 저장한다면 쿠키도 일종의 스파이웨어로 볼 수 있다. 국내에서 유통되는 외국산 소프트웨어인 FTP 프로그램 CuteFTP3.0, 채팅 프로그램 FreeIRC 등 280여 제품이 국내 한 업체에 의하여 스파이웨어인 것으로 조사된 바 있다.

스파이웨어를 제거하는 대표적인 프로그램은 미국의 Gibson Research사의 Optout 무료 공개 소프트웨어가 있다.

1.2.3 웹 로봇(Web Robot)

인터넷상에서 에이전트 기술을 이용하여 문서를 추출하고 그 문서에서 참조되는 링크를 분석하여 자동으로 그리고 계속적으로 링크를 따라다니는 프로그램으로 사용자 정보를 수집하는 데 활용되고 있으며, 스파이더나 지능형 에이전트 등으로도 불린다.

1.2.4 웹 버그(web Bug)

웹 버그는 웹 페이지에 어떤 목록을 갖고 심어 놓은 매우 작은(1*1 픽셀) 그래픽 이미지 파일로 육안으로는 구별할 수 없을 정도다. 웹 버그는 자신의 웹 서버에게 웹 버그가 설치되어 있는 페이지 URL, 방문 컴퓨터 IP, 열람 시간 등의 정보를 제공하여 사용자가 방문한 사이트를 추적하는 등 사용자 관련 정보를 유출할 수 있다.

웹버그를 식별하는 프로그램은 없지만 해당 웹 페이지나 이메일의 소스코드를 분석하여 보면 웹버그가 존재하는 지를 알 수 있다.

1.3 정보 분석 기술

정보 분석 기술의 대표적인 것으로 데이터 마이닝(Data Mining)으로, 대용량의 데이터를 패턴인식, 통계학 등의 기법을 이용하여 분석함으로써 의미있는 새로운 상관 관계, 패턴 그리고 경향들을 발견하는 프로세스로 고객의 성향이나 구매 패턴을 파악하는 인터넷 마케팅 전략에 사용되고 있다. 데이터 마이닝 기법으로는 분류, 군립, 연관성 분석, 연속 패턴 분석 등이 있으며, 데이터 마이닝 적용시 사용자 프로파일, 로그 파일, 쿠키 정보 등이 사용되기도 한다.

1.4 정보보호기술

많은 기술들이 적용 여부에 따라 프라이버시 침해 기술로 활용될 수 있듯이, 정보보호기술도 활용 여부에 따라 프라이버시 침해 기술로 활용될 수 있다. 생체인식정보를 이용한 각종 신분확인 기술과 이를 위한 스마트카드 등의 정보 저장 기술 등이 이에 해당되며 PKI 기술도 사용자의 관련 정보를 포함하고 있는 측면에서 해당될 수 있다.

특히, 네트워크 보호 장치인 침입탐지장치(Intrusion Detection System), 침입차단장치(Firewall), 그리고 Auditing 기능, biometrics 등은 프라이버시 침해 기술로 활용될 수 있다. IDS의 광범위한 사용을 통하여 각종 Auditing 데이터가 수집 저장되어 사용자 신분을 확인할 수 기술로 사용될 수 있다. 이외에도 인터넷 감시 기술들도 프라이버시 침해 기술로 포함될 수 있다.

2. 프라이버시보호기술(Privacy Enhancing Technologies)

프라이버시보호기술의 대표적인 기술로는 암호(Cryptography)와 익명 기술이 있다. 암호는 전자메일, 저장파일, 데이터베이스의 정보를 암호화하여 저장하여 외부의 접근이나 정보의 노출로부터 보호하는 데 사용되는 일반적으로 널리 알려진 기술이다. 익명성 기술은 정보의 노출 자체와는 무관하게 정보와 소유자간의 관계나 송수신자간의 관계를 비밀로 하여 프라이버시 보

호를 제공하는 것이다.

정보보호 서비스 제공을 위해서는 현재로는 암호 기술이, 프라이버시 보호를 위해서는 익명성 제공 기술이 사용되고 있다. 익명성 제공 기술로는 암호를 사용하여 익명성을 제공하는 기술과 암호를 사용하지 않고 익명성을 제공하는 기술이 소개되고 있다. 주로 인터넷이나 e-privacy 관한 자료에 나타난 익명성 제공은 주로 암호를 사용하지 않는 방식들이 널리 소개되고 있다. 물론 암호를 사용하지 않는 익명성 제공은 먼저 안전성에 문제점을 내포한 방식으로 볼 수 있으나 e-privacy 보호를 위해 널리 소개되고 있다.

미국 프라이버시정보센터인 EPIC[5]이 소개하는 프라이버시 보호 기술로는 익명 인터넷 검색 도구, 쿠키 막는 프로그램, HTML 필터 등이 있으며 관련 응용제품으로는 스누핑 방지 이메일(Snoop Proof Email), 웹 서핑시 개인정보유출을 방지하는 Surf Anonymous, 원치 않는 팝업 창이나 배너 광고를 막아주는 HTML Filter, 쿠키로 인한 개인정보유출을 방지하는 Cookie Busters, PGP로 대표되는 Email and File Privacy 보호기술, disk/telnet/web encryption 기술, 디스크나 파일을 복구할 수 없도록 하는 Disk/File Erasing Programs 등이 소개되어 있다.

한편, 독일 Fischer-Hubner[1]에 의한 프라이버시 보호 기술로는 통신레벨, 시스템 레벨, 응용 레벨에서의 사용자 신분 보호를 제공하는 것으로 DC Nets, MIX nets, Anonymous Remailers and Browsers, Onion Routing, Freedom Network, ISDN Mixes, Blind Signatures, ECash, Anonymous Payment Protocol, Pseudonymous Auditing and TTP 등을 열거하고 있다.

프라이버시 보호 기술은 크게 분류하여 사용자 선택 기능에 의한 PET와 보호 메커니즘에 의한 PET로 분류할 수도 있다.

2.1 사용자 선택 기능에 의한 프라이버시 보호 기술 (Products for providing Consumer Choice)

2.1.1 OPS(Open Profiling Standard)[12]

OPS는 1997년 Netscape, Verisign, FireFly Networks사가 컨소시엄을 구성하여 만든 것으로 고객이 자신의 개인정보를 Web 브라우저에 자동적으로 제공할지 아니면 제공하지 않을 지를 제어할 수 있는 권한을 고객에게 주는 방식이다. 고객이 방문한 웹사이트에서 개인 정보 제공과 상품에 대한 할인 혜택 등과의 흥정 거래를 통하여 개인의 제어권을 활용하도록 하는 방식으로 합법성만 오히려 제공하게 된다는 반대 주장에 의하여 P3P에 포함되게 되었다.

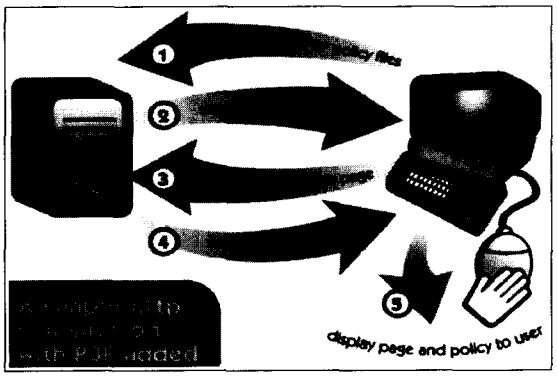
2.1.2 P3P(Platform for Privacy Preferences) 기술[13,14]

P3P는 W3C(the World Wide Web Consortium)에서 개발한 개인정보보호 표준기술 플랫폼으로써 웹 사이트에서 이루어지는 데이터 처리 관련 표준으로 제시된 것으로, 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보 공개 수준과 비교하여 정보를 선별적으로 제공하는 것이다. P3P는 익명을 제공하는 것이 아니며 개인 정보 제공 시 정보 제공에 대한 이용자의 선택과 결정을 가능하게 해주어 인터넷상의 프라이버시 보호를 위한 기술적인 해결 방안으로 고려되고 있다.

P3P 구현 방법은 이용자가 사이트를 검색할 때, 사용자측의 에이전트는 방문하고자 하는 사이트의 P3P 정책 파일들을 요구하고 이에 대응하여 해당 사이트에서는 자신의 프라이버시 정책 파일을 사용자측에 송부하게 된다. 이러한 과정에서 이용자가 설정한 프라이버시 선호 수준과 방문한 웹사이트간에 transaction이 발생하게 되어 이용자가 설정한 기준과 방문 사이트의 정책 기준이 일치하게 되면 요청된 홈 페이지가 전송되게 된다.

Internet Explorer상의 도구.인터넷 옵션을 통하여 이용자가 쿠키에 관련하여 프라이버시 선호 수준을 설정할 수 있다. 수준은 모든 쿠키 차단, 높음, 보통 높음, 보통, 낮음, 모든 쿠키 허용의 6단계로 구성되어 있다.

그러나, P3P는 컴퓨터 이용자에게 쿠키 수준을 설정해야 하는 번거러움, 프라이버시 기준 설정의 어려움, P3P를 지원하지 않는 사이트의 배제로 인한 프라



〔그림 1〕 P3P 구현 과정

이버시 보호 우수 사이트가 배제되는 현상, 구체적 법률 미비로 인한 집행력 부재, 복잡한 프로토콜을 기피하는 기업과 인터넷 검색 불편을 이유로 프라이버시 선호 수준을 낮게 책정하는 이용자로 인한 실효성의 의문 등으로 인하여 구현되고 있는 웹사이트들은 소수에 불과한 실정이다. 또한, P3P가 표준으로 채택될 경우, 프라이버시 보호 노력은 오히려 지체될 것이며 이러한 영향으로 P3P는 PET보다 PIT가 될 수 있는 소지가 있다.

2.2 보호 메커니즘에 의한 프라이버시 보호 기술 (Protection Mechanism)

보호 메커니즘에 의한 프라이버시 보호 기술은 대략 익명성 제공 기술, 침입차단시스템, 암호 기술, Cookie Crushers 등 정보보호와 관련된 기술들이 대부분이다. 침입차단시스템과 같은 네트워크 보호 기술이나 암호 기술들은 이미 설명한 바와 같이 프라이버시 침해 기술로도 활용되며 아울러 프라이버시 보호 기술로도 활용되는 기술이다. 이러한 기술들은 이미 널리 알려진 기술로써 여기서 별도로 자세하게 다루지 않는다.

다만, 프라이버시 보호 기술의 핵심적인 부분인 익명성 제공 기술에 대해서 본 논문에서 자세히 소개하고자 한다.

Ⅲ. PET와 익명성(Anonymity)

1. 익명성[1,15]

일반적으로 익명성은 이용자가 자신의 신분을 노출하지 않고 어떠한 자원이나 서비스를 이용할 수 있도록 해주는 기능을 말한다. 익명성에 관한 보다 이론적인 정의는 1990년 B.Pfitzman에 의하여 다음과 같이 행하여졌다[1]. 먼저, R_u를 어떠한 사건 E 동안에 이용자 U가 역할 R을 수행한다고 정의하고, A는 공격자이며, NC_A는 공격자 A와 협력하지 않는 이용자 집합이라고 하자.

"U($U \in NC_A$) is anonymous in role R for an event E to an attacker A if for each observation B: $\forall\ U' \in NC_A$: $0 \ll P(R_{U'} | B) \ll 1$. U is perfectly anonymous if $\forall\ U' \in NC_A$: $P(R_{U'}) = P(R_{U'} | B)$."

이외에도 프라이버시와 관련된 기능으로 Unobservability, Unlinkability, Pseudonymity 등이 있다. 이들의 의미는 서로 다르며 이들의 정의와 상관관계에 대한 연구[16]도 이루어지고 있다.

이러한 익명성은 단순히 신뢰할 만한 서버를 통하여 송신자와 수신자와의 관계를 비밀로 유지하여 익명성을 제공하는 방안과 정보보호 기술을 이용하여 익명성을 제공하는 방안으로 대별할 수 있다. 신뢰할 만한 서버를 이용하여 익명성을 제공하는 기술은 엄격한 의미에서 익명성이라고 말하기는 다소 어려운 면이 있지만 초기 Anonymous Remailer[17,18]가 여기에 해당된다. 정보보호기술을 이용한 익명성 제공 방안으로는 은닉서명(Blind Signature)[19]과 익명 통신로 등이 해당된다. 은닉서명은 서비스 제공자가 서비스 청구자의 신원을 알 수 없거나 정보를 얻지 않고도 적절한 전자서명이나 전자신용증서 서비스를 제공할 수 있도록 서비스 청구자의 익명성을 제공해 주는 기술로 전자화폐나 전자투표 등에 사용되는 기술이다. 익명 통신로는 송신자와 수신자간의 대응관계나 송신자와 송신자 메시지와의 대응 관계 등을 비밀로 유지하도록 하는 기술로, 전자 투표, 전자 여론 조사, 익명 이동 통신(휴대 전화),익명 ISDN[20] 등에 사용되고 있다.

2. 익명성 구현 기술

송신자 익명성 구현 기술로는 Dummy traffic[1], DC Networks[21], Crowds[22]등이 있으며, 송신자와 수신자 사이의 Unlinkability를 제공하는 데에는 Mix Networks[23], 그리고 수신자 익명성 구현 기술로는 메시지 방송(Message Broadcast)이나 암시 어드레스(implicit address) 이용 방안 등이 있다. 송신자 익명성 구현 기술인 Dummy Traffic은 의미 없는 메시지를 일정하게 보내어 트래픽 분석(Traffic Analysis)을 방지하여 언제 누구와 어떻게 등의 관련 정보를 제공하지 않는 기술이다.

수신자 익명성 구현 기술로는 메시지 방송이 가장 효과적이며 안전하나 방송을 할 수 없는 환경에서는 사용할 수 없는 방식이다. 암시 어드레스는 어떠한 환경에서도 사용 가능한 수신자 익명성 구현 기술로 보이지 않는 암시 어드레스(Invisible implicit address), 즉 해당 수신자만이 인식할 수 있는 어드레스를 이용하는 방식이다. 해당 수신자만이 어드레스를 인식하게 할 수 있는 방식으로는 수신자의 공개키로 어드레스를 암호화하여 송신하는 것으로 해당 비밀키를 갖고 있는 정당한 수신자만이 자신의 어드레스를 복호화하여 수신하게 되고 다른 수신자들은 누가 수신하였는 지 알 수 없게 된다. 이는 모든 수신자들이 자신의 메시지인지

확인을 위하여 복호화를 매번 실시하여야 하는 비효율적인 방식이다. 이를 개선하기 위하여 임의의 transaction pseudonymous를 이용한 방식으로 랜덤 발생기를 서로 공유하고 송신자는 message prefix를 송신하는 방식이 제안되어 있다.

익명성 구현 기술의 대표적인 MIX Network, DC Network, Shuffle Network[24]에 대하여 설명하고자 한다.

2.1 MIX Network[23]

송수신자간의 Unlinkability를 가지는 MIX Network는 1981년 D.Chaum[23]이 제안한 것으로 이후 많은 연구가 계속되어 오고 있다. MIX Network의 MIX 서버(센터)는 반복되는 메시지를 제거하거나, 입력되는 메시지를 저장하여 동시에 출력하거나, 입력 메시지를 복호화하여 랜덤수를 제거하거나, 이를 다시 랜덤하게 재정렬하여 다음 MIX 서버에게 전송하는 기능을 담당한다. 이를 경우 MIX 서버에 입력된 메시지와 출력된 메시지 간의 대응 관계를 알 수 없게 되어 Unlinkability를 제공하게 된다. 그러나, MIX 서버는 이들의 대응 관계를 알 수 있게 되어 안전성은 MIX 서버에 의존하게 된다. 안전성을 보다 강화하기 위하여 복수의 MIX 서버를 고려한 것이 MIX Network로 단 하나의 MIX 서버만이라도 honest한 경우에는 MIX Network는 안전하다고 말할 수 있다.

MIX Network 구성은 메시지별로 MIX 서버를 랜덤하게 선택하는 방법과 모든 메시지에 대하여 항상 고정된 MIX 서버를 선택하는 MIX Cascades 방법이 있다. MIX Network에 대한 공격 방식 등 자세한 설명은 인용 자료들을 참고하기 바란다.[15,23,24]

2.2 DC Network[21]

Unconditional sender and recipient untraceability를 제공하는 DC(Dining Cryptographer) Network는 1988년 D.Chaum[21]에 의하여 제안된 방식으로 효율성 문제로 인하여 많은 연구가 진행되지 않는 방식이다.

암호학자들이 식사를 한 후 한 사람만이 식대를 지불하였지만 지불한 사람 외에 다른 사람들은 누가 지불하였는지를 알 수 없게 하고자 하는 Dining Cryptographers Problem을 구현한 Network이다. 먼저, 각 참가자는 인접한 참가자와의 비밀 키 공유를 사전에 행한 후 자신의 메시지(자신이 지불하였을 경우에는 의미 있는 메시지, 그러나 자신이 지불하지 않았을 경우에는 모든 값이 0인 메시지)와 One time Pad 방식의 암호를 이용하여 암호화한 후 참가자 모두에게 broadcast한다. 이때, 각 참가자가 broadcast한 암호문들을 합하면 일정한 형태를 갖춘 메시지가 구하여진다.이때의 메시지가 지불한 참가자가 선택한 의미있는 메시지가 되어 DC Network를 구현하게 된다.

물론, 각 참가자는 honest하여야 하며, broadcast되는 네트워크는 신뢰할만한 네트워크 이어야 한다. 참가자가 dishonest하거나 메시지 충돌로 인한 문제점을 해결하기 위하여 해쉬함수를 이용하여 dishonest나 메시지 충돌 여부를 감지하거나, ALOHA, CSMA (Carrier Sense Multiple Access)등의 메시지 충돌 방지 방법[21]들이 제안되어 있다.

DC Network는 안전성이 탁월하나 사전 키 공유와 각 참가자의 메시지 전송량이 많은 비효율적인 방식으로 많은 연구가 계속되지 않은 방식으로 자세한 내용은 참고자료[15,21]를 이용하기 바란다.

2.3 Shuffle Network[24]

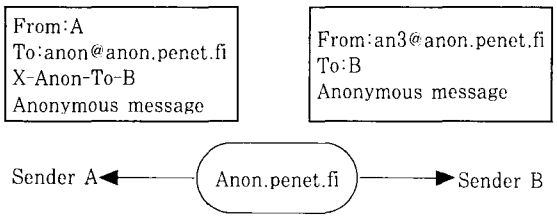
Shuffle Network는 MIX Network의 문제점인 안전성 향상을 위한 MIX 서버 개수를 증가시키고자 할 때 각 송신자가 보내어야 하는 메시지의 길이가 증가하는 점과 메시지 길이의 가변에 의한 공격에 취약한 점을 개선하기 위하여 제안된 방식이다. RSA 암호 방식을 사용하는 MIX Network에 비하여 ElGamal 암호 방식을 이용하는 Shuffle Network는 MIX 서버를 무한히 증가하여도 송신자가 전송하는 메시지의 길이에는 전혀 영향을 주지 않는 효율적인 방식이다.

즉, MIX Network에서 사용되는 랜덤 정보가 Shuffle Network에서는 지수승의 값으로 존재하여 기존 MIX Network가 제공하는 기능은 모두 제공하면서 메시지 길이의 증가는 발생하지 않는 특징을 갖고 있다. MIX Network와 Shuffle Network 공히 computational secure한 방식으로 sender and recipient anonymity를 제공하고 있다. Shuffle Network는 이러한 효율적인 측면에서 우수하여 많은 개선과 응용에 관한 연구가 활발히 계속되고 있다[15,25,26,27,28].

3. Anonymous Remailers

3.1 Type-0 Remailers[17,18,29,30,31]

단일 MIX 서버를 이용하여 메시지의 주소 등이 포



〔그림 2〕 Type-0 Remailer

함된 헤더 부분을 제거한 후 수신자에게 재전송하는 방식으로 〔그림 2〕와 같다.

Type-0 Remailer는 remailer(Anon Server)가 사용자의 실제 이메일주소와 가명 이메일 주소 매칭 테이블을 보관하여, 송신자가 보내어 온 송신자의 주소를 제거한 후 재송신하고 수신자에게는 가명 주소로 수신하게 하여 메일 송신자가 누구인지를 알 수 없게 하는 익명기술이다.

단일 MIX(Anon Server) 서버를 이용하는 Type-0 Anonymous Remailer는 송신자를 익명으로 할 수 있는 전자우편에 사용되는 방식으로 실제로 핀란드의 J.Helsingius에 의하여 Anon Server를 개설하여 운영하였다. 매일 7000여 통의 이용이 있을 정도로 활발하였으나 미국 FBI와 핀란드 경찰에 의하여 한 이용자의 주소를 유출하였다는 혐의를 받고 현재는 Anon Server가 폐쇄되어 사용되고 있지 않다[32].

Type-0 Anonymous Remailer는 사용하기가 쉬운 장점이 있으나 암호가 사용되지 않아 누구나 전송되는 메시지의 내용을 알 수 있으며, Anon Server의 입출력을 비교하여 추적을 용이하게 할 수 있는 점과 Anon Server가 Pseudo ID와 user ID와의 메핑 리스트 DB를 갖고 있어 DB의 안전성과 Anon Server의 신뢰성에 크게 의존하고 있는 점이 주요한 문제점이 되고 있다.

Type-0 Anonymous Remailer는 암호학적인 측면에서는 전혀 안전성이 없는 익명 방식이라고 말할 수 있다.

3.2 Type-1 Remailers[29,30,31,33]

Type-1 Anonymous Remailer는 Type-0 Remailer 방식의 문제점인 매칭 DB와 전송 데이터의 노출에 따른 문제점을 해결하기 위하여 만들어 진 것으로 remailer의 DB를 갖지 않으며 PGP 암호를 이용하여 암호문 수신, 복호 후 재송신하는 Remailer(MIX 서버) 체인을 갖는 Cypherpunk remailer 방식이다. MIX Network와 유사한 형태로 각 Remailer들은 암호문을 복호한 후에 다음 Remailer의 주소를 알고 암호화 된 메시지를 재송하게 되어, 최종적으로 누구에게 송신되는 메시지인지 모든 Remailers가 협력하지 않는 한 익명성이 유지되는 방식이다.

Remailer가 입력되는 메시지를 랜덤하게 순서를 바꾸지 않고 재전송하거나, 메시지의 크기를 추적하거나 또는 Replay 공격을 하는 등의 여러 가지 공격이 가능한 방식이다.

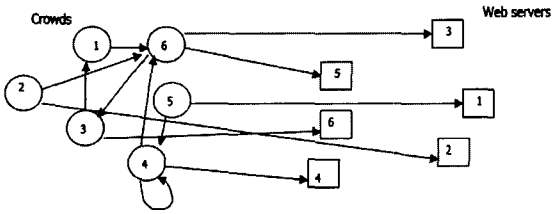
3.3 Type-2 Remailers[23,30,34]

Type-2 역시 Type-1 Anonymous Remailer의 안전성을 보다 강화한 것으로 D.Chaum이 제안한 MIX Network의 거의 유사하다. 암호를 이용하고 MIX Master Chain 형태를 유지하며 Replay attack, time/contents correlation attack 등을 고려한 코딩 방식에 의한 메시지 길이를 일정하게 하여 이전의 공격 방식들에 대한 안전성을 강화한 방식이다.

현재까지 제안된 Anonymous Remailers 중에서는 가장 안전한 방식으로 앞에서 설명한 MIX Network와 동일한 방식이라고 말할 수 있다.

4. Anonymous Web Transaction: Crowds[22]

익명으로 웹 브라우징을 할 수 있는 방안으로 단일 MIX 서버를 이용한 Anonymizer[18], pseudonyms을 이용한 Lucent Personalized Web Assistant[35], MIX Network을 이용한 Onion Routing[36], 상업적 MIX Network인 Zero Knowledge Systems사의 Freedom[37], 그리고 jondo 프로세서를 이용한 새로운 개념의 Crowds[22] 등이 있다. 여기서는 Crowds에 대하여 설명하고자 한다. Crowds[22]는 송신자의 익명성을 제공하며 MIX Network 보다는 효율적으로 월등한 방식으로 1996년 Reiter와 Rubbin에 의하여 제안되었다. Anonymous Web Transaction인 Crowds는 global eavesdropper에 대한 보호 대책이 없는 등 MIX Network 보다는 안전성이 아주 약한 방식이다. 이용자들은 jondo 프로세서라는 local machine으로 표현되는 다른 이용자 집합인 Crowds에 가입하여, jondo를 프록시로써 사용하도록 브라우저를 설정한다. jondo 들 사이의 통신은 사전에 공유된 암호 키를 이용하여 암호 통신을 행하며 이용자의 요청은 Crowds 가운데의 jondo들에게 랜덤하게 행하여지며 각 요청을 받은 jondo들은 웹 서버에 직접 전달하거나 랜덤하게 선택된 다른 jondo에게 전달할 수도



〔그림 3〕 Crowds 개념도

있다. 웹 서버 입장에서 보면 어떤 이용자가 요청하였는지 알 수 가 없으며, 즉 최종으로 요청한 이용자(jondo)가 최초의 요청자인지 아닌지, 어떤 Jondo와의 전달 과정을 거쳐 서버까지 오게 되었는지에 관한 경로 정보를 알 수 없어 송신자 익명성을 제공하게 되는 방식이다. 이를 도식적으로 표현한 것이 〔그림 3〕과 같다.

Ⅳ. 익명성의 역기능 그리고 고려사항

데이터 마이닝 기술, 해킹기술, 침입차단시스템이나 침입탐지시스템과 같은 네트워크 보호 장치와 같은 기술, 그리고 광범위하게는 정보화 기술 등은 동전의 양면과 같아서 e-privacy 보호 기술이 되기도 하며 침해 기술이 되기도 함을 알 수 있다.

한편, 암호 기술은 올바르게 사용되면 e-privacy 보호 향상에 크게 기여할 수 있으나 부정 사용을 하게 되면 즉, 유괴, 돈 세탁[38], 마약 거래, 무기 거래, 탈세, 위조 화폐, 불법 통신 수단, 테러 활용 등 법 집행 방해 또는 불능 상태를 야기하는 곳에 남용되면 오히려 암호 기술의 역기능만이 나타나게 된다. 암호의 양면성으로 인한 역기능을 방지하거나 줄이기 위해서는 적절한 규제, 키 복구 정책 등 법 집행 가능한 암호 사용, 즉 암호의 순기능과 역기능 의 적절한 균형 정책을 취하는 대책을 고려하게 된다.

익명성도 암호 기술과 마찬가지로 이러한 순기능과 역기능의 양면성[30,31]을 갖고 있다. HIV test, 언론 익명 제공, 증거 자료 제공, 화폐 등이 현용되고 있는 익명성의 순기능 측면에서 고려되고 있는 것이며 특히 e-privacy 보호 측면에서의 순기능은 아주 크다. 그러나, 인터넷에서의 익명성으로 인한 즉, 추적이 어려운 점을 이용한 음란물, 엽기, 폭력, 자살, 성매매, 반사회 사이트 등 불건전정보 범람, 사이버 성폭력, 언어폭력, 인신 공격 등 명예 훼손, 불법 복제(warez), 스팸 메일, DDoS 등 각종 해킹과 같은 역기능으로 인한 것도 아주 많다.

예를 들면, anonymous remailer를 이용하여 지적보호자료, 스파이 정보를 보내거나, 불법 자료, 스팸 메일 등을 배포할 수 있다. 익명 통신로가 해커에게 활용되어 서비스 거부 공격의 발신지를 익명으로 하는 데 활용될 수 있으며, Onion Routing도 해커에게 남용될 수 있다. 내용은닉서명도 완전한 범죄에 남용될 수 있으며 돈 세탁 등에 악용될 수 있다. 또한 이러한 익명성을 이용한 반 사회적인 행위 수단이 범람하는 반면, 익명행위자는 개인적인 피해가 없어 무책임하거나 행위결과에 대한 피해 부담이 적어 사회 전체가 전적으로 부담해야 하는 특성을 안고 있어 이러한 역기능은 계속되거나 확대되는 추세다.

더욱이, 기술적으로 범죄 유발 컴퓨터를 추적하는 것이 더욱 더 어려워지며 결국에는 법 집행이 곤란하거나 무력화되게 된다.

프라이버시 보호를 위한 익명성 제공에 따른 이러한 역기능을 방지하고자 프라이버시 보호 기술의 사용을 제한하거나 차단시킬 수는 없다. 왜냐하면, 사용 제한이나 차단이 먼저 익명성으로 인한 역기능 해소의 근본적인 해결책이 아니며, 프라이버시 보호를 위한 이용자들의 가능성을 크게 제한하는 결과가 되며 그리고 범죄자들은 추적당하지 않는 또 다른 수단이나 기술들을 찾기 때문이다.

물론, 익명성 제공을 통한 e-privacy 보호도 중요하지만 이로 인한 역기능에 대한 대책도 중요하다. 역기능 방지를 위한 적절한 규제와 순기능과 역기능의 적절한 균형 정책이 필요하다. 기술적인 관점에서 역기능 방지를 통하여 적절한 균형을 유지할 수 있는 대책들이 많이 연구되고 있다. 즉, 역기능이 발생할 시 e-privacy의 보호 기능을 다소 희생하여 역기능 제공자를 추적, 결과적으로 역기능을 방지하고자 하는 기술들이 많이 제안되고 있다.

e-privacy 보호기술 개발과 적용 확대는 익명의 가치에 대한 사회 평가에 크게 의존하는 특징을 갖고 있다. 현재의 e-privacy는 익명 그 자체의 가치에 의한 평가보다도 시장에 의한 상업적 가치나 범죄 예방 등의 가치에 의하여 평가되고 있는 실정이다. 예를 들면, D.Chaum이 설립한 네덜란드 Digicash사의 익명성 제공 전자화폐[19](프라이버시 강조)는 은행들의 실용전자화폐 방식(프라이버시보다는 이중사용방지 측면 강조)의 선호에 의하여 시장에서 평가받지 못하고 실패하고만 대표적인 사례가 될 것이다.

그리고 현존하는 익명성 구현 기술들의 익명성 제공은 극히 제한적으로 완벽하게 제공되지 못하고 있

다. 예를 들면, 전자 상거래에서의 전자화폐의 경우 인터넷을 통한 전자거래는 모두 익명으로 이루어지나 상품 배달 단계에서 상점에서 본인에게 전달하는 과정에서 상품 수령자의 주소나 관련 정보를 알게 되어 익명성 제공이 곤란해지는 등 완전한 익명성을 제공하기에는 한계[10]가 있다.

또한, 익명성 구현 기술의 수수료 및 사용 비용 문제, 성능지연, 비표준 등의 문제로 인하여 익명성 구현 기술의 활성화에 많은 문제점[10]이 있다. 그러나 이러한 문제점에도 불구하고 e-privacy 기능 향상에는 분명히 많은 기여가 있음은 확실하다.

익명성의 역기능을 고려하지 않은 e-privacy 보호 기술의 개발에는 한계가 있으며 e-privacy도 향상하며 역기능도 동시에 해결할 수 있는 방향으로의 기술 개발이나 정책들이 향후에는 보다 더 고려되어야 할 것으로 생각된다.

V. 결 론

e-privacy 보호를 위해서는 법 제도적(관리적) 보호가 아주 중요하며, 기술만으로는 해결이 쉽지 않으며 법 제도적 보호와 병행이 되어야 한다고 생각한다. 그리고 법 제도적 방안 외에 IT 기술에 의한 e-privacy 보호가 가능하다면 하나의 중요한 기여가 될 수 있다. 프라이버시 보호 기술의 연구 개발도 필요하며, 기술 개발 시에는 e-privacy 보호기술이 가져오는 역기능(특히 익명성으로 인한)을 해소하면서 프라이버시가 동시에 제공되는 기술 개발과 정책 추진이 바람직하다고 생각한다.

참고문헌

[1] Fischer-Hubner, "IT-Security and Privacy: Design and Use of Privacy Enhancing Security Mechanism", *LNCS 1958*, ISBN 3-540-42142-4, 2001.

[2] Ian Avrum Goldberg, A Pseudonymous Communications Infrastructure for the Internet, *PhD Thesis*, Univ. of California at Berkeley, 2000.

[3] 박춘식, "OECD, 프라이버시 그리고 시큐리티", *한국정보보호학회학회지*, 제6권 제3호, pp. 115-124, 1996.

[4] 조동기, 김성우,"인터넷의 일상화와 개인정보보호", *KISDI이슈리포트*, 정보통신정책연구원, 2003.

[5] http://www.epic.org/privacy/tools.html

[6] Takagi Hiromitsu, "RFID의 프라이버시(Japanese)", *IC Tag와 유비쿼터스사회연구위원회*, 2003.9.

[7] Takagi Hiromitsu, "Open화와 프라이버시 확보(Japanese)", *유비쿼터스 정보사회에서의 안심・안전한휴먼인터페이스에관한워크샵*, 2003.3.

[8] UMIST, Privacy Enhancing Technologies, State of the Art Review, http://www.co.umist.ac.uk/research/tech_reports/trs_2002_001_lam.pdf

[9] Roger Clarke, "Introducing PITs and PETs: Technologies Affecting Privacy", http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html

[10] 이인호, "정보통신기술의 발전과 프라이버시", 정보사회의 인권, *국가인권위원회 발간 자료집*, http://www.humanrights.go.kr/dataroom/committee_data/DacomitBookView.jsp?choice_board_id=all&search=이인호&choice=author&seqid=393&page_num=1

[11] 김 연수, 개인정보보호, *사이버출판사*, 2001.

[12] Part Hensley외 4, Implementation of OPS over HTTP, http://www.W3.org/TR/NOTE-OPS-OverHTTP

[13] http://www.w3.org/P3P/brochure.html

[14] 윤재석, " P3P 논의 현황과 문제점 및 국내 정책 방향", 2001.6, http://www.kisa.or.kr/Information_Security_Policy/Information_Security_Policy_m_02.html

[15] 박춘식, "안전하고 효율적인 익명통신로", *한국정보보호학회논문지*, 제6권 제1호, pp.3-14, 1996.

[16] A.Pfitzmann, "Anonymity, Unobservabiltiy, and Pseudonymity- A Proposal for Terminology", *Proceedings of Int'l workshop on Design Issues in Anonymity and unobservability*, LNCS 2009, pp. 1-9, 2000.

[17] Andre Bacard, Anonymous remailer FAQ, 1999, http://www.well.com/user/abacard/remail.html

[18] Anonymizer.com, http://www.anonymizer.com

[19] D.Chaum, "Blind Signatures for untraceable payments", *Proceedings of CRYPTO'82*, pp.199-203, 1983.

[20] A.Pfitzmann, B.Pfitzmann, M.Waidner, "ISDN-Mixes — Untraceable Communication with Very small bandwidth Overhead", *7th Intl' conf. on Information Security (IFIP/Sec'91)*, pp. 245-258, 1991.

[21] D.L. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", *Journal of Cryptology*, Vol. 1, No.1, pp. 65-75, 1988.

[22] M.K.Reiter and A.D.Rubin, "Crowds: Anonymity for Web Transactions", *ACM Transactions on Information and System Security*, Vol.1, No.1, pp.66-92, 1998.

[23] D.L. Chaum, "Untraceble Electronic Mail, Return Address, and Digital Pseudonyms", *Communications of the ACM*, Vol.24, No.2, pp. 84-88, 1981.

[24] C.S. Park, K.Itoh and K.Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology, *Proceedings of Eurocrypt'93*, pp. 248-259, 1993.

[25] C.S.Park and K.Kurosawa, "Secure Anonymous Channel against Active Attack", *Proceedings of 1995 Japn-Korea Joint Workshop on Information Security and Cryptology*, pp.15-23. 1995.

[26] M.Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers", *Proceedings of CRYPTO'98*, pp. 435-447, 1998.

[27] M.Jakobsson, "A Practical Mix", *Proceedings of CRYPTO'98*, pp.448-461, 1998.

[28] W.Ogata, K.Kurosawa, K.Sako and K. Takatani, "Fault Tolerant Anonymous Channel", *Proceedings of ICICS'97*, pp. 440-444, 1997.

[29] C.Gulcu and G.Tsudik, "Mixing Email with BABEL", *In Proceedings of the Internet Society Symposium on Network and Distributed System security, IEEE*, pp.2-16, 1996.

[30] Ian Goldberg, David Wagner and Eric Brewer, "Privacy-enhancing technologies for the Internet", *Proceedings of IEEE COMPCON*, 1997.

[31] Ian Goldberg, "Privacy-enhancing technologies for the Internet,II:Five Years Later", *The Workshop on Privacy Enhancing Technologies*, LNCS 2482, pp.1-12, 2002.

[32] Johan Helsingius,press release, 30 Aug, 1996. http://www.stack.nl/~galactus/remailers/index.html.

[33] Computer Cryptology, 2, December, 2001, http://www.faqs.org/faqs/privacy/anon-server/faq/use/part3/section-3.html

[34] Lance Cotrell, Mixmaster & remailer Attacks, 1995. http://www.obscura.com/~loki/remailer/remailer-essay.html

[35] Lucent Technologies, http://www.bell_labs.com/project/lpwa/

[36] M. G. Reed, P. F. Syverson and D. M. Goldschlag, "Anonymous Connections and Onion Routing:, *IEEE Journal on Special Areas in Communications*, Vol.16, No.4, pp. 482-494, 1998.

[37] P.Boucher, A.Shostack and I.Goldberg, Freedom Systems2.0 Architecture, December 2000, http://www.freedom.net/products/whitepapers/Freedom_System_2_Architecture.pdf

[38] 김춘수, 박춘식, 전희종, "익명통신로를 이용한 Escrow 전자화폐", *한국정보보호학회논문지*, 제9권 제1호, pp. 25-46, 1999.

〈著 者 紹 介〉

박 춘 식 (Choon-sik Park)
평생회원

1995년 : 일본 동경공업대학교 전기전자공학과 공학박사
1989년 - 1990년 : 일본 동경공업대학교 초빙연구원
1982년~현재 : 한국전자통신연구원 부설 국가보안기술연구소 책임연구원
2003년~현재 : 고려대학교 정보보호대학원 겸임교수
1990년~현재 : 한국정보보호학회 이사