PKI의 선택

홍 창 수*, 임 종 인*

*고려대학교, 정보보호대학원 정보보호학과

A Choice Of PKI

Chang-Su Hong*, Jong-In Lim*

*Graduate School of Information Security, Department of Information Security

Korea Univ.

요 약

본 논문에서는 PKI의 보급으로 변화 될 미래(가까운) 인터넷에서 개인의 프라이버시 침해와 관련하여, 고민해야 할 선택의 문제를 제시한다. 우리는 앞으로 규제되고 통제된 인터넷 공간에서 활동할 것이다. 그런데, 현실 공간과 사이버 공간에서의 가치충돌로 인해 발생할 당면 문제에 대해 우리는 문제 해결을 위해 현상을 해석하고, 여러 가지 해결 방안 중 사이버공간에 맞는 올바른 해석을 선택 해야한다. 한 예로 사이버 공간에서 행해지는 진보된 새로운 기술을 가진 감시자의 행위가 판단자(현실공간에서 삶을 영위하는 사람들)로 하여금 개인의 프라이버시 침해인 것인가에 대한 판단을 요구 할 것이다. 선택의 결과는 많은 논란과 여러 가지 해석의 차이를 불러일으킬 것이며, 그른 해석과 선택으로 인한 개인의 프라이버시 침해는 전혀 예기치 않은 곳에서 발생 할 것이다. 사이버 공간은 현실 공간과 유사하지만 전혀 다른 공간이다. 이에 따라 관련 법규의 해석과 적용 역시 현실 공간과 다르다. 이의 관점에서 현재 우리나라의 전자서명 및 전자거래 관련 법규와 PKI 구조에서 이에 따른 해석의 모델을 제시하고자 한다.

I. 서론

1890년 브랜다이스(Louis D. Brandeis) 대법관(당시 변호사)에 의해 "인간의 존엄성과 재산의 측면에서 마땅히 보호되고 지켜져야 할 법의 본질이며, 법의 근본원리로 그 개념은 점점 더 확대될 것이다" 라는 프라이버시에 대한 역사적 최초의 언급[1]이후 개인의 프라이버시는 시대를 앞선 그의 견해처럼 현대 생활에서 폭 넓게 해석되며, 중요한 요소로 자리 잡았다. 미국의 수정헌법[2]에서는 프라이버시와 관련된 법조문으로 4조, 5조, 9조가 주로 언급되고 있으며, 미국의 판례에서 프라이버시와 관련하여, 기술이 가져온 변화된 환경에 따른 위 조항의 해석여부를 놓고 역사적인 논란이 이루어지기도 했다[3][4].

21세기를 살아가고 있는 우리는 앞서 소개한 역사적인 판례사건보다 더 놀랍고 상상하기 힘들 정도의 기술의 발전과 그로 인한 새롭고 변화된 환경 속에서 삶을 영위하고 있다. 미국 국방부의 고등연구계획국(Advanced Research Projects Agency : ARPA)에 의해 1969년 설립된 군사목적의 컴퓨터 네트워크인 ARPANET[28]으로부터 출발한 Internet은 학문분야에서 꽃 피웠고 더 나아가 채팅, Cafe, 게임, 멀티미디어, 아바타 공간으로 그리고 전자상거래라는 실질적인 현물거래 및 사이버 거래가 이루어지는 공간으로 그 영역이 점점 더 확대 되어가고 있다. 현 시대를 살아가고 있는 사람들에게 사이버 공간은 말 그대로의 가상 공간이 아닌, 현실 공간의 확장된 개념으로 자리잡고 있으며, 현실 공간과 사이버 공간의 구분은 모호함을 더해가고 있다. 현실 공간은 아바타가 활동하는 사이버 공간으로 그 삶의 영역이 확대 되어가고 있는 것이다.

인터넷 초창기의 모토는 자유(Freedom)와 공개(Open) 그리고 익명성(Anonymity)이었다. 초창기 인터넷의 세 가지 미덕은 MIT교수인 리처드 스톨만(Richard Stallman)의 주도로 진행중인 자유 소프트웨어 재단 FSF(Free Software Foundation)의 GNU(GNU' s Not UNIX) 프로젝트[5]를 탄생시켰고, GNU 프로젝트를 필두로 현재의 인터넷은 괄목할만한 발달을 해 왔음은 누구도 부인 할 수 없을 것이다. 그러나, 자유, 공개, 익명의 세 덕목은 사이버 공간에서의 기하 급수적으로 증가하는 범죄를 효과적으로 막을 수 없었다. 증가하는 범죄와 악의적인 코드로 인해 인터넷 공간은 규제 불능의 사태에 직면하기도 하

며, 사이버 공간의 질서가 어지럽혀지고 있다.

국제적인 전산망 침해사고 대응 팀 CERT의 최근 보고에 따르면 조사가 이루어진 최초 1988년에는 신고 접수된 사고가 6건에서 현재 2002년 1분기에는 그 신고된 접수 건수가 무려 73,359건에 달하고 있다[6]. 사이버 공간에서의 범죄행위는 [표1]에서 살펴보듯이 최근 들어 급증하고 있으며 이에 대한 대책 마련이 시급한 상황이다.

표1: 연도별 보고된 침해사고 접수건수

Year	Incidents
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1,334
1994	2,340
1995	2,412
1996	2,573
1997	2,134
1998	3,734
1999	9,859
2000	21,756
2001	52,658
Q1~Q3, 2002	73,359
Total incidents reported	173,728

표 1 연도별 보고된 침해사고 접수건수

사이버 공간의 모토는 이제 자유는 "규제와 통제(Control)"로, 공개는 "보호(Security)"로, 익명은 "인증(Authentication)"이라는 새로운 모토로 바뀌어가고 있다. 사이버 공간은 새로운 모토에 걸 맞는 새로운 기술(PKI : 공개키 기반구조)을 채택했고, 이 새로운 기술은 기술 선진국을 중심으로 국가적인 지원을 받으며, 인터넷의 기반구조로 자리잡아가고 있다. 머지 않은 미래에 우리는 규제와 통제, 보호, 인증이라는 성격의 사이버 공간에서 새로운 생활을 맞이할 것이다.

미국의 프라이버시권과 관련된 수정헌법 각 조항들은 (4조, 5조, 9조) 현실세계에서의 논쟁을 거쳐[3][4] 사이버 공간에서도 문제해석과 문제 해결을 위한 선택이라는 관점에서 우리에게 시사하는 점을 많이 제공 할 것이다. 본 논문에서는 이와 같은 관점에서 새로운 모토로 우리에게 다가온 사이버 공간에서 발생할 개인의 프라이버시 침해는 어떻게 발생할 것이며, 이를 해결하기 위한 해석과 선택의 모델을 제시하고자 한다.

II. BlindNet v. AuthNet

2.1 PKI(Public Key Infrastructure, 공개키 기반구조)

기원전 2000년부터 사용된 암호는 1976년 Diffie와 Hellman에 의해 고안된 공개키 개념[7]이 등장하기 전까지 치환기법과 순열을 이용한 방법으로 암호화를 하는 암호화 키와 복호화 키가 동일한 대칭키 암호화 방식을 사용했다. 그러나 동일한 키를 사용할 경우 송신자와 수신자간에 키를 어떻게 분배할 것인가의 키 분배 문제와 메시지가 누구로부터 작성된 것인가에 해당하는 전자서명 기능이 어렵고, 복잡하다는 문제점이 있다. Diffie와 Hellman에 의해 제안된 암호화 키와 복호화 키가 서로 다른 비대칭키 방식의 공개키 암호화 기법은 암호학의 새로운 방법을 제시한 혁명적인 사건이었다. RSA[8]의 개발 이후 공개키 암호화는 널리 사용되었고 각종 프로토콜의 설계와 암호의 응용에 폭넓게 사용되고 있다. 공개키 암호화의 공격대상이 될 수 있는 공개된 공개키의 소유 증명을 위해 제 3의 신뢰기관(인증기관, CA: Certificate Authority)이 필요하게 되었고, 공개키의 소유 증명을 밝히는데 사용될 증명서(인증서, Certificate)가 탄생하게 되었다. 인증서의 용도는 공개키에 대한 소유증명 뿐만 아니라, CA에 의해 인증서 발급을 위한 등록과정에서 먼저 신원증명이 철저하게 이루어지며, 신원이 증명된 사용자에게 인증서 사용자의 구별되는 정보(DN: Distinguished Name)와, 사용자의 e-mail 정보 등이 인증서 안에 포함되기 때문에, 인터넷이라는 가상 공간의 여권과 같은 역할을 수행한다. 여권 소지를 밝히기 위해 현실 공간에서는 상대방에게 소지하고 있는 여권을 보여 주지만 PKI 구조의 사이버 공간에서는 인증서 기반의 인증시 사용자는 사용자의 인증 정보(user's authentication information)에 대해 전자서명을 수행한다. 기존의 ID/PWD 방식의 사용자 인증을 기본인증(Basic Authentication[26], Simple Authentication[27])이라 한다면 인증서 기반의 전자서명을 통한 사용자 인증을 강한인증(Strong Authentication)[26][27] 이라 한다.

인증서와 전자서명에 의한 손쉽고 강력한 인증 절차는 인터넷의 근본구조를

자유 ⇒ 규제와 통제

공개 ⇒ 보호

익명 ⇒ 인증

으로 바꾸어 놓을 사이버 공간이 선택한 새로운 기술이며, 도구이다.

PKI(Public Key Infrastructure)는 공개키 암호 시스템을 사용할 수 있는 기반구조로 특히, 인증기관에 의해 발행된 인증서를 이용한 공개키 암호 기반 구조를 말하며, [표2]와 같은 전자서명의 제반 기능들을 사용 할 수 있는 기반기술을 제공한다.

표2: 전자서명의 기능[29]

보안 서비스	설 명
전자서명의 위조불가 (Unforgeable)	합법적인 서명자만이 전자서명을 생성 할 수 있음.
서명자 인증 (User Authentication)	전자서명의 서명자를 불특정 다수가 검증 할 수 있어야 함.
부인봉쇄 (Non-Repudiation)	전자서명자는 전자서명행위 후에 서명한 사실에 대해 부인 할 수 없음.
변경불가 (Unalterable)	서명한 문서의 내용을 변경 할 수 없음
전자서명의 재사용 불가 (Not Reusable)	전자문서의 전자서명을 다른 전자문서의 전자서명으로 사용 할 수 없음.

표 2 전자서명의 기능

2.2 BlindNet, AuthNet, BrightNet

인터넷이라는 사이버 공간을 앞서 인터넷의 근본구조라 소개했던 {자유, 공개, 익명}과 {규제와 통제, 보호, 인증}이라는 세 가지 요소를 가지고 다음과 같이 분류할 수 있다.

- BlindNet
- AuthNet
- BrightNet

2.2.1 BlindNet

BlindNet = {자유, 공개, 익명}은 익명성이 보장되는 사이버 공간이다. 사용자의 행동을 감시하는 감시자 또한 존재하지 않으며 자유롭다. mp3 파일이라든가 소프트웨어의 등 모든 것이 공개되어 있고, 배포 또한 자유롭다.

2.2.2 AuthNet

AuthNet = {규제와 통제, 보호, 인증}은 PKI를 기반구조로 채택하며, 모든 데이터는 전자서명 방식에 의해 처리되어 전송되는 익명성이 보장되지 않는 사이버 공간이다. 전자서명 과정을 거치기 때문에 인가되지 않은 사용자는 활동 할 수 없으며, 인가된 사용자라도 구획기법(Zoning)에 따라 규제와 통제를 받게 되어 인가된 활동, 인가된 공간으로만 이동이 가능하다. 또한 mp3 파일이나 소프트웨어 등의 저작권은 보호되어 관리된다.

AuthNet은 효율성만을 고려한 구조로 잦은 전자서명의 부담을 없애 부담을 최소화하는 프라이버시는 보호 하지만, 존엄성으로서의 프라이버시[14]가 보호되지 않는 구조로 설계되어 있다. 즉 전자서명 행위는 이루어지나, 개인키를 응용프로그램에서 관리한다. 일단 사용자에 의해 최초의 전자서명 행위가 이루어지면(개인키는 PKCS#5[21]표준에 따라 password로 암호화되어 저장되어 있을 것이다. 최초의 전자서명 행위란 암호화되어 저장되어 있는 개인키를 복호화 하여, 언제든지 응용프로그램이 사용 할 수 있게 메모리나 임시파일 형태로 가공함을 의미한다.), 이후의 전자서명 과정은 사용자 자신도 모르게 응용프로그램에서 행하여지게 된다. 즉 인증과정(Strong Authentication)을 거쳐 서버에 접속한 사용자는 서버 접속 이후의 전송되는 데이터가 전자서명 되어 전송되는지 또한 어떤 데이터가 전송되는지 전혀 확인할 수 없는 구조의 사이버 공간이다.

최악의 상황으로 서버접속 이후의 모든 행위는 전자서명 되어 서버로 전송되며, 서버는 관리 정책에 따라 전자서명 데이터의 모든 데이터 혹은 중요한 행위에 대해 수집, 보관할 수 있다.

2.2.3 BrightNet

BrightNet = {자유, 공개, 익명 || 규제와 통제, 보호, 인증}은 BlindNet의 익명성과 자유 공개의 정신을 존중하며, 필요에 따라 사이버 공간을 규제하며, 통제한다. 컨텐츠 및 지적 재산권 보호를 위한 장치가 마련되어 있고, 지적 재산권의 공정사용과 같은 공공의 사용을 위해서는 공개와 허용을 원칙으로 한다. 즉, BrightNet은 BlindNet과 AuthNet의 구조를 모두 가진 사이버 공간이다.

사용자는 사이버 공간상의 자신의 위치(BlindNet에 있는지, AuthNet에 있는지)를 시각적으로 확인 할 수 있으며, AuthNet에서의 전자서명 시 전자서명 되는 데이터의 내용을 확인 할 수 있도록 설계되어 있다. 즉 공개된 규제, 규제의 투명성을 통해 AuthNet에서는 고려되지 않은 존엄성으로서의 프라이버시[14]를 보호한다.

2.2.4 사이버 공간의 설계자

앞서 살펴본 사이버 공간은

{자유, 인증, 익명, 공개, 규제와 통제, 보호}라는 요소들로 이루어진 공간이다. 이들 요소들은 사이버 공간 곳곳에 흩어져 고루 분포하고 있다. 그렇다면, 무엇이 이들의 성질을 분류하여 BlindNet, AuthNet, BrightNet 등으로 구분 지어 놓았는가? 사이버 공간은 진화하는 생명체가 아니다. 무엇인가에 의해 만들어지는 공간이다. 그 무엇은 사이버 공간을 움직이게 프로그램 짓는 수많은 S/W 들로 구성되어진다. 그리고 이것들이 서로 맞물려 돌아가면서 사이버 공간을 구성하게 된다. BlindNet을 AuthNet으로 바꾸려면 PKI를

채택한 S/W를 사용하면 손쉽게 해결된다. AuthNet을 BrightNet으로 바꾸려면 프라이버시의 어떠한 성질을 보호 할 것인가를 고민하여 기존 S/W를 수정하거나, 교체하면 가능할 것이다.

사이버 공간은 S/W에 의해 진화하며, 완성되어지는 공간인 것이다.

III. 해석과 선택의 문제

3.1 해석(Translation)

미국의 헌법학자이며, 사이버 법리학의 선두 역할을 하고 있는 로렌스 레식(Lawrence Lessig) 교수의 의견에 따르면, 현재의 문맥에서 원래 헌법의 고유 의미를 보존하기 위한 해독방법을 찾아내려고 하는 것이 해석(Translation)의 전략이며. 해석은 기술의 발전과 변화된 환경으로서의 사이버 공간이 제기하는 선택의 문제를 다루는 한 방법으로 정의하고 있다. 그 방법의 근본 기준은 다음과 같다.

(1) 과거로써 충분한가?

(2) 헌법 제정자들이 다루지 않은

선택들이 있는가?

(3) 우리가 결정할 수 있는 선택들인가?

1928년 美 연방정부에 의해 행해진 영장이 발부되지 않은 상태의 도청을 놓고 벌어진 Olmstead v. United States 판결[3]에 대해 대법관들의 상반된 헌법 해석(Translation)의 차이는 흥미롭다. 인터넷이라는 사이버 공간이 현재를 살아가고 있는 우리에게 초창기의 모습처럼 전문적이거나, 생소한 공간이 아닌 쉽고, 친숙한 공간으로 현재 사회 전반에 보급되었듯이 당시 미국에서 전화는 널리 보급된 통신 수단이었으며, 이를 감시하기 위한 전화 도청은 상당히 효과적이며 진보된 새로운 기술이었다.

Olmstead사건의 문제는 영장 없이 범죄의 증거가 감시되고 수집된 것이었는데, 부당한 수색이나 체포로부터 신체, 가택, 서류 및 동산의 안전을 보호받아야 할 개인의 권리를 침해해서는 안되며, 이때의 영장 발부 조건에 대해 명시하고 있는 미국의 수정헌법 제4조[2]의 해석에 대한 공방이었다.

태프트(William H. Taft) 대법원장은 판결문에서 " …압수 및 수색은 없었으며, 증거는 청각만을 사용해서 수집된 것이다… 수정헌법[2] 제 4조의 조항은 피고인의 집이나 사무실로부터 모든 세계로 연결되는 전화선을 포함하는 것으로 확대될 수 없다[3]." 라고 판결을 내렸다.

반면 브랜다이스 대법관은 "수정헌법이 제정될 당시 프라이버시를 침해 할 수 있는 수단으로써의 침입과 같이 도청 역시 새로운 기술, 변화된 환경에서 개인의 프라이버시를 침해 할 수 있는 수단으로, 따라서 수정헌법[2] 제4조의 보호를 받아야 한다" 라는 반대 의견을 제시하였다.

앞서 제시한 해석(Translation)의 전략 관점에서 보면 기술의 발전과 변화된 환경에서 원래 헌법의 고유 의미를 보존하기 위한 해독방법을 찾아 내려한 브랜다이스 대법관의 주장이 수정헌법[2] 제 4조의 조항을 올바르게 해석하여 내린 올바른 판단이었다. 또한, 시간과 문맥을 넘어서 그 의미와 가치를 보존할 수 있도록 헌법을 독해해내는 모델을 제공해 주었다[9]. 그러나 브랜다이스 대법관의 이러한 해석이 받아들여지는데 1967년 Katz v. United States 판결[4]이 있기까지 40년의 세월이 걸렸다.

3.2 프라이버시와 공간

1900년대에 걸친 미국에서의 판례와 비슷한 상황을 현재의 좀 더 진보된 기술과 변화된 환경의 사이버 공간으로 옮겨보자. 먼저, 사이버 공간을 고려하기에 앞서 프라이버시가 보호되지 않는 현실 공간을 다음과 같이 분류 할 수 있다.

(1) 공개된 공간

(2) 묵시적 동의에 의해 자신에 대한

감시를 허용한 공간

(3) 감시가 몰래 이루어지는 공간

3.2.1 공개된 공간

현실세계에서 프라이버시가 보장될 수 없는 가장 쉬운 예를 찾아보면 사람들이 많이 찾는 광장, 시장과 같은 개방된 공간을 들 수 있다. 그러나 이러한 곳은 프라이버시를 보호받을 수는 없지만 개인의 행동을 특정 감시자가 감시하거나 감시된 정보를 수집하지 않는다.

3.2.2 자신에 대한 감시를 허용한 공간

그렇다면 은행을 생각해 보자. 은행은 사람들이 많이 오가는 그 자체만으로 프라이버시가 보호 될 수 없는 공간이다. 게다가 곳곳에 여러 대의 감시카메라가 작동되고 있으며, 촬영된 정보는 일정기간 보존되어 진다. 어느 누구도 은행 ATM 기계 앞에서 개인의 프라이버시가 보호되리라고 생각하는 사람은 아무도 없을 것이다. 그렇다면 은행의 이러한 행위가 불법인 것인가? 은행에 들어서기 전 우리는 은행 유리창에 *"CCTV 작동중"* 이라는 스티커를 볼 수 있다. 은행 안에 들어가서도 이와 같은 스티커는 손쉽게 찾을 수 있다. 은행은 개인의 행동을 감시카메라로 감시하고 있다는 것을 고객에게 공개하고 있는 것이다. 만

약 고객은 개인의 행동이 감시된다는 사실을 알고 그것이 싫다면 감시카메라가 설치되어있지 않은 은행을 찾아가면 될 것이다.(시골의 작은 읍, 면 단위의 은행이면 모를까 요즘엔 거의 다 설치가 되어있는…) 감시 카메라가 설치되어 있으며 촬영된다는 사실을 알면서도 우리는 은행이 주는 인센티브-저축에 대한 이자와 안전한 금융자산 보호-때문에 은행이 나를 감시하도록 허용(묵시적 동의)한 것이다. 이 경우 은행의 감시카메라 작동은 개인의 묵시적 동의를 얻은 것으로 프라이버시 침해라고는 볼 수 없을 것이다.

3.2.3 감시가 몰래 이루어지는 공간

반면 은행이 감시카메라에 대한 설치와 그 사실을 고객에게 공개하지 않고 몰래 천장 안에 숨겨서 고객들을 감시하고, 감시된 데이터를 보관한다고 가정하자. 만약 이 사실을 알게 된 고객이 있다면 개인의 프라이버시 침해로 은행을 고소할 것이고, 정당한 사유가 인정되지 않는 한 은행은 불법적인 고객의 감시와 감시데이터의 보관으로 인한 개인의 프라이버시 침해로 패소 당할 것이다.

또 다른 예로1928년의 Olmstead 판결을 뒤집은 역사적인 1967년 Katz v United States 판결[4]은 공중전화 부스밖에 도청장치를 부착하여 전화통화 내역의 절반 정도를 녹음한 사건으로 40년전 브랜다이스 판사의 의견에 따라 Olmstead 판결과 그에 근거해서 내려진 수많은 판결들이 파기되었다.

3.2.4 사이버 공간은 어떠한가?

PKI구조는 국가적인 지원을 받으며, 머지 않은 시점에 우리에게 새로운 구조의 사이버 공간으로 다가 올 것이다. 어제 접속했던 인터넷 웹사이트가 내일에는 새롭게 개편되어 PKI구조가 적용되어 있을 것이다. PKI가 앞장에서 가정한 AuthNet의 구조로 구성되었다고 가정하자. 그 사이트에 접속하려면 사용자는 인증기관으로부터 발급 받은 공인인증서를 가지고 강한 사용자 인증(Strong Authentication, 전자서명)을 수행하여야만 하며, 서버는 전송되어 온 사용자의 인증정보(전자서명 데이터)에 대해 전자서명 검증을 수행한다. 전자서명 검증이 성공적으로 수행된다면 서버는 그 사용자를 인가된 사용자로 간주하고 서버 접속을 허용 할 것이다.

- 그리고는 이렇게 할 것인가?
- 나의 행위를 감시 할 것인가?
- 나를 그냥 내버려 둘 것인가?

PKI 구조(AuthNet)상 사용자는 자신의 신원증명을 전자서명이란 행위를 통해 손쉽고 강력하게 증명 할 수 있다. 반면 서버는 사용자가 서버 접속 후 행한 행동들에 대해 사용자로 하여금 전자서명케하여, 전자서명 된 데이터를 수집했다면, 사용자의 행동을 부인봉쇄 시킬 수 있다. 이 또한 전자서명 기술을 통해 증명 할 수 있다.

즉, PKI이전의 넷 구조(BlindNet)상에서는 힘들게 혹은 어쩌면 불가능하게 여겨졌던 사용자 인증과 행위에 대한 부인봉쇄가 사이버 공간의 구조를 바꿈으로써 손쉽게 해결된다.

접속을 허용한 서버는 나의 행위를 감시 할 것이다. 적어도 중요한 행위에 대해서 틀림없이 전자서명을 요구 할 것이다. 전자서명 시 개인키는 암호화되어 저장[21]되어있기 때문에 이를 사용하려면 개인키 패스워드를 입력해 복호화 한 후 사용해야 한다. 만약 전자서명이 빈번하게 이루어진다면 응용 프로그램은 전자서명에 대한 사용자의 부담을 줄이기 위해 인증서 기반의 강한 사용자 인증을 수행할 때(전자서명이 여러 번 이루어진다고 가정했을 때 첫 번째 수행하는 전자서명) 사용자에게 개인키 암호화용 패스워드를 묻고, 그 패스워드를 메모리 혹은 임시 파일 형태로 간직하고 있을 것이다. 그 이후의 전자서명 과정은 응용프로그램 스스로 수행하고 서버로 전송할 것이다(물론 이에 대한 보안강도(Security Level)의 세팅은 사용자의 환경설정에 의해 이루어지리라 생각되지만…).

앞의 시나리오에서 우리는 AuthNet에서의 전자서명 수행 과정과 서버의 전자서명 된 데이터의 수집의 예를 들었다.

3.3 PKI와 개인의 프라이버시

새로운 기술, 변화된 환경으로서 AuthNet에서의 개인의 프라이버시 침해는 어떠한 형태로 발생 할 수 있는가? 새로운 사이버 공간 PKI에서의 개인의 프라이버시를 침해 할 수 있는 요소를 찾기 위해 관련 법 조항을 살펴보면 다음 [표3]과 같다.

표 3: 관련법률

법 률 명	법률 제정 목적
전자서명법 법률 제 6,585호	- 전자문서의 안전성과 신뢰성 확보 - 전자문서의 이용을 활성화하기 위해 전자서명에 관한 기본적인 사항을 규정
정보통신이용촉진 및 정보보호등에관한 법률 법률 제 6,360호	- 정보통신망 이용 촉진 - 정보통신 서비스 이용자의 개인정보 보호 - 정보통신망을 건전하고 안전하게 이용할 수 있는 환경 조성
전자거래기본법 법률 제 5,834호	- 전자문서에 의한 거래의 법적 효력을 명확히 함. - 전자거래 촉진

표 3 관련 법률

3.3.1 정의(개인정보, 전자서명)

"전자서명법" "제1장 총칙 제2조(정의) 13항"[10]과 "정보통신망이용촉진및정보보호등에관한법률"[11] "제 4장 개인정보의 보호"에 의하면 *개인정보*란(개인정보: 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알 아 볼 수 있는 것을 포함한다.)) 이다.

한편 *개인정보를 수집하는 경우* "정보통신망이용촉진및정보보호등에관한법률"[11] "제 4장 22조에 근거, 당해 이용자의 동의를 얻어야 하며, 또한 개인정보 수집 시 필요한 최소한의 정보를 수집해야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 당해 서비스의 제공을 거부하여서는 안 된다. ("정보통신망이용촉진및정보보호등에관한법률"[11] "제 4장 23조)

*전자서명*은 "전자서명법" "제1장 총칙 제2조(정의) 2항"[10]과 "전자거래기본법"[12] "제1장 2조"에 의하면 "전자서명이라 함은 전자문서를 작성한 작성자의 신원과 당해 전자문서가 그 작성자에 의해 작성되었음을 나타내는 전자적 형태의 서명을 말한다."

3.3.2 PKI로 확장된 사이버 공간에서의 개인정보에 대한 해석

PKI에서 수행되는 전자서명과정과 전자 서명 검증과정은 아래 [그림1]과 같다.

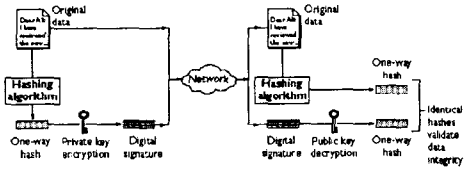

그림 1: 전자서명 및 전자서명 검증

서명자는 서명하려는 원본 전자문서를 해쉬함수를 사용해 One-way hash 값을 만들어내고, 그 값을 서명자 자신의 전자서명 생성키(개인키)를 사용해 암호화하여 전자서명값을 만들어낸다. 그렇게 해서 만든 전자서명 값을 보통

원본데이터 || 전자서명값 || 인증서

와 같은 데이터 구조로 전자서명을 검증하려는 사람에게 전송하면 검증자는 원본 데이터를 해쉬함수를 이용해 직접 One-way hash 값을 만드는 Re-hash 과정을 수행한 후 서명자가 보내준 전자서명값을 서명자의 인증서에 포함된 전자서명 검증키(공개키)로 복호화 하면 서명자가 전자서명 값 생성시 중간에 만들었던 One-way hash 값을 얻을 수 있다. 이렇게 해서 검증자는 Re-hash 한 값과 서명자의 전자서명 검증키로 서명값을 복호화 하여 얻어낸 One-way hash 값과 비교하여 일치하면 옳은 전자서명 값임을 확인 할 수 있다.

실제 전자서명 데이터 생성 시, 위와 같이 각 값들을 따로 전송하기도 하지만, 전자사명 데이터는 암호화 데이터, 전자서명 데이터의 구문 표준 문서인 PKCS#7 "Cryptographic Message Syntax standard"[22] 에 따라 다음과 같이 표현된다.

Version
DigestAlgorithm
ContentInfo(원본데이터)
Certificates(optional)
crls(optional)
SignerInfo(전자서명값)

그림2 : PKCS#7 Format

그렇다면, 전자서명 데이터가 개인정보가 될 수 있는 가능성을 살펴보자. 어떤 사람이 인터넷 뱅킹을 통해 계좌 이체를 수행했다고 보자.

원본데이터를 그 자체만으로는 개인정보라 할 수 없는 값으로 다음과 같이 설정해보자.

이체 수신 계좌 : 008-0975439-9xx **이체 금액 : 100,000원**

이 데이터를 전자서명 수행 한 후 전자서명값과 서명자의 인증서를 같이 첨부하여 PKCS#7[22] 포맷으로 검증자에게 보냈다고 하자. 검증자는 전자서명 검증 과정을 통해 서명을 수행한 사람이 누구이며, 이 데이터 역시 서명을 수행한 사람이 작성한 것임을 확신할 수 있다. 물론 이것은 전자서명이라는 개념 자체가 의도하는 바이므로 매우 성공적인 결과이다.

그러나, 개인정보의 차원에서 생각한다면 서명되기 전 원본 데이터는 데이터 원문 생성자가 누구인지 알아볼 수 없는 데이터이다. 그러나, 서명된 데이터는 서명 검증이라는 과정을 거치게 되면, 서명을 누가 했으며, 데이터의 내용 역시 위변조 되지 않았음을 알 수 있는 아주 중요한 개인정보가 되는 것이다(개인정보 : 당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알 아 볼 수 있는 것을 포함한다[10][11].).

원본 데이터가 위 예시처럼 단순한 값이 아니라, 만약 어떤 사람이 해당 사이트에 들어와서 어떤 순서로 무슨 작업을 행하는지, 그리고 타이핑되는 정보를 3.2.4에서 AuthNet의 시나리오처럼 사용자 모르게 응용프로그램이 전자서명을 수행하여 서버로 전송한다면 이것은 현재 존재하는

어떠한 트로이목마 해킹 툴 보다 강력한 해킹 툴이 될 것이다. 왜냐하면, 전자서명 검증은 서명자의 인증서와 해쉬 알고리즘만 알게 되면 전자서명을 불특정 다수가 검증 할 수 있기 때문이다. PKCS#7[22] 포맷은 이 조건을 모두 만족하고 있는 데이터 포맷인 것이다. 문제는 전자서명 데이터가 전자서명 검증을 통해 개인임을 판별 할 수 있는 개인 정보임에도 불구하고 현재 개인 정보라 하면 이름, 주민등록번호, 전화번호 등의 명시적으로 개인을 알아 볼 수 있는 것들로 협의적으로 이해하고 있다는 것이다[23][24].

실제로 PKI 공인인증체계에서 전자서명을 통한 인터넷 뱅킹 서비스를 제공하는 인터넷 뱅킹 웹사이트에서조차, 개인정보를 위에서 열거한 협의의 개념으로 사용하고 있다는 것이다. 그리고, 어떠한 정보가 전자서명 되어 은행 서버로 전송되는지 전혀 사용자는 알 수 없게 되어있다.

3.3.3 규제의 공개와 투명성

"전자서명 데이터의 수집과 보관의 어떠한 측면이 개인의 프라이버시를 침해 할 것인가?" 라는 질문에 대한 해답의 열쇠는 전자서명 데이터에 대한 데이터의 공개성과 전자서명 데이터를 수집하고 보관한다는 사실을 사용자에게 공개하는 부인봉쇄의 투명성 여부에 달린다.

따라서 전자서명 된 전자적 형태의 정보-전자문서는 개인정보에 해당하며, 그리므로 전자서명 된 전자문서의 전자거래 시 전자서명 된 전자문서의 수집 및 보관 에 대해 "정보통신망이용촉진및정보보호등에관한법률" [11] "제 4장 22조에 따라 사용자의 동의를 얻어야 한다.

PKI가 적용된 가장 좋으며, 많이 보급된 사례로 인터넷 뱅킹[20]을 들 수 있다. 인터넷 뱅킹 시 사용자는 공인인증기관에서 발행한 인증서를 사용하며, 뱅킹 거래 시 전자서명의 절차를 거친다. 그러나, 인터넷 뱅킹 측에서조차 개인정보를 명시적인 개인 데이터만으로 국한시켜 정보보호정책이 수립되어 있다는 것이다. 또한 인터넷 뱅킹 시 사용자는 어느 정보가, 어느 시점에서 전자서명 되어 전송되는지 알 수가 없다. 즉 다시 말하면, PKI 구조의 사이버 공간에서 사용자는 자신의 무슨 데이터가 감시되고 부인봉쇄 되는지를 사용자는 알아야 할 권리가 있음에도 불구하고 PKI 응용 프로그램들을 통해 알 수 없는 것이 현실이다.

현재의 PKI를 구성하고 있는 사이버 공간은 BrightNet이 아닌 AuthNet인 것이다.

또 다른 예로 SSL v3.0[25]은 인증서기반 로그인에 의한 Strong Authentication 기능을 지원하고, transaction non-repudiation[13]도 가능하다.

주목할 것은 두 번째 사항인 Transaction non-repudiation이 가능하다는 것이다. 전송되는 데이터에 대해 전자서명을 수행하게 되면 Transaction non-repudiation이 가능한 것이다.

3.4 선택

프라이버시는 개념에 따른 세 가지 형태로 구분될 수 있다[14].

(1) 부담을 최소화하는 프라이버시

(2) 존엄성으로서의 프라이버시

(3) 실질로서의 프라이버시

이 분류의 관점에서 미국의 휴대폰 위치 추적에 대한 논의를 살펴보자. 미국 연방수사국(FBI)은 공공의 안전을 이유로 휴대폰의 위치 추적이 가능하도록 강력하게 요구하고 있다. 이 사안에 대해 CDT(Center for Democracy and Technology, http://www.cdt.org)는 프라이버시 문제를 최소화하면서 유용한 시스템을 설계하도록 하는 의견을 제시했는데, 응급환자가 발생하거나 위급한 상황이 발생했을 때 911에 휴대폰으로 전화를 걸어 신고했을 때만 위치가 파악되도록 하는 것으로, 911 서비스가 발신지의 위치를 파악하는데 많은 도움을 줄 것이다[15]. 이 경우 휴대폰을 사용하는 사람들의 개인의 위치가 노출되는 부담을 최소화 할 수 있으며, 911에 전화를 했을 때에만 위치가 노출되므로 무작위 적인 감시를 당하게 될 때 발생할 존엄성이 무시 될 가능성이 최소화된다. 또한, 이러한 프라이버시 보호 조치는 위치 추적을 통해 규제를 강화하려는 美 연방수사국(FBI)의 권한에 실질적인 제한을 두게 된다. 美 연방수사국(FBI)도 CDT(Center for Democracy and Technology)의 의견에 이러한 가능성을 검토하였다

911에 전화했을 때에만 위치 추적이 가능하도록 하는 것은 기존 시스템의 S/W의 변경, 수정, 추가를 통해 이와 같은 새로운 시스템으로의 변경이 가능하다.

이 사례는 S/W를 수정함으로써 개인의 프라이버시를 최소화시키면서 유용한 시스템을 만들 수 있다는 가능성을 보여준다.

그렇다면, PKI 구조 내에서 개인은 기존의 인터넷을 사용할 때보다 개인정보(서명데이터)의 수집으로 필요이상의 부담을 느껴서는 안되며[16], 자신의 개인정보(서명데이터)가 서버에 전송되며 수집되고 있다는 사실을 정보통신 서비스 제공자는 사용자에게 통지함으로써 사용자가 무작위 적이며, 비밀스런 부인봉쇄를 당하고 있지 않음을 공개하여 규제의 투명성을 밝혀야 한다. 그리고 어떠한 정보가 서명되어 전송되었는지 공개되어야 한다[17]. 또한 프라이버시는 정부의 권한에 대한 실질적인 제한을 짓게 함으로써 더 큰 의미를 부여받는다[18].

이제 PKI는 개인정보 수집에 앞서 프라이버시

의 개념에 따른 세 가지 형태[14]에 따라 PKI의 S/W를 수정, 변경, 추가함으로써 프라이버시 침해의 가능성을 최소화하고 효율적이며, 유용한 시스템을 선택, 설계할 수 있다.

위 관점으로 PKI 구조에서 서버와 통신을 하는 클라이언트 프로그램은 다음과 같이 설계되어야 할 것이다.

첫째, 부담을 최소화하는 프라이버시를 보장하는 PKI

빈번한 전자서명으로 인한 사용자로 하여금 개인키 암호화용 패스워드를 자주 묻는다면 개인으로 하여금 부담을 증가시키는 것이므로, 메모리나 임시 파일로 보관을 하되 암호화 기법을 사용하여, 안전하게 관리 되어야 할 것이며, 응용 프로그램 종료 시 개인키 암호화용 패스워드가 시스템에 더 이상 저장되어 있어서는 안될 것이다.

둘째, 존엄성으로서의 프라이버시를 보장하는 PKI

전자서명 된 데이터가 서버로 전송된다면, 사용자는 어떠한 정보가 전자서명 되고 있으며(공개성), 사용자의 개인정보(전자서명데이터)를 수집하고 보관한다는 그 사실을 정보통신 서비스 제공자는 명문화하여, 사용자에게 알려, 동의를 얻어야 할 것이다.(투명성) 또한, 클라이언트 프로그램은 예로 SSL 채널을 통해 클라이언트 서버간 전송되는 데이터가 암호화되어 전송될 때 브라우저는 브라우저 하단에 작은 자물쇠가 굳게 잠긴 모습을 보여줌으로써 사용자의 데이터가 서버로 안전하게 전송 중임을 보여주고 있듯이 현재 행위가 전자서명에 의해 부인봉쇄 되고 있는지에 대해 시각적인 인터페이스를 제공함으로써 사용자로 하여금 그 사실을 쉽고, 직관적으로 알 수 있게 해야 할 것이다.

[그림 3][그림4]참조

그림 3: IE에서의 SSL 채널 형성시

그림 4: Netscape에서의 SSL 채널 형성시

셋째, 실질로서의 프라이버시를 보장하는 PKI

PKI구조 하에서 이러한 공개된 규제는 정부의 규제, 정보통신 서비스 제공자의 규제에 대해 한계를 짓게 함으로써 이를 사용하는 개인은 더욱 더 많은 프라이버시 보호를 받을 수 있게 할 것이다.

IV. 결론

사이버공간은 자유와 공개, 익명이라는 모토를 버리고 규제, 보호, 인증이라는 새로운 모토를 선택했다. 그 선택의 범위는 앞으로 더욱더 광범위하게 증가할 것이다. 이를 위한 도구로 PKI가 채택되었고, 공개키 암호화 기법을 이용한 전자서명 기술이 이를 뒷받침 해 준다. 개인의 프라이버시 보호 문제는 인간이 천부적으로 타고난 기본권의 하나로 보호되고 지켜져야 한다. PKI의해 전개될 사이버 공간에서 개인의 프라이버시가 침해 될 요소 중의 하나는 개인 사용자 자신에 의해 전자서명 된 정보의 수집 및 보관을 정보통신 서비스 제공자가 사용자에게 알리지 않았을 경우이다. 즉, 규제의 공개성과 투명성이 보장되지 않았을 때 발생한다.

당신이 나를 감시하는 것을 해결하는 방법은 그 감시를 막는 것이 아니라 내가 당신을 감시하도록 허용하는 것이다[19].

위 인용문은 많은 것을 우리에게 시사해 준다.

즉, 몰래 수집된 개인정보(전자서명 데이터)는 프라이버시를 침해 할 것이지만, 사용자가 자기를 감시하도록 허용한 상태에서의 개인정보(전자서명 데이터)의 수집과 보관은 프라이버시 침해라 볼 수 없다. 이를 위해서 사이버 공간을 규제하는 S/W가 변경, 수정, 추가되어야 할 것이며, 이를 위해 정부의 법제를 뒷받침하는 시행명령이나 지침 같은 법적, 행정적 조치가 이루어져야 할 것이다.

PKI가 만들어낼 미래의 인터넷은 빅 브라더가 아니다. 조지오웰의 1984년과 같은 암울한 미래가 아니다. 개인의 신원정보가 모두 드리나는 프라이버시가 보호되지 않고 모든 행위가 부인봉쇄 되는 AuthNet은 아니다. 밝은 곳에서 우리는 얼마든지 익명을 유지 할 수 있고, 프라이버시가 보호되는 공간을 찾을 수 있다. 원하면 숨을 곳을 찾을 수도 있다.

PKI가 적용된 차세대 사이버 공간의 세상은 AuthNet이 아닌 BrightNet이길 희망한다.

참고문헌

[1] Samuel D. Warren and Louis D. Brandeis "The Right to Privacy," 4 Havard Law Review 193, 1890

[2] Amendments to the United States Constitution

[3] Olmstead v. United States, 277 US 438, 470(1928), 464~65.

[4] Katz ㅂ United States 389 US 347, 353(1967).

[5] http://www.fsf.org/

[6] http://www.cert.org/stats/cert_stats.html

[7] Diffie, W., and Hellman, M. "New Direct ions in Cryptographic Techniques." IEEE Tran sactions on Information Theory, November 1976

[8] Rivest, R; Shamir, S; and Adleman, A. " A Method for Obtaining Digital Signatures and Public Key Cryptosystems." Communications o f the ACM, February 1978.

[9] Lawrence Lessig, "Code and Other Laws of Cyberspace", BASIC BOOKS, pp.111-121

[10] 전자서명법, 제정 법률 5,792호, 개정 법률 6,360호 개정 법률 6,585호

[11] 정보통신망이용촉진및정보보호등에관한법률, 법률 제6,360호

[12] 전자거래기본법, 법률 제5834호

[13] Implementing Web Site Client Authentication Using Digital IDs" , Verisign http://www.verisign.com/clientauth/kit/details.html

[14] Lawrence Lessig, "Code and Other Laws of Cyberspace", BASIC BOOKS, pp.147-149

[15] Center for Democracy and Technology, "Filing Before the FCC in the Matter of the Communications Assistance for Law Enforcement Act, CC docker no. 97-13," December 14, 1998, http://www.cdt.org/digi_tele/filing121498.html

[16] Michael Adler, "Cyberspace, General Searches, and Digital Contraband : The Fourth Amendment and the Net-Wide Search. " Yale Law Journal 105(1996):1093, 1109-10, 113 참조

[17] Cf. ibid., 1100; see also Brin, The Transparent Society, 158-61 (discussing mutual monitoring)

[18] Stuntz, "Substantive Origins," 395.

[19]Lawrence Lessig, "Code and Other Laws of Cyberspace", BASIC BOOKS, p.153

[20] "한국 인터넷뱅킹 이용자 530만명", 연합뉴스, 2002. 5. 29.

[21] PKCS#5: Password-Based Cryptography Standard http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/index.html

[22] PKCS#7: Cryptographic Message Syntax standard http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

[23] http://www.cyberprivacy.or.kr/indexf/indexf_e1.htm (개인정보보호방침 예시)

[24] http://kr.docs.yahoo.com/info/privacy.html (야후!의 개인정보 보호정책 예시)

[2 5] http://wp.netscape.com/eng/ssl3/draft302.txt

[26] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vsent7/html/vxconiisauthentication.asp

[27] http://snad.ncsl.nist.gov/snad-staff/tebbutt/x5cg/subsubsection2_4_8_1.html

[28] http://www.cybergeography.org/atlas/historical.html

[29] Bruce Schneier, Applied Cryptography Second Edition : protocols, algorithms, and source code in C , WILEY, p.35