

인터넷을 이용한 전자 투표 시스템 구현

김 중 규* · 허 용 석*

초 록

본 논문에서는 보안 기반의 전자 투표 시스템을 제안하고자 한다. 기존의 전자 투표 시스템은 유권자 인증과 투표 내용의 암호화 전송을 하지 않는 단순한 인터넷을 이용한 여론 조사에 불과하여 조사 결과의 신뢰도가 낮을 뿐만 아니라, 변조나 위조의 가능성이 많다.

이에 본 연구에서는 현재 이용이 확산되고 있는 인터넷과 WWW(World Wide Web) 환경에서 공개키 알고리즘을 기반으로 하는 투표 내용의 암호화 전송과 시스템 보안에 역점을 둔 전자 투표 시스템을 제안하고자 한다. 이 같은 전자 투표 시스템을 사용하게 되면 기존의 전 근대적 투표 방식에 의한 투표를 저조라는 문제를 해결할 수 있을 뿐만 아니라, 투표에 따른 시간적, 경제적, 인적 손실을 막을 수 있는 것이다.

I. 서 론

정보 통신 기술의 획기적인 발달로 인해 세계는 정보화 혁명에 휩싸여 있다. 특히 인터넷이라는 매체로 인해 세계의 컴퓨터 통신은 하나의 거대한 네트워크로 구성되었고, 정보화 혁명을 촉진시키는 매개체로서의 큰 역할을 하고 있다. 정보화 사회의 핵심은 컴퓨터와 통신을 이용한 각종 정보의 획득과 활용에 달려있다고 해도 과언은 아니다. 나아가 이것은 개인, 기업 뿐만 아니라 국가의 존립까지도 좌우 할 수 있는 것이다. 통신 기술과 전자 기술의 발전은 이를 더욱 가속화시켰고, 각종 응용 프로그램의 발전은 우리리의 생활을 더욱 편리하고, 질적인 향상을 가져왔다. 하지만 이를 악용하

는 해커의 등장으로 각종 병폐가 등장하였다.

이들은 중요한 시스템을 파괴할 뿐만 아니라, 각종 기밀을 빼내어 도용하거나 악용하고 있다. 이제 이들을 막아야만 우리들이 안심하게 편리한 인터넷 서비스를 이용할 수 있게 되는 것이다. 많은 편리한 응용프로그램들이 많이 개발되었지만 앞으로 더 보완되고 개발되어야 할 것도 과제로 남아 있다.

본 연구에서는 많은 응용 프로그램들 중의 하나로 해커의 침입을 막고 이용할 수 있는 전자 투표 시스템을 제안한다. 투표와 집계, 개표로 인한 인력, 자원의 낭비는 국가 경제의 큰 손실을 가져오고 있는 실정이다. 이에 전자 투표 시스템으로 그 손실을 막아보고자 한다.

* 대구대학교 정보통신공학부 교수

II. 전자 투표

1. 전자 투표의 장, 단점

(1) 전자 투표의 장점

첫째, 유권자들이 재택 원격 투표(home-centered tele-vote)가 가능하다.

둘째, 자동 개표가 가능하다. 투표 후 개표가 자동으로 집계되므로 시간적, 인적 손실을 획기적으로 막을 수 있다.

셋째, 투표에 따른 인적, 시간적, 경제적인 손실을 막아줄 뿐만 아니라, 전 근대적 투표방식을 타파하므로 투표율 향상을 가져올 수 있다.

(2) 전자 투표의 단점

첫째, 기술적인 문제를 들 수 있다. 전자 투표 시스템의 구성에 있어서 어떻게 설치하고, 운영해 나갈 것인가 등 여러 가지 기술적인 문제가 산재해 있다.

둘째, 일인 다투표, 대리 투표의 문제점이 발생할 수 있다. 이것은 유권자 인증에 해당하는 문제점이다. 아무리 각 유권자에게

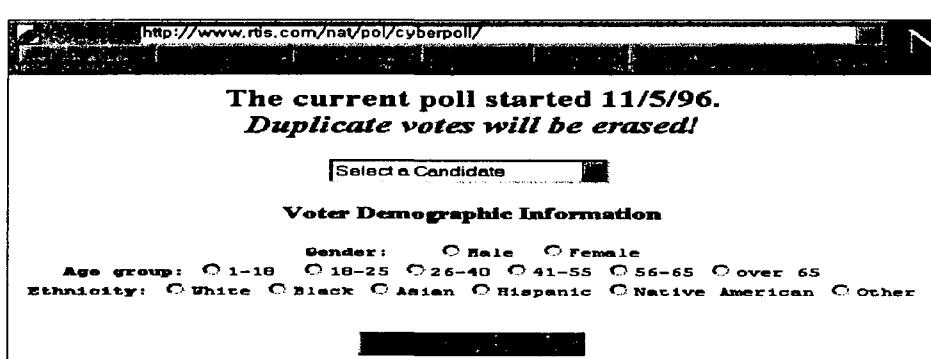
그만의 고유키를 준다고 해도 그것이 유출되지 않는다는 보장이 없다. 앞으로 이 부분에 대한 연구가 더 진행되어 더 신뢰할 수 있는 유권자 인증 시스템이 개발되어야 할 것이다.

셋째, 투표, 개표의 조작 가능성이 있다. 투표 시스템과 선거관리위원회의 집계시스템 사이에 투표 결과가 집계되는 동안 외부, 내부에서 변조가 발생할 수 있다.

2. 현재 전자 투표의 예

(1) 미국의 경우

전자 민주주의의 선두 주자로서 전자 투표가 많이 발전했을 뿐만 아니라, 적극 활용하고 있다. 그 예로 미국 대선의 공화당 후보전의 가상 투표가 <그림 1>에 나타내고 있다. 아직은 전자 투표라기 보다는 선거를 앞두고 인터넷 이용자들의 여론을 수집 공개 의미가 크다. 이를 통해 주요 정치 쟁점들에 대한 신속한 정보와 여론 수렴을 통해 선거에 적극 활용하고 있다. 미국도

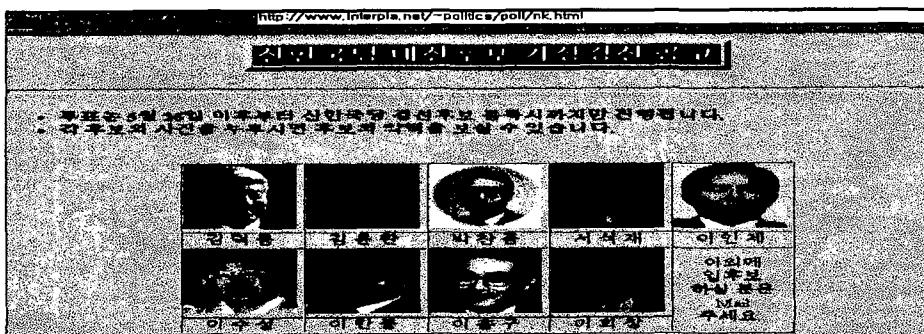


<그림1> 미국 공화당의 대통령 후보 가상 투표

각 웹 서버별로 투표 결과가 차이가 많이 난다. 이 주된 원인은 각 지지 후보자들의 선거원에 의해 많이 부정과 조작이라는 것이 일반적인 분석이고, 이것이 사이버 폴의 단점이기도 하다. 하지만 기존의 전화, 편지, 방문 등을 통한 지지도 조사에 비하면 시간적, 경제적인 면에서 획기적인 혁신이 아닐 수 없다.

(2) 우리나라의 경우

성이 떨어지는 편이다. 좀 더 확실하고 신뢰할 수 있는 방법이 강구되어야 하며, 이를 적극 활용할 수 있는 방안을 검토해야 할 것이다. 사용자면에서도 아직 인터넷을 이용하는 사람의 수가 특정층에 집중되어 있고 일반 가정보다는 학교, 연구 기관, 공공 기관, 연구소에 편중되어 있는 문제점도 안고 있다. 앞으로 이러한 점도 개선이 되어야 할 과제로 남아 있다.



<그림 2> 신한국당 대선 후보 가상 투표

우리나라에서는 아직 사이버 폴의 초기 형태로 이루어지고 있다. 각 정당들의 홍보와 의견 수렴의 흡 페이지가 등장하였고, 몇몇 정치인들만이 그들의 개인 홈페이지를 가지고 있다. 97년 대선을 앞두고 몇몇의 기관과 언론 매체등에서 사이버 폴 형태의 여론 조사를 통한 대선 주자들의 지지율을 파악하고 있다. 아직은 미국에 비해 조사 내용 면에서 다양하지 못하고, 조사 방법에 있어서도 편지나 전화를 많이 사용하는 편이다. 아직은 전 근대적인 방법에 의존하고 있으며 내용면에서도 각 조사기관에 따라 신뢰

3. 현재 전자 투표 시스템의 문제점

현재의 인터넷을 이용한 전자 투표는 단지 여론 조사에 불과한 전자 투표라기 보다는 사이버 폴(Cyber-Poll) 형태에 불과하다. 이는 유권자 인증이 제대로 되지 않고, 운영자들의 실리에 의해 조작이 가능하다는 것이다. 하지만 기존의 전화나 우편을 통한 여론 조사에 비해 접근, 통제가 신속하고 쉽게 될 뿐만 아니라, 인터넷이라는 매체를 이용한다는 데 의의가 있다. 앞으로 암호 알고리즘이나 보안 프로그램의 개발이 전제

된다면 더 신뢰할 수 있는 실질적인 전자 투표 시스템이 개발 될 것이다.

기존의 전자 투표는 다음과 같다.

첫째, 웹 서버의 보안을 미약하다. 단지, 웹에 대한 해킹이 날로 증가하는 데 전자 투표의 웹 페이지는 단지 기존의 보안 방식인 사용자 인증과 패스워드만을 사용할 뿐이어서 실제 투표에 운영 된다면, 해킹에 의한 변조, 위조 가능성이 많다.

둘째, 암호화 전송을 사용하지 않는다. 현재 웹에서의 서버와 클라이언트간의 인터페이스인 Common Gateway Interface(CGI)를 사용함으로 CGI 자체가 보안에 미흡함에 기인한다. 셋째, 유권자 인증의 기능이 없다. 일반적으로 웹에서 시행하는 전자 투표는 유권자 인증의 기능이 매우 약하다. 어떤 사이트에서는 일인 다투표가 가능하다. 패스워드만 바꾸면 여러 번 투표가 가능 할

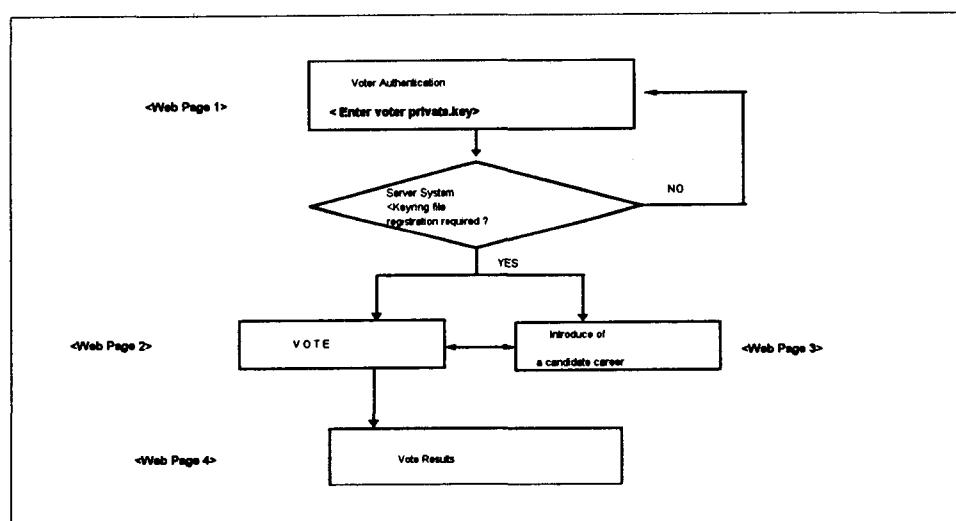
뿐만 아니라, 웹 사이트에 접수한 모든 사람이 투표를 가능하도록 해 놓은 곳도 있다.

III. 전자 투표 시스템의 구현

1. 전자 투표 시스템의 구성

(1) 웹 페이지

투표소 역할을 할 수 있는 웹 페이지를 구성한다. 후보의 약력 소개를 비롯한 자료들을 첨부하여 유권자의 이해를 돋도록 구성하였다. 제안된 전자 투표 시스템의 웹 페이지는 <그림 3>과 같이 유권자 인증, 투표, 후보 약력 소개, 투표 결과의 4 부분으로 나누어 진다.

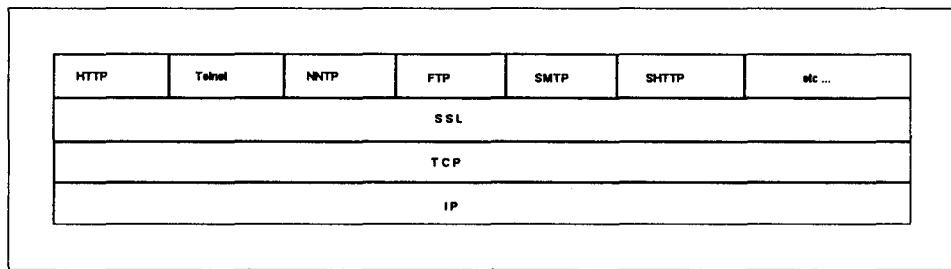


<그림 3> 전자 투표 시스템의 웹 페이지 구성

(2) 웹 서버 보안 (SSL)

선거관리 위원회의 서버 컴퓨터에 SSL를 설치하였다. 이는 날로 증가하는 웹 서버의 해킹을 막고, 투표소 역할을 하는 웹 페이지 변조를 막기 위함이다. 물론 서버와 투

자로 송수신함으로 상위 계층인 애플리케이션 계층의 각 서비스들을 지원 할 수 있다. 본 논고의 전자 투표 시스템은 애플리케이션 계층의 각 서비스 중 HTTP를 지원한다.



< 그림 4 > SSL 프로토콜

표소 사이의 인증 과정을 거쳐 새로운 암호화 채널을 통해 안전한 웹 전송을 할 수 있는 장점도 있다.

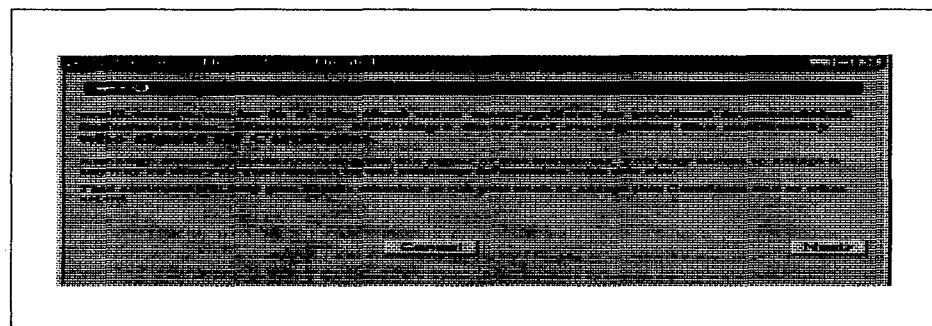
이 SSL 프로토콜은 테리사(Terrisa)가 개발해 넷스케이프와 Netsite의 암호화 중심 프로토콜로 사용하는 프로토콜이다. 서버와 클라이언트간의 인증으로 RSA와 X.509를 사용한다. < 그림 4 >에서와 같이 SSL은 네트워크 계층에서 안전한 암호 소켓 채

SSL 프로토콜의 서버와 클라이언트간의 작업은 다음과 같다.

첫째, 클라이언트와 서버의 연결을 확인한다.

둘째, 클라이언트와 서버 사이에 암호화기법을 통해 안전한 정보 전달을 목적으로 한다.

셋째, 정보의 무결성을 보장한다. 본 연구에서 제안한 선거관리위원회의 서버인 wall은



< 그림 5 > SSL 인증 메세지

SSL프로토콜 구동시 암호 소켓채널을 443번 포트를 사용하고 인증 메시지중 하나를 다음 < 그림 5 >에 나타내었다.

(3) 방화벽

투표소와 선거 관리 위원회사이에 네트워크를 보호하기 위하여 여러 방화벽중 FWT

K을 설치하여 사용하였다. 이 방화벽은 두 가지의 역할과 장점이 있다.

첫째, 애플리케이션 계층의 각 서비스별로 제어가 가능하다. 그러므로 본 연구에서는 Telnet, ftp, HTTP만을 허용하고, 나머지 서비스는 제공하지 않는다.

둘째, 투표소와 선거관리위원회의 시스템 사이에 IP 주소에 의해 제어를 하였다. 이는 다른 시스템에서의 접근을 막고자 하는 것이다.

(4) 자동 집계 프로그램

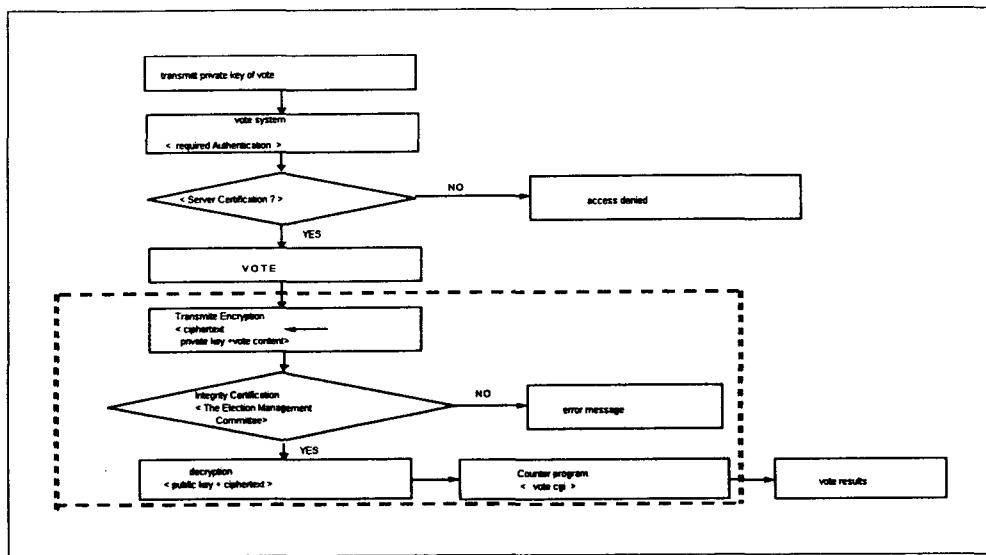
Perl(Practical Extraction and Report Language)를 이용하여 자동 집계 시스템을 구현하였다. 이 Perl은 좋은 유ти리티 언어로서 무료로 사용이 가능하고, 여러 플랫폼에서 사용이 가능한 장점이 있어 본 연구에서는 Perl4.0 이상에서 지원가능한 프로그램을 만들었다. 본 연구 시스템인wall 서버는 Perl5.003를 사용한다.

2. 전자 투표 시스템의 구현

(1) 전자 투표 시스템의 구현

본 연구에서 구현된 전자 투표 시스템의 절차는 < 그림 6 >과 같다.

첫째, 유권자는 자신의 비밀키를 선거관리 위원회로부터 전달 받는다. 이 때 유권자의



< 그림 6 > 전자 투표 시스템의 구현 설계

비밀키가 유출 되지 않도록 하는 것이 가장 중요하다. 이것이 유권자 인증을 강화 시킬 수 있는 방법이지만, 아직은 절대적으로 신임을 할 수 없다. 단지 비밀키의 해독이 어려움에 만족해야 한다.

둘째, 전달 받은 비밀키를 통해 유권자 인증에 사용한다. 적법한 유권자만이 투표장에 들어 갈 수 있고, 그렇지 못한 경우에는 접속이 거부된다.

셋째, 해당 후보자에게 투표를 하면, 유권자 인증에 사용된 비밀 키와 투표 내용이 암호화되어 선거관리위원회에 전송된다. 이 때 방화벽을 통과해야 하므로 보안성을 더욱 높여다고 볼 수 있는 것이다.

넷째, 전송된 암호문은 정보의 무결성(Integrity) 검증을 통한 확인 절차를 거친다. 이 확인 절차는 SSL 프로토콜에서 시행된다.

다섯째, 전송된 암호문은 선거관리위원회에 등록된 유권자의 공개 키를 가지고 해독이 된다. 이 해독문은 vote.cgi라는 Perl로 짜여진 카운터 프로그램을 통해 자동 집계되

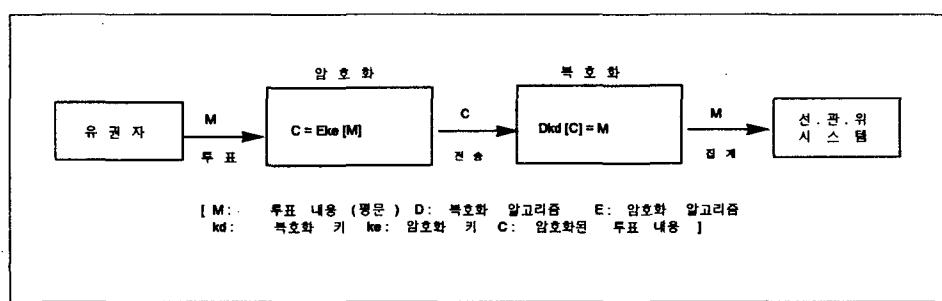
고 결과가 홈페이지에 나타나게 된다. 이 카운터 프로그램도 투표 숫자가 하나씩 하나씩 합산되어 보여주게 된다.

(2) 유권자 인증 강화

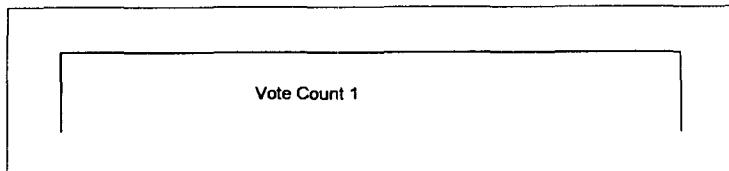
전자 투표시스템에서 유권자 인증부분은 매우 중요한 부분이다. 현재 웹에서는 영문자, 숫자, 특수 문자로 이루어진 패스워드를 사용한다. 보안성을 보장 할 수 없으므로 해킹을 당해 도용될 가능성이 높다. 그러므로 본 논고에서는 PGP(Pretty Good Privacy)를 이용하고자 한다.

(3) 투표 내용 암호화 알고리즘

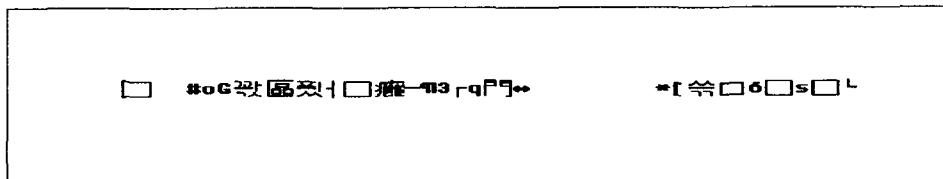
기존의 전자 투표 시스템은 암호화 전송을 하지 않는 관계로 해킹을 당해 내용이 변조될 우려가 많다. 본 연구에서는 이를 막고자 공개키 알고리즘을 사용하였다. <그림 7>과 같이 비밀 키는 투표 내용을 암호화에 사용되고 공개 키는 복호화에 사용되어 자동 집계로 연결된다.



< 그림 7 > 투표 전송 암호 알고리즘



< 그림 8 > 투표 내용 (전송 전)



< 그림 9 > 투표 내용 암호화 전송 (후보1 선택한 경우)

실제로 하나의 투표 내용을 예로 암호화 되는 것을 알아보자. 이 유권자는 1024bit로 만들어진 비밀키를 가지고 투표를 하였다. 그리고 1번의 후보를 선택하였다.

3. 전자 투표 시스템의 구현 예

(1) 유권자 등록

본 연구에서 제안한 방법으로 실제로 전자 투표 시스템을 구현하여 학생회장 선거를 유권자 수는 100명으로 설정하였다. 선거관리위원회의 서버로 사용되는 시스템의 구성은 다음과 같다.

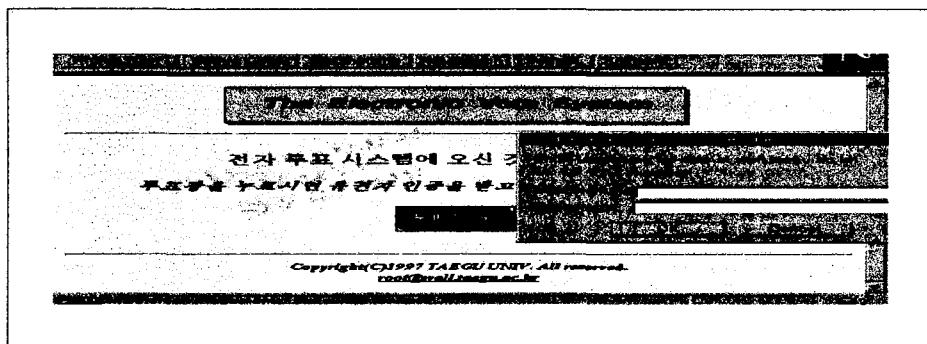
- ① 서버 시스템의 플랫폼 - Red Hat Linux 4.2.5
- ② PGP - PGP263ii
- ③ SSL - stronghold-2.1 (linux 용)
- ④ Perl - Perl5.003

(2) 유권자 인증

<그림 10>에서와 같이 실제로 구현된 전자 투표 시스템에서 유권자의 인증을 요구 한다. 유권자는 이름과 선거관리위원회에서 전달, 사전에 등록시켜 선거관리위원회 서버시스템에 비밀키와 공개키 파일을 따로 등록을 시킨다. 이 때 보안성을 높이기 위하여 1024bit로 생성하였다.

(3) 투표

유권자 인증을 거친 후 유권자는 원하는 후보에게 투표를 하게 된다. 기존의 전자 투표 시스템은 암호화 전송이 아닌 바로 전송되기 때문에 전송 도중 해킹을 당해 내용이 변조되어 악용될 수 있다. 그리고 바로 접계되어 서버에 전송될 경우 패킷이 지연되면 투표 접계의 변조가 가능하다. 그러므로 이러한 단점을 보완하기 위해 본 논문에서는 유권자가 투표를 하면 바로 유권자의 비밀키와 투표 내용이 암호화 되어 전송되기 때문에 내용 변조를 할 수 없게 된다.



< 그림 10 > 구현된 전자 투표 시스템의 유권자 인증

4. 구현된 전자 투표 시스템의 특징

(1) 인터넷 서비스중 하나인 웹에서 전자 투표를 시행하므로 시각적인 효과는 물론 기존의 전 근대적 투표 방법에서 탈피하여 편리한 투표가 가능하므로 투표율 향상을 기대 할 수 있다.

(2) 유권자 인증 기능이 강화 되었다. 기존의 유권자 인증에 사용되는 방법은 단순한 유권자의 패스워드를 요구함으로 보안성이 미약하다고 볼 수 있다. 하지만 본 논고에서 제안한 방법은 유권자의 비밀키를 1024bit로 만들어 사용함으로 보안성을 높일 수가 있다.

(3) 웹 보안 기능을 높였다. 웹 보안은 유권자 인증 보안 기능을 강화시킨 것에도 기인 하지만 HTTP를 SSL 프로토콜을 사용함으로 더욱 높일 수가 있는 것이다.

(4) 기존의 사이버 폴 형태의 여론 조사에 불과한 전자 투표 시스템을 보안이 강화된 실제적인 전자 투표 시스템으로 발전을 가능하게 하였다.

IV. 결 론

인터넷과 WWW의 확산에 의한 다양한 응용 프로그램들이 연구, 개발되어 우리의 실생활에 많은 도움을 주고 있다. 그 중 하

자 이 점	기존 전자 투표 시스템	제안된 전자 투표 시스템
유권자 인증	단순히 조합된 패스워드	비밀키 (공개키 알고리즘)
웹 보 안	웹 서버 자체 보안	S S L
투 표 전 송	일반적 CGI를 이용한 전송	암호화 전송 (공개키 알고리즘)
보 안 성	거 의 없 음	높 음
신뢰 도	낮 음	높 음

< 표 1 > 전자 투표 시스템의 비교

나인 전자 투표 시스템은 우리에게 새로운 투표 형태를 제공함과 동시에 투표율을 향상시킬 수 있는 기반을 제공한다. 하지만 우선 선결되어야 할 과제는 신뢰도와 편리성이 제공될 수 있도록 시스템의 보안이 이루어져야 한다. 기존의 전자 투표 시스템은 편리성은 강조되었지만, 시스템의 보안과 투표 내용의 암호화 전송이 이루어 지지 않은 이유로 신뢰도에서는 많이 떨어진다. 단지 기존의 여론 조사 방법에서의 변혁에 불과하다. 하지만 본 연구에서 제안된 전자 투표 시스템은 우선 기존의 전자 투표 시스템보다 더 유권자 인증이 강화되었을 뿐만 아니라 웹 서버의 보안도 강화시켰다. 특히 가장 중요한 것은 투표 내용을 암호화하여 전송함으로 투표 결과의 신뢰도를 보장할 수 있다는 것이다.

현재 인터넷을 이용한 전자 상거래에 대한 연구가 활발하다. 이 전자 상거래가 실행되기 위한 많은 문제점들 중에서 가장 중요한 것은 구매자의 대금 결재시 구매자의 비밀 번호와 인적사항을 어떻게 웹 상에서 안전하게 전송하는가에 달려있다. 이것 역시도 웹에서 안전한 암호화 전송이 관건이다. 따라서 본 연구에서 제안한 방법으로 응용도 할 수 있는 것이다.

참 고 문 헌

김 철, "암호학의 이해", 1996, pp221

류재철, "WWW/JAVA Security", NET SEC-KR '97, 1997, pp129

박현동외 3인, "전자우편의 보안 -PGP-", NETSEC-KR '96, 1996, pp131

이병도 역, 인터넷의 보안, 비앤씨, 1996, pp277

Bruce Schneier, "APPLIED CRYPTOGRAPHY", WILEY, vol. 2, 1996

Charlie Kaufman, Radia Perlman and Mike Speciner, "NETWORK SECURITY", Prentice Hall, 1995

D. Brent Chapman and Elizabeth D. Zwicky, Building Internet FIREWALL, O'Reilly &Associates, 1995, pp4

Deborah Russell and G. T. Gangemi Sr, "COMPUTER SECURITY BASICS", O'Reilly & Associates, 1991

Edward G. Amoroso, " FUNDAMENTALS OF COMPUTER SECURITY TECHNOLOGY", Prentice Hall, 1994

John Vacca, "Internet Security SECRETS", IDG BOOKS, 1996, pp276 pp279-280

Larry J. Hughes, "Internet Security Techniques", New Riders, 1995 pp474