

# 한국의 인터넷 보안의 현황과 문제점

조셉 마이클스

KU•KFOP 보고서

2014.4.7

# 목차

## I. 서론

## II. 본론

1. 한국 인터넷 개발 역사
  - 1) 인터넷 시설
  - 2) 암호화 역사
  - 3) 암호화 법률
2. 법률에 나타난 공인인증체제 묘사
3. 공인인증체제 실행
  - 1) 실행과 이용
  - 2) SEED 묘사
  - 3) 액티브X으로 분배
4. 단일 플랫폼
  - 1) 단일 플랫폼 초래된 이유
  - 2) 브라우저 사용율
5. 기본적인 시스템이 보안되지 않음
  - 1) 시스템 보안되지 않은 이유
  - 2) 인터넷 익스플로러의 안전 취약점
  - 3) 액티브X 문제점
  - 4) 윈도우XP 지원 끝
6. 슬래머 웹
7. 결론

## III. 결론

## IV. 참고 문헌

## I. 서론

한국의 인터넷 속도는 특히 모바일 분야에서, 다른 선진국에 앞서 세계적으로 가장 빠르다. 한국에서는 대학이나 연구자들이 자발적으로 인터넷 사용을 널리 보급하고, 빠르게 이용할 수 있도록 KISA, KNC, KRNIC와 같은 인터넷 관련 기관들을 설립하였다. 한국은 다른 국가보다 정보 통신 기술을 개발하고 사용 시작하고, 현재는 세계에서 가장 높은 초고속인터넷 사용률 가지고 있다. 그러나 정부가 국내 개발한 암호화 시스템을 의무적으로 사용하도록 규제를 정하여서 결국 여러 가지 문제가 발생하였다. 이 문서는 1990년대 빠른 속도로 정보 통신 기술을 사용 시작함이 컴퓨터 보안 기술 중규제로 어떻게 이어지기와, 그런 규제들은 공인인증체제로 어떻게 실행하기를 살펴본다. 다음, 이 문서는 왜 공인인증체제가 윈도우와 인터넷 익스플로러인 단일플랫폼 우세함으로 초래하기에 대해 볼 것이다. 그리고, 이 플랫폼의 보안 문제를 논의하며 그로 인해 어떤 문제 발생하는지 묘사할 것이다. 마지막으로, 이 문서는 문제를 해결할 방향을 추천할 것이다. 공인인증체제를 비판적게 살펴볼 필요성은 한국의 모든 전자상거래에 사용하는 뿐, 현대 사회에서는 전자상거래가 기본적인 것으로 되었기 때문이다.

## II. 본론

### 1. 인터넷 개발 역사

1) 첫 세계 국가의 컴퓨터 네트워크 중 하나인 한국의 네트워크는 1982년 5월에 수립했다. 이 네트워크는 1980년대 연구과학계와 교육계에 사용하고 네트워크연구에 주로 집중하였는데, 1990년대 중반까지는 대학교나 연구소에서만 사용할 수 있었으나, 기업과 개인에게까지 확산되었다. 1994년에 6월에 KT의 KORNET 을 시초로 몇 개의 상업 인터넷 서비스가 시작되었다. 한국은 초고속 인터넷 기반 시설을 빠르게 개발하여 2004년까지 초고속 인터넷에 접속하는 일반 사용자는 천백만 명 넘어섰다. 이는 한국 가정 인구의 70%를 차지하는 수치이다. (Chon, Park, Kang, Lee, 2005)

2) 알다시피, 한국의 인터넷 개발 속도와 확산은 세계에서 가장 빠른 부문 중 하나이다. 1990년대, 국민들은 이 새로운 기술들을 사용할 수 있도록 정부에 많은 요청을 했으나, 국제적 문제와 안정성의 문제로 충돌이 발생했다. 특히, 인터넷 개발자들, 회사원들과 기업인들은 상품을 판매하

고 서비스를 제공하는 다른 방식으로써 이 새로운 기술의 사용에 관심을 가졌다. 그러나, 디지털 정보가 쉽게 조작 되고, 변경될 수 있다는 것이 문제로 제기되었다. 예를 들어, 온라인 거래 후, 어떤 사람은 자신에게 유리한 쪽으로 기록들을 삭제한 후, 거래가 일어나지 않았다고 주장할 수 있다. 물론, 서류들을 포함하는 거래에서도 이러한 사기는 발생할 수 있다. 그래서 서명, 도장, 투명 무늬(빛에 비춰보았을 때 보이는 것), 또는 다른 수단들이 이 서류가 어디서 만들어 졌으며, 진정성을 증명하기 위해 사용된다. 이런 유사한 방식을 컴퓨터에서 사용하는 것을 암호화라고 하며, 정교한 수학 알고리즘을 사용한다. 물론 이런 암호화 방식은 깨질 수 있다. 그러나 그러기 위해서는 아주 많은 컴퓨터 전력과 시간이 요구되기 마련이다. 이러한 이유들로 암호화의 시행은 매우 안전한 방식이다. 그러나 인터넷 확산 이전에, 세계 의 대부분의 정부들은 안정성에 큰 위협을 받을 수 있는 암호화 기술의 민간 사용을 염려했다. 범죄자들도 암호화 서류를 사용하여, 범죄를 일으킨다면 어떻게 되겠는가? 그래서 사건 수사에 방해가 된다면 어떻게 하는가? 범죄가 국가 보안과 아주 중요한 연관성이 있다면 어떻게 되겠는가? 한국 정부는 90년대 초에 요구된 온라인상에서의 암호화 사용을 거절했다. 반면, 미국에서는 많은 연구자들이 세계 2차 대전 동안 암호화 알고리즘을 생성했으며, 수정 제 1조에서 언론의 자유를 보호하고 있기 때문에, 정부가 기술확산을 제한하는 것은 어려웠다. 그러나 그럼에도 불구하고 1997년, 미국의 전 FBI 국장인 프리, 루이스는 이와 같은 발언을 했다. “[...] 강력한 암호화의 사용확산은 궁극적으로 범죄와 싸우고, 테러를 막는 우리의 능력을 완전히 파괴시킬 수 있습니다. 깰 수 없는 암호화는 마약왕, 스파이, 테러리스트들이 성행하게 만들 것입니다. 심지어 범죄를 논하고, 처벌 받지 않을 방안들을 모색하기 위한 음모를 꾸미기 위해 폭력범들 또한 활개를 치게 될 것입니다.” (Freeh, 1997)

그 당시, 명백히 군사적 목적으로, 미국 정부는 암호화 기술 수출에 상당히 많은 제한을 하였으나 인터넷 사용의 증가로, 규제를 강화하기가 점점 더 어려워졌다. 결국 1990년대 후반에는 규제가 점점 완화되었다. 한국에서는 1999년 전자거래 기본법 제정에서 첫 암호화 사용을 허락했다. 동시에 전자 서명법이 통과되어 공인인증서 사용이 규제되었다. 이 인증서 시스템은 한국에 빠르게 전파되었으며, 몇 년 만에 전자 상거래의 대부분의 양식에서 법적 의무화 되었다.

## 2. 법률에 나타난 공인인증체제 묘사

전자 서명법과 공인인증체계가 명시된 관련 법들은 많은 규칙들을 명시한다. 앞으로 중요한 개념들이 본 보고서에서 논의될 것이다. 정부기관인 KISA(한국인터넷진흥원)는 한국정보인증(주)와 (주)코스콤과 같은 공인인증기관의 허가과 감독을 담당한다. 이러한 공인인증기관들은 기업 가입자들에게 인증서를 부여한다. 가입자들은 타인과 인증서를 공유하지 말아야 하며, 서명할 때, 반드시 인증서를 보유하고 있어야만 한다. 인증서는 전자 서명 문서에 사용되어지며, 이러한 시스템은 전자 서명이 기재된 후에 서명이 변경됐는지 확인할 수 있는 기능을 가지고 있다. (전자 서명법, 2013)

시스템의 이러한 요구에 더하여, 한국 정부는 미국에서 수출된 40-bit와 56-bit의 암호화 기술들은 너무 약하다고 판단했으면, 안전한 전자 상거래를 위해 더 강한 암호화 기술이 필요하다고 생각했다. 그러므로, 암호화 알고리즘이 국내에서 자체적으로 개발되었다. 정부의 요구를 만족시키기 위해 한국의 대학교들과 민간 기업이 KISA와 협력하여 암호화 알고리즘을 만들었다. 그 결과, 1998년, SEED라는 암호화 기술이 개발되었다.

### 3. 공인인증체제 실행

공인인증시스템은 1990년대 말에 만들어졌으며, 한국 전반에 걸쳐 빠르게 사용되었다. 예를 들어, 2000년말까지 20개의 한국 은행들이 이 시스템을 사용하는 인터넷 뱅킹 서비스를 제공하였다. 이 시스템의 기본이 되는 서비스들을 사용하기 위해서, 사용자들은 먼저 온라인 상에서 인증 테스트를 거쳐야만 한다. 그런 후 사용자들은 공인인증기관으로부터 전자인증서를 받을 수 있다. 이러한 절차가 끝나면, 사용자들은 특정기관의 소유권이 있는 소프트웨어를 사용할 수 있다. 사용자는 발급된 인증서를 컴퓨터 하드에 저장하거나 USB 플래시 드라이브와 같은 외부 저장장치에 저장해야만 한다. 사용자들이 전자상거래를 할 때, 디지털 인증서의 교환으로 사용자와 서비스의 안전한 연결이 시작된다. 세션키를 만드는 실질적 방법은 국민에게 공개되지 않았지만, 연구자들은 이 것이 SEED 암호 알고리즘을 사용한다고 추측해왔다. 사용자의 인증을 위해서, 몇몇 방식을 혼합하여 사용하기도 하는데, 이는 안정성을 높일 수 있다. 사용자 비밀번호, 일회용 비밀번호, 디지털 인증서, 개인 식별 번호와 심지어 생체 정보를 이용한 인증방식등이 이에 속한다. 일반적으로, 사용자가 처음 로그인할 때, 사용자 ID와 비밀번호를 사용하며, 특별한 핀(PIN)은 은행

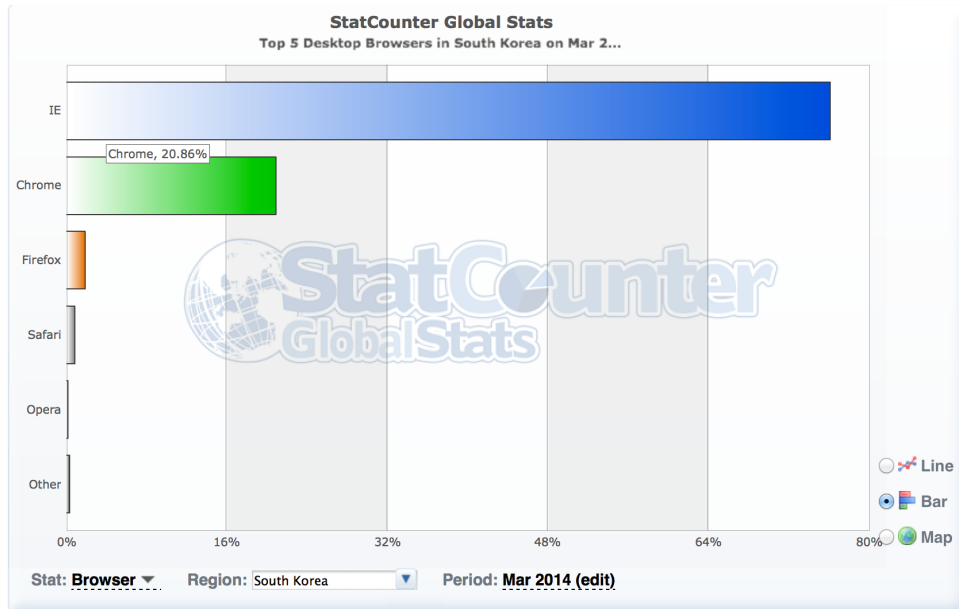
계좌 또는 신용카드 사용자들이 개인식별을 위해 사용한다. 또한 거래는 사용자 컴퓨터에 저장된 인증서 내에 있는 사용자 키의 사용으로 디지털 서명화 된다. (Kim, Huh, Anderson, 2009)

2) SEED는 128비트 대칭키 블록 암호이고, 인터넷 엔지니어링 태스크 포스에서 이를 승인한다. 이 것은 ISO/IEC 국제 표준화로 만들어졌지만, 인터넷 익스플로러, 크롬, 파이어폭스, 사파리와 같은 대부분의 유명한 브라우저에서는 브라우저를 처음 만든 회사 중의 하나인 넷스케이프에서 최초로 만든 TLS/SSL 국제 표준화를 따른다. 즉, 이것은 SEED를 사용하기 위해서는 외부 플러그인이 필요하다는 것을 의미한다. (Kim, Huh, Anderson, 2009)

3) 이 시스템이 개발되어질 당시인 1990년대 말, 한국의 많은 프로그래머들은 마이크로소프트사의 액티브 X 기술 적용을 어떻게 개발해야하는가를 배우고 있었다. 이 기술은 웹브라우저에 플러그인들을 설치할 수 있으며, 이와 마찬가지로 컴퓨터 자체적으로 프로그램을 설치할 수 있다. 그래서 이 기술은 보안 플러그인들을 쉽게 분배하기에 이상적이다.

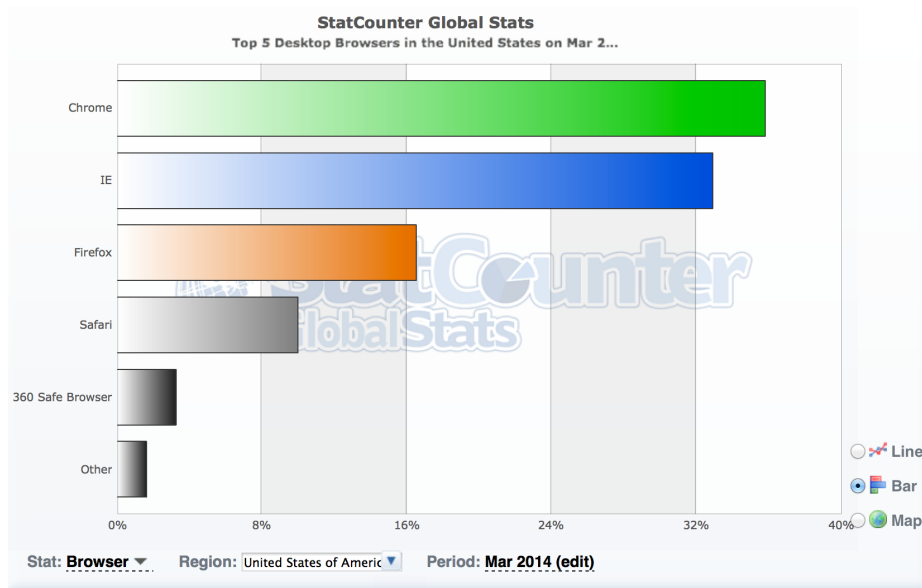
#### 4. 단일 플랫폼

1) 그러나 한국에서의 유일한 보안 플러그인을 설치 방식으로 액티브X 를 사용하는 것은 단일 플랫폼만을 우세하게 사용토록 하는 결과를 낳았다. 왜 이러한 상황이 발생했을까? 먼저, 우리는 액티브 X에 대해 더 많이 이해해야하며, 액티브X 컨트롤은 작은 프로그램이기 때문에, 기능적으로 마이크로소프트 윈도우의 소프트웨어 요소에 포함되어진다. 표면상 액티브X 컨트롤이 윈도우에게 의존하고 있지 않지만, 실제로는 액티브X 컨트롤이 대부분 윈도우를 필요하다. 이 상황 결과는 액티브X 컨트롤이 윈도우 밖에 운영하지 못해서 또 한국의 전자상거래 기술도 못해서 한국 사람이 윈도우 플랫폼을 사용으로 제한된다.



한국 브라우저 사용현황

2) 그럼 한국의 인터넷 기술 상황에 어떤 의미있는가? 최근 웹 브라우저 시장 점유율 통계 보면, 인터넷 익스플로러는 76%정도 넘어고 크롬은 20% 받았다. 다른 웹 브라우저들은 2%도 이루지 못한다. 이로 인해 브라우저 사용 다양성 별로 없기 볼 수 있다. (StatCounter)



미국 브라우저 사용현황

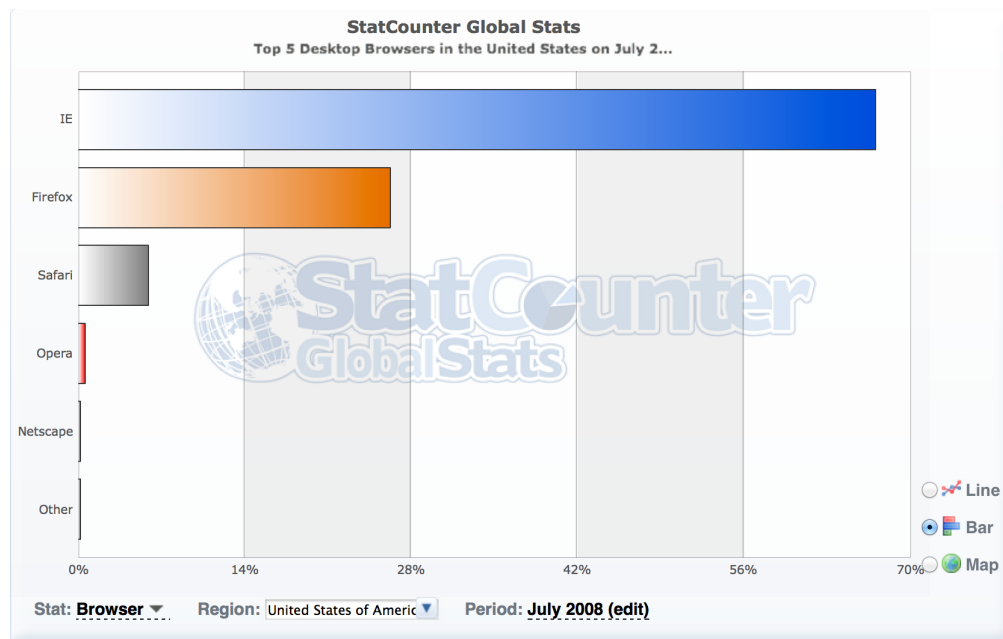
미국과 비교한다면, 완전히 다른 상황이다. 크롬이 제일 높은 36%정도 받았지만 다른 인터넷 익스플로러, 파이어폭스, 사파리도 다 10% 넘어서기 볼 수 있다. 이 것과 한국의 웹 브라우저 시장 점유율은 크게 대조된다. (StatCounter)

## 5. 기본적인 시스템이 보안되지 않음

1) 이러한 관점에서, 왜 이러한 문제들이 발생하였는지 의문을 가질지도 모른다.

만약 시스템이 정교한 공인인증서, 비밀번호, PIN, 의무적인 바이러스 방어 프로그램, 키 입력 암호화 소프트웨어 와 같은 아주 많은 안전장치를 가진다면, 완벽하게 안전하지 않을까? 그것은 브라우저의 다양성보다 더 중요하지 않을까? 문제는 안전하지 않은 플랫폼에 추가로 보안요소들을 추가한다고 해서 안전한 플랫폼이 되지 않을 것이며, 이 플랫폼의 인터넷 브라우저, 액티브X요소와 운영체제에 아주 많은 보안 문제들이 발생될 것이다.

2) 인터넷 브라우저 보안을 잘 이해하기 위해서, 브라우저의 개발 역사를 먼저 이해하는 것이 중요하다.



2008년도 미국 브라우저 사용 실정

미국에서 브라우저의 다양성이 항상 존재했던 것은 아니다. 2000년 초, 마이크로소프트사는 윈도우에 무료로 인터넷 익스플로러를 포함하여 배포함으로써, 주요 경쟁사인 넷스케이프를



제치고, 빠르게 표준화되었다. 2008년도만 해도 시장점유율 67%를 넘어섰던 인터넷 익스플로러는 2000년대 말과 2010년도 초에 시장점유율이 떨어졌다. (StatCounter) 그 이유는 인터넷 익스플로러가 우세한 이후, 마이크로소프트사가 집중적 개발을 멈췄으며, 동시에 그 것의 약한 보안성으로 많은 보안상의 문제들이 대두되었기 때문이다. 파이어폭스가 출시된 후, 인터넷 익스플로러의 사용자는 점점 줄어들었으며, 주목 받지 못하기 시작했다. 그래서 마이크로소프트사는 다시 개발하기 위한 노력을 재개했으나, 이미 너무 적은 규모였으며, 너무 늦은 출발이었다. 그로 인해, 항상 파이어폭스, 사파리, 크롬의 심한 경쟁에서 뒤쳐졌다. 다른 브라우저들이 대개 기능과 속도 개선을 먼저 시행하였기 때문에, 사용자와 인터넷 시장에서는 다른 브라우저를 선택하였으며, 인터넷 익스플로러의 시장점유율은 빠르게 하락하고 말았다. 그러나 한국의 사용자들은 기본적인 전자거래를 하기 위해 계속 인터넷 익스플로러를 사용해야만 했다. 그 결과, 한국사람들은 새로운 기술과 보안 개선을 받기 위해서 기다려야만 했다.

3) 인터넷 익스플로러의 보안상의 결함이 큰 문제로 발생하기 시작한 2000년대 초 중반, 액티브 X는 바이러스와 다른 악성 소프트웨어를 퍼뜨리는 주요 매개체 중의 하나였다. 악의적인 해커들이 컴퓨터에 소프트웨어를 쉽게 배포하고, 설치하는 액티브 X의 이러한 기능을 사용한다면 위험한 문제였다. 이 같은 이유로 마이크로소프트사는 액티브 X 컨트롤을 아예 제한하는 거 대신, 그 것을 다운로드 할 때, 사용자들이 설치를 계속할 것인지에 관한 창이 먼저 뜨게 하였다. “네”라는 버튼을 클릭하여 설치되면, 사용자들은 자신의 컴퓨터에서 원하는 것들을 할 수 있다. (사용자들은 본인 컴퓨터에서 조작할 수 있는 권리를 가진다.) (정기석, 2013)

더욱 안 좋은 것은, 해커가 원격 컴퓨터에서 프로그램을 직접 설치할 수 있게 만드는 안전 취약점도 있다. 지난 10년 동안 마이크로소프트가 이런 결함이 고치는 패치를 제공해야 한다. 최근 2013년 11월에도 안전 취약점을 패치하며, 이것은 공격자가 바이러스를 컴퓨터의 하드 디스크에 두기 전 메모리에 직접 저장할 수 있기 때문에 전형적인 바이러스 검색기, 컴퓨터 파괴 소프트웨어 검색기 등 보안 시스템이 기계가 감염되는 지 확인하기를 어렵게 만들어서 위급한 안전 취약점였다. (Stevenson, 2013)

4) 최근에 뉴스에서 자주 나타난 컴퓨터 안전 고민 중 하나는 윈도우XP의 지원이 끝나는 것이다. 이것은 마이크로소프트가 안전 취약점을 고치는 패치를 제공하기 끊기는 것이다. 마이크로소프트는 7년만에 지원이 끊길 날짜를 잡고, 그때부터 소비자들과 사업들에게 새 윈도우 버전으로 업그레이드하지 않으면 그의 PC들이 위험을 무릅쓸거라고 종용하고 있었다. 마이크로소프트는 윈도우XP가 현재 안보 위협을 위해 만들지 않았다고 주장한다. 마이크로소프트 윈도우통신국장인 톰 머피에 의하면, “XP는 오래 기간에 지원했어요. 보안 때문에 고객들이 그를 이용을 중단하고 필요하다. XP가 해마다 덜 보안하게 된다.” 그러나, 네트애플리케이션에 따르면 세계의 컴퓨터 중 18%가 아직 윈도우XP 사용하고 있다. 브라우저의 보안 면에서 윈도우XP에서 인터넷 익스플로러 버전 8까지 이용할 수 있어서 중대한다. 또한, 인터넷 익스플로러 8 지원도 끊기다. XP에서 최근 크롬과 파이어폭스 보전을 이용할 수 있지만 한국에서 유저가 전자상거래를 하고 싶으면 이 선택이 없다. (Perez, 2014) 그런데 기업에는 윈도우XP로부터 멀어지는 것은 원 과제 아니다. 컴퓨터 보안 회사인 파이어아이 기술국장인 제이선 스티어에 의하면 “문제는 이를 하기가 많은 시간과 돈을 써서 비현실적인 기간인 것이다.” (Worth, 2014)

한국에서 공인인증체제를 운영하려고 특별한 특허소프트웨어들을 이용하기가 많아서 윈도우XP에서만 이용할 수 있는 그런 시스템을 기업에서 사용할 것 같다. 이 소프트웨어는 업그레이드나, 수정이나, 대신해야 하며, 모든것이 비용이 많이 드는 것이다.

## 7. 슬래머 웹

2003년 1월 25일에 세계 인터넷에서 슬래머 웹을 퍼지하고 인터넷을 마비시킨 사건 발생했다. 슬래머는 마이크로소프트의 에스큐엘 프로그램을 감염한 후 자신을 무수히 복제하고 인터넷에서 퍼지는 바이러스다. 한국 경우에는 인터넷 통신망을 오래 동안 마비시켜서 해석자는 다른 나라에서도 발생했는데 저기는 조금 느리게 되거나 웹사이트 몇개가 다운되는 뿐, 한국의 통신망은 상대적으로 취약함을 볼 수 있다고 지적한다. (김재섭, 2004) 다른 해석자는 “2003년 한국에서 인터넷 마비시킨 사건이 발생 이유 중 하나는 단일운영체제이다.”

윈도우XP에서 슬래머가 사용 같은 안전 취약점 발견하기를 상상해 봅시다. 물론, 현재 XP 이용하는 컴퓨터 더 적어서 2003년 발생한 피해만큼 나쁘지 않을 것이다. 하지만, 지원 없어서 마

이크로소프트가 이 취약점을 고칠 패치를 제공할 예상하지 않다. 한국에 있는 컴퓨터 보안 회사들은 자신이 그런 피치 만들어야 되는데, 윈도우의 소스코드는 비공개 소스코드 때문에 하는 것이 아주 어렵고 마이크로소프트가 하는 것보다 더 오래 거릴 것 같다. 또한, 피치를 분배하는 것도 더 오래 동안 걸릴 것 같다.

### III. 결론 및 제언

현재 시스템의 문제를 반드시 해결해야 하는 입장있다. 인터넷 개발 역사에 통함으로써 보시다시피, 한국 사람들은 새 기술을 사용하고 시작하기를 매우 열렬하고, 쇄신, 자기 개선 등으로 사용하기 관심이 많지만 한국의 조절 구조는 국가가 보안되지않은 단일프랫폼에 제한된다. 한국 사람들은 보안 혜택을 받기 위할 뿐만 아니라, 소비자 선택 더 많아지고, 국제 시장에서 한국 기술의 경쟁력을 높이게 되려고 이 플랫폼에 탈출 방법이 필요하다.

이 문서의 입장에서는 한국 정부는 국제적인 암호화 표준인 TLS/SSL를 사용할 수 있도록 규제를 완화해야 한다는 것이다. 세계에 TLS/SSL는 모든 국가들이 사용해서 한국에서 충분하는 것 같다. 물론, 먼저 꼼꼼히 분석하며, 현재 공인인증체제의 보안, 특히 공인인증기관의 중앙집권의 위험, 또 TLS/SSL 등 다른 보안 시스템의 장점과 단점을 조사하고 평가하면 좋겠다고 생각한다. 공인인증기관의 중앙집권 문제 이유는 해커 위해 절호의 표적이며, 그 시스템에 침입하면 국내 모든 컴퓨터 안전상을 위협에 빠뜨릴 것이다. 반면에, 당연히 TLS/SSL는 완벽하게 만든 보안이 아니며, 문제와 안전 취약점도 있다. 규제를 완화하기 통해, 한국 정부는 기업과 단체가 자기에게 가장 좋은 보안 기능과 고객 서비스의 균형을 정할 수 있게 만들 것이다.

#### IV. 참고 문헌

1. 정기석, "전자금융거래시 공인인증서 의무사용 개선방안에 관한 연구", 융합보안논문지, 2013. Web. 29 Mar 2014.  
전자서명법 [시행 2013.3.23.] [법률 제11690호, 2013.3.23., 타법개정] <<http://www.law.go.kr/lsInfoP.do?lsiSeq=136752#0000>>
2. 김승주, "IT분야의 손톱 밑 가시, SEED", 디지털타임스, 15 July 2013. Web. 19 Mar 2014.
3. 김재섭, "초고속망 타고온 '위험한 편지'", 한겨레, 27 Jan 2004. Web. 6 April 2014.
4. 노승욱, "'인터넷 애물단지' 액티브엑스 퇴출...공인인증제 폐지 없인 '말짱 도루묵'", *MK News*, 24 March 2014. Web. 2 April 2014.
5. Alastair Stevenson, "Microsoft to patch Internet Explorer ActiveX Control zero-day vulnerability", *V3.co.uk*, n.p. 12 Nov 2013. Web.
6. Dan Worth, "Hackers hoarding Windows XP exploits for cut-off bonanza", *V3.co.uk*, n.p. 10 Mar 2014. Web. 3 April 2014.
7. Hyounghick Kim, Jun Ho Huh, and Ross Anderson, "On the Security of Internet Banking in South Korea," *Oxford University Computing Laboratory*, 2009. Web. 23 Mar 2014.  
<<http://www.cs.ox.ac.uk/files/2916/RR-10-01.pdf>>
8. Juan Carlos Perez, "Windows XP: Chronicle of a death foretold", *PCWorld*, IDG New Service., 7 April 2014, Web. 7 April 2014.

9. Kilnam Chon, Hyunje Park, Kyungran Kang, and Youngeum Lee, "A Brief History of the Internet in Korea," 한국인터넷 역사 프로젝트, 29 Oct 2005. Web. 20 Mar 2014.
10. StatCounter GlobalStats. *StatCounter*, 2014. Web. 5 April 2014.
11. Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, Before the Senate Judiciary Committee, 7 July 1997. Web. 6 April 2014.<[http://epic.org/crypto/legislation/freeh\\_797.html](http://epic.org/crypto/legislation/freeh_797.html)>