클라이언트 확인을 위한 Machine ID 선택

유현범, 이문호

전북대학교, 정보통신공학과

Choice of Machine ID for Client Certification

Hyon Bom Yu, Moon Ho Lee

Department of Information and Communication Engineering, Chonbuk Univ.

요 약

본 논문에서는 하드웨이의 Serail Number를 사용하여 보다 대중성 있고, 이동성이 있는 인증방법에 대하여 제안하였다. 서론에서는 컴퓨터 내부와 외부에 연결되는 Device ID들과 관련하여 각각의 선택에 대한 장단점을 알아보았고, 다음으로 이동성을 향상시키기 위해 대중화된 Device를 사용하는 것에 대해 말하였고, 대중화된 Device들을 사용하여 어떻게 적용을 시키는지에 대해 알아보았다. 마지막으로 본 논문이후로 연구되어야 하는 부분에 대해 알아보았다. Wolfram Research에서 만들어진 Mathematica라는 프로그램에서 사용되는 Machine ID에 대하여 먼저 알아보았고, Machine ID를 사용하여 일반 유지들이 사용하고 있는 인터넷 뱅킹 등에 사용되는 인증서를 보다 안전하고 이동성 있게 사용할 수 있는 방안으로 클라이언트에서 서버로 인증서가 확인이 된 후, 서버에서 다시 클라이언트로 갱신된 인증서를 보내어, 사용자는 갱신된 인증서에서만 다음 번 접속이 가능하도록 하였다.

I. 서론

수학분야에서 상당히 많은곳에서 사용되고 있는 Wolfram Research에서 만든 Mathematica프로그램은 인스톨부분에서 License Key와 Password를 요구한다. 이러한 두 개의 입력값들은 해당 컴퓨터의 Machine ID에 의해 항상 다르게 입력되길 요구한다. 즉, Mathematica라는 프로그램을 구입을 하였어도, A라는 컴퓨터에 인스톨할때의 두 입력값과, B라는, 다른 컴퓨터에 인스톨할때의 두 입력값이 서로 다르다는 것이다. 이것은 A라는 컴퓨터와 B라는 컴퓨터의 Machine ID가 서로 다름에 기인한 것이다. Chip 회로 설계를 위한 프로그램들중에서 HDD의 Serial Number를 체크하여, 처음값과 맞지 않을 경우, 해당 프로그램이 실행이 되지 않는 프로그램이 있다. 또한, 내부네트웍들 중에서 내부규정에 어긋난 사용이 적발될시에는 Mac Address를 체크하여, 해당 Mac Address를 사용하는 컴퓨터에 대한 외부 네트웍 사용을 금지시키기도 한다. 이러한 컴퓨터 내부의 Device Number들과 관련되어 사용되어지고 있는 분야가 많아지고 있는데, 본 논문에서는 단순히 클라이언트 컴퓨터를 확인하는 것이 아닌, 클라이언트 사용자의 접속을 인증하는 방법에 대하여, 이동성과 관련되어 Machine ID 선택에 대한 방법을 제안한다.

II. 본문

1. 내부 Machine ID

Machine ID는 컴퓨터를 구성하고 있는 모드 Device들의 Serial Number들을 가리킨다. 때에 따라서, Machine ID는 CPU와 Mainboard의 조합된 숫자를 가리킬때도 있고, 단순히 하나의 Device Serial Number를 가리킬때도 있다. 현재 구성되어 있는 네트웍들은 대부분 서버-클라이언트 환경을 이루고 있다. 이러한 네트??웍 구성하에서, 서버에 인증되지 않는 접속을 하여, 서버의 중요 환경을 바꾸거나, 중요 파일을 빼내오거나 하는 행동들이 행하여 지고 있다. 이러한 행위들에 의해 해당 서버에 바이러스가 침투되거나, 네트웍 트래픽을 유발시키는 일련의 행위들이 시도되는 클라이언트들은 해당 클라이언트들의 MAC address를 체크하여, 외부로 네트웍이 빠져나가지 못하도록 제약을 가 할수 있다. 그림 1에서 보는 것처럼 Machine ID는 컴퓨터 내부의 여러 Device 들의 Serial 번호들을 조합하여 사용하거나, 아니면, 각각의 Device들중 어느 하나만을 선택하여 사용하게 된다. 가장 많이 사용하는 것은 방금 언급한 MAC address이다.

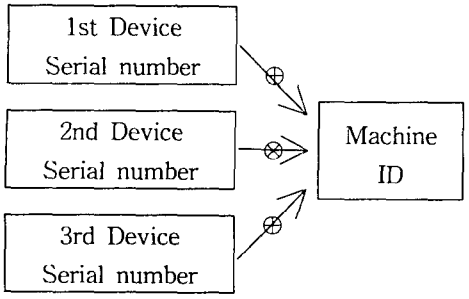

그림 1. Machine ID 생성

Machine ID로써 사용가능한 Device Number는 컴퓨터 내부에 장착되어있는 대부분의 Device에 대하여 가능하다. 보통의 경우, CPU, Mainboard, HDD, NIC의 Mac address를 사용을 하게 된다. 그러나, CPU와 Mainboard의 경우, 각각의 플랫폼마다의 Serial number이 틀려지기 때문에, 이를 사용하기 위해서는 각각의 플랫폼마다 특정한 연산을 시도하게 된다. 결국, 플랫폼에 관계없이 사용될수 있는 Device의 Serial number는 HDD와 NIC의 Mac address이다. HDD와 NIC는 이동하기가 불편하기 때문에, 각각의 Serial number를 사용한 임의의 인증방법은 효용성이 떨어지는 편이다.

먼저, Mac address를 사용할 경우, 해당 Mac address를 사용하고 있는 컴퓨터에 한해서만 인증이 되게 된다. 즉, 서버에 접속하는 지정된 단말기에 대해서만 인증을 할수 있다는 것이다. 물론, PCMCIA를 사용하여 컴퓨터를 옮겨 다닐 경우엔, 틀려질수 있겠지만, 데스크탑에 사용되는 고정된 네트웍카드의 경우, 그렇지 못하게 된다.

HDD를 사용하는 경우, 해당 HDD가 장착되어 있는 컴퓨터는 인증을 할 수가 있다. 하지만, 그러지 못한 컴퓨터, 즉 해당 HDD가 장착되어있지 않는 컴퓨터에서도 인증을 할 수가 있다. 그 방법은 HDD의 Serial number를 바꿔주는 것이다. 많이 사용되는 Ghost(하드 디스크 백업 프로그램)을 사용하여 A라는 HDD의 전체를 백업하여 B라는 새로운 하드에 복구시킬 경우, 하드디스크 B의 Serial number는 A라는 HDD의 Serial number와 같아지게 된다. 하지만, 이러한 방법으로 HDD의 Serial number를 바꾸게 될 경우, 백업되어 있는 용량으로 인하여 이동이 힘들어지게 된다. 물론, 현재는 이동성 하드디스크가 있으나, 역시 부피가 크고, 무겁기 때문에, 인증을 위해서 들고 다니는 것은 불편하다. HDD를 이용한 또 다른 방법으로는 HDD의 Serial number를 바꿔주는 프로그램을 가지고 다니면서 자기가 인증하기를 원하는 컴퓨터에 설치하여 자신이 기억하고 있는 인증을 위한 HDD의 Serial number로 바꿔서 하는 방법이 있다. 이 경우, 네트웍으로 Serial number를 바꿔주는 프로그램을 전송받아 사용하거나, 이동형 저장장치를 사용하여야 하고, 또한, 인증을 위한 HDD의 Serial number를 기억을 하고 있어야만 한다.

이러한 두 개의 Machine ID외에 또 다른 장치가 존재하는데, 그것은 바로 외부 저장장치이다. 앞서 살펴본 Machine ID는 컴퓨터의 내부에 장착되어있음으로써, 이동이 불편하기 때문에, 해당 컴퓨터만 인증하게 된다 . 하지만, 외부저장장치를 이용할 경우, 이러한 이동성에 있어서 많은 편리함이 생기게 된다.

2. 외부 Machine ID

외부의 Machine ID는 컴퓨터 외부에 연결되는 하드웨어뿐만 아니라, 외부에 연결된 하드웨어에 삽입되는 장치들도 포함을 한다. 외부 옵션장치뿐만 아니라, 외부에서 입력되는 장치들까지이다. 이러한 기기들은 예전부터 사용되어온 것으로써 프로그램의 락(Lock)을 위해 프린터포트에 연결하는 장치부터, 시리얼 장치등 여러 가지 장치들이 많이 있다. 최근에는 USB에 의해 인증을 하는 장치까지 제품으로 개발되어 판매되고 있다. 외부에서 입력되는 장치들의 경우, 스마트카드 리더 등을 꼽을 수가 있다. 하지만, 이렇게 외부에서 얻을 수 있는 Machine ID의 경우, 이를 사용키 위해서는 특별히 개발된 외부 하드웨어를 필요로 한다. 즉, 스마트카드를 사용키 위해서는 스마트카드를 읽기 위해 특별히 고안된 리더가 필요하다는 것이다.

외부에 연결되는 하드웨어로써의 Machine ID의 경우, 해당 하드웨어를 인증하는 부분, 즉, 프로그램상에서 외부에 연결된 하드웨어를 감지하고, 인식하는 부분을 뛰어넘는 방식을 택할 경우, 해당 하드웨어는 필요가 없게 된다. 물론, 네트웍상으로 해당 하드웨어를 감지하고 인식하여, 해당 하드웨어의 Machine ID를 전송해야한다고 하였을 때, 로컬상에서만 사용되었던 앞서의 방법은 통용되지 않지만, 하드웨어적인 특성상 이동 및 실치에 있어 불편함이 있는 것은 사실이다. 스마트카드리더나, SMC(Smart Media Card) 리더등의 외부 하드웨어에서 입력을 받게 되는 장치들의 경우, 해당 리더들을 설치해야 하는 불편함이 있다. 어떤 컴퓨터가 인증이 필요할 경우, 해당 리더들을 하드웨어적으로 설치하는 것이 선행되어야하며, 그 이후 해당 미디어들을 사용하여 인증을 할 수가 있게 된다.

3. 이동시를 위한 Machine ID 선택

이동을 위한 Machine ID의 경우, 해당 Machine ID가 가질수 있는 가지수가 어느정도 한정이 되어있다.

NIC의 Mac address의 경우, 00 c0 98 95 18 0d처럼 약 12개의 16진수의 자리를 가지고, 네트웍상에서 유일한 address를 갖고 있다.

이렇게 12개의 16진수는 NIC의 경우,

그림 2 HDD Serial 확인

281,474,976,710,656만큼을 생성할수 있는 Machine ID를 가지고 있다. 이렇게 많은 넘버를 가질뿐더러, 이 Machine ID는 네트워상에서 유일한 넘버를 지니고 있기 때문에, 한번 인증되면, 다른 NIC의 넘버들과 중복이 될 수 없으므로, 인증하기에 굉장히 편리하게 된다. 그러나, 한번 인증된 Machine ID를 계속 사용하려면, 해당 NIC를 제거, 실치를 반복하여 사용자가 인증을 원하는 컴퓨터에 실치를 하여 인증을 해야 한다. 보통의 NIC는 컴퓨터 내부의 슬롯에 인스톨되어있으므로, 이동이 번거롭고, PCMCIA나 USB를 사용할 경우, 이미 실치되어있는 NIC의 사용을 세컨드로 옮기거나, 사용하지 않도록 하여, PCMCIA나 USB로 네트웍에 접속을 하게 하여, 인증된 해당 기기로써 네트웍사용을 하게 된다.

그림 3 Mac Address 확인

HDD의 경우, E075-0E6A와 같이 16진수 8자리로써 Machine ID를 가지고 있다. 이것은 현재 IP 주소로 사용되는 수와 같은 4,294,967,296개의 Machine ID를 가지게 된다. 인증을 위해 HDD의 Machine ID를 사용할경우엔, 현재 IP가 부족한것과 같은 상황을 만들게 되고, 또한, HDD의 Machine ID는 확인하기가 쉬울뿐더러, 프로그램에 의해 해당 Machine ID를 확인된 Machine ID로 변경을 하는게 쉽다.

NIC처럼 가질수 있는 Machine ID가 많을뿐더러, 이동이 편리한 것으로써 CD가 있다. CD는 Machine ID를 생각한다면, 해당 Cd-reader가 가지고 있는 Machine ID를 생각하게 된다. 하지만, CD자체로도 HDD와 같은 수인 16진수 8자리의 Serial number를 가지고 있고, HDD처럼 이동이 불편한 단점도 없다. 또한, 현재 인증서를 사용할 수 있는 Mobile Device들을 제외하고는 대부분의 컴퓨터들은 다른 장치의 추가적인 실치 없이도 CD를 읽어들일 수가 있다.

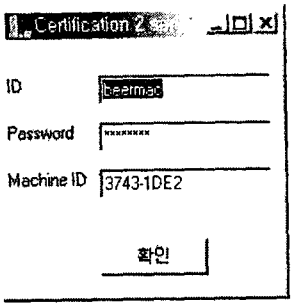

그림 4 Machine ID의
서버로의 전송

그림 4에서 보는것처럼, 프로그램은 해당 CD의 숫자를 읽어들여 서버에 전송을 하게 된다. 서버에서는 인증시에 시디의 ID와 입력되어있는 사용자의 아이디와 패스워드를 요구하게 되고, 입력된 시디의 Serial number와 사용자의 ID/Password가 전송이 된다. 전송이 된 데이터에 의해 서버는 해당 컴퓨터에 대한 인증을 해주고, 사용자는 서버에 접속을 할 수가 있게 된다.

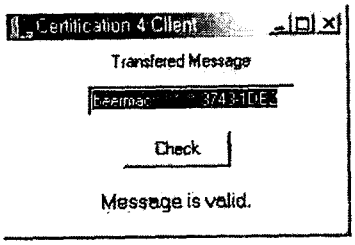

그림 5 전송된 ID 인증

이러한 전송체계하에서 인증서를 시디안에 저장할 경우, 보다 확실한 인증을 할 수 있게 된다. 즉, 위에서처럼 ID/Password 및 Machine ID와 그에 연관된 인증서를 함께 전송하게 된다면, 해당 Machine ID는 고정이 되므로, 인증서만 확실하다면, 인증함에 있어서도 문제가 없게 된다. 또한, 이러한 인증서에 관련되어서는 접속한 서버에서는 사용되어진 인증서를 폐기하고, 새로운 인증서를 클라이언트로 보내어, 해당 인증서를 CD안에 다시 저장하게 한후, 해당 인증서에 대한 정보가 있던 서버의 데이터베이스를 갱신하여, 다음번 접속시에는 해당 CD에 갱신된 인증서가 있어야만 접속이 가능하도록 할 경우, 고정된 인증서가 아닌, 자동으로 다음번에 접속할 갱신된 인증서를 보관이동하게 되므로, 한번사용된 인증서는 타인이 사용할 수가 없게 된다. 물론, 이 부분은 현재 CDRW가 많이 보급되어있기에, 미니 RW CD에

인증서를 저장을 하여 다음번 인증을 위해 소지할수 있게 된다.

이에따라, 사용자는 기존의 ID, Password를 입력한후 클라이언트에 저장되어있던 인증서만을 사용했어야 하지만, 이동하면서도 편리하게 인증을 시도할수 있으며, 클라이언트에 저장되어있던 인증서의 유출에 관련되어 보다 안심할수 있으며, 인증서의 신규, 갱신, 폐기에 대한 점에 대해 생각하지 않아도 된다.

표 1 차세대 메체들과의 비교

	장점	단점
USB Device	소형, 보관 간편, 추가적인 기기필요없슴	컴퓨터에만 사용됨
스마트 카드	보관이 비교적 간편	추가적인 카드 리더기가 필요
이동형 ID장치	저가, 보관이 비교적 간편, CD로 생산된 제품에 대해서도 인증용이, 추가적인 기기 필요없슴	컴퓨터외에 사용하려면 추가적인 장비필요.

임의의 CD에 대해 각각의 Serial number가 존재하지만, CD의 특성상 HDD의 Serial number처럼 쉽게 바뀌지 않고, NIC의 Mac address처럼 고정이 되는 특징을 가지게 된다. 임의의 사용자가 A라는 음악시디를 구입을 하였을 경우, 해당 사용자는 음악시디안의 내용에 대해 대가를 지불한것이기 때문에, mp3파일을 소유할 수 있는 권한을 가진다. 해당 사용자가 인터넷으로 A라는 음악시디안의 내용을 mp3파일로 다운받으려 하였을 때, 해당 시디의 serial number를 등록케 하여, 음악시디를 구입을 하였음을 음반업체에 확인을 하게 될 경우, 해당 음반업체의 경우, 해당 음악시디의 mp3파일에 대한 저작권료를 이미 받은것이 되므로, 문제가 생기지 않을 것이다. 인터넷 뱅킹을 사용하는 유저들의 경우, 본인만이 사용하는 컴퓨터에 인증서를 인스톨하여 사용을 하거나, 저장장치에 인증서를 저장하여 가지고 다니는 경우가 많다. 인증사이트는 유저가 시디의 일련번호에 의해 해당 사이트의 인증을 하게하여, 인증된 일련번호의 시디를 입력받음에 한해 인증을 시도하도록 제한을 가할 경우 인증서를 고정된 컴퓨터에 저장하거나, 플로피디스크등에 저장하여 이동하는것보다 더 확실하고 안정적으로 매체를 소지하고 다닐수 있게 될 것이다.

4.결론

본인임을 확인하기 위한 방법으로 스마트카드를 비롯, USB장치나 암호화된 추가인스톨하드웨이들이 많이 만들어지고 있다. 하지만, 대부분의 장치들은 비용이 많이 들뿐더러, 대부분은 리더와 같은 추가적인 하드웨어를 필요로 한다. 하지만, 컴퓨터 자체에 연결되어있는 Device들의 Machine ID를 사용을 하게 된다면, 추가적인 하드웨어 없이 인증을 할 수 있을 것이다. 또한, 이러한 여러 Device들중에서 가장 보편적으로 많이 사용되고 있는 Mini CD를 사용을 할 경우, 이동하기에 매우 편리하고, 추가적인 장비가 필요하지 않기 때문에, 많은 비용이 감소되리라 생각된다. 또한, HDD와 같은 16진수 8자리뿐이지만, CD안에 보다 긴 숫자를 가지고 있는 파일을 추가적으로 사용을 할 경우 유일무이한 만들어진 Machine ID를 생성할수 있을뿐더러, 인터넷뱅킹 사용시 인증과 함께 요구하는 비밀키 요구시에 해당 시디의 Machine ID에 의해 진행되게 한다면, 비밀키보다도 더 효용성, 안정성, 이동성을 가지고 있는 매체가 될것이라고 생각된다.

5.참고문헌

[1] 박성준, "전자서명을 이용한 사용자인증", 정보보호21C, pp70-73, 2002년 5월

[2] 조소영, "스마트카드를 이용한 사용자 인증", 정보보호21C, pp75-79, 2002년 5월

[3] Pierre L'Ecuyer. "Efficient and Portable Combined Random Number Generators" , Communications of the ACM June 1988

[4] Donald Knuth ,"Seminumerical Algorithms" , The Art of Computer Programming, Vol 2,Reading MA:Addison Wesley, 1981 pp441- 443

[5] 서동일,김기영,이상호 " 온/오프라인 기술통합을 활용한 PC기반의 침입탐지시스템 설계", JCCI 2001, pp607-611, 2001년 4월

[6] 이종우, 특허등록번호1003347200000, "보안기능을 갖는 어댑터 및 이를 이용한 컴퓨터 보안시스템"

[7] http://www.delmadang.com/

[8] http://www.zdnet.co.kr