

*Active X 가 무엇일까?

1. 정의

마이크로소프트에서 만든 XCOM(컴포넌트 오브젝트 모델)과 OLE(오브젝트 링크 앤 임베딩) 기술 두 개를 합쳐서 이름을 새로 붙여준 것. 대부분 좁은 의미로 Internet Explorer에서 애드온으로 사용되는 ActiveX Control들을 말한다. 액티브X는 거대한 소프트웨어 프레임워크지만 대한민국에서는 '인터넷 익스플로러에 붙어서만 실행되는 MFC 응용프로그램' 정도로 인식되는 것이 일반적이다.

2. 문제점

액티브X 기술이 대단히 편리한 기술임에는 틀림없다. 90년대에만 해당 각종 다운로드 서비스, 게임 실행, 음악 재생 등 사용자의 인지 없이도 온갖 프로그램을 웹페이지 접속만으로 실행할 수 있었으며 한국이 일약 인터넷 강국으로 떠오르게 된 발판이기도 하다. 당시의 기술로는 액티브X가 없었다면 저런 것은 만들 수조차 없었거나 매우 느려서 쓸모가 없었다. 90년대 당시 자바 애플릿을 채용한 곳도 있었으나 너무나 느렸기 때문에 사용자로부터 외면을 받았다. 하지만 이 기술은 한가지 큰 위험요소를 지니고 있었는데, 위에서도 써놓았듯 사용자의 간섭 없이도 자동으로 설치된다는 것은 곧 보안의 허점을 의미했다. 사실 이미 IE5 때부터 자동으로 설치되는 것은 막혀 있었고, 설정만 한다면 아예 액티브X가 실행되지 않도록 할 수도 있었다. 하지만 일단 설치된 후엔 멋대로 사용자의 컴퓨터를 주무른다. 때문에 웹 페이지 접속만으로 온갖 악성 프로그램이 실행되는 것은 일상다반사였고 컴퓨터를 모르는 사람은 물론이고 아는 사람의 PC에까지 허구한 날 바이러스와 악성코드가 창궐하기 일쑤였다.

3. 문제점 상세

>>운영체제와 웹 브라우저 차별

액티브 X는 인터넷 익스플로러8에서만 거의 정상적으로 지원하며 앞에서 언급한 대로 웹 브라우저 안에서 사실상 윈도우즈 실행 파일(exe)을 실행시키는 것이다. 즉, 액티브X가 들어간 웹 사이트의 내용물은 윈도우즈가 아닌 다른 운영체제에서는 실행이 불가능하다. 이러한 이유로 매킨토시용 인터넷 익스플로러에서는 액티브 X를 실행시킬 수 없었다. 애초에 실행시킬 exe가 운영체제에 안 깔리니 그럴 수 밖에. 그리고 같은 윈도우즈 사용자라도 파이어폭스 등 다른 브라우저를 사용할 경우 액티브X를 사용한 페이지가 제대로 표시되지 않는다.

>>인터넷 익스플로러에서의 버전 간 호환성 관련 문제

인터넷 익스플로러의 버전이 높으면 높을수록 액티브X의 능력을 확장시키기는 커녕 보안 문제와 속도 문제로 오히려 능력은 제한하기 때문에 익스플로러에 있어서 버전 간 호환성 관련 문제를 일으키고 있다. 이를테면 인터넷을 돌아다니다 "Internet Explorer 6(IE6)은 오래된 브라우저입니다. Internet Explorer 8을 설치하세요!" 와 같은 글을 보고 IE8을 설치한 상태에서 타 사이트로 가서 기존에 쓰던 액티브X를 실행했더니 안 되는 경우가 대표적인 사례라 할 수 있다.

>>액티브X 설치시 웹 브라우저 강제 종료

액티브X를 안정적으로 설치하기 위해 무작정 현재 작업 중인 모든 웹 브라우저 창을 강제종료 시키는 경우도 있다. 대부분은 강제종료 여부를 물어보지만 간혹 가다 안 물어보는 액티브X도 있어서 문제. 사실 이 프로그램들은 컴퓨터의 제어권을 취득하고 커널에 기생하는 특수한 경우를 제외하고는 웹 브라우저 강제종료가 필요 없다. 단순히 웹 브라우저 창을 새로고침만 하면 되는 문제다. 전부 강제종료 시켜놓고 다시 띄워주는 것이 아닌, 설치만 끝낸 채 홀연히 사라지는 프로그램이 대다수라는건 덤이다. 웹 브라우저를 강제종료하는 이유는 플러그인 업데이트 시킬때 dllhost.exe 프로세스를 종료해야 하기 때문이다. 액티브X를 실행시킬 때 dllhost.exe라는 프로세스가 실행된다. 이 프로세스를 강제로 종료를 해야지 업데이트된 액티브엑스를 정상적으로 구동시킬 수 있다. 그런데, dllhost.exe를 종료시키면 웹 브라우저가 종료된다. 따라서 웹 브라우저가 강제로 종료되는 것이다.

>>브라우저 속도 저하 및 다운 문제

IE의 플러그인 기술이다 보니 많이 설치될 경우 브라우저가 느려지는 현상이 발생한다. 파이어폭스에서 부가 기능을 많이 설치할 경우 발생하는 현상과 동일하다. 문제는 파이어폭스에서의 부가 기능은 보통 필수가 아니지만 IE는 국내 웹 환경에서 사용을 강요하는 일이 많기 때문에 이런저런 ActiveX가 설치되고 결국은 IE의 속도를 떨어뜨려 사용자의 복장을 터지게 하는 주요 원인이 된다.

>>악성코드의 온상

신뢰할 수 있는 곳(예를 들면 은행 사이트나 정부 기관, 어도비 사)에서 나온 액티브X라면 악성 코드가 나올 가능성이 희박하나 문제는 제작자와 제작사가 불명이거나 신뢰할 만한 액티브X로 보이도록 가장한 것도 있다는 것이다. 습관적으로 설치를 누르는 행위는 악성코드 감염의 첫 걸음이다.

4. ActiveX의 현재

정부에서 엄청난 뒤통수를 후려 갈겼다. 보안 응용프로그램을 직접 다운받아 설치하는 방식으로 대체하겠다는 것. ActiveX를 퇴출하는 대신 exe 파일을 직접 다운로드 받아 설치하여 쓰란 소리다. 이 때문에 국가에서 운영하는 사이트들에 들어가면 빠지는건 시간문제다. ActiveX는 최소한 익스플로러에서 인증서 체크라도 하는데, 응용 프로그램을 직접 다운받아 설치하면 그런 거 없다. 보안 측면에선 더 위험하다. 이걸 SSL 프로토콜만론 보안이 완벽하게 이루어지지 않는다는 업계들의 요청을 받아들인 조치이다. 하지만 그 대처법으로 선택한 게 ActiveX보다 보안상으로 더 취약한 방법인 것이다. 무엇보다 프로그램 직접 다운로드 방식은 쇼핑몰에서 약간 장난을 치면 애드웨어를 이것저것 설치할 수 있다. 이미 설치 프로그램에 애드웨어 설치 동의를 끼워넣는 마케팅은 활성화된지 오래이다. 게다가 IE 뿐만이 아니라 다른 브라우저에서도 사용가능하다는 말이 눈가리고 아웅인게, 기존의 ActiveX는 결제시에만 플러그인으로 불러서 쓰던걸 아예 윈도우 프로그램으로 설치를 해버려 시스템에 상주를 시켜버려 리소스를 좀먹게 된다. 그렇기 때문에 어떤 브라우저를 쓰든 플러그인으로 불러올 필요는 없는 대신에 컴퓨터가 느려지거나 오류를 내뿜게 되는 것이다.

*국내 웹에 Active X가 정착되게 된 이유 및 배경

1. SEED

한국인터넷진흥원(KISA)에서 1999년에 개발한 대칭키 암호화 알고리즘으로, 블록암호 기술로 인해 DES나 AES같은 암호 알고리즘과 친척뻘이다. 암호화키가 128비트라서 AES에 가깝다는 설명이 종종 있지만 실제로는 알고리즘 구조와 기술적으로 DES가 더 가까운 친척뻘이다. 128비트의 평문을 암호화하며, 키 크기는 128비트이다. 총 16라운드에 걸쳐 암호화를 진행하며, Addition, XOR, bit-rotation등의 연산식을 사용하여 암호화를 수행한다.

이 높은 대한민국 인터넷에 산재되어 있는 ActiveX의 주범이다. 그러나 그 당시 상황도 생각해 봐야 하는데, 미국이 자국 기술보호 등을 이유로 해외에 제공되는 웹 브라우저 보안 수준을 40비트로 제한시켰는데 이 따위 암호기술로는 인터넷 뱅킹은 꿈도 못 꿀 일이었기 때문이다. 인터넷 뱅킹을 하기 위해서는 128비트급의 암호 알고리즘이 최소한의 필수 선택이었다. 당시의 브라우저가 기본적으로 제공하는 40비트 암호화는 1997년의 컴퓨팅 환경에서도 겨우 3.5시간만에 깨지는 허술한 체계였고 당시의 표준이었던 DES의 56비트 암호화도 슬슬 위험해지던 시기였다. 덩달아 이게 등장하던 1990년대 후반에는 이미 PC통신으로 이루어지고 있던 홈뱅킹 서비스에서 해킹 사고가 터진 일이 여러 차례 있어서 온라인 금융의 보안에 대한 관심도 높던 시기였다. 따라서 3-DES의 112비트라도 되어야 그나마 안정성을 보장할 수 있었다. 이러한 문제를 타개하기 위해서 KISA에서는 자체적으로 128비트 키를 가지는 새로운 알고리즘의 개발에 착수하게 된 것. 128~256비트 키를 갖는 표준 알고리즘인 AES가 공개되어 아무나 갖다 쓸수 있는 오늘날의 기준으로 보면 완벽한 삽질(...)이기는 하지만 당시에는 AES도 없었고 미국의 암호화 수출제한 정책이 해금되기 전이라 SEED는 기술적으로 충분한 가치가 있었다.

어쨌든 급하게라도 128비트급인 SEED가 개발되어 배포되고 이를 통해서 대한민국 인터넷 뱅킹이 시작되긴 했는데, 문제는 웹 브라우저에 당연히 지원도 안 되었고 주요 TLS/SSL 라이브러리에도 없었던 것이다. 그래서 SEED를 쓰기 위한 관련 라이브러리와 프로그램 배포를 위해서 ActiveX란 놈을 어거지로 이용하였으며, 이게 대한민국의 ActiveX 역사의 시작이 되었다.

2. 금융권

금융권 웹사이트가 액티브X를 애용하는 이유는 책임을 피하기 위해서이다. 사용자 부주의(백신 미사용 등)로 해킹 등의 금융 사고가 발생한다 하더라도 웹사이트를 운영하는 금융권 쪽에서 책임을 져야 하는 조항이 있으며, 금융 사고 예방책으로 사용자에게 보안 프로그램을 제공해야 하는 의무가 있는데 이 보안 프로그램들이 전부 액티브X 기반이다. 결국 각종 보안 프로그램을 잔뜩 설치하게 함으로써 은행 측에서는 책임 회피(키보드 보안 플러그인 설치했나요? 전자서명 설치했나요?보 안 모듈은요? 가상 키보드는요? 왜 nProtect를 평소에 실행시키지 않았죠? 등)를 할 수 있고, 사용자의 PC는 액티브X로 떡칠이 되는 것이다.

*기술적 부채(Technical Debt) ?

1. 개요

기술적 부채(또는 기술 부채)는 지금 당장 해두지 않아도 되거나, (상대적으로 덜 필수적인) 안해도 티가 잘 나지 않는 작업들을 이런저런 이유로 포기하거나 미뤘다가 파생된 결과가 부채(debt)의 개념으로 돌아오는것을 지칭한다. 이 부채라는 것이, 빨리 해소하지 않으면 실제 빚처럼 점점 더 커진다는 것도 비슷하다.

2. 원인

>>사업적인 이유: 기술적인 문제를 해결하기 위해서는 시간과 돈이 더 필요한데, 이런 문제를 해결하다가 완료가 늦어지면 그 기간만큼 사업을 정상적으로 할 수 없으므로, 수익성이 악화된다. 당연히 윗선에서는 그걸 좋지않게 여기고, 어떻게든 빨리끝내라고 압박을 가한다. 결국 마감기한에는 잘 굴러가는것처럼 내놓는다.

>>기술적 부채에 대한 이해 부족

>>테스트 스위트(Test Suite) 부족: 어떤 일부 상황에만 적용가능한 임시방편으로 해결하게 된다.

>>문서 부족: 관련 문서(나 주석) 없이 코드를 작성할 경우, 차후 그 코드에 관련된 설명 문서를 만드는것이 그 부채가 된다.

>>지식 부족: 깔끔하게 코드를 작성하는 방법을 모를때

3. 결과

이 빚은 미래에 어떤 형태로든 갚게 되는데, 뭔가 끝낸것 같은 시점 이후의 디버깅을 비롯한 문제해결 작업같은것이 이에 해당된다. 이런 문제해결 작업은 지체되면 지체될수록 작업에 필요한 시간과 비용은 더 커져만가니 실제 빚 개념과도 유사하다고 할 수 있다. 그리고 문제점이 누적되어서 '어디서부터 손대야 하는지 모르는 수준'에 다다르게 되면, 유지보수의 수준이 아니라 시스템 재구축을 해야 하는 상황에 이를 수도 있다. 경우에 따라서는 기존의 것을 완전히 폐기하는 매몰비용까지 고려해야 한다는 것. 이 재구축에 소요되는 시간과 비용 + 매몰비용이 갚아야할 빚에 해당된다.

*위 내용을 조사하면 느낀 점

ActiveX가 초반에 도입된 이유와 정황은 나름의 타당성이 있었다. 허나 문제는 빠르게 변화는 환경에 합리적으로 대응하지 못한 점이다. 금융권 암호화 알고리즘 SEED의 보급을 위해 어쩔 수 없이 도입한 ActiveX는 차후 보안적으로나 사용편의성이나 모든 면에서 취약했다. 허나 한국의 IT산업은 퇴출당하는 ActiveX를 끝까지 끌고가는 (심지어 대안이란게 exe 다운로드라는..) 과오로 बैंकिंग이든 전자상거래든 거대한 기술적 부채를 감내하고 있다. 물론 ActiveX 이슈는 단순한 기술적 부채로 보기엔 복합적인 산업병폐이다. 보안회사, 금융회사, 유통회사 등등 다양한 산업에서 각기 자신의 이익과 책임회피로 나타난 비극이라고 볼 수 있다. 이러한 국내 IT산업의 가장 큰 흑역사(역사가 아닌 현실인가?)를 보면서 두 가지를 느낀다

첫째로는 기술선도이다. 결국 기술적으로 리드하지 못하기 때문에 미국정부든 마소든 정책 변화에 따라 국내 기업 및 정부가 열심히 휘둘린 사례라 볼 수 있다. 중간에 극복할 수 있는 기회와 시점은 많았으나 일단 발단이 그렇다. 기술 선도하는 기업 또는 국가는 기술환경을 우리쪽에 유리하게 끌고갈 수 있다.

둘째로는 합리적인 기술 선택이다. 다양한 이해관계가 엮인 본 문제는 합리적 선택으로 결과가 나오기 힘들었다. 누군가의 생존 또는 이득을 위해 사회적인 막대한 비용이 지불된 셈이다. 빠르게 변화하는 기술환경에 마치 린 스타트업과 같은 자세를 가져야 한다. 얼리어답터와 같은 실험적인 수준까지는 아니더라도 기술의 트렌드에 뒤쳐지지 않는 자세를 가져야하며, 기존에 투자한 시간과 비용을 매몰비용으로 인정하지 못하면, 사업 자체가 매몰될 것이다.