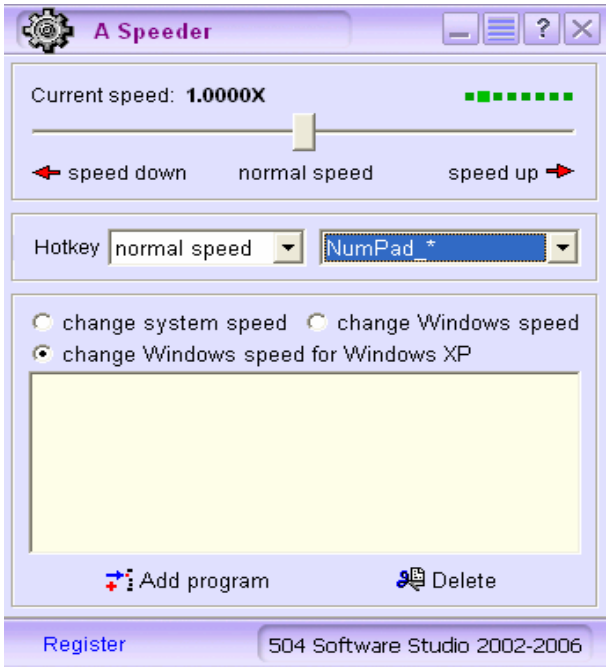
1. 스피드핵의 종류와 동작 방식

지난 달 오토마우스에 이어 이번 달에는 스피드핵에 대해 다루어보려고 한다. 게임 프로그램의 특성상 Time-Based로 수행되어 지는 동작들이 많으며, 이러한 동작들은 대부분 Windows에서 제공하는 Timer 관련 함수들을 사용하여 구현하게 된다. 게임 해킹 방법중 스피드핵이라는 방법은 바로 이 Time-Based의 동작을 조절하기 위하여 시스템의 Timer 칩이나 Timer 관련 함수들의 결과값을 임의로 조작하는 행위를 말하며, 이러한 행위에 의하여 게임 프로그램은 원하지 않는 결과를 만들어 내게 된다. 스피드핵은 오토마우스와 더불어 가장 많이 사용되는 해킹툴로서 게임에 관심이 있는 사람이라면 한번쯤은 들어봤을 만한 해킹툴이다. 그만큼 유명하고 널리 애용(?)되었다는 의미이다. 그럼 이제부터 스피드핵의 종류와 동작방식에 대해서 자세히 살펴보도록 하겠다.

스피드핵의 정의

스피드핵은 말 그대로 게임의 스피드를 마음대로 조절이 가능하도록 해주는 해킹툴이다. 2005년에 공용툴 형태로 많이 제작되다가 2006년부터는 특정 게임을 대상으로하는 전용툴 형태로 제작되고 있다. 그러나, 2007년에 들어서는 많이 사라지고 있는 추세이기도 하다.

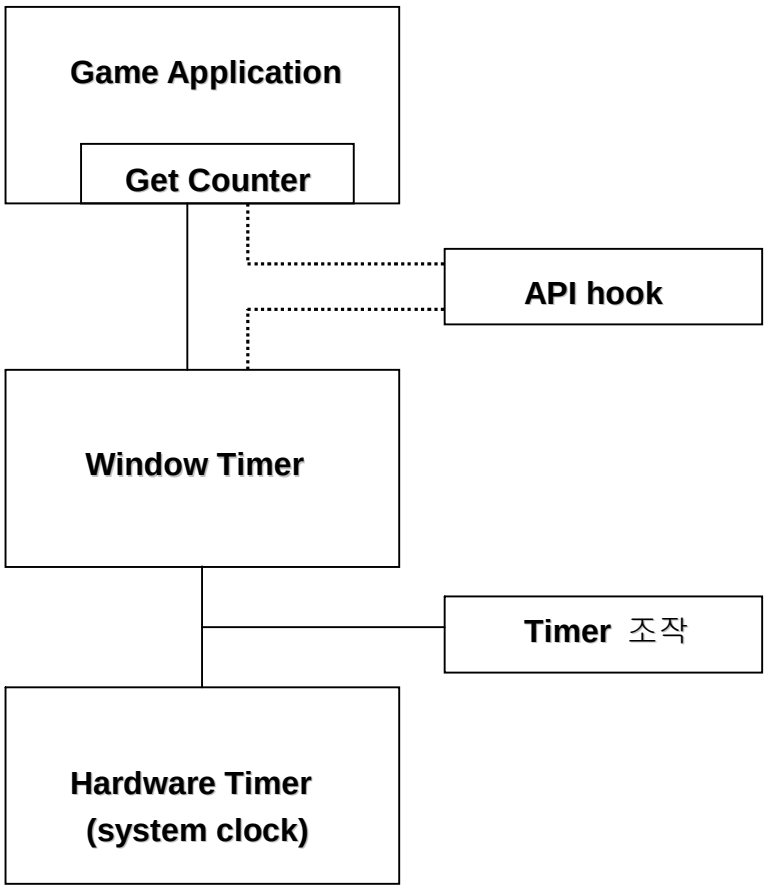


[그림 **1]** 유명한 공용 스피드핵인 **SpeederXP**와 **A Speeder**

스피드핵을 이용할 수 있는 경우는 속도를 빠르게 하여 플레이를 빠르게 진행할 수 있다. 예를 들어 MMORPG 에서 공격속도와 이동속도를 빠르게 할 수 있으며, 레이싱 게임 등에서 이동속도를 빠르게 조절할 수 있다. 이렇게 할 경우 서버와 주고받는 패킷의 양이 늘어나게 되어 게임서버에 부하를 줄 수 있게 된다. 또한, 스피드핵을 사용하지 않는 다른 유저가 볼 때는 스피드핵을 사용하는 유저의 캐릭터가 너무 빨리 움직이게 되어 유저의 불만을 일으키게 되고, 게임의 발란스를 무너뜨리는 상황을 야기할 수 있다.
반대로 스피드핵을 이용하여 속도를 느리게 하는 게임도 있다. 예를 들어, 골프게임이나 바둑, 고스톱과 같은 보드게임에서 사용될 수 있는데, 골프게임의 경우 타구의 정확도를 맞추기 위해 순간적으로 속도를 느리게 하여 사용할 수 있으며, 고스톱이나 바둑의 경우 자신의 차례에서 속도를 느리게 하여 상대방보다 더 많은 시간 동안 생각을 할 수 있도록 하는데 사용을 한다.

스피드핵의 동작 방식
스피드핵은 그 동작방식에 따라 소프트웨어 방식의 스피드핵과 하드웨어 방식의 스피드핵으로 구분할 수 있다.
소프트웨어 방식의 스피드핵은 게임에서 사용하고 있는 시간관련 함수들을 후킹하고 함수의 결과값을 조작하여 게임의 속도를 조절하는 방식을 말하며, 스피드핵이 후킹 대상으로하는 시관관련 함수들은 timeGetSystemTime, timeGetTime, timeSetEvent, GetTickCount, QueryPerformanceCounter,

GetMessageTime, SetTimer 둥이 있다. 여기서 후킹이라함은 쉬운 표현으로 제어의 흐름을 가로채는 것을 말한다. 예를들어, 스피드핵이 GetTickCount를 후킹했다고 가정해보자. 게임내의 시간을 설정하는 부분에서 시간조절을 위해 GetTickCount를 호출하게되면, GetTickCount이 정상적으로 처리되어야 하는 경로 중간에 스피드핵이 그 흐름을 가로채게되고 자신이 원하는 결과값을 되돌려 줌으로써 마음대로 속도를 조절할 수 있게 된다.
하드웨어 방식의 스피드핵은 시스템에서 사용하는 8254 PIT(Programmable Interval Timer) 칩을 조작하여 시스템의 속도를 조작함으로써 게임의 속도를 조절하는 방식을 말한다.



[그림 **2]** 스피드핵의 동작 원리

2. 스피드핵 방어 방법
지금까지 스피드핵의 종류와 동작방식에 대해서 살펴보았고, 이제부터는 이렇게 동작하는 스피드핵을 게임 내에서 어떻게하면 동작을 차단하고 감지할 수 있는지 간단하게 살펴보도록 하겠다.

스피드핵을 방어하는 가장 보편적으로 많이 사용되는 방법은 게임서버와 클라이언트간의 주기적인 시간동기화나 시간변화량을 체크하여 차단하는 방식이다. 시간 동기화 방법은 게임서버과 게임 클라이언트가 주기적으로 시간을 맞추어 클라이언트의 게임 진행 속도를 조절 하는 방식이다. 게임 클라이언트의 진행 속도를 스피드핵을 사용하여 조작하더라도 게임서버와의 시간 동기화를 통해 조작된 시간 만큼을 다시 보상하여 적용하는 방식이다. 시간변화량 체크 방식은 게임서버와 게임클라이언트간의 시간 변화량을 주기적으로 체크하여 클라이언트와 게임 서버간의 시간변화량 차이가 일정 수준을 넘어서면 스피드핵으로 감지하는 방법이 있다. 두 가지 방법 모두 주의해야 할 것은 변화된 시간을 보상하는 로직과 시간변화량의 판단 로직이 모두 서버에 존재해야 한다는 것이다. 만일, 클라이언트에 판단 로직이 존재할 경우 해당 로직을 조작하고자 하는 또 다른 해킹 문제에 직면할 수 있게 된다.

3. 마치며

이번에는 스피드핵의 동작방식과 종류 등에 대해 집중적으로 살펴보았다. 앞서 설명했지만, 스피드핵은 게임 개발사와 보안업체의 끈임없는 노력의 결실로 지금은 거의 퇴치되고 있는 해킹툴 중의 하나이다. 보안업체와 게임 개발사들이 서로 협력하여 온라엔 게임 보안에 대한 노력과 연구가 끊임없이 이루어져서 비단 스피드핵 뿐 아니라 다른 해킹 영역에도 좋은 결과가 나왔으면 하는 바램이다. 다음에는 지금까지 설명한 해킹방법보다 좀 더 고급기법인 실행파일 조작과 메모리 조작에 대해서 살펴보도록 하겠다.