성균관대학교
정보통신대학

졸업작품

플래시 취약점과 조작된 웹 사이트를 통한 원격코드 실행 분석 및 구현

황지만
성균관대학교 정보통신대학

Analysis and Implementation of Remote Code Execution through Flash Vulnerability and Crafted Web Site

Hwang Jiman
Sungkyunkwan University

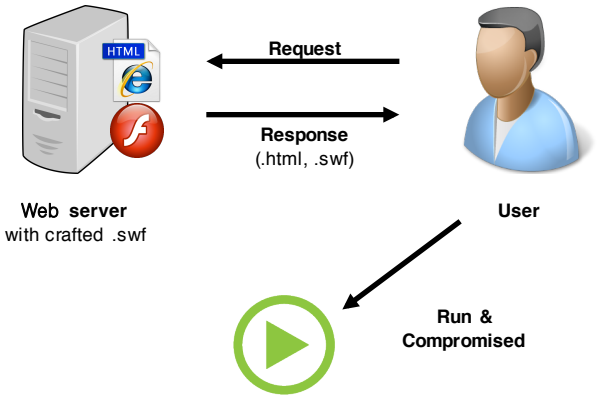
지도 교수: 최형기 교수님

연구실명: 인터넷 보안 연구실

개 요

Flash player의 PC 점유율은 90%에 육박한다. 즉, 거의 모든 PC깔려있다고 해도 무방한데, Flash player의 취약점과 조작된 웹 사이트를 이용하면 악의적인 해커가 짧은 시간 내에 다수의 피해자를 만들어낼 수 있어 위험하다. 안타깝게도 대부분의 사용자들은 인터넷상의 link를 별다른 의심 없이 누르는 경우가 많으며, 이에 따라 피해를 볼 수 있다. 한 번 점령당한 PC는 그 피해가 해당 PC만으로 끝나는 것이 아니라 같은 네트워크 상의 다른 컴퓨터를 공격할 수도 있고, DDOS로 악용될 수도 있어 그 피해가 커질 수 있다. 본 작품에서는 이러한 Flash player의 취약점을 심층 분석하여 피해가 발생할 수 있는 원리를 밝힌다.

시스템 구성



Web server	**조작된 웹 사이트와 플래시 파일을 사용자에게 제공한다.**
User	**인터넷상의 웹 사이트가 악성 사이트인지 모른 채 접속하여 악성 플래시 받고, 실행 후 공격을 당하게 된다.**
Html file	**사용자가 요청하는 웹 페이지. 악성 플래시파일을 사용자에게 보내고, 실행하게 한다.**
Flash file (.swf)	**이번 작품에서 다루는 플래시 취약점을 일으키도록 제작된 플래시 파일. Html 파일에 의해 사용자에게 전송되어 해당 컴퓨터에서 공격자가 의도한 코드를 실행한다.**

Internals

1. Heap영역 확보
   - 아래 과정을 수행하기 위해 Heap공간 확보
   - Heap-spray
2. 전체 메모리 액세스
   - 모든 메모리(커널, 비할당영역 제외) 접근 가능
   - Pixel Bender Vulnerability
3. Shellcode 삽입
   - 공격자가 원하는 임의의 악성코드
4. Heap영역에 실행 권한 부여(DEP우회)
   - 삽입된 Shellcode에 실행 권한 부여
   - Function Table, VirtualProtect() in WinAPI
5. Shellcode 실행

결 과

- Windows 7 에서 접속
- Shellcode: 계산기 실행
- User측에서 Shellcode 실행 확인

결론

뉴스에서나 듣던 보안 취약점을 심층적으로분석해보았다. Flash player의 취약점부터 시작하여 이를 발전시킨 뒤 웹 사이트를 이용하면 다수의 사용자에게 피해를 입힐 수 있다는 것을 알았다. 또 단순히 링크를 클릭 하는 것만으로도 컴퓨터에 피해가 올 수 있다는 것을 직접 겪었으므로, 앞으로는 링크를 클릭할 때 주의를 기울여야한다. 또한 이러한 보안 취약점에 대한 패치가 업데이트를 통해 이루어지므로 업데이트를 부지런히 해야 보안 사고를 막을 수 있다.