커널 모드 코드 서명초보자 안내서

출처: https://www.scip.ch/en/?labs.20190919

우리가하는 일 중 하나의 매혹적인 측면은, 우리가 미리 알지 못하는 주제를 다루고 짧은 시간 내에 많은 지식을 수집해야한다는 사실입니다. 일반적으로 방금 배운 내용을 바로 적용 할 수 있도록 주제에 익숙해 져야합니다.

최근에 Windows에서 커널 모드로 코드를 실행하고 싶었으므로 전제 조건과 함정이 어디에 있는지 배웠습니다. 이것이 바로이 실습의 핵심입니다. Windows 커널 모드의 코드 서명 주제에 대한 초보자 안내서입니다.

이론

코드 서명 소개

운영 체제 Microsoft Windows는 **사용자 공간**과 **시스템 공간** (커널 공간이라고도 함)을 구분합니다. 내부 또는 민감한 운영 체제 리소스에 직접 액세스 할 수없는 일반 응용 프로그램은 **사용자 공간**에서 실행됩니다. **커널 공간**에서 실행되는 코드는 시스템의 안정성 또는 보안에 더 많은 액세스 및 운영 체제에 직접적인 영향을 미칩니다. 결과적으로 커널 공간의 코드 요구 사항이 더 높습니다.

Windows Vista 64 비트가 릴리스되었을 때 Microsoft는 커널 공간에 코드를로드하기 위해 서명이 필요했습니다. Windows 8에서는 드라이버 패키지도 서명해야했습니다. 그리고 Windows 10에서 Microsoft는 **WHDC**(Windows Hardware Dev Center)에서 새 드라이버를 서명해야했습니다.

드라이버를 변경하면 기존 서명이 유효하지 않으므로 드라이버에 서명하면 소프트웨어의 무결성이 보장됩니다. 둘째, 소프트웨어의 출처를 결정할 수 있습니다. 하드웨어 개발자 센터에 등록 할 때 Microsoft는 최소한 소프트웨어의 계정을 추적 할 수 있기 때문입니다. 또한 참여 조건 중 하나는 Extended Validation Code Signing 인증서 또는 EV CS 인증서를 사용하는 것입니다.

EV CS 인증서가 발급되기 위해서는 인증 기관 (CA, *certificate authority*)이 발급 과정의 일부로 신청자에 대한 세부 점검을 수행합니다. 인증서를 신청하는 모든 회사는 올바른 주소, 공식 전화 번호 및 소프트웨어 서명 담당자와 같은 공개적으로 확인 가능한 정보를 제공해야합니다. 이 연락처는 전화로 확인됩니다. 검증에 성공하면 EV 코드 서명 인증서가 회사 이름으로 발행되고 USB 토큰으로 제공됩니다.

현재 웹 사이트를위한 EV 인증서의 목적에 대한 논의가 진행 중입니다. 보안 연구원 인 트로이 헌트 (Troy Hunt)는 자신의 블로그 기사에서 확장 검증 인증서가 (정말로, 정말로) 죽었다; 그는 무료 솔루션으로 대체 할 수 있다고 생각합니다. 그러나 Microsoft에서는 EV CS 인증서를 사용해야하므로 커널 모드 코드 서명에 대한 대안은 없습니다.

Windows 요구 사항

한 걸음 물러서서 다른 버전의 Windows 요구 사항을 살펴 보겠습니다. Microsoft의 드라이버 서명 정책에 따르면 Windows 7 64 비트, Windows 8 및 Windows 10에서 버전 1511까지는 드라이버에 SHA1을 사용하여 서명해야하며 사용 된 인증서는 Microsoft의 교차 인증서 목록에있는 CA에서 제공해야합니다. Windows 10 버전 1607 ~ 1709의 경우 SHA1 또는 SHA2가 서명 알고리즘으로 허용되고 Windows 10 버전 1803 이상에서는 SHA2 만 허용됩니다. 서명도 Microsoft 루트 기관에서 가져와야합니다. 다시 말해, Windows 10 버전 1607을 새로 설치하면 Hardware Dev Center에서 서명하지 않은 새 커널 드라이버가 더 이상로드되지 않습니다.

이러한 변경 사항은 Windows 10 버전 1607의 드라이버 서명 변경이라는 제목의 블로그 기사에 자세히 설명되어 있습니다. 이전 버전과의 호환성을 위해 Microsoft는 예외를 정의하여 모든 드라이버를 다시 서명 할 필요는 없습니다.

- Windows 10 버전 1607 이전에 배포되었고 이후에 업데이트 된 컴퓨터는 여전히 크로스 서명 드라이버 설치를 허용합니다
- 보안 부팅이없는 컴퓨터에서도 여전히 크로스 서명 드라이버를 설치할 수 있습니다
- 인증서 체인에 지원되는 교차 서명 CA가 포함 된 2015 년 7 월 29 일 이전에 발급 된 인증서 서명이 있는 드라이버는 여전히 허용됩니다.

따라서 현재 Windows 10 버전의 모든 새 드라이버는 EV CS 인증서로 서명 한 다음 Windows 하드웨어 개발자 센터에서 확인한 다음 Microsoft에서 서명해야합니다.

PRACTICE

드라이버 서명

Microsoft는 테스트 서명 구현 지침이 포함 된 포괄적 인 Windows 드라이버 서명 자습서를 제공합니다. 그러나 세션의 드라이버 서명 적용 옵션을 비활성화하려면 운영 체제를 특수 모드로 부팅해야합니다. 그런 다음 고유 한 인증서를 작성하고 이를 사용하여 드라이버에 서명하고로드 할 수 있습니다. 이 단계는 초기 시도 및 테스트에 유용 할 수 있습니다. 그러나 자체 서명 된 드라이버는 현재 Windows 버전의 외부 컴퓨터에서 사용할 수 없습니다.

드라이버에 서명하려면 WDK (Windows Driver Kit)가 필요합니다. WDK에서 가장 중요한 도구는 SignTool입니다. 드라이버 서명 및 잠재적 검증에 사용됩니다. 서명 목적으로 인증서 파일 (PFX)을 사용하지 않는 것이 좋습니다. 대신 운영 체제의 인증서 저장소로 인증서를 가져온 다음 서명 프로세스를 수행하는 것이 좋습니다. 또한 EV CS 인증서는 PFX 파일이 아닌 USB 토큰 또는 스마트 카드로 제공됩니다.

가장 간단한 형태의 드라이버 서명 명령은 다음과 같습니다.

```
signtool.exe sign /v /n "SubjectName" DriverFile.sys
```

매개 변수 / n은 인증서의 공통 이름입니다. 그러나 드라이버가 커널 모드로 로드 되려면 교차 서명 된 CA의 인증서를 사용해야합니다. 교차 인증서 목록에서 적절한 CA 인증서를 다운로드 할 수 있습니다. 그런 다음 이 인증서는 / ac 매개 변수를 사용하여 통합됩니다.

```
signtool.exe sign /v /n "SubjectName" /ac CrossSignedCARoot.cer DriverFile.sys
```

드라이버는 Windows 10 용 SHA2로 서명해야합니다. 드라이버에는 서명 타임 스탬프도 포함되어야합니다. 해당 CA의 타임 스탬프 서버를 사용할 수 있습니다.

```
signtool.exe sign /v /n "SubjectName" /ac CrossSignedCARoot.cer /fd sha256 /td
sha256 /tr http://timestamp.example.com/rfc3161 DriverFile.sys
```

이런 방식으로 서명 된 드라이버는 Windows 7, 8 및 이전 버전의 Windows 10에서 사용할 수 있습니다.

서명 확인

Signtool.exe 응용 프로그램은 서명을 확인하는 데 사용됩니다. 확인 과정에서 플러그 앤 플레이 드라이버 (PnP)를 검증하기위한 매개 변수 /pa와 커널 모드 드라이버를위한 /kp가 구분됩니다.

```
signtool.exe verify /pa /v DriverFile.sys
```

```
signtool.exe verify /kp /v DriverFile.sys
```

확인 중에 다음과 같은 오류가 발생할 수 있습니다.

- The signing certificate is not valid for the requested usage : EV CS 인증서가 필요합니다. 다른 인증서는 커널 모드로 허용되지 않습니다
- The provided cross-certificate would not be present in the certificate chain : 교차 인증서 목록에서 다운로드 한 인증서가 인증서 체인과 일치하지 않습니다. 적절한 루트 인증서를 선택해야합니다
- A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider : 드라이버가 교차 인증서를 사용하여 서명되었지만 하드웨어 개발 센터가 아닌 버전 1607의 Windows 10 메시지

인증서의 인증서 체인은 certutil.exe를 사용하여 확인할 수 있습니다. Pentesters 는 이제 클라이언트에서 certutil을 실행해야하는 합법적 인 이유가 있습니다.

```
certutil.exe -dump Certificate.cer
```

결론

서명 할 때까지 EV CS 인증서 응용 프로그램 확인 및 USB 토큰 전달 대기 시간, 자체 서명 및 일반 CS 인증서 사용 실패 및 Microsoft 문서 읽기를 포함하여 2 주가 걸렸습니다. 드라이버가 Windows에서 커널 모드로로드되도록합니다. 이 기사는 다른 사람들이 이 목표를보다 빠르고 쉽게 달성하는 데 도움이 될 것입니다. 의견을 보내거나 자신의 경험을 공유하십시오.

Links

- https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/get-started-with-the-hardware-dashboard
- https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/signtool
- https://docs.microsoft.com/en-us/windows-hardware/drivers/download-the-wdk
- https://docs.microsoft.com/en-us/windows-hardware/drivers/install/cross-certificates-for-kernel-mode-code-signing#cross-certificate-list
- https://docs.microsoft.com/en-us/windows-hardware/drivers/install/kernel-mode-code-signing-policy—windows-vista-and-later-#signing-requirements-by-version
- https://docs.microsoft.com/en-us/windows-hardware/drivers/install/windows-driver-signing-tutorial
- https://techcommunity.microsoft.com/t5/Windows-Hardware-Certification/Driver-Signing-changes-in-Windows-10-version-1607/ba-p/364894
- https://www.troyhunt.com/extended-validation-certificates-are-really-really-dead/