Joachim Gebauer

Code Signing

Programme als vertrauenswürdig kennzeichnen

Wer Anwendungen installiert oder mit Webapplikationen interagiert, geht davon aus, dass beides sicher ist. Dabei zeigt sich, dass Cyberkriminelle bevorzugt mit gefälschten Apps operieren. Mit dem Verfahren Code Signing können Entwickler ihr Programm mit einem unabhängigen, manipulationssicheren Gütesiegel kennzeichnen und so dem Anwender signalisieren, dass er dem Programm berechtigterweise vertrauen kann.

Die meisten Rechner werden heute über Downloads infiziert, seien es E-Mail-Anhänge oder Dateien, die der Anwender auf einer Webseite herunterlädt. Täglich findet z.B. Symantec 1,7 Millionen neuer Varianten dieses Schadcodes. Cyberkriminelle haben ihren Aktionsradius inzwischen auf Smartphones und die Welt von Android-Apps ausgeweitet. Bekannte Apps werden kopiert, um Schadfunktionen ergänzt und unter ähnlichen Namen in die App-Shops gestellt. 3600 Schadcodes hat Symantec bisher für Android erfasst, Tendenz weiter steigend.

Das Vertrauen zwischen Software-Anbieter und Anwender, das essenziell ist für Transaktionen im Internet, wird dadurch stark belastet. Wie können die Endanwender noch wissen, welchen Software-Plattformen, Netzwerken und Angeboten man trauen kann? Und wie sollen Soft- und Hardwarehersteller ihre Innovationen fördern, aber gleichzeitig ihre Produkte schützen?

Eine Antwort ist der Einsatz des Verfahrens „Code Signing". Prinzipiell umspannt es den Quellcode eines Programms mit einer digitalen Schutzfolie, welche die Identität des Unternehmens anzeigt und zugleich bestätigt, dass die Zeilen seit der Signierung unverändert sind.

Der Vertrauensmechanismus

Der Entwickler oder das Unternehmen, welches die Anwendung oder die Webapplikation erstellt, können ihren Objektcode grundsätzlich auf zwei Arten signieren. Entweder sie tun es in Eigenverantwortung und signieren ihn mit einem eigenen, selbst generierten Zertifikat. Oder sie können sich an eine seriöse, etablierte Signaturstelle wenden, um von dort ein öffentliches Zertifikat zu beantragen, um damit zu arbeiten.

Wer den ersten Weg wählt und seine Software selbst signiert, dessen Signatur fehlt die Bestätigung eines unabhängigen Dritten. So bleibt fraglich, ob das in der Signatur genannte Individuum tatsächlich auch der Entwickler ist oder ein Saboteur, der sich als der Entwickler ausgibt. Folglich wird der Endnutzer mit der Frage allein gelassen, ob die Software tatsächlich frei von Manipulation ist. Hinzu kommt, dass selbst generierte digitale Zertifikate zur Codesignatur nicht widerrufen werden können. So kann ein Hacker, der bereits Zugang zum System eines Endnutzers hat, leicht Datendiebstahl begehen.

Daher ist es gerade im professionellen Geschäftsbereich und bei Online-Transaktionen üblich und ratsam, sich an eine seriöse Zertifizierungsinstanz wie Symantec zu richten. Während des Registrierungsprozesses werden Informationen über den Entwickler und das Unternehmen gesammelt, um beide eindeutig zu authentifizieren. Diese Validierung kann bis zu mehreren Tagen dauern, abhängig von der bereitgestellten Informationen und deren Qualität. Überprüft werden unter anderem der Eintrag ins Handelsregister und die Adresse des registrierten Bevollmächtigten des Unternehmens. Erst wenn diese Prüfung positiv abgeschlossen ist, wird dem Programmierer oder Unternehmen sein von der Root CA der Zertifizierungsstelle signierte Zertifikat auf sicherem Wege zugeschickt.

Der Hintergrundprozess

Mit Hilfe dieses Zertifikats und dem standardisierten Public-Private-Key-Verfahren wird der Objektcode schließlich digital signiert. Dazu nutzt der Entwickler seinen privaten Schlüssel und fügt dem Code die digitale Signatur hinzu. Danach wird das Programm auf eine Webseite oder in einem App-Shop hochgeladen oder anderweitig zum Download zur Verfügung gestellt.

Wenn der Nutzer das Programm oder den Webdienst per Browser ansteuert, wird die Signatur automatisch mit Hilfe des bekannten öffentlichen Schlüssels und des Zertifikats entschlüsselt. Wenn Software-Plattformen und Anwendungen, wie Browser, die digitale Signatur verifizieren, greifen sie dabei auf das „Root"-Zertifikat zu. So finden sie heraus, ob die Zertifizierungsstelle (CA), die das Zertifikat ausgestellt hat, vertrauenswürdig und bereits etabliert ist.

Außerdem wird neben dem Zertifikatcheck automatisch eine mathematische Quersumme berechnet – der so genannte Hashwert. Der Wert aus dem tatsächlich heruntergeladenen Objektcode muss dabei identisch sein mit dem Wert, der in der Code-Signatur eingetragen ist. Wurde nur ein Bit im Code manipuliert, stimmen beide Werte nicht mehr überein. Gefälschter Objektcode ist dadurch klar identifizierbar.

Korrekter, signierter Code einer vertrauenswürdigen Quelle wird entweder automatisch akzeptiert oder es erscheint eine Sicherheitswarnung, die den Endanwender auffordert, sich die Signatur-Informationen anzusehen und zu entscheiden, ob er dem Code vertraut. Diese Funktion ist abhängig von der Entwicklungssprache und -plattform, der Anwendung und den Sicherheitseinstellungen des Clients.

Fazit

Code Signing hilft Herstellern und Anbietern von Software, eine vertrauensvolle Bindung zu ihren Kunden herzustellen. Sie können die Echtheit der Software sicherstellen und garantieren, dass die heruntergeladene Software nicht manipuliert wurde. Auf diese Weise können die Vorteile des Internets für den Software-Vertrieb voll genutzt werden.

Joachim Gebauer, Technical Account Manager bei Symantec