Pressemitteilung – 26. Oktober 2023

AxProtector CTP für besseren Schutz vor Produktpiraterie und Reverse Engineering

- **Die Mechanismen zum Softwareschutz von Wibu-Systems verwenden neuartige Obfuskationstechniken.**
- **Die neue Compile-Time-Protection-Technologie nutzt das LLVM-Compiler-Framework, um wirksame Schutzziele zu erreichen.**
- **AxProtector CTP gewährleistet die Sicherheit der Anwendung bei gleichzeitiger Einhaltung plattformspezifischer Richtlinien, ohne dass die Anwendung zur Laufzeit geändert werden muss.**
- **Diese neue Erweiterung der CodeMeter Protection Suite unterstützt die Betriebssysteme Windows, Linux und macOS.**

Die neue Obfuskationstechnik verschleiert den Code von C/C++-Anwendungen bis zur Unkenntlichkeit

Karlsruhe – **Wibu-Systems, ein weltweit führendes Unternehmen für Softwareschutz und Lizenzierung, hat seine CodeMeter Protection Suite zum automatischen Schutz von Software vor Piraterie und Reverse Engineering erweitert. Die neue Funktion Compile Time Obfuscation (CTO) ist für AxProtector Windows, AxProtector Linux und AxProtector macOS verfügbar. Um diese Funktion zu nutzen, wurde die neue Technologie AxProtector Compile Time Protection (CTP) eingeführt.**

Diese neuartige Technologie verfolgt einen völlig neuen Ansatz beim Softwareschutz, bei dem die gesamte Anwendung bereits während des Kompilierungsprozesses obfuskiert wird. AxProtector CTP bringt den Schutz der Anwendung mittels Obfuskationstechnologien auf das gleiche Niveau wie verschlüsselungsbasierte Schutzwerkzeuge. AxProtector CTP verschleiert Symbole und den Ablauf der Anwendung, fügt zusätzliche Blöcke ein und versteckt logische Verknüpfungen im Code, um den Schutz vor Reverse Engineering zu erhöhen. Die Technologie AxProtector CTP

ist bereits als Option CTO in den Produkten AxProtector Windows, AxProtector Linux und AxProtector macOS enthalten. Sie unterstützt Intel, ARMHF und AARCH64 und funktioniert derzeit mit den Programmiersprachen C und C++. Auf Anfrage werden weitere Programmiersprachen unterstützt.

Die richtigen Abwehrmaßnahmen gegen Cyber-Angriffe zu finden ist eine wichtige Aufgabe. Dank der Vielseitigkeit von LLVM ist AxProtector CTP in der Lage, mehrere Betriebssysteme, Architekturen und Plattformen zu unterstützen. Mit AxProtector CTP können umfassende Abwehrtechniken reibungslos integriert werden, um die Sicherheit von Anwendungen für verschiedene Anwendungsfälle zu erhöhen. Zusätzlich sind alle Funktionen der AxProtector-Produkte, wie beispielsweise die flexible Lizenzierung durch vertrauenswürdige kryptografische Algorithmen, auch in der neuen CTP-Technologie verfügbar. Die enge Verknüpfung zwischen Lizenzierung, Verschlüsselung und Obfuskation sorgt für einen optimalen Schutz von Anwendungen.

Während reine Verschlüsselungslösungen die Anwendung nach der Kompilierung verschlüsseln und während der Laufzeit entschlüsseln, modifiziert AxProtector CTP die Anwendung bereits während der Kompilierung, sodass keine Veränderungen während der Laufzeit erforderlich sind. Dadurch werden plattformspezifische Richtlinien, die eine Veränderung der Software während der Laufzeit verhindern, wie beispielsweise die macOS hardened runtime, eingehalten. Außerdem wird so ein besserer Schutz vor Angreifern erreicht, die über eine Lizenz zur Ausführung der geschützten Anwendung verfügen.

Der Schutz, den der neue AxProtector CTP bietet, erfordert eine spezielle Build-Umgebung mit einem Plug-in von Wibu-Systems. Dazu sind nur minimale Anpassungen am Compiler notwendig. Aktuell wird der Clang-Compiler unterstützt. Der Softwareentwickler kann diese Anpassungen nach einer Anleitung selbst vornehmen oder einen bereits modifizierten Compiler von Wibu-Systems erhalten. Da der Clang-Compiler von den meisten gängigen Entwicklungsumgebungen wie Visual Studio und Xcode unterstützt wird, stehen die Funktionen von AxProtector CTP sofort zur

Verfügung, einschließlich des plattformübergreifenden Schutzes, wie er von den Standard-AxProtectoren geboten wird.

> *„In einer Welt, in der sich Cyber-Bedrohungen täglich weiterentwickeln, reicht es nicht, sich nur auf Verschlüsselung zu verlassen. AxProtector CTP geht hier einen Schritt weiter, indem es Ihre Software zur Kompilierungszeit obfuskiert und diese so zu einem Puzzle macht, das selbst für die erfahrensten Hacker nahezu unlösbar ist“, erklärt Stefan Bamberg, Director Sales and Key Account Management bei Wibu-Systems.*

4.352 Anschläge bei durchschnittlich 55 Zeichen pro Zeile

Bild: AxProtector CTP nutzt fortschrittliche Obfuskationsmechanismen, um den Schutz von Windows-, Linux- und macOS-Anwendungen vor Piraterie und Reverse Engineering zu erhöhen.

Weiterführende Informationen

- Die Pressemitteilung als Audiofile: https://www.wibu.com/fileadmin/Audiofiles/press_releases/WIBU_AxP-CTP_DE.mp3
- Die Pressebilder stehen optimiert für den Druck und Online-Veröffentlichungen bereit: https://wibu.sharefile.com/d-s0c428e48929e4ff1a9a1f034b3843a6f
- Weitere Informationen zu CodeMeter Protection Suite: https://www.wibu.com/de/produkte/protection-suite.html

Über WIBU-SYSTEMS AG

WIBU-SYSTEMS AG, www.wibu.com
Elke Spiegelhalter, Presse und Öffentlichkeitsarbeit
Tel.: +49-721-93172-11, Fax: +49-721-93172-22, elke.spiegelhalter@wibu.com

Bildmaterial auf Anfrage oder https://www.wibu.com/de/bildmaterial.html.

Wibu-Systems ist ein weltweit führendes Unternehmen in den Bereichen Cybersicherheit und Softwarelizenzmanagement. Das Ziel ist, einzigartige, preisgekrönte und international patentierte Sicherheitslösungen zu liefern, die das in digitalen Assets eingebettete geistige Eigentum schützen und die Möglichkeiten der Monetarisierung von technischem Know-how erweitern. Die kompatiblen Hardware- und Softwaremodule der umfassenden Suite bieten Softwareherstellern und Herstellern intelligenter Geräte Schutz vor Piraterie, Reverse Engineering, Manipulationen, Sabotage und Cyberangriffen auf allen gängigen Plattformen und in verschiedenen Branchen.

In unseren Social-Media-Kanälen gibt es weitere Informationen: