Im Rahmen des Hacker-Contests demonstriert Wibu die Effektivität der Blurry-Box-Kryptographie.
Bild: Pixabay

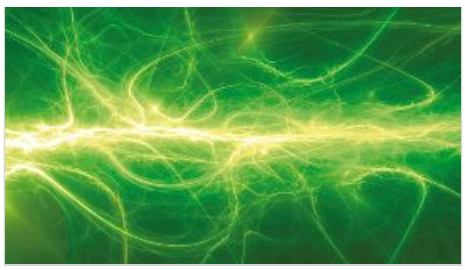
Hacker-Wettbewerb auf der Hannover Messe

WER HACKT DIE SOFTWARE, DIE SICH SELBST NEU ERFINDET?

TEXT: REGINA LEVENSHTEIN

11.04.2017 | Wer das Preisgeld in Höhe von 50.000 Euro mit nach Hause nehmen will, muss beim Hacker-Wettbewerb von Wibu auf der Hannover Messe etwas scheinbar Unmögliches bewältigen: eine Software knacken, die sich stetig neu schreibt.

TAGS | CYBERSECURITY SOFTWARE-DESIGN SOFTWARE-ARCHITEKTUR HACKER KRYPTOGRAPHIE VERSCHLÜSSELUNG HACKATHON WIBU-SYSTEMS AG



Moderne Stromversorgung und insbesondere der elektronische Leitungsschutz können heute schon im Bereich Industrie 4. ...

Mit Blurry Box-Kryptographie nutzt Wibu insgesamt sieben Cybersecurity-Verfahren. Das Ziel: Raubkopierern den Angriff so komplex und aufwändig gestalten, dass es sich eher rentiert, eine vergleichbare Software von Null auf selbst zu entwickeln als sie zu klauen. Im Rahmen des Hacker-Wettbewerbs will Wibu die Blurry Box nun auf die Probe stellen. Hier geht es zu weiteren Infos und der Anmeldung für den Hacker-Contest.

Diese sieben Faktoren machen die Blurry Box nahezu unknackbar

Das Grundprinzip von Blurry Box-Kryptographie beruht auf einem beziehungsweise. mehreren sicheren Schlüsseln in einem Dongle und der Tatsache, dass Software im Regelfall komplex ist. Für den Softwareschutz macht sich Wibu sieben Prinzipien zunutze:

- **Erzeugung von Varianten:** unktionen in der Software werden zu Varianten der Funktion vervielfältigt. Damit wird die Komplexität der Software erhöht. Eine Wrapper-Funktion übernimmt die Auswahl, welche der Varianten abhängig von den gegebenen Eingangsparametren der Funktion ausgeführt wird.

BILDERGALERIE

Sieben Faktoren sollen für Raubkopierer den Aufwand zum Hacken der Software so sehr in die Höhe treiben, dass es sich für sie eher rentiert, eine eigene Software von Null auf zu schreiben.

Bild: Wibu-Systems

- **Modifikation der Varianten:** Die einzelnen Varianten werden so modifiziert, dass diese nur in dem für diese Variante gültigen Wertebereich funktioniert. Damit wird verhindert, dass ein Angreifer die Wrapper Funktion so patched, dass immer die gleiche Variante ausgeführt wird.
- **Verschlüsselung der Varianten:** Alle Varianten werden verschlüsselt, sodass ein Angreifer den Code nicht analysieren kann, ohne den Code entschlüsselt zu haben.
- **Einfügen von Fallen:** Zusätzlich zu den bereits erzeugten Varianten werden weitere Varianten als Fallen eingefügt und ebenso verschlüsselt. Eine Falle enthält einen Sperrcode. Wird die Falle über den Dongle entschlüsselt, sperrt sich dieser selbst und kann nicht mehr zum Entschlüsseln verwendet werden. Damit wird verhindert, dass ein Angreifer alle Methoden ohne Analyse deren Funktionsweise entschlüsseln kann.
- **Auswahl der Variante im Dongle:** Die Wrapper-Funktion verwendet den Dongle für die Auswahl der Variante. Dazu werden die Eingangsparameter an den Dongle gesendet und dieser gibt die zu verwendende Variante zurück. Damit ist es dem Angreifer nicht mehr möglich, eine Falle von benötigten Varianten durch alleinige Analyse einer entschlüsselten Wrapper-Funktion zu unterschieden. Er müsste den Code für alle möglichen Eingangsparameter ausführen, um dies sicher unterscheiden zu können.
- **Zustandsspeicher im Dongle:** Der Entwickler weiß, dass Funktionen nur in einer von ihm vorgegebenen Reihenfolge durchlaufen werden können. Die zuletzt entschlüsselte Methode wird im Dongle als Zustand gespeichert. Bei der nächsten Entschlüsselung wird dann geprüft, ob dieser Zustand erwartet wurde. Falls nicht, kann eine Falle ausgelöst werden. Damit wird verhindert, dass ein Angreifer alle Varianten an einer beliebigen Stelle in der Software ausprobiert. Er müsste immer wieder zum Ausgangspunkt zurückgehen, was den Aufwand steigert.
- **Entschlüsselungs-Verzögerung:** Im Normalbetrieb wird nur eine bestimmte Anzahl an Entschlüsselungen pro 30 Sekunden durchgeführt. Diese Anzahl wird als maximal erlaubte Anzahl an Entschlüsselungen im Dongle gespeichert. Der Dongle verlangsamt seine Entschlüsselungen dementsprechend. Damit wird zusätzlich zur Komplexität auch der Zeitaufwand für den Angreifer erhöht.

Wibu Systems auf der Hannover Messe vom 24. bis 28. April 2017 in Hannover: Halle 8, Stand D05

Firmen zu diesem Artikel

WIBU-SYSTEMS AG

KARLSRUHE, DEUTSCHLAND

21 Artikel/News 2 Videos