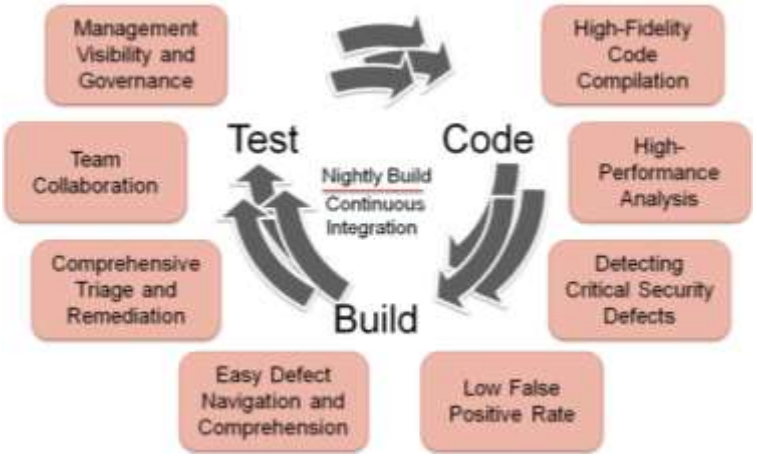
Einführung

Die **Security & Quality Software GmbH** bietet Dienstleistungen und Werkzeuge für die automatische, messbare Überprüfung und den Test der Sicherheit und Qualität der Software während der Entwicklung an. OpenSource Bestandteile werden aufgedeckt, Versionen, Exploids und rechtliche Hinweise angezeigt. In Kombination mit Verschlüsselung und Verschleierung der fertigen Applikationen gegen Angriffe und Raubkopien können Organisationen Software sicherer bauen, analysieren und ausgeben. Die zentrale, in bestehende Prozesse integrierte Gesamtlösung, spart Kosten, optimiert Vorgehensweisen, verkürzt Entwicklungszeiten und verbessert somit die Sicherheit und Qualität der Produkte messbar.

Software-Eigenentwicklung

Entwickler werden dabei unterstützt, schwer auffindbare und kritische Sicherheits- und Qualitätsprobleme automatisiert frühzeitig zu finden und zu beheben. Dabie werden Messkriterien für die Sicherheit und Qualität eingeführt und überwacht. Folgende Aufgabenstellung werden adressiert:

- Lauffähigkeit und Laufzeitverhalten der Anwendung
- Identifikation von Sicherheitsdefekte und Einfallstore für Angreifer
- Valide Messbarkeit der Software zu jedem Zeitpunkt
- Erhöhte Planbarkeit der Softwareeigen- und Fremdentwicklung



Bausteien des Softwareentwicklungsprozesses

- Schnellere Verfügbarkeit der Produkte durch Zeit- und Kostenersparnisse
- Überwachung und zeitliche Abschätzung von Abgabe- und Lieferterminen (Risikoanalyse)
- Höhere Kundenzufriedenheit durch bessere, stabilere und sicherere Produkte
- Verbesserung der Produktwartbarkeit und schnellere Produktanpassungen
- Produktivitätsverbesserung der Entwicklung und Testabteilung durch produktunterstütze Automatisierungen

Nutzen bei extern entwickelter Software

Auswahl an Fremdsoftware in Applikationen

Das Einbinden von Software von Fremdherstellern birgt ein Restrisiko mit ein. Die extern entwickelten Programme müssen mit den gleichen Metriken für Sicherheitsverwundbarkeiten, Sicherheitsrisiken, Qualität, Identifikation von OpenSource Komponenten und Wartbarkeit wie bei der Eigenentwicklung untersucht werden.

<u>Situationsbeschreibung</u>

- Viele IT Abteilungen haben nicht die Werkzeuge, Spezialisten und das Budget, um Fremdcode zu testen
- Traditionelle Bewertungsmethoden sind teuer, unvollständig, arbeitsreich und skalieren nicht
- Zulieferer geben den Quelletext nicht frei und verweigern den Zugriff in einer Cloud Umgebung

<u>Mögliche Lösungsansätze</u>

Die Zulieferer überprüfen die Software über ein Kontrollportal bei ihrem Kunden auf die Erfüllung der vorgegebenen Metriken hin. Sie können ihren Kunden auch mit entsprechenden Werkzeugen erstellte Prüfzertifikate aushändigen oder SQ Software zertifiziert beim Lieferanten die Software anhand ihrer vorgegebenen Metriken.

Freimanner Strasse 14 85737 Ismaning, Germany
Phone: +49 (89) 388 699 84 Kontakt: contact@sq-software.com **www.sq-software.com**

Software-Schutz (Code Obfuscation und Anti-Tampering) gegen

- Reverse Engineering (Feindliche Wiederherstellung, Diebstahl der Urheberrechte, Nachbauten etc.)
- Nicht autorisierte Modifikationen => Integritätsschutz der Anwendung

Effizient und effektiv gegen Reverse Engineering

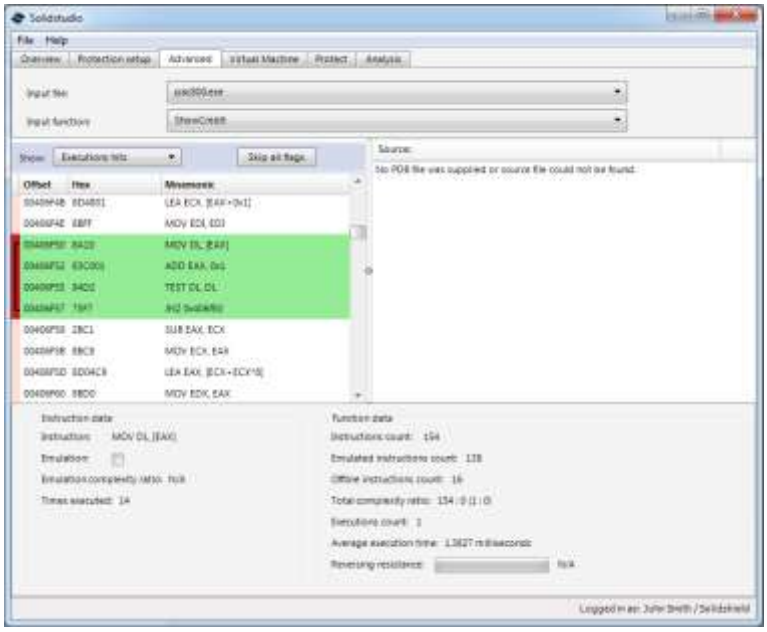
Die Virtualisierung löst die Strukturen des Original Quelltexts auf, transferiert die Daten in einen spezifischen Bytecode und verschleiert die Programmzeilen in einer virtuellen Maschine. Der Quelltext ist somit nie im Speicher sichtbar.

Effizient und effektiv gegen Tampering

Bei Ausführung dekodiert **SOLIDSHIELD** das verschleierte Programm Zeile um Zeile. Ein automatisches Zerlegen ist somit nicht möglich. Die Dichte und Tiefe der Verschlüsslung kann einfach in **SOLIDSTUDIO** angepasst werden.

Laufzeitverhalten

Mit **SOLIDSTUDIO** kann die Veränderung der Laufzeit in der GUI kontrolliert und angepasst werden. (Halb-) Automatisch werden sogenannte Hot-Spots, die nach der Virtualisierung die Laufzeit sehr stark beeinflussen, angezeigt und (per Mausklick) ausgeschlossen (s. Bild).



rot/schwarze Markierung: Schleife mit 14-maligem Durchlauf. Die Funktion wurde durch Mausklick aus der Virtualisierung ausgeschlossen werden (grün).

JAVA Bytecode Virtualisierung

SOLIDSHIELD ist die einzig verfügbare, wirksame und effiziente Verschleierungslösung für JAVA-Code.

Isolierte Code Ausführung

Mit **CLOUDSHIFT** können beliebige Funktionen in einem abgesicherten, getrennten Prozessor (ARM basiertes Dongel) oder jeder Standard Hardware ausgeführt werden (machine bound execution). Das Heraustrennen einer Funktion und Ausführen in der Cloud (oder einer exterenen Hardware) dauert Sekunden. Der Quelltext bleibt unverändert.

Technisch

- CPU Unterstützung: x86 32/64bit, PowerPC, ARM (in Vorbereitung) und andere
- Linux, Windows, VxWorks RTOS Unterstützung
  Schützt DLL's, Windows, Linux und VxWorks Programmbibliotheken und SO's (Shared Objects)
- Programmiersprachen unabhängig: C, C++, ADA, Assembler, Fortran etc.
- Unterstützung interpretierender Sprachen: **JAVA**, (C# und .Net in Vorbereitung)

Zusammenfassung

Code Obfuscation MIT	Code Obfuscation OHNE
Selektiver, kontrollierter und benutzergeführter Virtualisierung mit Verschleierung von ausgewählten Funktionen	Größere Laufzeitverlängerung
Auslagerung von Codeteile auf sichere und überwachte Platformen	Zusätzlicher Treibersoftware
Hardwaregebundener Ausführung der Software	Änderung des Quelltextes