Pressemitteilung

softScheck **"Kostengünstiges Security Testing auf Smart Devices – agil**:
Systematische und vollständige Identifizierung bisher nicht-erkannter Sicherheitslücken (Zero-Day-Vulnerabilities) in Software (und Hardware)"

Köln/Sankt Augustin 25. Oktober 2012

softScheck Geschäftsführer Prof. Dr. Hartmut Pohl:

Die Sicherheit von Apps kann durch Anwendung der 3 Tool-gestützten Verfahren 'Threat Modeling', 'Static Source Code Analysis' und 'Fuzzing' erreicht werden. In einem Tutorial werden diese 3 Verfahren erstmals zum Security Testing einer Android-App (am Beispiel von SCRUM) hands-on auf dem Software-QS-Tag 2012 der Imbus AG in Nürnberg am 8. November 2012 präsentiert. Nach einer Einführung in die verwendete Testumgebung und das Android SDK werden die Verfahren vorgestellt:

Threat Modeling

Bereits mit dem Design einer App muss eine grundlegende, sichere Architektur entwickelt werden (Security by Design). Hierzu werden in einem ersten Schritt Szenarien der neuen App identifiziert. Danach erfolgt eine Analyse der Entry Points und der zu schützenden Assets. Aus den gesammelten Daten können nun Tool-gestützt Threats erstellt werden. Die Threats müssen anschließend durch einen Experten bewertet, priorisiert und in das Product Backlog aufgenommen werden. Danach werden Threats mit einer hohen Priorisierung in den nächsten Sprint eingearbeitet. An einem konkreten Beispiel wird erläutert, wie die Ergebnisse aus dem Threat Modeling in SCRUM verwendet werden können.

Static Source Code Analysis

Das Software-Release wird Tool-gestützt auf die Einhaltung syntaktischer Programmierkonventionen der Programmiersprache und auf die Einhaltung der Programmierrichtlinien überprüft. Ziel ist hier: Hilfe bei der Auswahl der richtigen Tools, Aussortierung von False-Positives und die Priorisierung der auftretenden Fehler für nachfolgende Sprints.

Fuzzing

Den Eingabeschnittstellen des Software-Release werden Tool-gestützt Testdaten übergeben, um im Programmcode unberücksichtigte Eingabedaten zu erkennen. Als konkretes Beispiel wird ein auf WebKit basierender Browser mit einem für diesen Zweck optimierten Fuzzer getestet. Ziel ist, Fuzzing an einem konkreten Beispiel zu präsentieren. Dazu wird ein kurzer Einblick in die Auswahl des wirkungsvollsten Fuzzers für eine gewählte Applikation gegeben.

Über softScheck

Die softScheck GmbH mit Sitz in Sankt Augustin hat sich im Bereich Informationssicherheit – speziell Identifizierung von bisher nicht-erkannten Sicherheitslücken in Software (und auch Hardware) neue, attraktive Wachstumsfelder erschlossen.

softScheck führt regelmäßig **Sicherheitsprüfungen** durch. Erfolgreich eingesetzt werden dabei u.a. die beiden Verfahren **Threat Modeling** und **Fuzzing**, die die Identifizierung bisher nicht-erkannter Sicherheitslücken ermöglichen.

Angriffe auf die IT sind nur erfolgreich durch die Ausnutzung von Sicherheitslücken. Werden also die Sicherheitslücken identifiziert und behoben, laufen alle Angriffe gegen diese Sicherheitslücken ins Leere!

softScheck bietet seit Jahren erfolgreich die Identifizierung bisher nicht-erkannter (!) Sicherheitslücken (Zero-Day-Vulnerabilities) in Software und Hardware an und übernimmt für Sie den gesamten Security-Testing Process.

Eingesetzt werden dazu erfolgreich – auch Tool-gestützt – die folgenden 7 Verfahren:

1. **Security by Design**: Entwicklung von Sicherheitsarchitekturen für Software
2. **Threat Modeling**: Überprüfung der Sicherheitsarchitektur auf bisher nicht-erkannte Sicherheitslücken
3. **Static Source Code Analysis** zur Überprüfung von Implementierungsfehlern
4. **Penetration Testing** u.a. zur Überprüfung auf bereits bekannte Sicherheitslücken
5. **Dynamic Analysis - Fuzzing**: Test der ausführbaren, kompilierten Datei auf bisher nicht-erkannte Sicherheitslücken – kein Quellcode nötig, sowie
6. **Explorative Testing** und manuelles Code Auditing.
7. Und letztlich werden auch **Covert Functions** – undokumentierte, verdeckte Funktionen – u.a. auch auf Smartphones und mobile Devices identifiziert und analysiert.

Das softScheck Alleinstellungsmerkmal ist seit Jahren die kostengünstige und sehr erfolgreiche Durchführung von Security Tests inklusive der Identifizierung bisher nicht-erkannter Sicherheitslücken in jeder Art Software wie

- **Anwendungssoftware** wie Webapplications, ERM, CRM, SCM, ERP, E-Business, CIM etc. und Netzwerk-Protokollen
- **Embedded Systems** (auch die Hardware) und **Industriesteuerungssoftware** (Industrial Control Systems – auch proprietärer Systeme), SCADA sowie
- Apps und Applets für smart and mobile Devices.

Dies verhindert Angriffe (erhöhtes Sicherheitsniveau: Ohne Sicherheitslücken kein erfolgreicher Angriff!) und erspart dem Hersteller und den Anwendern der eingesetzten Software (internationale Unternehmen - große, mittlere und auch kleine sowie Behörden) bis zu 99% der Wartungs- und Fehlerbehebungskosten.

softScheck bietet auch an, die Verfahren in den jeweiligen Software-Entwicklungsprozess der Kunden zu integrieren inkl. Programmierrichtlinien, Abnahmeverfahren und Schulungen.

In den letzten beiden Jahren hat softScheck den durchschnittlichen Aufwand zur Identifizierung bisher nicht-erkannter kritischer (d.h. aus dem Internet ausnutzbarer) Sicherheitslücken (u.a. auch durch den Einsatz eigener Testdaten) ganz **erheblich** gesenkt.

softScheck dürfte damit europäischer Marktführer in der Identifizierung bisher nicht-erkannter Sicherheitslücken (Zero-Day-Vulnerabilities) in Software und Hardware sein.

Weitere Informationen: http://www.qs-tag.de/tutorial-voss/#c14062

Kontakt:

Anja Wallikewitz softScheck GmbH

Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29

Bonner Straße 108
53757 Sankt Augustin

anja.wallikewitz@softScheck.com

www.softScheck.com