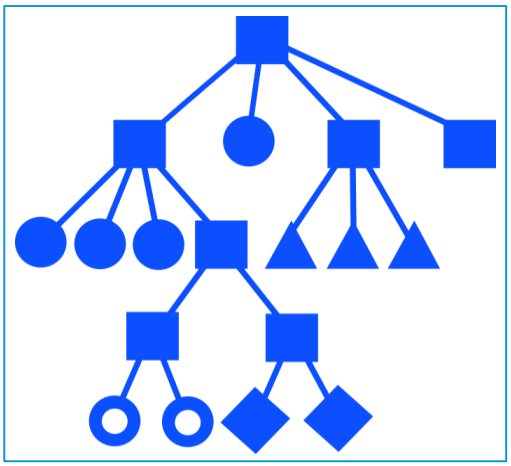
PTB innovationen
Technologieangebot



Prinzip der Kodierstruktur von FLOUDS, die eine Erweiterung auf beliebige Arten von Objekten ermöglicht und platzsparender im Vergleich zu pointerbasierten Verzweigungsbäumen ist. Die Symbole stellen reale oder virtuelle Geräte dar.

Vorteile

- **Sicherheit vor Manipulationen intelligenter Schadsoftware**
- **Platzsparende Integritätsprüfung**
- **Cloudbasierte Übertragung der Prüfergebnisse abgesichert**

Ansprechpartner:

Dr. Bernhard Smandek
Technologietransfer
Telefon: +49 531 592-8303
Telefax: +49 531 592-69-8303
E-Mail: bernhard.smandek@ptb.de

Dr. Daniel Peters
Arbeitsgruppe
Eingebettete metrologische Systeme
Telefon: +49 030 3481- 7916
E-Mail: daniel.peters@ptb.de

Physikalisch-Technische
Bundesanstalt
Bundesallee 100
D-38116 Braunschweig

www.technologietransfer.ptb.de

Mehr Sicherheit für Messgeräte durch Hash-basierte Prüfung

Nach dem neuen Mess- und Eichgesetz muss die Software in einem Messgerät regelmäßig auf Datenintegrität überprüft werden. PTB Forscher entwickelten für diese Überprüfung ein sicheres Verfahren: Genutzt wird dabei anstatt herkömmlicher Checksummen-Berechnung eine robustere Hash-Überprüfung mittels Seperationskernen. Das garantiert mehr Sicherheit gegen Manipulationen durch intelligente Schadsoftware und spart Platz für das Speichern der Dateisystemstruktur. Für die geplante Überprüfung von Messgeräten über riskante, offene Netzwerke, z.B. über Cloud-Systeme, gewährleistet das neue PTB-Verfahren eine ausreichende Daten-Sicherheit. Umständliche Vorort-Prüfungen könnten somit völlig entfallen.

Intelligente Schadsoftware kann sich während herkömmlichen Dateiintegritätsprüfungen verstecken und vorgenommene Änderungen an z.B. Messdaten verbergen. Vor allem bei Messgeräten, die im gesetzlichen Messwesen behandelt werden, ist die Sicherheit der Daten zu gewährleisten. Voraussetzung für die neue PTB-Prüfung ist die Installation eines sicheren Mikrokerns (oft auch Separationskern genannt) innerhalb des Messgerätes. Dieser kann über virtuelle Maschinen jede ausgelagerte Datei aus realen oder virtuellen Geräten kryptografisch sichern und verhindert damit ungewollte Manipulationen. Da die Speicherkapazität von eingebetteten Systemen wie Messgeräten oft begrenzt ist, werden Datenreduktionsalgorithmen, wie das von der PTB entwickelte FLOUDS („*Filesystem Level Order Unary Degree Sequence*“), angewendet (s. Bild).

Wirtschaftliche Bedeutung

Potentiell können alle Messgeräte, bei denen gesetzliche Anforderungen zur sicheren Auswertung und Archivierung der Messdaten erforderlich sind, mit dem neuen Prüfverfahren ausgestattet werden. So können z.B. Vorort-Prüfungen mit komfortableren Server-Cloud-Lösungen ersetzt werden.

Entwicklungsstand

Das Verfahren wurde ausführlich getestet. Das deutsche Patent ist unter der Nummer DE 10 2016 110 479 A1 offengelegt. Bei Interesse bieten wir Ihnen an, dieses Verfahren in gemeinsamen Projekten weiterzuentwickeln oder direkt zu lizenzieren.

#0424 / 01.2018