Das Wichtigste in Kürze

Endgeräteintegrität

Integritätsprüfung der Komponenten

Hypervisor

Erfassung sicherheitskritischer Parameter in-box und out-box

Sicherheit

Innovative Anomalieerkennung basierend auf Sensordaten, Schutz sicherheitskritischer Anwendungen durch starke Isolation und Information-Flow-Control

Zentrale Komponente

Wissensbasis und Feedback-System zur verbesserten Anomalieerkennung

Basiert auf TURAYA

Konsortium

if(is) internet-sicherheit.

Westfälische Hochschule

Institut für Internet-Sicherheit if(is)
www.internet-sicherheit.de

hgi Lehrstuhl für Systemsicherheit

RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Systemsicherheit
www.syssec.rub.de

Sirrix AG security technologies

Sirrix AG security technologies
www.sirrix.com

AVIRA

Avira Operations GmbH & Co. KG
www.avira.com

iTES

Innovative Trustworthy Endpoint Security

Das Projekt iTES ist ein Forschungsprojekt im Bereich Vertrauenswürdige IT-Systeme

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

im Rahmen der BMBF-Ausschreibung "Anomalieerkennung auf Rechnersystemen", mit Mitteln des BMBF unter dem Förderkennzeichen 16BY1207A

Zielsetzung

Die Forderung nach einer vertrauenswürdigen Datenverarbeitung (TrustedComputing) ist nicht neu. Seit Beginn der elektronischen Datenverarbeitung wurden neben offenen Daten auch geheime und sensitive Daten verarbeitet. Doch die Zahl der Angriffe auf Computersysteme und die Verbreitung von Schadprogrammen (Malware) nimmt ständig zu. Dabei liegt der Zeitraum für die Ausnutzung von bekannt gewordenen Sicherheitslücken durchschnittlich bei wenigen Tagen. Und während die Komplexität der Angriffe ebenfalls zunimmt, werden gleichzeitig immer weniger Kenntnisse benötigt, um entsprechende Angriffe durchzuführen. Bedingt durch diese Entwicklung und die immer häufigere Nutzung sicherheitskritischer Anwendungen ist der Bedarf nach vertrauenswürdiger Datenverarbeitung in den letzten Jahren stark angestiegen.

Das Ziel von iTES ist es eine Architektur zu schaffen, die mit besonderer Rücksicht auf vertrauenswürdige Datenverarbeitung eine bedarfsgerechte Sicherheitsumgebung bietet. Bedeutende Partner aus Industrie und Forschung haben sich zusammengeschlossen, um die Entwicklung in diesem Bereich voran zu treiben.

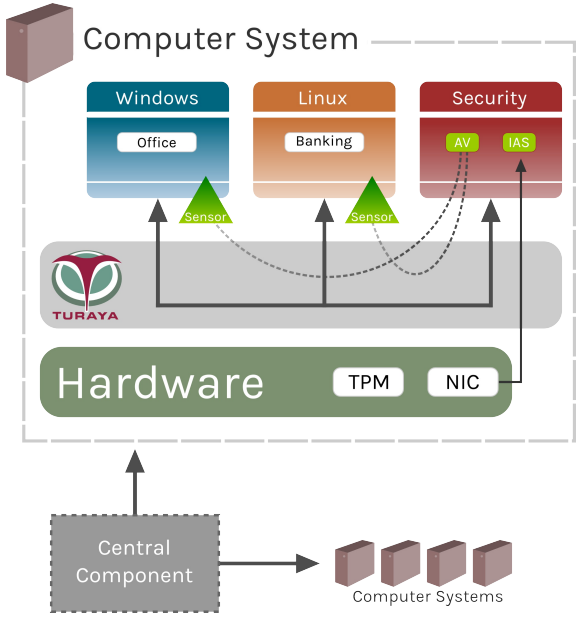
Architektur

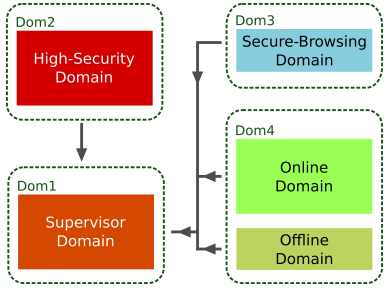
Endgeräteintegrität

Die Integrität muss schon bei Start des Systems gewährleistet sein, ohne dabei Fremdsoftware vor dem Boot-Prozess des Systems platzieren zu müssen. Eine Abweichung vorher definierter Zustände muss dabei als Anomalie erkannt und als Integritätsverletzung des Systems identifiziert werden. Durch die Erforschung von Reaktionsmustern sollen sichere Zustände kritischer Systemkomponenten wieder hergestellt werden.

Hypervisor

Der Hypervisor stellt die Schnittstelle zwischen Host und Guest-Systemen (Compartments). Erforscht werden hierbei Möglichkeiten der Datengewinnung über eine in den Hypervisor zu integrierende Sensorenschnittstelle.





Sicherheit

Die Architektur sieht vor, dass unterschiedliche Arbeitsbereiche des Nutzers je nach Anwendung in unterschiedliche Compartments aufgeteilt werden. Hierbei soll durch individuelle Restriktionen der Ressourcen das Sicherheitslevel bestimmt werden (Security Domain). Eine Kommunikation der einzelnen Compartments soll dabei nur über fest definierte Schnittstellen möglich sein, so dass bei einem Befall durch Malware deren Ausbreitung eingedämmt werden kann. Dieses Vorgehen schützt ebenfalls die analysierende Sicherheitssoftware des Systems (Supervisor Domain). Innerhalb dieser Domain findet die lokale Datenaufbereitung der einzelnen Sensoren statt. Hierbei ist ein besonderer Schwerpunkt auf die Erforschung und Entwicklung innovativer Mechanismen der Anomalieerkennung gelegt.

Zentrale Komponente

Eine weitere Ebene der Auswertung soll in Form einer zentralen Instanz realisiert werden. Diese sammelt datenschutzkonform Informationen der einzelnen Endgeräte. Hierdurch soll einerseits eine Wissensbasis geschaffen werden, die unter anderem einen Gesamtüberblick ermöglicht. Andererseits werden die Anomalieerkennungsmethoden der Endgeräte synchronisiert und optimiert.