VuTAT

Vorhaben Nr. 16231 BG/2

Vulnerability Tests of AT components

Schwachstellenanalyse von Automatisierungskomponenten - Entwicklung eines Frameworks zur automatisierten Untersuchung von Ethernet-basierten Komponenten der Automatisierungstechnik (AT) zur Aufdeckung von IT-Sicherheitsschwachstellen

Abschlussbericht

Kurzfassung:

Durch eine zunehmende Verwendung standardisierter IT-Technologien in der Welt der Automatisierungstechnik wird der Einsatz, seit Jahren erfolgreich in der Office-Umgebung verwendeter, TCP-IP-basierter Protokolle und Anwendungen ermöglicht. Ein großer Vorteil ergibt sich hierbei durch eine einheitliche Vernetzung von Komponenten der Automatisierungstechnik auch über die Grenzen der Feldebene hinweg (vertikale Integration), welche eine praktisch ortsunabhängige Steuerung, Kontrolle und Wartung dieser Komponenten erlaubt. Durch den Einsatz dieser Standardtechnologien und der weitergehenden Vernetzung ergeben sich allerdings auch zusätzliche Gefährdungen des störungsfreien Betriebs solcher automatisierungstechnischen Anlagen durch Angriffe über Netzwerke und durch Schadsoftware. Da diese Angriffe ihre destruktive Wirkung auf Grundlage vorhandener Protokoll- oder Implementierungsschwachstellen (Vulnerabilities) entfalten, kommt dem Einsatz schwachstellenfreier Komponenten für einen störungsfreien und sicheren Betrieb von Anlagen eine große Bedeutung zu.

Vorrangiges Projektziel war die Entwicklung eines Frameworks zur Analyse und Erfassung von Schwachstellen verschiedener Komponenten der Automatisierungstechnik, welche Ethernet-basierte Kommunikationsprotokolle nutzen. Hinsichtlich einer möglichen Nutzung dieses Frameworks ist insbesondere auch an einen entwicklungsbegleitenden Einsatz durch Entwickler und Tester gedacht, die nicht zwingend über vertiefte IT-Sicherheitskenntnisse verfügen. Letztendlich konnte im Rahmen von VuTAT eine PC-basierte Testumgebung mit Hilfe von „Commercial off-the-shelf“ (COTS)-Komponenten und frei verfügbarer Software (OpenSource) realisiert werden, mit welcher eine weitgehend automatisierte Nutzung des Frameworks ermöglicht wird.

Das Grundgerüst der Testumgebung bildet der freie Netzwerk- und Schwachstellenscanner OpenVAS [17], welcher eine Vielzahl von Schwachstellentests bereitstellt, die von einer aktiven Nutzergemeinschaft implementiert werden. Erste Tests mit

speicherprogrammierbaren Steuerungen (SPS) als Device under Test (DuT) produzierten vielfach falsche Fehlerreports aufgrund von instabilem Lastverhalten der getesteten Geräte, so dass die verwendeten Automatisierungskomponenten zuerst mit Hilfe von Communication Robustness Testing (CRT) auf die Robustheit ihrer Implementierungen getestet werden sollten. Dies beinhaltet generische Protokolltests zur Überprüfung des Geräteverhaltens beim Empfang von fehlerhaften Netzwerkpaketen und Last-Tests.
Nach den von dem ISASecure Compliance Institude (ISCI) [8] bereitgestellten Testspezifikationen „Embedded Device Security Assurance“ (EDSA) [9] werden die Ergebnisse der Tests anhand der Antwortpakete (d.h. über die Netzwerkschnittstelle), aber auch über das Verhalten der „Essential Services“ des DuT bestimmt. Diese Kernfunktionen sind im Falle der im Projekt untersuchten Steuerungen die ausgeführten Programme in Verbindung mit den Steueraufgaben ihrer Ein- und Ausgänge. Zur Implementierung von CRT-Testfällen, wurde der frei verfügbare Paketgenerator Scapy [21] verwendet. Um einen automatisierten Testablauf von integrierten Robustheits- und Schwachstellentests auf Basis des OpenVAS-Frameworks zu ermöglichen, wurde schließlich eine Softwarekomponente entwickelt, welche auch eine Überwachung von IOs und eine vom Verhalten des DuT abhängige Testablaufsteuerung gestattet.
Verschiedene speicherprogrammierbare Steuerungen von fünf Herstellern wurden mit dem entwickelten Framework getestet. Die Tests, welche neben im Handel erhältlichen Automatisierungskomponenten auch Prototypen untersuchten, zeigten eine Reihe von Schwachstellen auf, wodurch der Bedarf zur Durchführung entsprechender Tests nachdrücklich bestätigt wurde.

Berichtsumfang:	136 Seiten, 36 Abbildungen, 27 Tabellen, 29 Literaturverweise
Beginn der Arbeiten:	01.10.2009
Ende der Arbeiten:	31.12.2012
Zuschussgeber:	BMWi / IGF-Nr. 16231 BG/2
Forschungsstellen:	inIT - Institut für Industrielle Informationstechnik Hochschule Ostwestfalen-Lippe
	ifak - Institut für Automation und Kommunikation e.V. Magdeburg
Bearbeiter und Verfasser:	Prof. Dr. Stefan Heiss Jan-Christopher Brand, Tino Doehring
Vorsitzender des Projektbegleitenden Ausschusses:	Frank Schewe, PHOENIX CONTACT Electronics GmbH
Vorsitzender des Beirates:	Thomas Pilz, Pilz GmbH & Co.KG