SicAri
Eine Sicherheitsarchitektur und deren Werkzeuge zur ubiquitären Internetnutzung

Verbundprojekt gefördert vom Bundesministerium für Bildung und Forschung

Erfolgskontrollbericht

Förderkennzeichen 01AK062B

Roland Rieke, Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Peter Ebinger, Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)

Februar 2008

Konsortialführung

Prof. Dr. Claudia Eckert
Darmstädter Zentrum für IT-Sicherheit
Hochschulstr. 10
D-64289 Darmstadt
E-Mail: claudia.eckert@sec.informatik.tu-darmstadt.de

Stellvertretender Projektkoordinator
Dr.-Ing. Michael Kreutzer
Darmstädter Zentrum für IT-Sicherheit
Hochschulstr. 10
D-64289 Darmstadt
E-Mail: kreutzer@dzi.tu-darmstadt.de

Inhaltsverzeichnis

Kapitel 1

Rahmendaten

Zuwendungsempfänger	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Förderkennzeichen	01AK062B
Vorhabenbezeichnung	SicAri
Laufzeit des Gesamtvorhabens	01. Oktober 2003 bis 30. September 2007
Laufzeit der Beteiligung der Fraunhofer-Gesellschaft	01. Oktober 2003 bis 30. September 2007

Kapitel 2

Aufgabenstellung

2.1 Gesamtherausforderung

Die zentrale Herausforderung des Projektes SicAri (eine Sicherheitsarchitektur und deren Werkzeuge für die ubiquitäre Internetnutzung) lag in der Bereitstellung einer Sicherheitsplattform, die in immer kleiner werdenden Endgeräten, mit neuen Vernetzungsmechanismen und insbesondere bei mobilen Einsatzszenarios leicht einsetzbar ist. Der Begriff „leicht“ meint die Eigenschaft, dass die Plattform an gegebene Rahmenbedingungen ohne großen Aufwand angepasst werden kann und einzelne Werkzeuge je nach Bedarf genutzt werden können. Typische Geräte sind mobile Endgeräte, typische Einsatzszenarios sind der sichere Zugang zum leitungsgebundenen Internet, zu drahtlosen Netzen (mit Infrastuktur – WLAN oder ohne Infrastuktur – Ad-Hoc-Netze) und zu Peer-to-Peer-Netzen. Die automatische Generierung von Policies erlaubt die leichte Einsetzbarkeit in diesen Szenarien.

In SicAri sollten IT-Sicherheitswerkzeuge für die SicAri-Plattform auf der Basis standardisierter und wissenschaftlich fundiert erforschter Mechanismen entwickelt sowie neue Sicherheitsmechanismen vorgeschlagen werden. Die rechtliche Betrachtung der Plattform mit ihren Einsatzgebieten und der einzelnen Werkzeuge begleitete das Verbundvorhaben als Querschnittsthema.

Die SicAri-Werkzeuge sind auf den folgenden Schichten angesiedelt: Anwendungen, Cyberlaw, Hardware, Policies, Protokoll-Engineering, kryptographische Basistechnologie – die Plattform selbst ist auf der Middleware-Ebene zu finden und soll bei Firmen und Einzelnutzern zur Anwendung gebracht werden.