Institut
Forschung
- Zielsetzung
- Publikationen
- **Projekte**
- Projektserver
- Kooperationen
- Konferenzen
- Workshops

Lehre
Mitarbeiter
Presse und Jobs
Intranet
Sitemap

Fakultät IEF | Institute der Elektrotechnik | Projekte

Suchbegriff...

Mitarbeitersuche...

Startseite » Forschung » Projekte » Abgeschlossene Projekte - eine Auswahl » Secure Web Services für ambiente eingebettete Systeme (DFG)

Titel

Secure Web Services für ambiente eingebettete Systeme (DFG)

Kurzbeschreibung

Eine Schlüsseltechnologie im Bereich der eingebetteten Systeme ist der offene Standard des Devices Profile for Web Services (DPWS). Dieser wurde speziell für ressourcenarme Systeme entwickelt und basiert auf den etablierten und offenen WebService-Spezifikationen. Seit 2008 ist die Universität Rostock Mitglied des Standardisierungsgremium OASIS (https://www.oasis-open.org/) und kann somit ihre Kompetenz in dem Bereich Standardisierung des Devices Profile for Web-Services einbringen.

Eine große Herausforderung beim Portieren von Web Services (WS) Security auf ressourcenarme Systeme bildet die Ver- und Entschlüsselung von Informationen. Für eine möglichst sichere Übertragung von vertraulichen Informationen sind sehr komplexe Ver- und Entschlüsselungsalgorithmen in Verbindung mit entsprechend langen Schlüsseln (z.B. 1024 bit) notwendig.

Dies hat einen negativen Einfluss auf die Rechenzeit, den Speicherbedarf und daraus resultierend auf die Batterielaufzeit. Darüber hinaus darf die Antwortzeit auf eine Anfrage nicht zu groß sein. Zusätzlich müssen ausreichend Ressourcen zum Parsen und Verarbeiten der XML-Nachricht zur Verfügung stehen.

Die aktuellen Sicherheitskonzepte webservicebasierter Architekturen sollen im Rahmen des Promotionsthemas untersucht, insbesondere das für MuSAMA besonders relevante DPWS-Konzept, sowie neue Ansätze zur Integration von Sicherheit und Privatheit entwickelt werden.

Sicherheits- und Privatheitsanforderungen sind im Bereich der Webservices noch unzureichend fundiert, hier sollen folgende wissenschaftliche Fragestellungen untersucht werden:

- Wie kann sichergestellt werden, dass nur vertrauenswürdige Applikationen die Dienste des Ensembles nutzen können?
- Wie kann sichergestellt werden, dass die Daten eines solchen Dienstes durch den Nutzer kontrolliert und nur innerhalb von vertrauenswürdigen bzw. zulässigen Umgebungen verwendet werden können?
- Wie kann verhindert werden, dass eine Applikation, böswillig oder auf Grund von Programmierfehlern, Ressourcen blockiert und damit z.B. ein Denial-of-Service möglich wird?
- Wie kann garantiert werden, dass die Daten bei unerwarteten Gerätezuständen, etwa bei Teilausfall der Hardware, nicht von Unbefugten eingesehen werden können?
- Wie kann bei dem WS-Eventing-Mechanismus, wenn der Client zum Server wird, gewährleistet werden, dass das Event an den richtigen Empfänger versendet wird?

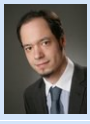
Förderung

- Dieses Projekt wird gefördert durch das Graduierten Kolleg MuSAMA (DFG).

Laufzeit

- 3 Jahre, ab 01.07.2010

Bearbeiter



Dr.-Ing. Sebastian Unger

Prof. Dr.-Ing. Dirk Timmermann
E-Mail
Tel.: +49 381 498 7250
Fax: +49 381 498 118 7251
Raum: W1205

Veröffentlichungen (Auszug)

Sebastian Unger, Stefan Pfeiffer, Dirk Timmermann:
How much Security for Switching a Light Bulb - The SOA Way Folien
8th International Conference on Wireless Communications and Mobile Computing, pp. 1034-1039, ISBN: 978-1-4577-1379-8, Limassol, Zypern, August 2012

Sebastian Unger, Stefan Pfeiffer, Dirk Timmermann:
Dethroning Transport Layer Security in the Embedded World Folien
The Fifth IFIP International Conference on New Technologies, Mobility and Security, keine Seitenzahlen, ISBN: 978-1-4673-0229-6, Istanbul, Türkei, Mai 2012

Stefan Pfeiffer, Andreas Lehmann, Sebastian Unger, Dirk Timmermann:
Secure Information Flow Awareness for Smart Wireless eHealth Systems Folien
9th International Multi-Conference on Systems, Signals and Devices (SSD'12), Chemnitz, Deutschland, März 2012

Sebastian Unger, Elmar Zeeb, Holger Grandy, Frank Golatowski, Dirk Timmermann:
Extending the Devices Profile for Web Services for Secure Mobile Device Communication
Internet of Things 2010, ISBN: 978-1-4244-7414-1, Tokyo, Japan, November 2010

Links

- Offizielle Projektseite: www.musama.de

nach oben

letzte Änderung: 01.04.2016

Kontakt
Fakultät für Informatik und Elektrotechnik
Institut für Angewandte Mikroelektronik und Datentechnik
Haus 1, Raum 1207 (Sekretariat)
Richard Wagner Str. 31
18 119 Rostock-Warnemünde
Telefon: +49 381 498 72 51
Fax: +49 381 498-118 72 51

Schnelleinstieg
Publikationen
Anfahrt
Kontakt
Laborpraktikum
Lehrangebot
Highlights
Projekte