New Directions in Efficient and Tamper-Resilient Public-Key Cryptography for Ubiquitous Computing

Ergebnisse in Kürze

Schneller und besser verschlüsseln!

Ein EU-Projekt hat die Zusammenarbeit auf dem Gebiet der Kryptografie gefördert. Die resultierenden neuen Anwendungen kryptografischer Algorithmen bedeuten eine schnellere und bessere Verschlüsselung und tragen dazu bei, spezielle drahtlose Geräte zu abzusichern.

DIGITALE WIRTSCHAFT

© Thinkstock

Bestimmte Typen von Computernetzwerksystemen, beispielsweise Geräte zur Verbindung drahtloser Sensoren oder Tags, sind Hackerangriffen nahezu schutzlos ausgeliefert. Während die Systeme gegenüber direkten Angriffen gut geschützt sind, kann man über indirekte Mittel, welche den kryptografischen Schlüssel und andere Sekundärdaten extrahieren, auf sie zugreifen.

Dieses Problems nahm sich das EU-finanzierte Projekt "New directions in efficient and tamper-resilient public-key cryptography for ubiquitous computing" (ND-ETCRYPTOUC) an. Hauptziel war die Sicherung der entsprechenden Geräte, indem wirksame Kryptografie mit öffentlichem Schlüssel (Public Key) zum Einsatz in diesem Kontext verfügbar gemacht wird. Die Verfügbarkeit wurde über drei komplexe technische Ziele auf Basis von

kryptografischen Algorithmen erzielt. Ein weiterer Zweck war die Weiterentwicklung der Karriere eines türkischen Forschers mittels einer Serie von gemeinsam durchgeführten Austauschmaßnahmen, wodurch auch der Wissenstransfer mit Europa gefördert wurde. Das Projekt lief vier Jahre und wurde im Juni 2014 abgeschlossen.

Innerhalb des ersten Berichtszeitraums wurde das erste Ziel vollständig abgearbeitet. Die restlichen wurden teilweise erreicht und werden im Lauf der nachfolgenden Perioden abgeschlossen.

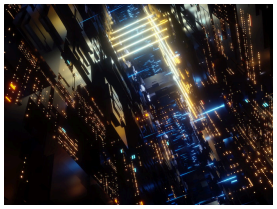
Der Forscher traf zahlreiche andere Forscherinnen und Forscher an Universitäten und kommerziellen Einrichtungen in Europa und in der Türkei und arbeitete mit ihnen zusammen. In einer Reihe von Vorschlägen förderten seine Anwendungen der verschiedenen Algorithmen die Verbesserung der kryptografischen Geschwindigkeit und Leistungsfähigkeit. Die Resultate der Zusammenarbeit wurden als Konferenz- und Zeitschriftenartikel veröffentlicht. Er hielt überdies verschiedene Gastvorträge und Seminare sowie gestaltete und lehrte mehrere gut aufgenommene großangelegte Kurse für Aufbaustudiengänge. Überdies betreute er eine Gruppe von Forschungsstudenten.

Dank des ND-ETCRYPTOUC-Projekt sind nun anfällige Geräte besser geschützt. Der Austausch hat außerdem zur positiven Zusammenarbeit mit europäischen Wissenschaftlern und Institutionen geführt.

Schlüsselbegriffe

Verschlüsselung | Kryptografie | drahtlose Geräte | Hacking | rechtswidriger Zugang zu Informationssystemen | Sekundärdaten | Ubiquitous Computing | ubiquitäre Computernutzung | Wissenstransfer

Entdecken Sie Artikel in demselben Anwendungsbereich



Neue Lösungen für Verschlüsselung: Daten vor dem Ansturm der Quantencomputer in Sicherheit bringen

7 Juni 2019

Fortschritte in der Erkennung von Herzrhythmusstörungen

30 November 2022

Blockchain-Technologie ermöglicht sichere, kostengünstige und einfache Zahlungen für alle

26 Juni 2020

Die Bevölkerung in den Mittelpunkt von Lösungen für die nachfrageseitige Steuerung stellen

21 Februar 2024

Projektinformationen

ND-ETCRYPTOUC

Finanziert unter

ID Finanzhilfevereinbarung: 256544

Projekt abgeschlossen

Startdatum
1 Juli 2010

Enddatum
30 Juni 2014

Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Gesamtkosten
€ 100 000,00

EU-Beitrag
€ 100 000,00

Koordiniert durch
BAHCESEHIR UNIVERSITESI
Türkiye

Dieses Projekt findet Erwähnung in ...

MAGAZIN RESEARCH*EU

Close-up on nanotechnology

Letzte Aktualisierung: 9 Januar 2015

Permalink: https://cordis.europa.eu/article/id/151367-faster-and-better-encryption/de