Sichere Verschlüsselung leicht gemacht

WERKZEUGKOFFER GEGEN DATENKLAU

CACE

Computer Aided Cryptography Engineering

Programm: 7. EU-Rahmenprogramm für Forschung, technologische Entwicklung und Demonstration

Förderlinie: Informations- und Kommunikationstechnologien (ICT)

Projekttyp: Kleines Verbundprojekt (STREP)

Projektkosten: 4,7 Mio. Euro, davon 3,5 Mio. EU-Förderung

Laufzeit: 1. 1. 2008 - 31. 12. 2010

Projektkoordinator: Technikon Forschungs- und Planungsgesellschaft mbH

Projektwebsite: www.cace-project.eu

Kryptografie, also die Verschlüsselung von Informationen, ist ein wichtiges Instrument gegen Computerkriminalität. Für Programmierer und Hersteller von Hardware stellt sie aber eine große Herausforderung dar. Im Rahmen des EU-Projekts „CACE“ soll jetzt ein „Werkzeugkoffer“ dafür entwickelt werden.

In unserer Informationsgesellschaft ist der Schutz privater oder unternehmensbezogener Daten unumgänglich. Entsprechende Mechanismen werden daher auch bei jeder modernen Computeranwendung und in jedem technischen System erwartet. Doch die Entwicklung von Systemen, die gegen unbefugte Zugriffe geschützt sind, und von Verschlüsselungsmechanismen für Informationen ist eine große Herausforderung in der Software- und Hardwareentwicklung.

Im Rahmen des von der EU geförderten Projekts „CACE“ (Computer Aided Cryptography Engineering) soll jetzt ein „Werkzeugkoffer“ entwickelt werden, der es auch Nicht-Experten im Bereich Kryptografie erlaubt, in ihren Software- und Hardwareprojekten entsprechende Verfahren einzubauen. Zudem soll es mit CACE auch möglich werden, entsprechende Systeme auf ihre Schwachstellen hin zu untersuchen. Das Ziel des Projekts ist es, dass Programme und Systeme in Europa günstiger und fehlerfreier entwickelt werden können. Bisher gibt es kein Angebot vergleichbaren Umfangs.

Der Werkzeugkoffer soll eine Reihe von Programm- und Funktionsbibliotheken, Hilfsmittel und Übersetzungsprogramme umfassen und systemunabhängig eingesetzt werden können (auf verschiedenen technischen Plattformen und mit verschiedenen Programmierumgebungen).

Die Verschlüsselung von Informationen, um sie vor den Augen Unbefugter zu schützen, wird seit mehr als 2.500 Jahren verwendet. Besondere Bedeutung hat sie bei politischen und vor allem militärischen Aufgaben bekommen. Im Zeitalter des Computers haben historische Verfahren zur Verschlüsselung allerdings längst ausgedient - sie sind mit der Rechenleistung moderner Computer viel zu leicht zu entschlüsseln.

Heute werden entweder synchrone

SERVICE

Ihr Wegweiser durch die Europäischen und Internationalen Programme: Information, Beratung, Coaching von der Projektidee bis zum Projektabschluss bieten Ihnen die ExpertInnen der FFG.

Profitieren Sie vom umfassenden Service und optimieren Sie damit Ihre Erfolgschancen im „Match“ um europäische Forschungsgelder.

FFG

Projektkoordinatoren Angelika Holzweber, Klaus-Michael Koch

Fotos: Delater/Pixelio, TommyS/Pixelio, beigestellt

oder asynchrone Verfahren zur Verschlüsselung verwendet. Beim synchronen Verfahren gibt es einen einzelnen geheimen Schlüssel (Code), den nur Sender und Empfänger kennen, um ihre Informationen zu kodieren und zu dekodieren. Beim asynchronen Verfahren arbeitet man mit einem öffentlichen und einem privaten Schlüssel. Mit dem öffentlichen Schlüssel kann jeder seine Informationen kodieren, aber entschlüsseln kann nur der rechtmäßige Empfänger, der über den privaten Schlüssel verfügt.

cace

PROJEKTPARTNER

Organisation	Land
Technikon Forschungs- und Planungsgesellschaft mbH (Projektkoordinator)	Österreich
Ruhr University Bochum	Deutschland
University of Bristol	Großbritannien
Eindhoven University of Technology	Niederlande
University of Minho	Portugal
Bern University of Applied Sciences	Schweiz
Aarhus University	Dänemark
University of Haifa	Israel
Sirrix security technologies AG	Deutschland
Helsinki University of Technology	Finnland
Nokia Oye	Finnland
Alexandra Institute	Dänemark

Aktivitäten der FFG im Bereich Europäische und Internationale Programme werden von der Republik Österreich und der Wirtschaftskammer Österreich finanziert.