CrypTool können eine Vielzahl von kryptographischen Verfahren angewendet und analysiert werden, um dem Anwender grundlegende und fortgeschrittene Konzepte der Kryptologie zu verdeutlichen.

Die aktuelle Version bietet zahlreiche zusätzliche Verfahren. Neben einem Ausbau der klassischen Verfahren wurden u.a. eine Visualisierung von Authentisierungsmöglichkeiten im Netz (Challenge Response) und drei auf dem chinesischen Restsatz beruhende Anwendungen integriert. Mit Hilfe einer Hash-Demo kann die Sensitivität von Hashverfahren demonstriert werden. Des Weiteren beinhaltet die Version 1.4.00 eine Veranschaulichung für einen Seitenkanalangriff gegen ein typisches Hybridverschlüsselungsprotokoll. Ebenfalls enthalten sind drei auf Gitterreduktion basierende Angriffe gegen das bekannte RSA-Verfahren sowie die Implementierung von MAC-Verfahren.

Mit Hilfe der integrierten Animationssoftware ANIMAL, einer Java-Applikation der TU Darmstadt, die es erlaubt, die Einzelschritte von Algorithmen oder die Komponenten von Datenstrukturen beliebig genau zu modellieren und diese dann abzuspielen zu lassen, können die Algorithmen Caesar, Vigenère, Nihilist oder DES detailliert dargestellt werden.

Über die stark erweiterte Online-Hilfe kann der interessierte Anwender jederzeit weitere Hintergrundinformationen zu den implementierten Verfahren erhalten, wobei CrypTool sowohl in einer deutschen als auch in einer englischen Version verfügbar ist.

Aufgrund der Breite der enthaltenen Verfahren, der Veranschaulichung und der Ausgabe von Zwischenergebnissen bietet das Programm eine wirkliche Hilfe, um Verständnis für diese Protokolle und Verfahren zu wecken. Eingesetzt wird CrypTool weltweit zur Schulung und Awarenessbildung sowohl in Hochschulen als auch in Firmen und Behörden.

Entwickler können ohne Registrierung auch die Sourcen von CrypTool 1.4.00 über die CrypTool-Homepage herunterladen. Diese Sourcen lassen sich mit Visual Studio 2003 (VC++ v7.1) kompilieren. Ferner gibt es einen Sourcezweig im Subversion-System, der sich auch mit VS2005 (VC++ v8.0) übersetzen lässt.

Ein Unterprojekt der Entwickler hat gerade begonnen, CrypTool auf Java zu portieren und dabei aktuelle Softwarearchitektur und ein neues Design umzusetzen. Frei-

willige Mitentwickler sind jederzeit willkommen.

Helmut Reimer

Signtrust übernimmt die Trustcenter- Dienste für DATEV

Die DATEV (Datenverarbeitungszentrale der steuerberatenden Berufe Nürnberg) kooperiert mit der Deutschen Post als Trustcenter-Dienstleister. Alle technischen Dienstleistungen werden ab dem 1.1.2007 vom Geschäftsfeld Signtrust der Deutschen Post Com übernommen. Das Nürnberger Unternehmen bleibt weiterhin als Zertifizierungsdiensteanbieter für steuer- und rechtsberatende sowie wirtschaftsprüfende Berufsstände tätig, betreibt aber künftig kein eigenes Trustcenter mehr. Alle Zertifikatsinhaber der erwähnten Berufsgruppen werden weiterhin direkt von der zuständigen Kammer oder von der DATEV betreut.

Mehr Informationen sind unter www.signtrust.deutschepost.de zu finden.

Helmut Reimer

TC Code Signing ermöglicht sichere Software Downloads

Wie Künstler ihre Werke signieren, können Software-Entwickler nun auch ihre neuesten Programmcodes fälschungssicher signieren: Mit TC Code Signing bringt TC TrustCenter dafür eine Zertifizierungs-Lösung auf den Markt.

Besonders Software-Unternehmen, die ihre Produkte im Internet zum Download bereitstellen – ob gratis oder im Verkauf – können mit dem TC Code Signing Zertifikat die Authentizität ihrer Software bestätigen. Selbst bei der Übertragung der Software auf mobile Geräte sind Anbieter und Anwender so auf der sicheren Seite, denn das Zertifikat verhindert unbemerkte Betrugsfälle und Software-Änderungen oder Fälschungen durch Unbefugte.

Mit TC Code Signing können Entwickler ihre aktiven Programminhalte digital signieren. Zwei Versionen stehen dafür zur Auswahl: Microsoft Authenticode und Sun Java Code Signing Zertifikate für Microsoft Authenticode entsprechen digitalen Zertifikaten für .exe-, .dll-, .class-, .msi- und .ocx- (ActiveX) Dateien für Windows – Zeitstempeldienst inbegriffen. Mit Code

Signing Zertifikaten für Sun Java können Entwickler digitale Signaturen für JAR-Dateien (Java Archive) und sonstige Java-Applikationen generieren, die eigenständig oder im Internet Explorer oder in Netscape-Browsern installiert werden können.

TC Code Signing ist ab sofort erhältlich und kann online beantragt werden. Weitere Informationen unter www.trustcenter.de

Helmut Reimer

Studie: Jugendliche sind im Netz leichtsinnig

Europäische Jugendliche riskieren die Sicherheit ihrer PCs, um an kostenlose Inhalte zu gelangen. Dies belegen die Ergebnisse einer neuen Studie von McAfee. Besonders während der Schulferien neigen Teenager dazu, viel Zeit Online zu verbringen. Die Gefahren für Familien-PCs sind jetzt größer als jemals zuvor.

Im Rahmen der Studie wurden Jugendliche im Alter zwischen 13 und 17 Jahren aus sechs europäischen Ländern befragt (Deutschland, Frankreich, Großbritannien, Italien, Niederlande und Spanien). Dabei stellte sich heraus, dass 40 Prozent der Befragten sich nicht für die Risiken interessieren, die beim Download von Musik oder Videos durch Viren und andere Bedrohungen entstehen. Mehr als die Hälfte der Jugendlichen (56 Prozent) nutzen zudem Peer-to-Peer-Programme (P2P) wie Kazaa und Limewire, um an illegalen Content zu kommen. Die von diesen Programmen verwendeten P2P-Netze gelten als bekannte Quellen für schädliche Inhalte.

Die Ergebnisse der Studie brachten zudem eine weit verbreitete Apathie und Ignoranz gegenüber den Gefahren zu Tage, denen die Jugendlichen ihre eigenen wertvollen Daten, wie Musik und Photos aussetzen, indem sie ihre Rechner für Cyberkriminalen öffnen.

Ein Viertel der Befragten (24 Prozent) verschwendet beim Surfen keinen Gedanken an Internetsicherheit und knapp ein Drittel (30 Prozent) bringt seine Sicherheitssoftware nur selten auf den neuesten Stand. Für den Rest der Benutzer in der Familie ist diese Tatsache besonders bedenklich, da immerhin 21 Prozent dieser Jugendlichen intern die Aufgabe übernommen haben, die Familien-PCs abzusichern.

Weitere wichtige Ergebnisse der McAfee-Teenage-Security-Studie sind: