"Mystery-Twister" auf der Cebit
RUB-Institut stellt weltweiten Wettbewerb vor
Messestand mit Seitenkanalattacken und Kryptographie

Mysteriös zugehen wird es ab kommenden Donnerstag, 18. März 2004, auf der Cebit in Hannover: Kryptographen vom Horst Görtz Institut für Sicherheit in der Informationstechnik (HGI) der Ruhr-Universität stellen ihren weltweiten Wettbewerb "Mystery-Twister" vor, der im Oktober startet. Außerdem können die Besucher am Stand eine Chipkarte knacken. Der Messeauftritt der Bochumer Wissenschaftler ist Teil des Gemeinschaftsstandes "Forschungsland NRW" auf der Cebit, auf dem sich insgesamt 15 Hochschulinstitute präsentieren.

Der Weg ist das Ziel

Der Mystery-Twister ist ein internationaler Wettbewerb zur Kryptographie. Im Vordergrund steht der Spaß, Neues zu entdecken und Geheimnissen auf die Spur zu kommen. Bei den Aufgaben mit ansteigendem Schwierigkeitsgrad ist der Weg das Ziel: Zu Beginn sind die Aufgaben ohne Vorbildung lösbar, "unterwegs" werden dann weitere Informationen bereitgestellt, um die kommenden Herausforderungen zu meistern. So können die Teilnehmer zum Beispiel lernen, welche Prinzipien hinter dem Geldautomaten oder der elektronischen Unterschrift stecken. Die erste Runde des Wettbewerbs startet am 1.10.2004, die Teilnahme ist kostenlos.

Angriff auf die Chipkarte

Auf der CeBit wird eine Seitenkanalattacke in der Praxis vorgestellt, welche den Stromverbauch von Chipkarten analysiert und anhand dieser Messdaten in der Lage ist, auf der Karte ausgeführte Verschlüsselungsalgorithmen zu brechen.
Speziell in diesem Szenario ist auf den angegriffenen Chipkarten der Algorithmus Advanced Encryption Standard (AES) implementiert, welcher momentan als nicht "knackbar" gilt und sich deshalb großer Beliebtheit erfreut.
Den Besuchern der CeBit wird ermöglicht, vor Ort einen geheimen Schlüssel auf die Karte zu schreiben. Auf einem zweitem Rechner wird dem Benutzer dann vorgeführt, dass es möglich ist, innerhalb von 5 Minuten den gesamten geheimen Schlüssel mittels Analyse des Stromverbrauchs der Chipkarte zu bestimmen.

Forschungsland NRW

Forschungsleistungen transparent zu machen und ihren praktischen Nutzen zu zeigen, ist Ziel des Gemeinschaftsstands Forschungsland NRW, der sich seit 22 Jahren auf der Hannover Messe, seit einigen Jahren auch auf der Cebit und anderen Messen präsentiert. Um Kooperationen zwischen Wissenschaft und Wirtschaft anzuschieben, ist der Gemeinschaftsstand eine der ersten Adressen im Technologietransfer.

Weitere Informationen

Dr. Tanja Lange, Lehrstuhl Informationssicherheit und Kryptologie (Prof. Dr. Hans Dobbertin),
Horst Görtz Institut für Sicherheit in der Informationstechnik, NA 5/74,
Tel. 0234/32-23260, Fax: 0234/32-14430, E-Mail lange@itsc.ruhr-uni-bochum.de
Zum HGI: http://www.rub.de/hgi
Zum Wettbewerb "Mystery-Twister“: http://www.mystery-twister.com
Zum Forschungsland NRW: http://www.forschungsland.nrw.de