Horst Görtz Institut
für Sicherheit in der Informationstechnik

HGI-News

Horst Görtz Institut für Sicherheit in der Informationstechnik
Ruhr-Universität Bochum, Universitätsstr. 150, D-44780 Bochum
Tel.: +49 - (0)234 - 32 23262, Fax.: +49 – (0)234 – 32 14430
Web: http://www.hgi.ruhr-uni-bochum.de

Nr. 12 Montag, 11. Oktober 2004

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Mittwoch / Wednesday HGI Kolloquium Datensicherheit	13.10.2004 Ab 18.00 Uhr, IHK Bochum, Ostring 30-32, 44787 Bochum **Prof. Dr. Jörg Schwenk**, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität Bochum „**Public-Key-Infrastruktur (PKI) in der Praxis**“
Mittwoch / Wednesday HGI Kolloquium Datensicherheit	13.10.2004 Ab 18.00 Uhr, IHK Bochum, Ostring 30-32, 44787 Bochum **Dr. Eberhard von Faber**, T-Systems „**Security-Suite mit Chipkarte und Leser. Der Anker zur Datensicherheit**“

HGI KOLLOQUIUM DATENSICHERHEIT

Sehr geehrte Damen und Herren,
wir freuen uns Ihnen mitteilen zu können, dass am 13. Oktober 2004 ein Kolloquium zum Thema Datensicherheit“ stattfindet. Initiiert wird dieses Kolloquium vom Horst Görtz Institut für Sicherheit in der Informationstechnik, der IHK Bochum, ruhrsecure – Das Netzwerk für IT-Sicherheit – sowie dem Amt für Wirtschaft- und Beschäftigungsförderung der Stadt Bochum.

Zu dieser Veranstaltung wollen wir Sie hiermit herzlich einladen.

Als Referenten konnten wir gewinnen:

Prof. Dr. Jörg Schwenk, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität Bochum
mit einem Vortrag zum Thema: „Public-Key-Infrastruktur (PKI) in der Praxis.“

Dr. Eberhard von Faber, T-Systems
mit einem Vortrag zum Thema: „Security-Suite mit Chipkarte und Leser. Der Anker für Ihre Datensicherheit.“

Nach den Vorträgen, die jeweils ca. 30 Minuten dauern, bietet sich für Sie die Möglichkeit einer vertiefenden Diskussion mit den Referenten. Zusätzlich werden Sie sich nach der Veranstaltung im Foyer mit anderen Unternehmern und Spezialisten zum Thema austauschen.

Ab Montag, dem 25.10.2004 beginnt wieder das wöchentliche HGI-Seminar. Im Rahmen des Seminars werden praktische und Forschungsaspekte der modernen IT-Sicherheit von Gästen und HGI-Mitgliedern vorgestellt. In der Regel findet das Seminar montags um 14:00 im IC-Gebäude der RUB statt. Gäste sind jederzeit willkommen. Mehr Info zu den Vorträgen unter: *www.crypto.rub.de/seminars.html*

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

21.07.2004, 11.00 Uhr
IC 4/39, Ruhr-Universität Bochum
Jean-Pierre Hubaux, Ecole Polytechnic Fédéral de Lausanne (EPFL)
„**Two Security Questions in Wireless Networks**"

Abstract
Wireless communication systems have become part of our daily life, and yet several basic security questions still need to be addressed. In this talk we will provide two examples to illustrate this concern, and we will describe the solutions we propose.
The first example is in the mundane framework of WiFi hotspots: we will show that the increasing programmability of IEEE 802.11 network adapters makes it very easy for a greedy user to deviate from the MAC protocol in order to increase his own bandwidth at the expense of the other, well-behaved users. We will also describe our solution to this problem, called DOMINO, which consists in a piece of software to be installed at each Access Point. DOMINO is protocol compliant and is able to detect and identify a cheater in a matter of seconds. DOMINO is described at http://domino.epfl.ch
The second is related to secure positioning. A number of techniques have been proposed over the last years to allow wireless devices to position themselves in absolute coordinates and with respect to each other. However, very little work has been done to secure these operations. We will show the vulnerability of the existing solutions to a number of attacks, and we will propose a solution based on a distance bounding protocol.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

26.07.2004, 14.00 Uhr
IC 4/39, Ruhr-Universität Bochum
John Malone-Lee, University of Bristol
„**A General Construction for Simultaneous Signing and Encrypting**"

Abstract
We show how a weak key encapsulation mechanism (KEM) may be used with a signature scheme and a symmetric encryption function to give a provably secure method for simultaneous signing and encrypting. We describe an appropriate security definition for such a scenario and argue that the security of our construction is guaranteed by the security of the components. A corollary of our general result is the first "signcryption" scheme that has a proof of security without requiring the random oracle model.

THE 8TH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC2004)

20.-22.09.2004
Ruhr-Universität Bochum

ECC 2004 is the eighth in a series of annual workshops dedicated to the study of elliptic curve cryptography and related areas. The main themes of ECC 2004 were:

- The discrete logarithm problem.
- Efficient parameter generation and point counting.
- Provably secure cryptographic protocols.
- Efficient software and hardware implementation.
- Side-channel attacks.
- Deployment of elliptic curve cryptography.

It is hoped that the meeting will continue to encourage and stimulate further research on the security and implementation of elliptic curve cryptosystems and related areas, and encourage collaboration between mathematicians, computer scientists and engineers in the academic, industry and government sectors.

There were 15 invited lectures (and no contributed talks), with the remaining time used for informal discussions. There were both survey lectures as well as lectures on latest research developments.

Organizers:

- Gerhard Frey (University of Duisburg-Essen)
- Tanja Lange (Ruhr-Universität Bochum)
- Alfred Menezes (University of Waterloo)
- Christof Paar (Ruhr-Universität Bochum)
- Scott Vanstone (University of Waterloo)

Speakers:

- Roberto Avanzi (University of Duisburg-Essen, Germany)
- Paulo Barreto (University of Sao Paulo and Scopus Tecnologia, Brazil)
- Pierrick Gaudry (LIX Paris, France)
- Ming-Deh Huang (University of Southern California, USA)
- Marc Joye (Gemplus, France)
- Norbert Lütkenhaus (University of Erlangen, Germany)
- Alexander May (University of Paderborn, Germany)
- Kim Nguyen (Bundesdruckerei GmbH, Germany)
- Wayne Raskind (University of Southern California, USA)
- Matt Robshaw (Royal Holloway University of London, UK)
- Werner Schindler (BSI, Germany)
- Jasper Scholten (KU Leuven, Belgium)
- Hovav Shacham (Stanford University, USA)
- Igor Shparlinski (Macquarie University, Australia)
- Nigel Smart (University of Bristol, UK)
- Thomas Wollinger (Ruhr-Universität Bochum, Germany)

Conference Programme:
The schedule of talks is available at: *http://www.cacr.math.uwaterloo.ca/conferences/2004/ecc2004/timetable.html*

Titles and abstracts for the talks are available at:
http://www.cacr.math.uwaterloo.ca/conferences/2004/ecc2004/abstracts.html

SUMMER SCHOOL

13.-17.09.2004
Ruhr-Universität Bochum

For the first time the ECC workshop was held together with a summer school on elliptic curve cryptography. This summer school was organized by VAMPIRE, the Virtual Application and Implementation Research Lab within the European project ECRYPT.
The school took place September 13-17, 2004, in the Ruhr-University Bochum. The target audience were students, PhD students and practitioners with background in applications and industry.
More information about the summer school can be found at: *http://www.rub.de/itsc/tanja/summerschool.*

VERÖFFENTLICHUNGEN / PUBLICATIONS

R. Gabriel, K. Rüdiger, S. Neuber (Hrsg.) (2004). „IT-Sicherheit als Managementaufgabe" - Workshop des Instituts für Sicherheit im E-Business, Arbeitsbericht Nr. 5 des Instituts für Sicherheit im E-Business, Bochum 2004

J. Lange (2004). Sicherheit als materielle Gestaltungsanforderung an computergestützte Informationssysteme, Arbeitsbericht Nr. 4 des Instituts für Sicherheit im E-Business, Bochum 2004

KONGRESSE, TAGUNGEN, FORSCHUNGSAUFENTHALTE / CONGRESSES, MEETINGS, RESEARCH ABROAD

Tanja Lange nahm vom 09.-10. August an der „Selected Areas of Cryptology (SAC)"-Konferenz in Waterloo, Kanada, teil. Sie hielt dort einen Vortrag über das Thema „Efficient Doubling on Genus Two Curves over Binary Fields" (mit Marc Stevens, Eindhoven).

Kerstin Lemke und **Sandeep Kumar** nahmen vom 11.-13.August an dem „Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004)" in Boston, USA, teil. **Kerstin Lemke** hielt dort einen Vortrag mit dem Titel „DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction".

Sandeep Kumar war vom 30. August – 1. September in Antwerpen, Belgien. Er hielt dort auf der „International Conference on Field-Programmable Logic and Applications (FPL) 2004" einen Vortrag zum Thema „Reconfigurable Instruction Set Extension for Enabling ECC on an 8-bit Processor".

Prof. Dr. Brigitte Werners und **Philipp Klempt** nahmen vom 01.-03. September in Tillburg, Niederlande, an der „Operations Research 2004 – International Conference" teil. **Philipp Klempt** hielt dort einen Vortrag zum Thema „Verfahren zur Evaluation von IT-Sicherheit".

Andre Adelsbach nahm am 20. September am „ACM Workshop Multimedia and Security Workshop 2004" in Magdeburg teil. Er hielt dort einen Vortrag zum Thema „Key Assignment Strategies for CPPM".

Kerstin Lemke ist vom 14.-15. Oktober in Brügge, Belgien. Sie hält dort im Rahmen des „SASC-Workshops" einen Vortrag mit dem Titel „Some Thoughts about Implementation Properties of Stream Ciphers".

Redaktionsschluß für
„HGI – News" Nr. 13
Mittwoch, 03. November 2004
12.00 Uhr.

Redaktion:
Oliver Rausch
Email: oliver.rausch@ruhr-uni-bochum.de

Aleksandra Sowa (Geschäftsführerin, HGI)
Email: aleksandra.sowa@ruhr-uni-bochum.de

HGI – News by email
Abonnement unter: http://lists.ruhr-uni-bochum.de/mailman/listinfo/hgi-news

Das Archiv vorheriger Ausgaben ist unter http://www.hgi.ruhr-uni-bochum.de erreichbar.