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. 13 Montag, 08. November 2004

VORLESUNGEN IM WS 04/05 / LECTURES IN WS 04/05

Titel	Lehrstuhl	Dozent	Termin Vorlesung	Termin Übung
Schutz kritischer Infrastrukturen und Informationssicherheit	LS für Kommunikations-sicherheit	Dr. Willi Stein	freitags 11.00- 12.30 Uhr und 13.30 – 15.00 Uhr	
Implementierung kryptographischer Verfahren	LS für Kommunikations-sicherheit	Prof. Dr.-Ing. Christof Paar	donnerstags 10.00 – 12.00 Uhr	
Programmiersprachen	LS für Netz- und Datensicherheit	Prof. Dr. Jörg Schwenk	montags 9.15 – 11.00 Uhr	montags 8.15 – 9.00Uhr oder donnerstags 11.15 – 12.00 Uhr
Systemsicherheit	LS für Netz- und Datensicherheit	Prof. Dr. Jörg Schwenk	dienstags 12.00 – 14.00 Uhr	montags 11.00-12.00 Uhr
Kryptographische Protokolle	LS für Netz- und Datensicherheit	Prof. Dr. Jörg Schwenk	montags 14.00 – 16.00 Uhr	n. V.
Einführung in die Computertechnik	LS für Netz- und Datensicherheit	Dr.-Ing. Helmut Jacob	dienstags 12.00 – 14.00 Uhr und freitags 8.00 – 10.00 Uhr	
Einführung in das Recht des elektronischen Geschäftsverkehrs	Juristische Fakultät	Prof. Dr. Borges	dienstags 12.00 – 14.00 Uhr	

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI KOLLOQUIUM DATENSICHERHEIT

13.10.2004, 18.00 Uhr
IHK zu 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."

Dr. Eberhard von Faber, T-Systems
„Security-Suite mit Chipkarte und Leser. Der Anker für Ihre Datensicherheit."

Initiiert wurde 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.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

25.10.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Andre Adelsbach, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität Bochum
„**CPPM: Broadcast Encryption for Content Protection on Pre-Recorded Media** "

Abstract
Broadcast encryption, originally introduced by Amos Fiat and Moni Naor at Crypto '93, is widely considered a mature and important building block to achieve secure and practical content distribution. Originally targeting Pay-TV applications, today, 10 years after its invention, the major application of broadcast encryption is secure media-based content distribution, e.g., as part of the CPPM standard.
In my talk I will first give a brief introduction to broadcast encryption and discuss its role for content distribution on physical media. The main part of my talk will discuss the CPPM standard, which is based on broadcast encryption and used to protect the new DVD-Audio media. I will assess CPPM's overall security based on the published specifications and point out options for practical improvements.

ISEB XCHANGE SEMINAR

03.11.2004, 17.30 Uhr
GC 4/50
Christian Einhaus, Lehrstuhl für Finanzierung und Kreditwirtschaft
"IT- Sicherheit als Operationelles Risiko"

HGI SEMINAR KRYPTOGRAPHIE

05.11.2004, 14.15 Uhr
NA 01/99
Xiaoyun Wang, Shandong University,
Xuejia Lai, Shanghai Jiaotong University,
Magnus Daum, Ruhr-Universität Bochum
"Which Hash Functions will survive?"

Abstract
Hash functions are an important primitive in many cryptographical applications, for example in digital signature schemes, where instead of a message its short hash value is signed. In practical implementations hash functions have to be fast and secure. The latter means, that it is impossible to find so-called "collisions", i.e. pairs of different messages with the same hash value.
However, presently no method is known to prove the security of hash functions. As in case of block ciphers for instance, their design in practice follows more an adhoc approach. In reality, with only very few exceptions, hash functions of the MD4 family are applied. Recently there has been great progress in the analysis of these hash functions.
At Crypto 2004 rump session in Santa Barbara, collisions for many hash functions of MD4 type were announced by Xiaoyun Wang, for example for SHA-0, RIPEMD, HAVAL-128, MD5. We are proud to present a talk of Xiaoyun Wang and Xuejia Lai, two cryptographers whose analysis was the most spectacular news at Crypto 2004.
A survey of the current situation in the cryptanalysis of hash functions of the MD4 family will be given. It starts with a short introduction on some main aspects and properties of cryptographic hash functions given by Magnus Daum.

Then the techniques used by Dobbertin, Chabaud/Joux and Biham/Chen in their respective attacks will be roughly sketched. Finally Wang and Lai will describe ideas and methods they used in their attack.

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

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

Prof. Dobbertin ist vom 08. November bis zum 03. Dezember zu einem Forschungsaufenthalt an der Universität Toulon in Frankreich.

Redaktionsschluß für
„HGI – News" Nr. 14
Mittwoch, 01. Dezember 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.