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. 14 Dienstag, 01. Februar 2005

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Mittwoch / Wednesday
ISEB XChange-Seminar im WS 2004/2005

02.02.2005
18.00 Uhr, IHK Bochum, Ostring 30-32, Bochum
Dipl.-Ök. Susanne Neuber, Lehrstuhl für Marketing, Mitglied des ISEB
„Kosten- und Erlöswirkungen der IT-Sicherheit"

Dipl.-Ing. Dipl.-Wirtsch.-Ing. Philipp Klempt, Lehrstuhl für Unternehmensforschung und Rechnungswesen, Mitglied des ISEB
„Evaluation der IT-Sicherheit"

Donnerstag / Thursday
Gastvorlesung zur Veranstaltung „Implementation of Cryptographic Algorithms"

03.02.2005
10.15 Uhr, IC 4/30, Ruhr-Universität Bochum
Dr. Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI)
„**Zufallszahlengeneratoren**"

ANKÜNDIGUNG / ANNOUNCEMENT

GI FACHTAGUNG "SICHERHEIT 2005"
5.-8. April 2005, Regensburg
André Adelsbach and Ulrich Greveler
„Satellite Communication without Privacy – Attacker's Paradise"

FIRST INFORMATION SECURITY PRACTICE AND EXPERIENCE CONFERENCE (ISPEC 2005)
11.-14. April 2005, Singapore
André Adelsbach, Ulrich Huber and Ahmad-Reza Sadeghi
„Secure Software Delivery and Installation in Embedded Systems "

André Adelsbach, Sebastian Gajek and Jörg Schwenk
„Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures"

9. DEUTSCHER IT-SICHERHEITSKONGRESS DES BSI

Mai 2005

André Adelsbach, Sebastian Gajek and Jörg Schwenk

„Phishing – Die Täuschung des Benutzers zur Preisgabe geheimer Benutzerdaten"

André Adelsbach, Ulrich Greveler and Jörg Schwenk

„Fair DRM – Ermöglichen von Privatkopien und Schutz digitaler Waren"

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

24.01.2005, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
David Amanor, FH Offenburg und Ruhr-Universität Bochum
„Efficient GF(p) Multiplication in Hardware"

Abstract
Modular multiplication is a core operation in many public key crypto systems such as RSA Reference (RSAREF), Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM) and several others. The Montgomery method is considered the fastest algorithm for modular multiplication reported in the open literature.
Recently, two new algorithms for modular multiplication and their corresponding architectures were proposed in [1]. These algorithms are optimizations of the Montgomery method and interleaved modular multiplication algorithm.
In this talk both software (Java) and hardware (VHDL) implementation of the existing and newly proposed algorithms and their corresponding architectures for doing modular multiplication will be presented. The implementations are scalable to any precision of the input variables x, y and m.
The VHDL models of the multipliers were extensively simulated with input variables of precision ranging from 32 bits to 512 bits and they produced the expected results. After simulation, the models were synthesized using Mentor Graphics Precision RTL Synthesis tools followed by place and routing.
The area and timing report generated by the synthesis tool was used as the basis for comparing the multipliers.
References: [1] Bunimov, V., Schimmler, M.: "Area – Time Optimal Modular Multiplication".

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

10.01.2005, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Kai Schramm, Horst Görtz Institut für IT Sicherheit,
Pankaj Rohatgi, IBM Watson Research Center NY, USA
„New Applications of Template Attacks"

Abstract
Side channel attacks try to break cryptographic implementations by analyzing leakage information such as power consumption, EM radiation or timing behaviour. An advanced form of side channel attacks are so-called template attacks. Template attacks apply multivariate gaussian noise statistics to classify the state of a processor. In general, template attacks consist of two phases. First an adversary must have access to a test device, which he uses to train statistical models. Then, the adversary uses to these models to attack an identical target device.
In order to classify the state of a processor template attacks only require a single side channel trace, which makes them ideal to attack stream ciphers or any cipher, which uses ephemeral keys.
In this work we want to present new applications of template attacks.
First, we show that a single side channel trace carries enough information for template attacks to classify the state of a single bit.
This leads to a new attack, which combines template classification and standard differential power analysis (DPA) to break cryptographic implementations that are protected against DPA using the masking countermeasure.
The main idea is to build templates for classifying bits used in the execution, that are usually randomized. This can be done by a manufacturer, or by anyone who gets access to a single smart-card where the random number generator is biased or has been made biased. If such templates can be built, then all similar smart-cards become vulnerable to DPA, even if they have DPA protection and perfect RNGs.
This attacks also calls into question the current approach of relying on third party certification of smart-cards. Even if the certifier verifies all the code and countermeasures on a smart card, and the smart card works perfectly, it is breakable by anyone who is able to build templates (e.g., someone involved in design, manufacturing or testing of cards, or anyone getting access to a faulty card) and this backdoor cannot be detected during certification.

VERÖFFENTLICHUNGEN / PUBLICATIONS

Mark Manulis and Jörg Schwenk. „Pseudonym Generation Scheme for Ad-Hoc Group Communication Based on IDH". Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), Lecture Notes in Computer Science, volume 3313, pages 107-124. Springer-Verlag, 2005.

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

Prof. Schwenk nahm am 24.11.2004 an einem „Meeting Point"-Treffen zum Thema „Datensicherheit und Datenschutz im Internet" in der Staatskanzlei in Düsseldorf teil. Er hielt dort einen Vortrag zum Thema „Phishing".

VERSCHIEDENES / VARIOUS THINGS

Am 26.11.2004 wurde das Netzwerklabor des Lehrstuhls für Netz- und Datensicherheit eröffnet. Das Labor soll es unseren Studenten der IT-Sicherheit ermöglichen, sowohl alle Internet-Sicherheitstechnologien als auch alle Angriffs-tools selbst auszuprobieren. Da besonders der zweite Teil mit Gefahren für die Konfiguration der verwendeten Rechner einhergeht, ist ein spezielles Labor erforderlich, in dem zudem alle Platteninhalte als Images vorgehalten werden. Bei der Eröffnung wurde das Labor interaktiv vorgestellt.
Weitere Informationen zum Netzwerklabor und der Eröffnungsveranstaltung finden Sie unter:
http://www.nds.rub.de/netzlabor/indexm.html

Auf dem Nestfest der Fakultät ET/IT am 21.01.2005 wurde die Diplomarbeit von **Sebastian Gajek** zum Thema „Phishing und SSL" ausgezeichnet.

Außerdem wurde an diesem Tag von der AQAS das Akkreditierungsverfahren zum **Studiengang „Master ITS"** eröffnet.

Die Dissertation von Herrn **Dr.-Ing. Thomas Wollinger** erhält den Preis der Ruth und Gert Massenberg Stiftung für seine Arbeit mit dem Thema: „Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems".
Die Verleihung findet am 3. Februar 2005, 20 Uhr, im Rahmen des Semesterabschlusskonzertes der Ruhr-Universität Bochum im Audimax statt.

Redaktionsschluß für
„HGI – News" Nr. 15
Mittwoch, 30. März 2005
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.