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. 05 Freitag, 17. Oktober 2003

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday
HGI Seminar Kryptographie und Datensicherheit

20.10.2003
13.15 Uhr, NA 1/51 (Friedrich Sommer Raum)
Yvo Desmedt, Florida State University, USA
„Using Economics and Artificial Intelligence to Identify Critical Infrastructures“

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Yvo Desmedt, Florida State University, Florida

„Using Economics and Artificial Intelligence to Identify Critical Structures“

Abstract
Infrastructures are called critical, if the shut down of these may seriously affect our economy or even the survival of potentially millions of people. The attack could be a combination of physical means (e.g. using explosives) with hacking. Such a type of attack is often called cyber terrorism or cyber war. (Note that information warfare is a much broader concept including such tools as propaganda.)

Cyber attacks differ from traditional attacks since these can be replicated and done remotely. In this lecture we focus on the potential vulnerabilities of critical infrastructures, and on developing scientific methods to identify which infrastructures are critical. We do not make predictions whether such an attack will take place. This depends on the intend of the enemy to use it facing the potential consequences and on the knowhow of the enemy of what to attack and how.

We introduce several new models. First we use artificial intelligence to model our computerized infrastructures. Using economical models, we propose an alternative way to model the enemy. In the traditional approach to address security threats in distributed computations the adversary will be bounded to break into k machines. Today such a model is questionable since the cost to break into k+1 machines running the same operating system is clearly less than the cost of breaking into k machines using very different platforms.

SICHERE DATENKOMMUNIKATION IM AUTOMOBIL
ESCAR© - EBEDDED IT-SECURITY IN CARS

18. – 19. 11. 2003
Radisson SAS Hotel Köln, Messe-Kreise 3, 50679 Köln

In einem typischen Mittelklassewagen sind in der Regel über 30 diverse Computer eingebaut. Von der Motordiagnose bis zur Navigation kommt kaum ein komplexes Teilsystem des Autos ohne Rechnerunterstützung aus. Durch die Abstimmung dieser eingebetteten Computer und durch Schnittstellen nach außen spielt die digitale Kommunikation im und mit dem Auto eine immer wichtigere Rolle.

Natürlich haben Sicherheits- und Qualitätsfragen dabei eine hohe Bedeutung. Maßnahmen und Werkzeuge, die eine sichere Kommunikation im Automobilbereich ermöglichen, sind bei anderen Anwendungen der Informationstechnik teilweise bereits erprobt. Die Automobilindustrie ist sich natürlich dieser Herausforderung im Sinne erweiterter Leistungsangebote, aber auch der damit verbundenen Risiken in ihrer Verantwortung als Hersteller längst bewusst.

Ein Aspekt jedoch der modernen Automobilkommunikation, der bisher nicht systematisch behandelt wurde, ist die Absicherung der IT-Anwendungen. Dieses Thema wird in dem gleichen Maße an Bedeutung gewinnen, in dem Automobile mit IT-Funktionalität durchsetzt werden. Spätestens mit der Kommunikationsanbindung von Fahrzeugen an externe Einheiten, z.B. über das GSM oder UMTS-Netz, wireless-LAN (WiFi) oder Bluetooth-Verbindungen, wird das Gefahrenpotential sprunghaft ansteigen. Ohne ädequate Sicherheitsmaßnamen Werden viele zukünftige X-by-wire Anwendungen nicht realisierbar sein. IT-Sicherheit stellt von daher eine "enabling Technology" für die meisten der zukünftigen IT-basierten Anwendungen dar.

Der ESCAR-Konferenz wird als weltweit erste Veranstaltung zu diesem Themenkreis das erste Mal führende Experten aus den Bereichen IT-Sicherheit, automotive IT und Kommunikationstechnik zusammenbringen, um die Herausforderungen und Lösungsmöglichkeiten zu diskutieren.

Weitere Information und Anmeldung unter: **http://www.escarconference.org**

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Selcuk Baktir, Worcester Polytechnic Institute, USA
18.09.2003, 11.00 Uhr
IC 4/39, Ruhr-Universität Bochum

„Optimal Tower Fields for Elliptic Curve Cryptography“

Abstract
Elliptic curve cryptography relies heavily on the existence of efficient algorithms for finite field arithmetic. Optimal Extension Fields (OEFs) have been found to be especially successful in embedded software implementations of elliptic curve schemes. In the elliptic curve scalar-point multiplication, a large number of field multiplications and inversions are computed. This poses a significant problem in embedded systems where computational power is quite limited. Despite recent improvements, inversion is still the slowest operation in elliptic curve implementations. In this talk, this issue will be addressed by introducing a specialized tower field representation, named Optimal Tower Fields (OTFs), which facilitates efficient finite field arithmetic.

The recursive direct inversion method developed for OTFs will be presented. It will be shown that the asymptotic complexity of OTF inversion algorithm is phenomenally as low as O(m^2), which is same as the asymptotic complexity of multiplication and a significant improvement over the O(m^2 log_2 m) asymptotic complexity of Itoh-Tsujii method. We will see that this complexity is further improved to O(m^(log_2 3)) by utilizing the Karatsuba-Ofman algorithm. We will also see that OTFs are in fact a special class of OEFs, and an OTF element may be converted to OEF representation via a simple permutation of the coefficients. Hence, OTF operations are available to OEFs whenever a corresponding OTF exists.

The implementation results of OTF inversion algorithm on the ARM family of processors will be presented for a medium and a large sized field whose elements can be represented with 192 and 320 bits, respectively. Finally, we will comment on the remarkable speed-up advantage of using OTF inversion in performing elliptic curve point multiplication operation.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Kerstin Lemke
22.09.2003, 11.00 Uhr
IC 4/39, Ruhr-Universität Bochum

„Side Channel Attack Scenarios against the DES and RSA“

Abstract
In the meantime 'Side Channel Cryptanalysis' includes a wide area of scenarios that can be used to attack the implementations of cryptographic algorithms. These scenarios exploit the inherent or forced leakage of data processing units and generally do not leave any damage to the cryptographic device.

This presentation aims to review the main scenarios that are published against the DES and RSA implementations. Generally, variations of these attacks can be applied at various algorithms. The focus will be on the power analysis as SPA ("Simple Power Analysis") and DPA ("Differential Power Analysis") and on the fault analysis. Generic countermeasures are discussed.

HGI KOLLOQUIUM „E-CRM IM PUBLIC SECTOR“
15.10.2003, 14.00 Uhr
NA 1/58 (Friederich Sommer Raum, Ruhr-Universität Bochum

Sebastian Tengler, Lehrstuhl für Produktionswirtschaft, Ruhr-Universität Bochum

„Die Bedeutung der Informationssicherheit am Beispiel von CRM und SCM"

VORLESUNGEN IM WINTERSEMESTER 2003/04

Prof. Dr. Dobbertin	„Einführung in die Algebra”, dienstags und freitags jeweils 14.00 – 16.00 Uhr, NA 01/99
	„Kryptographie I“, mittwochs 14.00 – 16.00 Uhr, IC 4/161
Prof. Dr.-Ing. Paar	„Einführung in die Datensicherheit und Kryptographie I”, donnerstags, 12.15 – 13.45 Uhr, HZO 80
Prof. Dr. Schwenk	„Programmiersprachen“, montags, 9.00 – 11.00 Uhr, IC 4/161 und freitags, 10.00 – 12.00 Uhr, HZO 80
	„Systemsicherheit“, montags, 11.00 – 12.00 Uhr und dienstags, 10.00 – 12.00 Uhr, jeweils IC 4/161
Dr. Lange	„Endliche Körper und ihre Anwendungen“, dienstags, 12.15 – 13.45 Uhr, NA 4/64 und mittwochs, 12.15 – 13.45 Uhr, NA 5/64

GÄSTE / GUESTS

Prof. Yvo Desmedt 13.10.2003 – 14.11.2003

Biographie:
Yvo Desmedt received his Ph.D. (Summa cum Laude) from the University of Leuven, Belgium (1984). He is presently a professor at Florida State University (Computer Science) and a visiting professor of Information Security at Royal Holloway, University of London. His interests include cryptography, network security and computer security. He has authored more than 100 papers in international conferences and journals. He was program chair of PKC (Public Key Cryptography) 2003, the 2002 ACM Workshop on Scientific Aspects of Cyber Terrorism and Crypto '94. His first paper that described a potential cyberterrorism scenario dates back to 1983. He is an editor of the Journal of

Computer Security and of Information Processing Letters and is a director of the International Association for Cryptologic Research.

Yvo Desmedt is ranked as the 2nd most prolific author (out of 1165 researchers) in Crypto/Eurocrypt. He has given invited lectures at several conferences and workshops in 5 different continents and more than 100 invited lectures for industry and academia. He is a recipient of the Society of Worldwide Inter-bank Funds Transfer (SWIFT) award.
We view as a futuristic hacker one that tries to optimize the attack instead of just demonstrating the vulnerability of the system, as a modern one does. We then describe different models to study which infrastructures are critical to such a futuristic hacker. One of these is based on flow. Can the enemy reduce the maximum flow to below a critical value (e.g. too low to sustain water to a population)? A disadvantageous of this model is that when modeling multiple applications, it does not take an impact factor of that application into account. An economical model is proposed to study such a "weighted" critical capacity.

Alexander Kholosha 03.11.2003 – 07.11.2003

Technische Universiteit Eindhoven

ANKÜNDIGUNGEN DER HGI-PARTNER / ANNOUNCEMENTS BY CO-OPERATING ORGANISATIONS

CALL FOR PAPERS:
DETECTION OF INTRUSIONS AND MALWARE & VULNERABILITY ASSESSMENT (DIMVA 2004)

06./07.07.2004
Dortmund
Veranstalter: Fachgruppe SIDAR der Gesellschaft für Informatik e.V. (GI)

Die Fachgruppe SIDAR (Security - Intrusion Detection and Response) der Gesellschaft für Informatik e.V. beschäftigt sich mit der Erkennung und Beherrschung von Vorfällen der Informationssicherheit und veranstaltet vom 6.-7. Juli 2004 einen Workshop zum Thema Erkennung von Schutzzielverletzungen (Intrusion Detection), Malware-Bekämpfung (Malicious Agents) sowie Ermittlung von Verwundbarkeiten (Vulnerability Assessment).

Ziel des Workshops ist es, eine Übersicht zum Stand der Technik und Praxis in Industrie, Dienstleistung, Verwaltung und Wissenschaft im deutschsprachigen Raum zu geben. Insbesondere sollen Ergebnisse aus den Bereichen Forschung, Entwicklung und Integration vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden. Rechtliche Rahmenbedingungen und wirtschaftliche Faktoren sollen ebenfalls betrachtet werden.

Das Programmkomitee lädt ein zur Einreichung von

- vollen Beiträgen über bisherige Ansätze und Erfahrungen sowie laufende Entwicklungen, insbesondere zu Theorie, Entwurf, Implementierung, Analyse und Evaluierung sowie über rechtliche Rahmenbedingungen.

- vollen Beiträgen und Kurzbeiträgen über Praxisstudien und wirtschaftliche Faktoren bei der Einführung oder Anwendung in Referenzprojekten (Fallstudien).

Weitere Informationen unter: **http://www.gi-fg-sidar.de/dimva2004**

Redaktionsschluß für
„HGI – News“ Nr. 06
Mittwoch, 29. Oktober 2003
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.