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. 07 Montag, 08. Dezember 2003

Das Horst Görtz Institut wünscht den Lesern der HGI-News und ihren Familien ein gesegnetes Weihnachtsfest und einen guten Start ins Jahr 2004.

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

Montag / Monday
HGI Seminar Kryptographie und Datensicherheit

08.12.2003
13.15 Uhr, IC 4/39, Ruhr-Universität Bochum
Ammar Alkassar, Universität des Saarlandes
„Secure Object Identification - Or: How To Solve The Chess-Grandmaster-Problem“

Montag / Monday
HGI Seminar Kryptographie und Datensicherheit

15.12.2003
13.15 Uhr, IC 4/39, Ruhr-Universität Bochum
Philippe Rivard, COSY Group, Ruhr-Universität Bochum
Der Titel wird noch bekanntgegeben.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Ammar Alkassar, Universität des Saarlandes

„Secure Object Identification - Or: How To Solve The Chess-Grandmaster-Problem“

Abstract
Many applications of cryptographic identification protocols are vulnerable against physical adversaries who perform real time attacks. For instance, when identifying a physical object like an automated teller machine, common identification schemes can be bypassed by faithfully relaying all messages between the communicating participants. This attack is known as mafia fraud.
In my talk I will give an overview over different approaches to cope with that fraud. One approach, the Probabilistic Channel Hopping system, solves this problem by hiding the conversation channel between the participants. The security of this approach is based on the assumption that an adversary cannot efficiently relay all possible communication channels of the PCH system in parallel.

ANKÜNDIGUNG / ANNOUNCEMENT

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT
12.01.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Sandeep Kumar, COSY Group, Ruhr-Universität Bochum

„Embedded End-to-End Wireless Security with ECDH Key Exchange“

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT
19.01.2004, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
Stefan Lucks, Universität Mannheim

Der Titel des Vortrages wird noch bekanntgegeben.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT
26.01.2004, 13.15 Uhr
N IC 4/39, Ruhr-Universität Bochum
Johannes Ueberberg, SRC GmbH, Bonn

„Sichere Zahlungsverkehrsmodelle im Internet“

VORHERIGE VERANSTALTUNGEN / PAST ACTIVITIES

SEMINARSERIE VON YVO DESMEDT
Prof. Yvo Desmedt, Florida State University
04.11.2003, 11.00 Uhr, NA 5/64, Ruhr-Universität Bochum
10.11.2003, 16.00 Uhr, NA 4/24, Ruhr-Universität Bochum
11.11.2003, 16.00 Uhr, NA 5/64, Ruhr-Universität Bochum
13.11.2003, 10.00 Uhr, NA 4/64, Ruhr-Universität Bochum
„Some Mathematical Aspects of Threshold Cryptography and Secret Sharing“

Abstract
Secret sharing allows a dealer to distribute shares of a secret such that:
-) any set of authorized parties can recover the secret from their shares
-) any non-authorized parties have as much information about the secret as they had initially.
Secret sharing combined with cryptography, allows secure distributed computation. One can, in particular, compute a digital signature jointly in such a way that no unauthorized set of parties will learn anything new

about the secret (except the digital signature). Secret sharing has other applications, that enable reliable communications in untrusted networks. To achieve these properties different algebraic and combinatorial properties are introduced. This series of lectures starts with an introduction to the concepts of secret sharing, (in particular threshold schemes), homomorphic secret sharing, multiplicative secret sharing, zero-knowledge secret sharing, etc.
Algebra has played a major role in Threshold Cryptography. In this context, the state of the art on homomorphic and multiplicative secret sharing schemes is surveyed. Module theory is applied to obtain a redistribution of a secret without the need for a trusted dealer. Non-interactive secure distributed computation is then discussed. We also survey the link between secret sharing and error-correcting codes and discuss some applications.
Finally, mechanical keys can often be viewed as secret shares without algebraic properties. We discuss how combinatorics can then be used to redistribute mechanical secret shares.
REQUIRED BACKGROUND: elementary group and ring theory. The required module theory will be introduced.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Andre Adelsbach, Universität des Saarlandes
06.11.2003, 11.00 Uhr
IC 4/39, Ruhr-Universität Bochum
„Über die Unsicherheit Nicht-Invertierbarer Wasserzeichenverfahren“

Abstract
Durch die Verfügbarkeit leistungsfähiger Kommunikationsnetze und intensiver Standardisierungsbemühungen im Bereich des Digital Rights Managements wird die Verteilung von digitalen Inhalten in den kommenden Jahren starken Zuwachs erfahren und es werden neuartige, dezentrale Verteilungs- und Wertschöpfungsketten basierend auf digitalen Werken entstehen. In diesem Zusammenhang besteht für die Urheber digitaler Werke ein grundlegendes Problem darin, ihre Urheberschaft an ihren Werken zu beweisen, beispielsweise um Urheberschaftsdispute vor Gericht gewinnen zu können.
Eine bekannte Klasse von Disputauflösungsverfahren basiert auf speziellen Wasserzeichen-Verfahren, welche die sogenannte „Nicht-Invertierbarkeitseigenschaft" erfüllen. Da reine Wasserzeichen-Verfahren meist invertierbar sind, wurden kryptographische Mechanismen eingesetzt, um diese Wasserzeichen-Verfahren nachträglich „nicht-invertierbar" zu machen.
In diesem Vortrag wird ein Überblick über Wasserzeichen-Verfahren, Disputauflösungsverfahren sowie Nicht-Invertierbarkeitskonstruktionen gegeben. Insbesondere wird der Einfluss der False-Positive Wahrscheinlichkeit des Watermarking-Verfahrens auf die Sicherheit von Nicht-Invertierbarkeitskonstruktionen nachgewiesen und gezeigt, dass diese Konstruktionen unsicher sind, wenn die False-Positive Wahrscheinlichkeit nicht vernachlässigbar klein ist.

KOLLOQUIUM DES GRADUIERTENKOLLEGS

Prof. Yvo Desmedt, Florida State University
06.11.2003, 15.15 Uhr
Hörsaal ES 09, Institut für Experimentelle Mathematik (IEM), Universität Essen
„Robust and Secure Communications and its Impact on PKI“

Abstract
From a web page of Microsoft we learn:
In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is “Microsoft Corporation". The ability to sign executable content using keys that purport to belong to Microsoft would clearly be advantageous to an attacker who wished to convince users to allow the content to run.
Note that VeriSign is one of the largest "Certifying Authorities" in the USA.
This lecture starts by surveying the importance of PKI, which relies on so called "digital certificates". The aforementioned case illustrates that such digital certificates may not be trusted. This may be due to insider mismanagement or to the fact that the computers that generate these digital certificates are vulnerable to hacking. Methods to deal with such insider's or outsider's "attacks" are discussed and compared. This leads to the more general question on how to reliably communicate over a network with active attackers. Solutions have been proposed for several decades. Recent progress on how to achieve this adding privacy and authenticity is also discussed. Finally the question of how these issue become more complex when dealing with unknown networks, as they occur in ad-hoc networks is briefly discussed.

KOLLOQUIUM DES GRADUIERTENKOLLEGS

Dr. Roberto Avanzi, Universität Duisburg-Essen
06.11.2003, 16.15 Uhr
Hörsaal ES 09, Institut für Experimentelle Mathematik (IEM), Universität Essen
„Countermeasures against Differential Power Analysis for Hyperelliptic Curve Cryptosystems "

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Prof. Yvo Desmedt, Florida State University
10.11.2003, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
„Cryptanalysis of Several of the UCLA Watermarking Schemes for Intellectual Property Protection of Digital Circuits/Designs"

Abstract
We analyze four recently proposed watermarking schemes for intellectual property protection of digital designs. The first scheme watermarks solutions of a hard optimization problem, namely the graph coloring problem. The remaining three schemes belong to a family of techniques for watermarking digital circuits on programmable hardware. They were referred to as constraint-based watermarking. All of these schemes are different from usual image and audio watermarking in that they must maintain the correctness of the watermarked objects. Therefore their watermarks cannot be embedded in the form of small errors as usually done in audio and visual watermarking. Though similar constraint-based schemes existed for watermarking software, these schemes are the first ones applied to protect hardware designs.
In this lecture, we apply a novel method to break the first of these schemes. We show how to modify a watermarked object in such a way that every signature strings can be extracted from it. Thus anyone can claim ownership of the object, yet leave no traces of who leaked the object. According to our best knowledge, this method is new and it may be of its own interest. In the other three watermarking schemes, we show how to locate and to remove the watermark embedded in the object, without knowing the secret key used in the embedding.
This presentation is based on joint work with Tri V. Le.

SICHERE DATENKOMMUNIKATION IM AUTOMOBIL
ESCAR© - EMBEDDED 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.
Die ESCAR-Konferenz brachte als weltweit erste Veranstaltung zu diesem Themenkreis das erste Mal führende Experten aus den Bereichen IT-Sicherheit, automotive IT und Kommunikationstechnik zusammen, um die Herausforderungen und Lösungsmöglichkeiten zu diskutieren.

HGI SEMINAR KRYPTOGRAPHIE UND DATENSICHERHEIT

Prof. Dr.-Ing. Christof Paar, Lehrstuhl für Kommunikationssicherheit, Ruhr-Universität Bochum
01.12.2003, 13.15 Uhr
IC 4/39, Ruhr-Universität Bochum
„Eingebettete IT-Sicherheit im Automobil"

Abstract
Es wird zunehmend deutlich, dass die Informationstechnik innerhalb von Automobilen rapide an Bedeutung gewinnt. Zum einen wird die Informationstechnik für grundlegende Fahrzeugfunktionen (Motorsteuerung, Bremsen, Lenkung) eingesetzt, daneben für Sekundärfunktionen wie Wegfahrsperre, Airbag etc. und letztlich für Anwendungen wie

Telematik, online Streckenführung und in-car Entertainment. Ein Aspekt der modernen Informationstechnik, 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. Wir glauben, dass das Fehlen von adäquaten Sicherheitsmaßnamen ein ernsthafter Hinderungsgrund für die Einführung zukünftiger IT-Anwendungen sein kann, die große finanzielle und technische Bedeutung in Fahrzeugen der Zukunft haben kann. Gleichzeitig lassen sich zahlreiche neue Geschäftsmodelle im Automobilbereich durch robuste IT-Sicherheit realisieren.

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

Prof. Dr.-Ing. Christof Paar hielt im Rahmen der ESCAR-Konferenz in Köln am 18. November 2003 einen Vortrag zum Thema „Eingebettete Sicherheit im Automobil.

PREISE / AWARDS

Ingo Riedel vom Lehrstuhl für Kommunikationssicherheit gewann mit seiner Diplomarbeit zum Thema „Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform“ in der Kategorie Studierende den 2.Preis des „CAST (Competence Center for Applied Security Technology)-Förderpreises IT Sicherheit 2003”.
Um die Ausbildung in IT-Sicherheit in Betrieben, Berufsakademien und Hochschulen zu fördern, verleihen die CAST-Mitglieder seit 2001 jährlich den CAST-Förderpreis.
Der Preis soll herausragende Leistungen belohnen und junge Menschen aller Bildungswege ermutigen, sich mit dem wichtigen Thema IT-Sicherheit auseinander zu setzen. Er ist mit insgesamt 18.000 EUR dotiert.
Herr Ministerpräsident Roland Koch hat die Schirmherrschaft über den diesjährigen Förderpreis übernommen.

Redaktionsschluß für
„HGI – News“ Nr. 08
Mittwoch, 07. Januar 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.