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. 06 Donnerstag, 30. Oktober 2003

VERANSTALTUNGEN DIESES MONATS / ACTIVITIES OF THIS MONTH

QUO VADIS – DIGITALE SIGNATUR
DAS PRODUKT AN DIE NUTZER BRINGEN.

20.11.2003, 16.00 Uhr
Haus für IT-Sicherheit, Lise-Meitner-Allee 4, 44801 Bochum

Vier Jahre nach der Schaffung rechtlicher, ökonomischer und technischer Rahmenbedingungen für die Einführung von digitalen Signaturen, sind in Deutschland erst 25.000 Signatur-Zertifikate ausgestellt.

Obwohl ihre technische Seite ausgereift ist und sie auf einer soliden rechtlichen Grundlage stehen, finden Digitale Signaturen kaum Akzeptanz auf dem Markt. Kritik an dem Konzept der Digitalen Signatur und ihren Machern ist zu hören: Bisher wurden allzu oft bloß oberflächliche Schlagworte über die Risiken und Chancen der Nutzung von Digitalen Signaturen verbreitet.

Der Erfolg der Signaturen verlangt aber mehr als nur Risiken und Chancen aufzuzählen. Hier sind Informationen mit Substanz gefragt, die den Nutzen Digitaler Signaturen verdeutlichen und zeigen, wie Digitale Signaturen an den Nutzer gebracht werden können.

An dieser Stelle will unsere Konferenz an die bisherige Diskussion anknüpfen und ihr zu einem konstruktiven Ergebnis verhelfen. Im Kreise von Experten aus Politik, Wirtschaft und Wissenschaft wollen wir im Rahmen der gemeinsamen Konferenz des Horst Görtz Instituts und der Initiative D21 das Leitkonzept erläutern und einen Anstoß zu einer breiten, in allen Bereichen der Gesellschaft stattfindenden Debatte geben.

Wir laden Sie herzlich zu dieser Veranstaltung ein.

Prof. Dr. Hans Dobbertin
Geschäftsführender Direktor
des Horst Görtz Instituts

Barbara Zimmers
Geschäftsführerin
der Initiative D21

Programm

16:oo Uhr Begrüßung
Prof. Dr. Hans Dobbertin
Geschäftsführender Direktor
des Horst Görtz Instituts

Katharina Ahrens
Leiterin der Presse- und Öffentlichkeitsarbeit,
Initiative D21

16:2o Uhr „Evaluierung der Signaturrichtlinie und Novellierung des Signaturgesetzes“
Prof. Dr. Alexander Rossnagel
Universität Kassel

16:4o Uhr „Digitale Signaturen und IT-Sicherheit – Herausforderung für die Politik“
Jörg Tauss (MdB)

Bildungs-, forschungs- und medienpolitischer
Sprecher der SPD-Bundestagsfraktion,
Beauftragter zur Reform des
Datenschutzrechtes der SPD-Bundestagsfraktion

17:oo Uhr „Markt der elektronischen Signaturen in Deutschland“
Andreas Vollmert
Projektleiter, msc Multimedia
Support Center GmbH

17:2o Uhr „Das Signaturgesetz und seine praktische Umsetzung“
Jürgen Schwemmer
Leiter des Referats für Elektronische
Signatur, Regulierungsbehörde für
Telekommunikation und Post, RegTP

17:4o Uhr Pause

18:oo Uhr Diskussionsforum:
„Quo Vadis Digitale Signatur“
Jochen Knaab
Leiter Geschäftsfeld Zertifizierungsdienstleistungen
S-TRUST, Deutscher Sparkassen Verlag

Jürgen Schwemmer
Leiter des Referats für Elektronische
Signatur, Regulierungsbehörde für
Telekommunikation und Post, RegTP

Jörg Tauss (MdB)
Bildungs-, forschungs- und medienpolitischer
Sprecher der SPD-Bundestagsfraktion,
Beauftragter zur Reform des
Datenschutzrechtes der SPD-Bundestagsfraktion

Andreas Vollmert
Projektleiter, msc Multimedia
Support Center GmbH

Jan C.E. Wendenburg
CEO AuthentiDate International AG

Moderation: Dr. Udo Vorholt
Universität Dortmund

18:45 Uhr Eröffnung der Diskussion mit Experten und Teilnehmern der Konferenz

19:15 Uhr Zusammenfassung und Schlusswort

19.45 Uhr Ende der Veranstaltung

Weitere Information und Anmeldung unter: **http://www.hgi.ruhr-uni-bochum.de**

Donnerstag / Thursday Kolloquium des Graduiertenkollegs	06.11.2003 15.15 Uhr, Institut für Experimentelle Mathematik (IEM), Universität Essen, Hörsaal ES 09 **Prof. Yvo Desmedt**, Florida State University, USA „Robust and Secure Communications and its Impact on PKI“
Donnerstag / Thursday Kolloquium des Graduiertenkollegs	06.11.2003 16.15 Uhr, Institut für Experimentelle Mathematik (IEM), Universität Essen, Hörsaal ES 09 **Dr. Roberto Avanzi**, Universität Duisburg-Essen „Countermeasures against Differential Power Analysis for Hyperelliptic Curve Cryptosystems “
Dienstag – Mittwoch / Tuesday – Wednesday Sichere Datenkommunikation im Automobil ESCAR© - Embedded II-Security in Cars	18.-19.11.2003 Radisson SAS Hotel Köln, Messe-Kreise 3, 50679 Köln
Donnerstag / Thursday “Quo Vadis – Digitale Signaturen”	20.11.2003 16.00 Uhr, Haus für IT-Sicherheit, Lise-Meitner-Allee 4, 44801 Bochum

KOLLOQUIUM DES GRADUIERTENKOLLEGS

Prof. Yvo Desmedt, Florida State University

„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.

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.

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

Yvo Desmedt, Florida State University, Florida
20.10.2003, 13.15 Uhr
NA 1/58 (Friedrich Sommer Raum), Ruhr-Universität Bochum

„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.

VERÖFFENTLICHUNGEN / PUBLICATIONS

Prof. Dr. Roland Gabriel, Martin Gersch, Rüdiger, Klaus. „Sicherheit im E-Business – Eröffnungsworkshop des Instituts für Sicherheit im E-Business", Arbeitsbericht Nr. 3 des Instituts für Sicherheit im E-Business, Bochum 2003.

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

Prof. Dr. Roland Gabriel und Klaus Rüdiger präsentierten am 22.10.03 im Rahmen eines zweitägigen Forschungsaufenthaltes am Institut für Wirtschaftsinformatik (IWI) der Universität St. Gallen, Schweiz das Europäische Kompetenzzentrum für IT-Sicherheit (EUROBITS) sowie ausgewählte Forschungsprojekte des Instituts für Sicherheit im E-Business (ISEB).

Jörg Lange hielt am 22.10.03 im Rahmen eines zweitägigen Forschungsaufenthaltes am Institut für Wirtschaftsinformatik (IWI) der Universität St. Gallen, Schweiz den Vortrag „Trusted Computing – Chancen und Risiken der TCPA / TCG-Initiative„.

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. Gabriel

„Wirtschaftsinformatik I“, dienstags, 14.00 – 16.00 Uhr, HZO 20

„Aufbau betrieblicher Informationssysteme“, donnerstags, 14.00 – 16.00 Uhr, H-GB

„Entscheidungsunterstützungssysteme (Management Support Systeme)“, donnerstags, 10.00 – 12.00 Uhr, HZO 60

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. 07
Mittwoch, 26. November 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.