4. Deutscher IT-Sicherheitspreis 2012

INHALT

Grußwort von Stifter Dr.-Ing. e. h. Horst Görtz

Am 29.11.2012 wird der Deutsche IT-Sicherheitspreis zum 4. Mal verliehen. Der Preis ist bei deutschen Forschungsstätten an Universitäten und in Unternehmen, die IT-Sicherheitsprodukte oder -dienstleistungen anbieten, beliebt und erfreut sich großer Beteiligung. In diesem Jahr befand die Jury, dass unter den eingereichten Arbeiten vier so exzellent waren, dass jeweils zwei Arbeiten den ersten und den zweiten Preis erhalten sollen. In diesem Jahr haben sich 32 Teams beworben. Die Jury hat die eingereichten Arbeiten in zeitaufwendiger Arbeit bewertet und die besten zehn sowie unter diesen die Preisträger ausgewählt. Für die geleistete Arbeit danke ich den Mitgliedern der Jury.

Zum ersten Mal wird 2012 eine Broschüre vorgelegt, in der die besten zehn Arbeiten und deren Schöpfer vorgestellt und öffentlich gewürdigt werden.

Die Gewinner der ersten drei deutschen IT-Sicherheitspreise haben die Preisgelder zur Weiterentwicklung ihrer Lösungen benutzt:

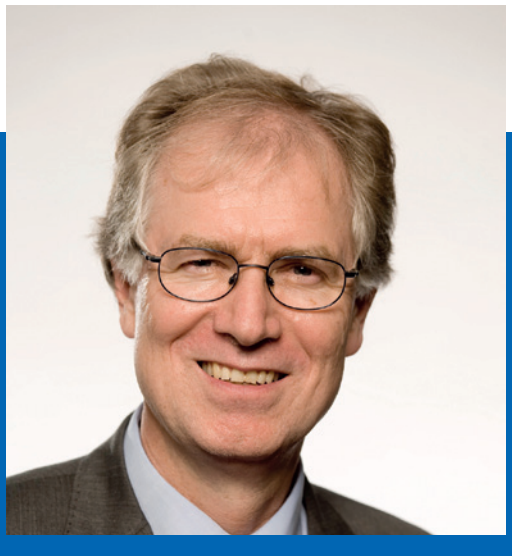
Der Gewinner des ersten Preises 2006, Herr Thomas Dullien, Gründer der Sabre Security GmbH in Bochum (seit 2007 zynamics.com), wurde für eine neue Software ausgezeichnet, die bislang unbekannte Schadprogramme schnell erkennt. Er hat seine Firma 2011 Google verkauft, die die Technologie weltweit nutzt.

2008 hat den ersten Preis eine Forschergruppe um den inzwischen zum Professor an der TU Karlsruhe berufenen Dr. Jörn Müller-Quade erhalten. Sein Thema war „Bingo Voting - Verifizierbare Wahlen mit Wahlmaschinen“. Das Thema ist immer noch in der Diskussion, aber noch nicht praktisch realisiert.

Gewinner des ersten Preises 2010 war eine internationale Forschergruppe um Professor Christof Paar von der Ruhr-Universität Bochum. „PRESENT - Kostenoptimierte Sicherheit für pervasive Rechnerwelten“ wurde entwickelt von Gregor Leander (TU of Denmark), Prof. Christof Paar (Ruhr-Universität Bochum) und Dr. Axel Poschmann (Nanyang TU). Es handelt sich um eine Chiffre für kosten- und energiebeschränkte Geräte wie RFID-Etiketten oder Konsumerelektronikgeräte. Das Design der Chiffre zeichnet sich durch extreme Hardware-Effizienz aus und ist, nicht zuletzt wegen seiner größtmöglichen Einfachheit, nur drei Jahre nach seiner Veröffentlichung zur meist beachteten modernen Chiffre geworden. Die International Electrotechnical Commission (ISO/IEC) hat PRESENT 2012 standardisiert und in den neuen internationalen Standard für „Lightweight Cryptography“ aufgenommen. Die Chiffre ist eine der sehr erfolgreichen Entwicklungen von IT-Sicherheit „made in Germany“.

Dr.-Ing. e. h. Horst Görtz
Gründer der Horst Görtz-Stiftung

Grußwort von Schirmherr Michael Hange



Der Prozess der Verlagerung von Geschäftstätigkeiten in die virtuelle Welt ist ungebrochen. Die Digitalisierung und Vernetzung haben uns faszinierende Möglichkeiten eröffnet, die bis vor wenigen Jahren noch unvorstellbar waren. Mehr denn je sind wir daher auf ein fehlerfreies und sicheres Funktionieren der Informationstechnik angewiesen. IT-Sicherheitsvorfälle in großen Unternehmen oder Viren wie Duqu und Stuxnet führen uns aber immer wieder vor Augen, wie angreifbar unsere Informations- und Kommunikationstechnologie ist.

Die Schaffung von IT-Sicherheit ist daher keine Einzelmaßnahme, sondern immer ein Prozess, der die kontinuierliche Betrachtung und Anpassung verschiedener Faktoren erfordert. Für diesen Prozess werden wegweisende Sicherheitslösungen benötigt, die praxisnah und umsetzbar sind.

Der Deutsche IT-Sicherheitspreis, der in diesem Jahr zum vierten Mal verliehen wird, trägt dazu bei, die Innovationskraft der deutschen Wirtschaft zu stärken.

Ob bei Verkehrsleitsystemen, der Stromversorgung oder auch Abrechnungssystemen aller Art – in vielen Fällen ist uns gar nicht mehr bewusst, wie sehr wir uns auf die digitale Technik verlassen. Besonders in der Wirtschaft hat sich die Informations- und Kommunikationstechnologie zum erfolgskritischen Faktor entwickelt. In Deutschland ist mittlerweile fast jedes zweite Unternehmen vom Internet abhängig. Die Integrität und Verfügbarkeit von IT-Systemen bilden eine zentrale Frage der Daseinsvorsorge.

Wirtschaft, Staat und Gesellschaft stehen damit vor einer gemeinsamen Herausforderung. Einerseits müssen wir die Chancen, die sich aus der Technologie bieten, nutzen. Andererseits müssen wir die Risiken dieser Vernetzung minimieren. Der Staat kann dabei nur die Rahmenbedingungen schaffen – zur Gewährleistung von IT-Sicherheit setzen wir auf die Mitwirkung von Wirtschaft und Nutzern. Notwendig sind dafür umsetzbare und praxistaugliche Ideen. Und genau diese Eigenschaften sind herausragende Auswahlkriterien bei der Verleihung des Deutschen IT-Sicherheitspreises.

Aus diesem Grund habe ich die Schirmherrschaft für den IT-Sicherheitspreis wieder gerne übernommen. An dieser Stelle gilt mein besonderer Dank der großzügigen Unterstützung durch die Horst Görtz-Stiftung, die auch in diesem Jahr wieder die attraktiven Preisgelder zur Verfügung stellen konnte.

Die wissenschaftliche Forschung ist ein prägender Baustein zur Schaffung von IT-Sicherheit „made in Germany“, für die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) steht. Die Bedeutung Deutschlands als IT-Standort und Innovationstreiber ist sehr groß, nicht zuletzt durch eine erfolgreiche Grundlagenforschung an den Hochschulen. Um diese starke Position zu erhalten, sind wir alle aufgefordert, die fruchtbare Zusammenarbeit von Wissenschaft, Wirtschaft und Verwaltung zu optimieren und dies auch mit den erforderlichen Investitionen zu unterstützen. Die Preisträgerinnen und Preisträger sind Beispiele dafür, wie wissenschaftliche Forschung im Bereich IT-Sicherheit heute in Zusammenarbeit mit Unternehmen und Verwaltung erfolgreich umgesetzt werden kann.

Ich gratuliere allen Finalistinnen und Finalisten sowie den Preisträgerinnen und Preisträgern sehr herzlich.

Michael Hange
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik

Der Wettbewerb

Mit dem Deutschen IT-Sicherheitspreis möchte die Horst Görtz-Stiftung IT-Sicherheitslösungen „made in Germany“ fördern und bundesweit bekannt machen.

Ziel des Stifters Dr.-Ing. e. h. Horst Görtz ist es, die Innovationskraft der deutschen Wirtschaft zu stärken.

Eine hochkarätige Jury prämiert alle zwei Jahre die besten marktrelevanten Konzepte und Lösungen aus den Bereichen IT-Sicherheit, Kryptografie, System- und Netzsicherheit sowie Abwehr von Cyberangriffen.

Die Bewertung der eingereichten neuen Lösungen und Konzepte erfolgt in einem zweistufigen Verfahren. Zunächst werden die Kurzbeschreibungen aller eingereichten Arbeiten gesichtet. Vielversprechende Bewerbungen dürfen in der zweiten Phase als Langfassung eingereicht werden.

In der zweiten Phase bewertet die Jury die Detailkonzepte nach drei unterschiedlich gewichteten Kriterien: Hauptkriterium ist der Innovationsgrad, außerdem werden die realen Marktchancen und die Nutzbarkeit beurteilt. Anschließend legt die Jury anhand der Bewertungen die zehn besten Arbeiten und darunter die Preisträger fest.

Für den 4. IT-Sicherheitspreis wurden aufgrund der hohen Qualität der besten Einreichungen erstmals vier Arbeiten für die ersten beiden Plätze ausgewählt. Durch die Teilung der Preisgelder ergibt sich folgende Dotierung:

1. Platz (2x): 50.000 Euro
2. Platz (2x): 30.000 Euro

In den Jahren 2006 und 2010 wurden jeweils drei Preise vergeben: Der erste Platz war mit 100.000 Euro dotiert, der zweite Platz mit 60.000 Euro und der dritte Platz mit 40.000 Euro. In 2008 wurde der dritte Preis auf zwei herausragende Einreicher aufgeteilt. Die früheren Preisträger finden Sie am Ende der Broschüre.

Die Preisträger werden immer Ende November bei einer feierlichen Preisverleihung ausgezeichnet und sind dazu angehalten, das Preisgeld für die weitere Forschungs- und Entwicklungsarbeit einzusetzen.

Die Mitglieder des Beirats und der Jury sind anerkannte IT-Sicherheitsexperten aus Wissenschaft und Wirtschaft.

Schirmherr

Michael Hange,
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik

Beirat

Prof. Dr. Joachim Posegga,
Universität Passau

Stefan Strobel,
cirosec GmbH

Thomas Terschersich,
BITKOM

Die Gutachter

Prof. Dr. Günter Müller,
Albert-Ludwigs-Universität Freiburg

Dr. Rainer Baumgart,
secunet Networks AG

Dr. Dirk Hochstrate,
G Data Software AG

Ismet Koyun,
Kobil Systems GmbH

Wolf-Rüdiger Moritz,
Infineon Technologies AG

Prof. Dr.-Ing. Christof Paar,
Ruhr-Universität Bochum

Dr. Gerd Schabhüser,
Bundesamt für Sicherheit in der Informationstechnik

Prof. Dr. Michael Waidner,
TU Darmstadt | Fraunhofer Institut für Sichere Informationstechnologie (SIT)

Dr. Thomas Wille,
NXP Semiconductors GmbH

Klaus Dieter Wolfenstetter,
Deutsche Telekom AG

Die Horst Görtz-Stiftung

Dr.-Ing. e. h. Horst Görtz gründete die gleichnamige Stiftung 1996 mit dem Ziel, Wissenschaft und Technik in Forschung und Lehre zu fördern. Einen besonderen Schwerpunkt legte er dabei schon immer auf die IT-Sicherheit.

HGS
Horst Görtz
Stiftung

Weitere Informationen zur Stiftung finden Sie unter:
http://www.horst-goertz.de


1


2


3


4

5

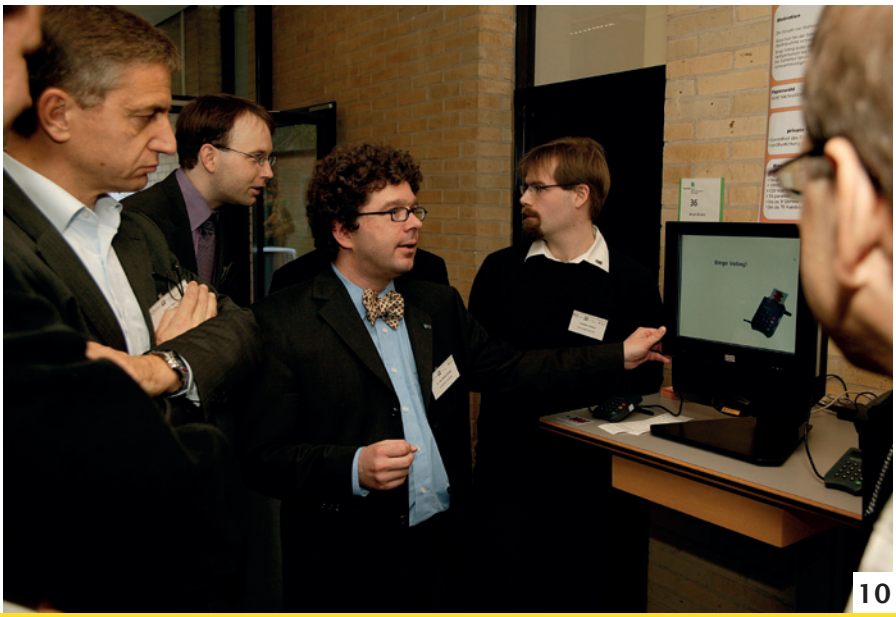
6

IMPRESSIONEN DER PREISVERLEIHUNGEN

7


8

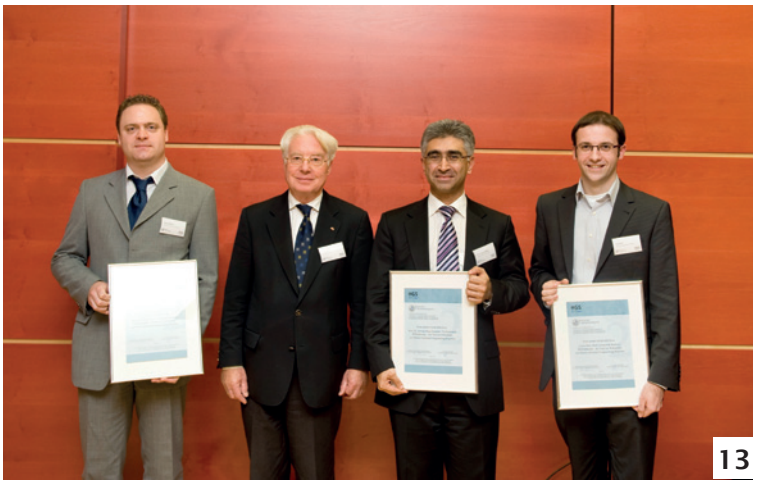

9


10


11

2006 | 2008 | 2010 | 2012

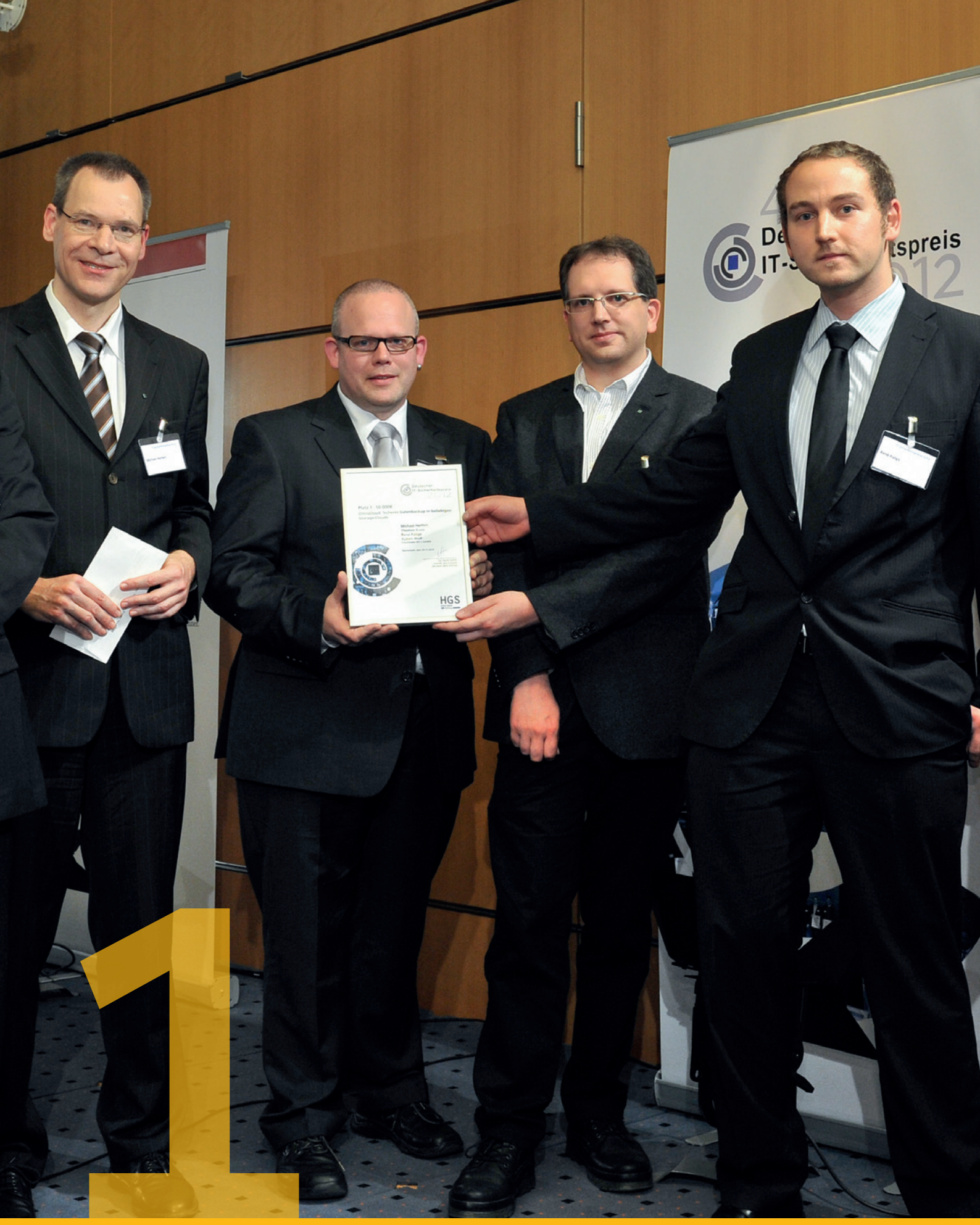
1. Laudator Prof. Dr. Günter Müller von der Universität Freiburg mit Roboter Bruno
2. Prof. em. Dr. Dieter Bartmann (2. v. r., 3. Platz 2008)
3. Dr. Gerhard Schabhüser, BSI
4. Alle Preisträger 2006 (s. S. 21)
5. Alle Preisträger 2008 (s. S. 22)
6. Gastredner Prof. Dr. Jörg Schwenk
7. Prof. Dr. Michael Waidner, Direktor CASED und Fraunhofer SIT
8. Stifter Dr.-Ing. e. h. Horst Görtz
9. Andreas Schuster (3. Platz 2008)
10. Prof. Jörn Müller-Quade (Mitte, 1. Platz 2008)
11. Dr. Erik Dahmen, Prof. J. Buchmann (2. Platz 2008) und Jutta Gerlicher



IMPRESSIONEN DER PREISVERLEIHUNGEN 2010 | 2012

12. 1. Preis: Prof. G. Leander (li.), Prof. C. Paar (re.), Dr. A. Poschmann (nicht im Bild) und Stifter Dr.-Ing. e. h. H. Görtz (mitte)
13. 2. Preis: M. Winandy (li.), Prof. A-R. Sadeghi (3. v. re.), L. Davi (re.) und Dr.-Ing. e. h. H. Görtz (2. v.li.)
14. 3. Preis: Prof. G. Schäfer (li.), Dr. M. Roßberg (re.) und Dr. e. h. Horst Görtz (mitte)
15. Schirmherr M. Hange, Präsident des BSI (li.) und Dr.-Ing. e. h. H. Görtz.
16. Live-Band Toru Jazz

PREISTRÄGER 2012



1

1. Preis:

OmniCloud – Sicheres Datenbackup in beliebigen Storage-Clouds

Das Fraunhofer-Institut SIT hat mit OmniCloud eine Software-Lösung entwickelt, mit der Unternehmen ihre digitalen Daten sicher und preisgünstig in der Cloud speichern können. OmniCloud verschlüsselt die zu sichernden Daten client-seitig vor der Übertragung an einen Cloud-Speicherdienst und schützt Firmengeheimnisse so vor unerwünschtem Zugriff, auch vor dem Cloud-Anbieter selbst. OmniCloud wurde als Lösung für kleine und mittlere Unternehmen entwickelt, die einerseits die Vorteile von Cloud-Speichern nutzen möchten, jedoch kein Budget für den Aufbau einer Private-Cloud-Lösung besitzen. Andererseits stellen sie hohe Anforderungen an die Sicherheit der gespeicherten Daten. Die vorgestellte Lösung besitzt ein hohes Sicherheitsniveau und lässt sich leicht in bestehende Prozesse und Systeme integrieren.

OmniCloud: Sicherheit eines konventionellen Backups mit den Kostenvorteilen eines Cloud-Backups

Zusätzlich zur Verschlüsselung der Dateiinhalte verschleiert OmniCloud die Datei- und Verzeichnisnamen sowie die Verzeichnisstrukturen. Benutzer müssen sich vor dem Zugriff auf OmniCloud authentifizieren. Mittels eines Zugriffskontrollmechanismus lassen sich Zugriffsrechte von Benutzern feingranular definieren. Im Gegensatz zu vielen anderen Verschlüsselungslösungen eignet sich die Software-Lösung für dynamische Teams und berücksichtigt typische Unternehmenssituationen wie Mitarbeiterausfälle und Änderungen von Zuständigkeiten. Möglich wird dies durch eine Trennung von Identitäts- und Schlüsselmanagement. Dadurch lassen sich etwa Vertretungsregelungen ganz einfach realisieren – ohne Passwort-Weitergabe und aufwendige erneute Verschlüsselung der Daten.

OmniCloud unterstützt bereits jetzt eine Vielzahl existierender Cloud-Speicherdienste und lässt sich besonders einfach mit existierender Anwendungs-Software und Backup-Lösungen verbinden – selbst wenn diese keine Cloud-Anbindung vorsehen. OmniCloud selbst benötigt keine Installation auf den jeweiligen Endgeräten, sondern stellt sich dem Benutzer ähnlich wie ein Netzwerklaufwerk dar.

OmniCloud ermöglicht die Umsetzung individueller Speicherstrategien, zum Beispiel die doppelte Sicherung bestimmter Daten in unterschiedlichen Cloud-Speichern oder lokalen Festplatten oder die gezielte Streuung von Datenbeständen über verschiedene Cloud-Speicher hinweg. Außerdem ist OmniCloud in der Lage, verschiedene Cloud-Speicherangebote zu kombinieren. So können Nutzer mehrere vorhandene Cloud-Speicher zusammenschließen und als ein großes Laufwerk in die eigene Unternehmensumgebung einbinden.

Zusätzlich verhindert OmniCloud Dopplungen innerhalb des Backups und sorgt so für Einsparung von Speicherplatz und Kosten. In Unternehmen sind Dateien oft mehrfach vorhanden. OmniCloud findet diese und sorgt dafür, dass nur ein Datensatz in die Cloud wandert.

Gleichzeitig bietet OmniCloud eine Art Umzugsdienst, wie man ihn aus dem Bereich der Stromanbieter kennt. Dadurch verhindert die Software, dass Unternehmen ungewollt von einem Cloud-Anbieter abhängig werden.

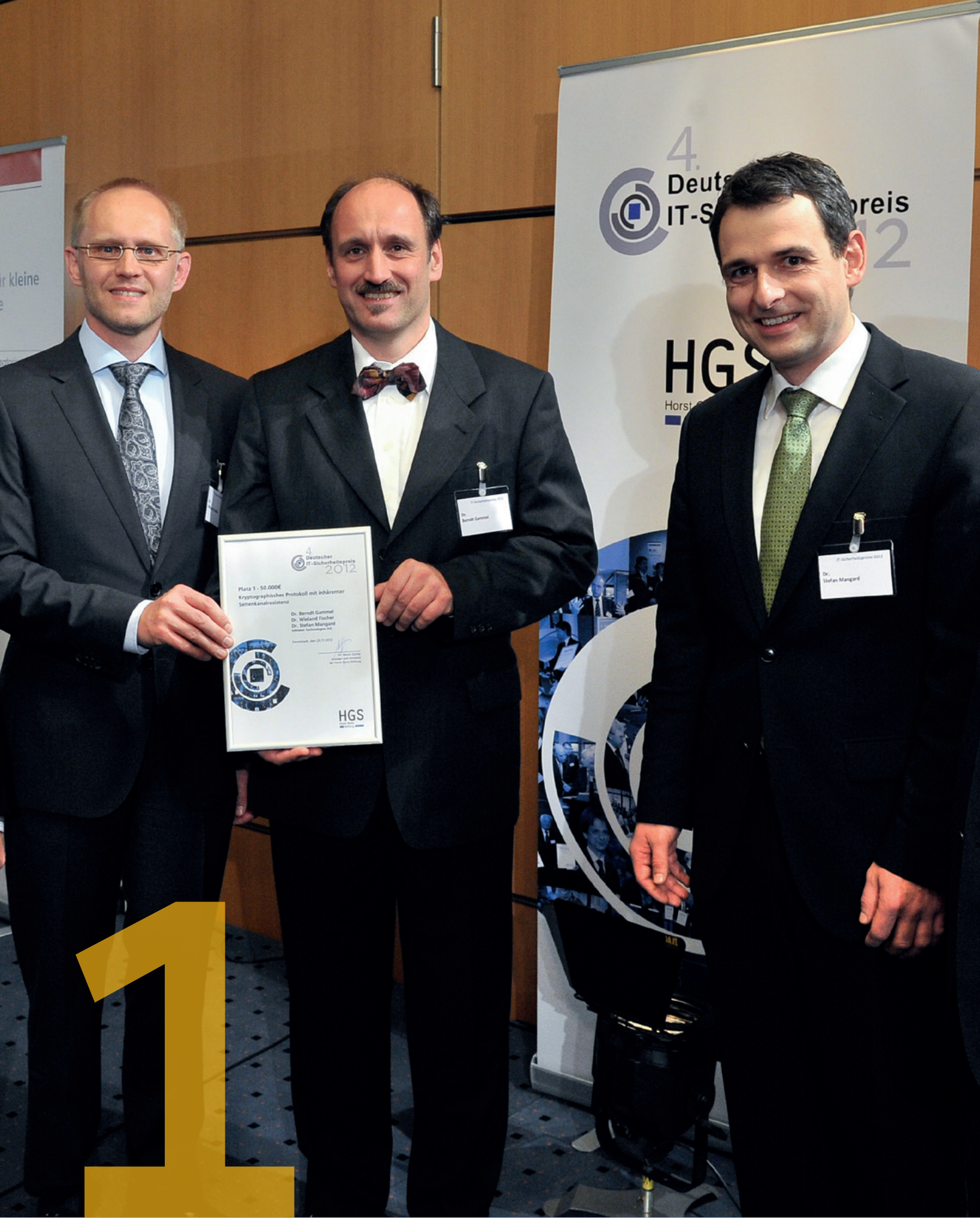
Michael Herfert
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

Thomas Kunz
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

René Palige
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

Ruben Wolf
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

Im Bild von links:
M. Herfert, R. Wolf, T. Kunz, R. Palige


4. Deutscher IT-Sicherheitspreis 2012
HGS
Platz 1 - 50.000€
Kryptographisches Protokoll mit inhärenter Seitenkanalresistenz
Dr. Berndt Gammel
Dr. Wieland Fischer
Dr. Stefan Mangard
HGS
Dr. Berndt Gammel
Dr. Stefan Mangard

1

1. Preis:

Kryptographisches Protokoll mit inhärenter Seitenkanalresistenz

Sicherheits-Chips werden für viele sensible Anwendungen eingesetzt, beispielsweise für elektronische Tickets, Zugangsschlüssel oder Bezahlvorgänge. Deshalb benötigen sie einen Schutz gegen Angriffe durch Hacker, insbesondere gegen sogenannte Seitenkanalangriffe. Die heute bekannten Gegenmaßnahmen sind jedoch oft zu aufwendig, um sie in ressourcenbeschränkten Anwendungen einzubauen. Das trifft insbesondere für kleine kontaktlose Sicherheits-Chips zu, die in Massenanwendungen wie dem öffentlichen Nahverkehr eingesetzt werden. Das vorgestellte Verfahren schafft deshalb Seitenkanalsicherheit direkt auf Ebene des kryptographischen Protokolls. Dieser Ansatz reduziert die Kosten für Gegenmaßnahmen auf ein absolutes Minimum und ermöglicht gleichzeitig hochwertige Anwendungen auf kleinen Sicherheits-Chips in Massenanwendungen.

Nachhaltiger Schutz vor Seitenkanalangriffen für hochwertige Anwendungen auf ressourcenbeschränkten Sicherheits-Chips

Seitenkanalangriffe ermöglichen die Extraktion von geheimen Schlüsseln aus kryptographisch abgesicherten Systemen (s. auch S. 14). Insbesondere trifft dies auf alle Geräte zu, die in einer ungesicherten Umgebung arbeiten, wie Chipkarten, mobile Geräte und auch RFIDs. Für die eingesetzten kryptographischen Authentifizierungs- und Nachrichtenübertragungsverfahren, beispielsweise mit Challenge-Response-Verfahren, MAC und Verschlüsselung, sind sogenannte Blockchiffren wie der Advanced Encryption Standard (AES) von zentraler Bedeutung.

Das vorgestellte Protokoll basiert auf der Idee, die in Blockchiffren eingesetzten Schlüssel niemals mehrfach zu verwenden. Dies verhindert schon im Kern die häufigsten Angriffe durch Mehrfachausführung, stellt aber insbesondere bei der Authentifizierung eine besondere Herausforderung dar. Das neue Protokoll löst diesen Konflikt, indem es für jede gegenseitige Authentifizierung über das Protokoll einen neuen Schlüssel generiert.

Die Innovation liegt darin, die Aufgaben der physikalischen Sicherheit und der kryptographischen Sicherheit auf zwei Komponenten aufzuteilen. Die erste Komponente, eine sogenannte Non-Leaking Map, ist die Hauptkomponente im Schutz gegen Seitenkanalangriffe, während der AES als kryptographischer Algorithmus die kryptographische Stärke liefert. Durch diese Trennung sinken die Implementierungsanforderungen für den AES auf ein Minimum. Das verringert die Angriffsfläche und den Ressourcenbedarf für Gegenmaßnahmen erheblich.

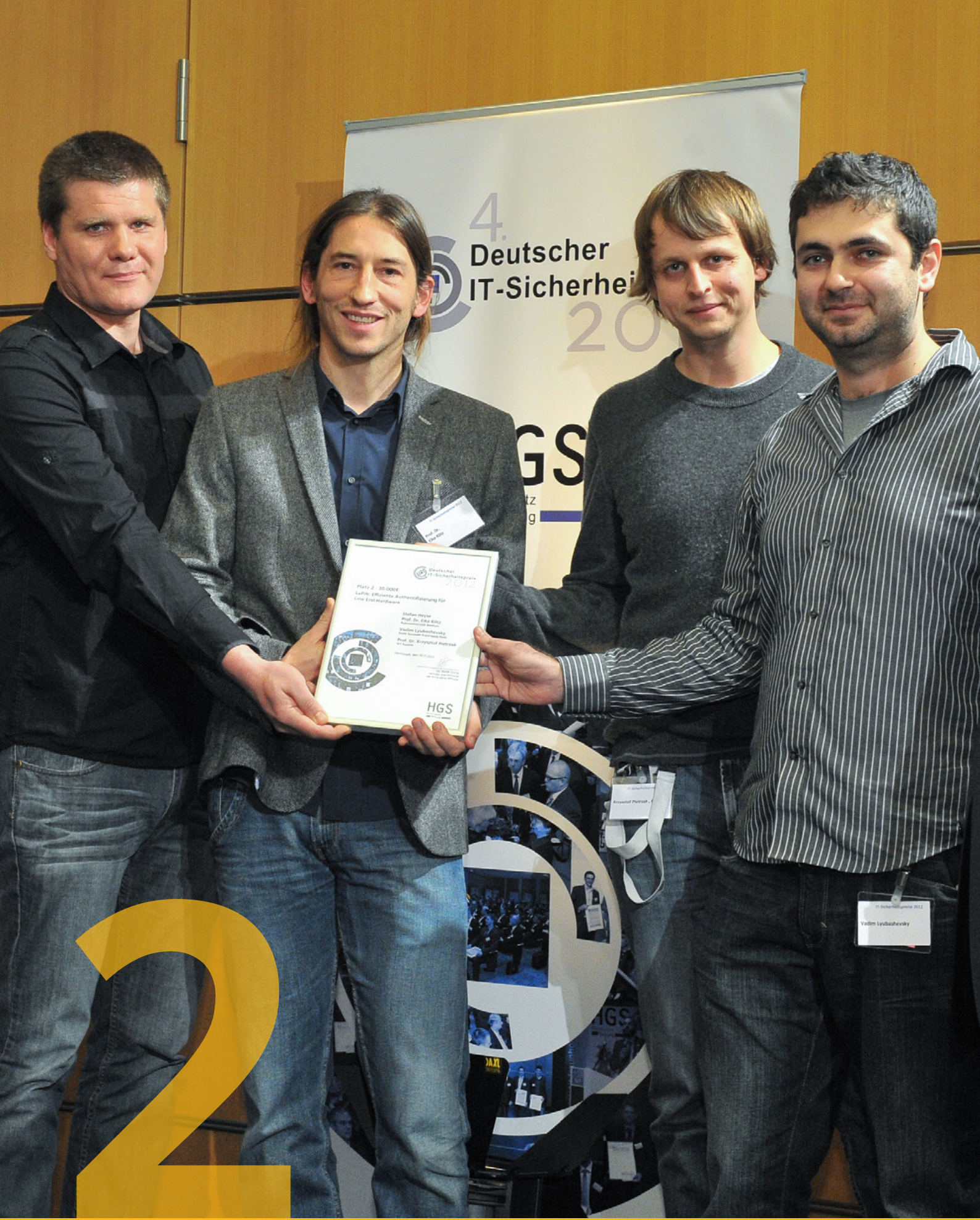
Das neue Protokoll wird bereits im CIPURSE™ open security standard der OSPT Alliance eingesetzt. Dieses internationale Industriekonsortium wurde gegründet, um einen neuen, offenen Standard für sichere Ticketing-Lösungen für den Nahverkehr zu definieren.

Dr. Berndt Gammel
Infineon Technologies AG

Dr. Wieland Fischer
Infineon Technologies AG

Dr. Stefan Mangard
Infineon Technologies AG

Im Bild von links:
W. Fischer, B. Gammel, S. Mangard



2

2. Preis:

LaPiN – Effiziente Authentifizierung für Low-End Hardware

Ein Authentifizierungsprotokoll ist ein interaktives Protokoll, durch welches sich ein Nutzer bei einem Server authentifizieren kann. Nur ein durch den geheimen Schlüssel authorisierter Nutzer soll in der Lage sein, sich erfolgreich zu authentifizieren. In der Regel geschieht dies durch ein sogenanntes Challenge-Response-Protokoll. Hierbei schickt der Server eine kurze zufällige Challenge an den Nutzer, welcher mit einer Verschlüsselung der Challenge antworten muss.

Ein Anwendungsbereich für Authentifizierungsprotokolle, der in den letzten Jahren rapide an Bedeutung gewonnen hat, sind kleine eingebettete Systeme. Bei solchen Systemen sind die verfügbaren Ressourcen wie Strom-, Energie- und Flächenverbrauch extrem beschränkt. Dieser Trend führt zu einer erhöhten Nachfrage nach Authentifizierungsprotokollen mit minimalem Ressourcenverbrauch. Die traditionellen Challenge-Response-Protokolle bieten hier nur bedingt geeignete Lösungen an.

Das LaPiN Protokoll verfolgt einen alternativen Ansatz. Es ist extrem simpel und kann auf einer Fläche implementiert werden, welche um eine Größenordnung kleiner ist, als es für vergleichbar sichere Challenge-Response-Protokolle nötig wäre.

Darüber hinaus ist es beweisbar sicher unter der sogenannten Ring-LPN Annahme, welche nach heutigem Wissensstand selbst von Quantencomputern nicht gebrochen werden kann.

LaPIN: Authentifizierungsprotokoll mit kleiner Implementierung und beweisbarer Sicherheit

Die algebraische Struktur von LaPiN macht es zudem besonders einfach, das System gegen sogenannte Seitenkanalangriffe zu schützen, da effiziente Techniken aus der Public Key-Kryptographie verwendet werden können, wie das sogenannte „blinding“.

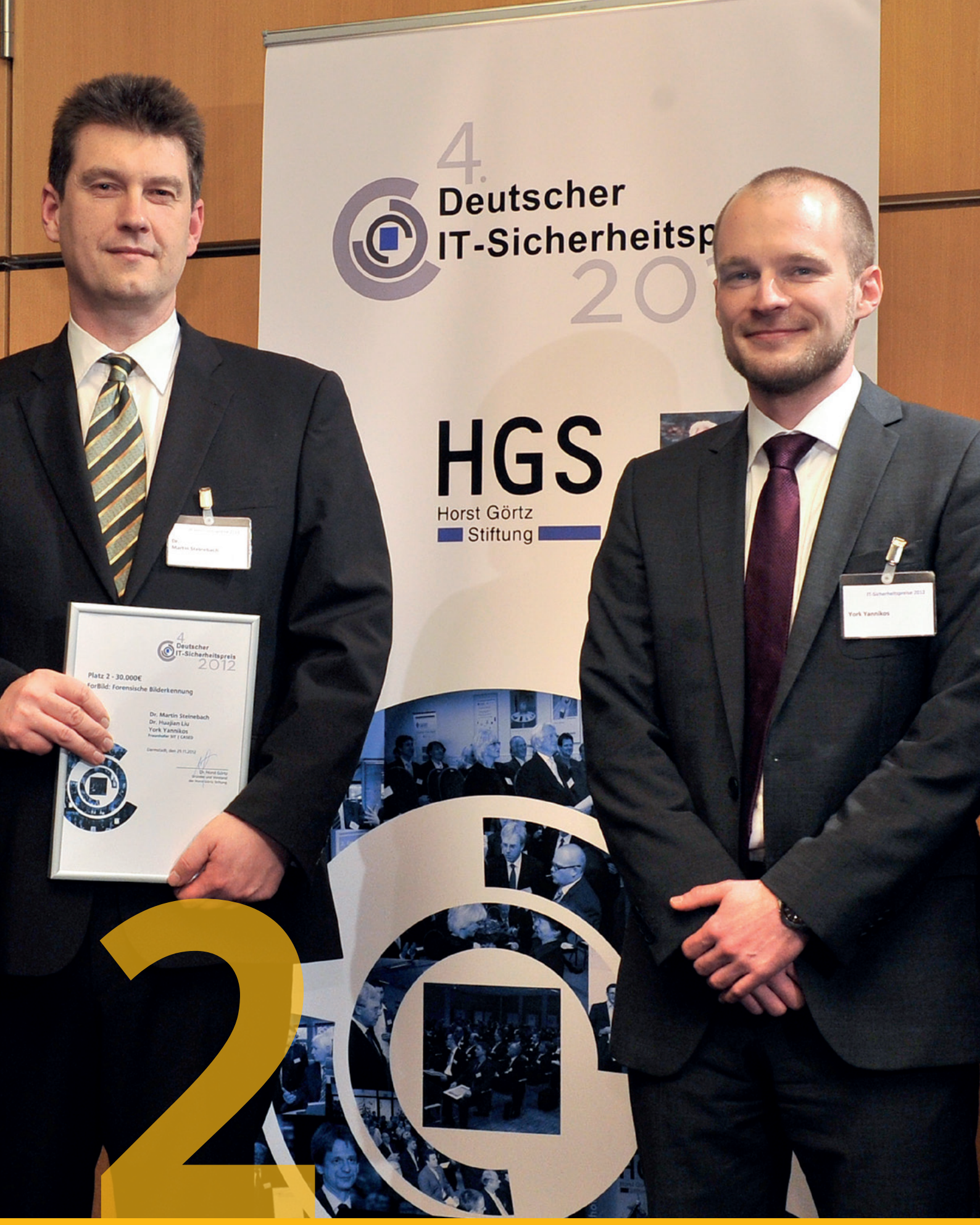
LaPiN wurde auf einer 8-bit basierten Smartcard implementiert (AVR ATmega163), 8-bit Typen sind zahlenmäßig die weltweit meistverbreiteten Prozessoren und kommen typischerweise in Anwendungen zum Einsatz, die Authentifikation erfordern.

Stefan Heyse
Prof. Dr. Eike Kiltz
Ruhr-Universität Bochum

Dr. Vadim Lyubashevsky
École Normale Supérieure Paris

Prof. Dr. Krzysztof Pietrzak
IST Austria

Im Bild von links:
S. Heyse, E. Kiltz, K. Pietrzak, V. Lyubashevsky


4.
Deutscher
IT-Sicherheitsp
HGS
Horst Görtz
Stiftung
Platz 2 - 30.000€
ForBild: Forensische Bilderkennung
Dr. Martin Steinebach
Dr. Huajian Liu
York Yannikos
York Yannikos

2

2. Preis:

ForBild – Forensische Bilderkennung

Ermittler bei Polizei und Staatsanwaltschaft müssen auf der Suche nach illegalem Bildmaterial oft große Mengen von Daten durchsuchen. Um die Massen von Bildern möglichst schnell und effizient automatisch durchkämmen zu können, benutzen sie Methoden und Werkzeuge der IT-Forensik. Die Preisträger haben im Projekt ForBild diese Methoden getestet, erweitert und präzisiert: Über sogenannte robuste Hashs können Bilder schnell und sicher identifiziert werden.

ForBild: Ergänzung zu herkömmlichen Hashs zur Verfolgung von kinderpornographischem Material

Meist handelt es sich bei dem illegalen Bildmaterial um kinderpornographische Bilder. Derzeit erkennt eine automatisierte Suche kinderpornographisches Bildmaterial nur dann zuverlässig, wenn eine identische Kopie dieses Bildes bereits in einer Datenbank hinterlegt ist. Wenn ein Nutzer ein Bild in ein anderes Datenformat umwandelt oder auch nur in einem Bildbetrachter-Programm öffnet und speichert, ist eine Identifizierung über herkömmliche automatische Verfahren nicht mehr möglich.

Eine Alternative beziehungsweise Ergänzung zu diesen etablierten Mechanismen sind sogenannte robuste Hashs. Diese Technik nutzt nicht die Datei-Eigenschaften zur Bilderkennung, sondern orientiert sich an der menschlichen Wahrnehmung: Wenn ein Bild für ein menschliches Auge identisch erscheint, ist auch der Vergleichswert identisch. Damit ignoriert das Verfahren bei der Identifikation einer Bilddatei mögliche Veränderungen der Größe, des Rauschfaktors oder des Dateiformats und konzentriert sich auf optische Übereinstimmungen.

Um einen robusten Hash zu erstellen, skaliert man ein Bild herunter auf 16 x 16 Pixel und wandelt es in 256 Graustufen um. Aus dieser Liste von Graustufen wird der Median ermittelt, also der Wert, der genau in der Mitte der von hell nach dunkel sortierten Graustufen liegt. Die Graustufen werden jetzt in Bits umgewandelt, dafür wird jedem Grau ein binärer Wert zugeordnet: Ein Grau unterhalb des Medians bekommt eine 0, eine Graustufe über dem Median eine 1. So werden die 256 Graustufen in 256 Bitwerte umgewandelt. Sie beschreiben das Bild ausreichend genau und sind robust gegenüber Skalierungen, Umspeicherungen und ähnlichen Veränderungen der Datei.

Das robuste Hashverfahren hat der ForBild-Projektpartner LSK Data Systems in ein CD-Lesegerät integriert. Damit können Ermittler einen Stapel CDs mit Bildmaterial, das sie überprüfen wollen, in das Gerät eingeben und die Daten automatisch überprüfen lassen. Auf der Suche nach einschlägigem Material werden die Bearbeiter so zeitlich und psychisch entlastet.

Dr. Martin Steinebach
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

Dr. Huajian Liu
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

York Yannikos
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt | CASED

Im Bild von links:
M. Steinebach, Y. Yannikos

NOMINIERTE 2012

In alphabetischer Reihenfolge

BizzTrust: Sichere Duale Nutzung von Smartphones und Tablets im Unternehmen

Die BizzTrust-Sicherheitsarchitektur für mobile Endgeräte erlaubt es, Unternehmensdaten sowie die Firmen-Infrastruktur kontextabhängig zu schützen.

BizzTrust basiert auf zwei Mechanismen: 1) Eine Klassifizierung von Daten und Anwendungen (Apps) in die logisch voneinander isolierten Domänen *privat* und *beruflich*. Somit lassen sich einfache, aber erweiterbare Multi-Level-Sicherheitssysteme umsetzen, um private und berufliche Daten strikt voneinander zu trennen. 2) Eine technisch innovative Synchronisation der Zugriffskontrollmechanismen auf die einzelnen Schichten des Betriebssystems, die in dieser Form erstmalig ist. So können Zugriffsregeln aus den semantisch reicheren höheren Schichten (Middleware Erweiterung) auf die sehr mächtigen Zugriffkontrollmechanismen der niedrigeren Schichten (Kernel Erweiterung) abgebildet werden.

Sven Bugiel
Prof. Dr. Ahmad-Reza Sadeghi
Technische Universität Darmstadt | CASED
Fraunhofer SIT

Stephan Heuser
Bhargava Shastry
Fraunhofer SIT | CASED

CloudMiner: Automatisches Tool zur Security- und Datensicherheits-Analyse von Clouds

CloudMiner erlaubt erstmals eine anbieterunabhängige, automatische Untersuchung der Sicherheits- und Datenschutzaspekte beliebiger Clouds. Ein erfolgreicher Test in Public Clouds zeigt, dass mehr Transparenz auf Kundenseite gewonnen und die Vertrauenswürdigkeit gestärkt werden kann.

Ein Informationsfluss aufgrund der Ressourcenteilung zwischen verschiedenen Benutzern würde die Isolations- und Vertraulichkeitsanforderungen verletzen. Um verdeckte Kanäle zu erkennen, nutzt CloudMiner einen neu entwickelten, speziellen Betriebssystemkern. Dieser kommt in verschiedenen Virtuellen Maschinen (VM) gleichzeitig zum Einsatz und kann fehlerhafte Datenbereinigungs-Algorithmen oder Fehler in der Ressourcenaufteilungen ausfindig machen, indem er bestimmte Muster schreibt, anschließend Speicher freigibt (Memory Poisoning) und verteilt nach diesen Mustern sucht.

Sven Bugiel
Stefan Nürnberger
Prof. Dr. Ahmad-Reza Sadeghi
Technische Universität Darmstadt | CASED
Fraunhofer SIT

Steffen Schulz
Ruhr-Universität Bochum
Macquarie University, Australia

Nominierte

Frozen DOM: Neuartiger Schutz gegen Cross-Site Scripting-Angriffe und Web-Malware

Web-basierte Angriffe wie Cross-Site Scripting sind seit zehn Jahren eine akute Bedrohung. Mit der Einführung von HTML5 vergrößert sich das Angriffsfenster: die Deaktivierung von Javascript schützt nicht mehr, neue Ansätze müssen entwickelt werden.

Das Konzept Frozen DOM ermöglicht es, eine neuartige Schutzschicht für Webseiten zur Verfügung zu stellen, ohne Webseiten-Code, Server oder andere Infrastruktur signifkant anpassen zu müssen.

Bei Frozen DOM verhindert eine geladene Javascript-Bibliothek die Ausführung von gefährlichen Skripten oder von HTML5-Elementen. Der Ansatz ist für ECMA Script 5 und 6 realisierbar. Erste praktische Tests haben exzellente Ergebnisse geliefert.

Tilman Frosch
Mario Heiderich
Prof. Dr. Jörg Schwenk
Horst Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum

FSS4CA: Minimierung von Revokationsfolgen

Zertifizierungsdiensteanbieter (ZDA) stellen digitale Zertifikate aus, die zur Identifizierung des Urhebers einer digitalen Signatur dienen. Wird bekannt, dass betrügerische Zertifikate ausgestellt wurden, müssen diese sofort zurückgezogen werden (Revokation). Wird jedoch bei den aktuell verwendeten Verfahren ein ZDA-Zertifikat revoziert, so werden alle Zertifikate, die dieses in Ihrer Vertrauenskette haben und alle damit erstellten Signaturen, ungültig. Wegen der weitreichenden Folgen wird auf die Revokation häufig zulasten der Sicherheit verzichtet.

Das vorgestellte vorwärtssichere Signaturverfahren FSS4CA, minimiert die Auswirkungen der Revokation. Im Gegensatz zu bestehenden Lösungen benötigt FSS4CA weder zusätzliche Infrastrukturen oder vertrauenswürdige dritte Instanzen, noch entsteht ein Mehraufwand bei der Signaturprüfung. FSS4CA erlaubt es, strikte Revokationsmechanismen für die kompromittierten Zertifikate umzusetzen, ohne die Verfügbarkeit zu beeinträchtigen. Durch die konsequente Revokation bei Anzeichen von Missbrauch sowie vereinfachte Revokationsprüfung wird die Sicherheit und die Performanz im Vergleich zu heute etablierten Systemen signifikant erhöht.

Andreas Hülsing
Johannes Braun
Prof. Johannes Buchmann
Martin A. G. Vigil
Technische Universität Darmstadt | CASED

Dr. Alexander Wiesmaier
AGT Group (R&D) GmbH

Persistente Verschlüsselung mit XML-Encryption

Das vorgestellte System setzt XML-Encryption auf innovative Weise ein, um hochsensible Daten auf öffentlichen Cloud Storage-Servern sicher und vertraulich abzulegen. Dadurch wird es möglich, die enormen Kostenvorteile von Cloud Storage auch für sensible Daten zu nutzen.

Die beschriebene Lösung hebt sich durch Flexibilität und Feingranularität hervor. Zusätzlich ermöglicht sie eine partielle Verschlüsselung einzelner Datenblöcke innerhalb einer Datenstruktur und damit die Suche auf unverschlüsselten Metadaten in der Cloud ohne die Notwendigkeit einer vorherigen Entschlüsselung. Ein Schlüssel-Management-Schema erlaubt die gemeinsame Bearbeitung verschlüsselter Dokumente.

Zur Verwaltung, Indizierung und partiellen Auswertungen der Daten ist zusätzlich das Hinzufügen von unverschlüsselten Metadaten möglich.

Meiko Jensen
Christopher Meyer
Prof. Dr. Jörg Schwenk
Juraj Somorovsky
Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum

Sicheres Browser-basiertes Single Sign-On mit SAML Holder-of-Key und RFC 5929

Browser-basierte Single Sign-On (SSO) Protokolle ermöglichen es Nutzern, vom Arbeitsplatz mit nur einem Passwort auf zahlreiche Anwendungen zuzugreifen. Sie besitzen aber auch inhärente Schwachstellen.

Das vorgestellte SSO-Protokoll ist eine effektive Gegenmaßnahme für eine Vielzahl von real existierenden und auf allen sieben Schichten des ISO/OSI-Modells angesiedelten Angriffen. Selbst komplexe Angriffe können vereitelt werden. Es besteht zwar weiterhin die Möglichkeit, dass ein bösartiger Angreifer Assertions erbeutet, jedoch können diese nicht mehr zweckentfremdet eingesetzt werden, da die Identitätsinformationen kryptografisch an den Browser des rechtmäßigen Benutzers gebunden sind. Unter der Annahme, dass TLS sicher ist, kann das Protokoll nach bisheriger Erkenntnis nur dann gebrochen werden, wenn der Angreifer den privaten Schlüssel des Client-Zertifikats besitzt.

Soll die Anonymität des Clients gewahrt bleiben, bieten zwei Bindings die Möglichkeit, ein vom Server durch den SSO-Vorgang erzeugtes Session-Cookie kryptografisch an den TLS-Handshake bzw. das Server-Zertifikat zu binden ohne Informationen über die Identität des Nutzers zu beinhalten. Dies verhindert u. a. die in letzter Zeit sehr populären Session Hijacking-Angriffe.

Andreas Mayer
Adolf Würth
GmbH & Co. KG

Meiko Jensen
Florian Kohlar
Prof. Dr. Jörg Schwenk
Horst Görtz Institut
für IT-Sicherheit
Ruhr-Universität Bochum

Sebastian Gajek
Tibor Jager
Lijun Liao
Karlsruher Institut für
Technologie

Ehemalige Preisträger

1. Deutscher IT-Sicherheitspreis 2006

1. Preis:

Detektor für Trojaner

100.000 Euro erhielt Thomas Dullien, Geschäftsführer der Sabre Security GmbH in Bochum, für eine neue Software, die bislang unbekannte Schadprogramme schnell erkennt.

Thomas Dullien
Sabre Security GmbH

2. Preis:

Echtheitszertifikat für Funk-Etiketten

60.000 Euro erhielten Dr. Erwin Heß und Dr. Bernd Meyer von Siemens Corporate Technology in München für eine Entwicklung, die Informationen auf RFID-Transpondern sicherer macht.

Dr. Erwin Heß
Dr. Bernd Meyer
Siemens AG, CT IC 3

3. Preis:

Eintrittskarte für Datenpakete

40.000 Euro erhielten Dr. Roger P. Karrer und Dr. Ulrich Kühn von den Deutsche Telekom AG Laboratories in Berlin für eine Innovation, die Netzwerke vor Angriffen schützt.

Dr. Ulrich Kühn
Dr. Roger P. Karrer
Deutsche Telekom AG Laboratories

Firmenangaben zum Zeitpunkt der Preisvergabe

Ehemalige Preisträger

2. Deutscher IT-Sicherheitspreis 2008

1. Preis:

Bingo Voting – Verifizierbare Wahlen mit Wahlmaschinen

100.000 Euro erhielten Prof. Dr. Jörn Müller-Quade, Michael Bär, Christian Henrich und Carmen Stüber vom Europäischen Institut für Systemsicherheit, Stefan Röhrich von den NEC Laboratories und Jens-Matthias Bohli, von Rohde & Schwarz SIT für ihr elektronisches Wahlverfahren.

Michael Bär
Christian Henrich
Prof. Dr. Jörn Müller-Quade
Carmen Stüber
EISS, Universität Karlsruhe (TH) - KIT

Jens-Matthias Bohli
NEC Laboratories Europe, Heidelberg

Stefan Röhrich
Rohde & Schwarz SIT GmbH

2. Preis:

Zukunftssichere digitale Signaturen - FutureSign

60.000 Euro erhielten Prof. Dr. Johannes Buchmann und Dr. Erik Dahmen vom Fachgebiet Theoretische Informatik an der TU Darmstadt für ihr langzeitsicheres Signaturverfahren.

Prof. Dr. Johannes Buchmann
Dr. Erik Dahmen
Technische Universität Darmstadt

3. Preis:

PTFinder/PoolFinder und Psylock

40.000 Euro (je 20.000 Euro) erhielten der Bonner Entwickler Andreas Schuster und Prof. Dr. Dieter Bartmann vom Lehrstuhl für Wirtschaftsinformatik II der Universität Regensburg. Schuster für seine Tools, die schädliche Codes im Betriebssystem von Windows-PCs aufspüren und Bartmann für sein Tippverhaltensbiometrie-Tool.

Prof. em. Dr. Dieter Bartmann
Universität Regensburg für Psylock

Andreas Schuster
T-Systems GEI GmbH für PTFinder/PoolFinder

Firmenangaben zum Zeitpunkt der Preisvergabe

Ehemalige Preisträger

3. Deutscher IT-Sicherheitspreis 2010

1. Preis:

PRESENT – Kostenoptimierte Sicherheit für pervasive Rechnerwelten

100.000 Euro erhalten Prof. Gregor Leander von der TU Denmark, Prof. Christof Paar von der Ruhr-Universität Bochum und Dr. Axel Poschmann von der TU Nanyang für ihre Chiffre für kosten- und energiebeschränkte Geräte.

Prof. Gregor Leander
Technical University of Denmark

Prof. Dr. Christof Paar
Ruhr-Universität Bochum

Dr. Axel Poschmann
Nanyang Technological University

2. Preis:

ROPdefender – Ein Tool zur Prävention von Return-Oriented Programming-Angriffen

60.000 Euro erhalten Prof. Ahmad-Reza Sadeghi von der TU Darmstadt sowie Lucas Davi und Marcel Winandy von der Ruhr-Universität Bochum für ihre Arbeit zur Abwehr von auf Return-Oriented Programming basierenden Angriffen.

Prof. Dr. Ahmad-Reza Sadeghi
Technische Universität Darmstadt

Lucas Davi, Marcel Winandy
Ruhr-Universität Bochum

3. Preis:

Secure Overlay for IPsec Discovery (SOLID)

40.000 Euro erhalten Dr. Michael Roßberg und Prof. Günter Schäfer von der TU Ilmenau für ihre Arbeit „Secure Overlay for IPSec Dicovery“.

Dr. Michael Roßberg
Prof. Dr. Günter Schäfer
Technische Universität Ilmenau

Firmenangaben zum Zeitpunkt der Preisvergabe

Bildnachweise

Seite 1:
© daniel aeschlimann photography

Seite 2:
Bundesamt für Sicherheit in der Informationstechnik

Seiten 5 und 6 sowie Seite 7 unten:
CASED | Fotostudio Michels | juergenmai.com

Seite 5 mitte rechts:
Horst Görtz-Institut für IT-Sicherheit

Seite 7:
- Bild 10, 11 und unten rechts: Pressestelle Ruhr-Universität Bochum

- Bild 12 und 13: Horst Görtz-Institut für IT-Sicherheit

Seite 9, 11, 13 und 15:
CASED | juergenmai.com

Impressum

Herausgeber:
Horst Görtz

Anschrift:
Horst Görtz-Stiftung
Taunusstraße 38a
61267 Neu-Anspach
www.horst-goertz.de
horst.goertz@horst-goertz.de
Telefon +49 6081-96 11 93

Redaktion:
Anne Grauenhorst
Center for Advanced Security Research Darmstadt

Gestaltung:
Nina Rimbach
Fraunhofer SIT

4. Deutscher IT-Sicherheitspreis 2012