Fraunhofer-SmartCard-Preis 2014 für
Dr. Jens Bender, Prof. Dr. Marc Fischlin und Dr. Dennis Kügler:
24. SIT-SmartCard Workshop am 5 /6.02. 2014
Laudatio von Dr. Gisela Meister

Lieber Herr Fischlin, lieber Dennis, lieber Jens
liebe Freunde des SIT-SmartCard Workshops,
verehrte Gäste

„Gentlemen do not read each others mail."

Dieses Zitat ist auf Henry Lewis Stimson[1] zurückzuführen, der mit dieser Begründung den Vorläufer der NSA, die sogenannte Black Chamber in den Friedenszeiten nach dem 1. Weltkrieg auflöste. Von solchen sogenannten Gentlemen Agreements ist heutzutage allerdings bei der NSA wohl keine Rede mehr und auch weltweit sollten wir nicht davon ausgehen, dass wir es überall mit Gentlemen zu tun haben.

Umso wichtiger, ist es, dass unsere IT Sicherheits-Systeme[2] und, was insbesondere den Bürger betrifft, unsere elektronischen Ausweissysteme, mit modernen Sicherheitsmaßnamen, geschützt werden, um so unbefugte Verwendung und unbefugtem Ausspähen von sensitiven Daten in der Praxis auszuschließen.

Auf der einen Seite bedeutet das, fortlaufende Sicherheitsuntersuchungen nach dem aktuellen Stand der Technik durchzuführen, und auf der anderen Seite neue Systeme zu entwerfen oder alte zu verbessern, die ein gewünschtes Maß an Sicherheit bieten. Die SmartCard als integraler Teil des Ausweisdokumentes ist dabei eine zentrale Komponente, wird sie doch in Ausweissystemen als Sicherheitsanker und zur Speicherung von sensitiven Daten verwendet.

Ein weiterer Aspekt, der bei offenen Systemen zu Buche schlägt, wie das ja bei elektronischen Ausweissystemen der Fall ist und sein sollte, ist der Interoperabilitätsaspekt: Ausweissysteme, ihre Komponenten und die vorgesehenen Sicherheitsmaßnahmen sollten national, auf europäischer Ebene und international standardisiert sein.

Aber das brauche ich in diesem Kreis ja eigentlich nicht zu erwähnen, gerade dieser Aspekt liegt uns allen hier am Herzen, unter anderen denke ich da an Michael Hegenbarth als ISO /IEC WG 8 Convenor und ehemaliger DIN-

---

[1] Henry Lewis Stimson (September 21, 1867 – October 20, 1950), Außenminister in den Jahren 1929 bis 1933 in den USA und für die Auflösung der Back Chamber verantwortlich zehn Jahre nach deren Gründung, mit der ihm nachgesagten Begründung (siehe Zitat). Die Black Chamber war die erste kryptoanalytische Institution der USA in Friedenszeiten und ein Vorläufer der National Security Agency (NSA).

[2] Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.

Vorsitzender und auch natürlich an mich selber jetzt als frisch gewählte DIN-Vorsitzende unseres Karten-Komitees.

Ich möchte nun den zentralen Punkt meiner Ausführungen formulieren:
Eine hohe Bedeutung für die Qualität von IT Sicherheitssystemen, bei denen Smartcards zum Einsatz kommen und die für sogenannte Government-Anwendungen verwendet werden, liegt in der kompetenten Entwicklung von kryptografischen Sicherheitsprotokollen für SmartCards.

In diesem Zusammenhang möchte ich Ihnen das folgende Zitat etwas neueren Datums, von einem ebenfalls prominenten US Bürger, nicht vorenthalten von dem, zugegebener Maßen, etwas populärwissenschaftlich agierenden Kryptografen, Bruce Schneier[3]:

„It is insufficient to protect ourselves with laws, we need to protect ourselves with mathematics."

Als gelernte Mathematikerin kann und sollte ich da allerdings nur zustimmen.

Um alle die eben dargelegten Aktivitäten zu verfolgen und zu bündeln, bedarf es eines persönlich hohen Engagements und einer hohen Fachexpertise, aber auch strategischer Weitsicht.

Daher freue ich mich ganz besonders, dass ich dieses Jahr auf Bitte unserer SIT-SmartCard-Preisverleihungs-Jury, einer Gruppe bestehend aus drei Experten als 23., 24. und 25. Preisträger des SIT-SmartCard Workshops 2014, unsere Glückwünsche und den SIT-SmartCard-Preis überreichen darf. Unsere Preisträger waren als Team auf all diesen vorher geschilderten Themenfeldern unterwegs und haben nie die zugrundeliegende Strategie aus den Augen verloren: Die Schaffung eines modernen sicheren interoperablen Ausweissystems. Dieses ist

- national ausgewiesen durch den Personalausweis und deutschen Reisepass,
- europäisch unterstützt durch den europäischen ePass und für demnächst geplant durch das eIDAS-Token und
- international standardisiert durch aktive Mitgestaltung der ICAO Standards,

insgesamt designt auf der Basis von kryptografisch und formal nachweislich sicheren SmartCard-gestützten Kryptoprotokollen. Der nächste Schritt, die Nutzung der Protokolle auch für andere eGovernment-Anwendungen, wie z. B. den elektronischen Führerschein, steht kurz bevor. Die weitere Nutzung der Protokolle z. B. im NFC Umfeld ist bereits in Diskussion.

[3] Bruce Schneier (* 15. Januar 1963 in New York) ist ein US-amerikanischer Experte für Kryptographie und Computersicherheit und Autor verschiedener Bücher über Computersicherheit.

Unsere diesjährigen Preisträger heißen:

v.l.n.r.: Prof. Dr. Marc Fischlin, Dr. Dennis Kügler und Dr. Jens Bender

Wenden wir uns zunächst Eurem beruflichen Werdegang zu:

Von Ihnen Herr Fischlin, existiert sogar eine Website (www.fischlin.de), auf die ich an dieser Stelle zusammen mit Ihrem Beitrag und angehängten CV verweisen möchte. Hervorheben möchte ich auch an dieser Stelle Ihre Position als Heisenberg-Professor für Kryptographie und Komplexitätstheorie an der TU Darmstadt. In Ihrer Dissertation befassten Sie sich bereits mit Kryptoprotokollen, präziser mit der Erzeugung von Trapdoor Commitment Schemes. Diese wurde dem FB Mathematik im Dezember 2001 von Ihnen vorgelegt. Erster Gutachter war der bekannte Mathematiker Prof. Schnorr von der Johann Wolfgang Goethe-Universität Frankfurt am Main. Ihre Dissertation und auch Diplomarbeiten vorgelegt dem FB Mathematik und ein Jahr später dem FB Informatik sind im Internet verfügbar und nachlesbar.

Insbesondere möchte ich hier auf Ihre Beiträge zur kryptografisch sicheren Beweisführung der in den elektronischen Ausweisen und kontaktlosen eID-Karten verwendeten PACE und später auch EAC-Kryptoprotokollen und anderer Verfahren hinweisen.

Von Euch, Dennis und Jens, steht als BSI Referatsleiter bzw. Stellvertreter keine Website im Internet zur Verfügung. An dieser Stelle möchte ich jedoch auf Euren gemeinsamen Artikel in diesjährigen SmartCard Workshop-Band zu PACE hinweisen mit den jeweils angehängten CVs. Daher nur in Kürze ein paar für uns interessante Zusatzinformationen:
Dennis Kügler studierte Informatik an der TU Darmstadt und promovierte im Bereich „Kryptographie“ 2002 mit dem Titel „Ein missbrauchsfreies anonymes

elektronisches Zahlungssystem", die beiden Gutachter Prof. Buchmann und Prof. Beutelspacher sind dem SmartCard Workshop-Publikum auch bestens durch diverse Vorträge bekannt.
Die Dissertation von Jens Bender an der Bergischen Universität Wuppertal erfolgte 2006 im Grundlagenbereich der Mathematik und zwar zur Darstellung endlich erzeugter Algebren – im Internet nachzulesen.
Dennis Kügler und Jens Bender haben zahlreiche Artikel zur Nutzung von PACE und EAC im Zusammenhang mit dem Personalausweis veröffentlich. Beide haben auch hier bereits zu diesem Thema beim SmartCard Workshop referiert und waren sehr aktiv präsent in nationalen, europäischen und internationalen Gremien und auch bei Kongressen[4]. In Verbindung mit der deutschen SmartCard-Sicherheits-Industrie gab es fortlaufend Aktivitäten seit circa Ende 2004[5] und teilweise auch in Verbindung mit der französischen Industrie, mit dem Ziel PACE und EAC für Government Anwendungen national, europäisch und später auch weltweit zu etablieren. Aus Sicht unserer DIN-Standardisierungs-aktivitäten hätten wir uns allerdings manchmal eine noch eine intensivere Abstimmung gewünscht.

Nach Ansicht der Jury ist neben den bereits zitierten Aktivitäten und insbesondere den Veröffentlichungen im Rahmen des Personalausweises die gemeinsame Arbeit von allen Preisträgern zur Initiierung und zum Sicherheitsbeweis der Protokolle PACE und EAC hervorzuheben[6]. Es ist meines Erachtens ein bisher einmaliges Vorgehen in der Standardisierung von Protokollen, das auch zeitnah mit deren Standardisierung ein kryptografischer Sicherheitsbeweis vorgelegt wurde. Dieses Vorgehen setzt Maßstäbe für die Standardisierung und Nutzung weiterer Protokolle.

Als aktuelle Preisträger darf ich Euch an dieser Stelle den Preis für die bisher erbrachten Leistungen im Bereich „Sicherheit und Standardisierung von kryptographischen Protokollen" übergeben und möchte Euch bitten, Euch weiterhin so eindrucksvoll und mit Freude zu engagieren.

Ich möchte meine Ausführungen mit einem alten Sprichwort schließen, woran man unschwer erkennen kann, dass sich unsere Vorfahren auch schon mit Security und Privacy beschäftigt haben, jedoch noch zu ganz anderen Schlussfolgerungen kamen:

„A secret between two is a secret of God, a secret among three is everybody's secret."

Wir danken Euch respektvoll für Eure große Leistung und wünschen Euch für die bevorstehenden Jahre weiterhin viel Freude, Gesundheit und Glück.

---

[4] im Einzelnen: DIF, DIN NIA 17.3/4, CEN TC 224 WG 15/WG 16, BIG, ISO/IEC SC 17 WG 3 und ICAO, um nur die meisten zu nennen.
[5] Jens Bender seit 2007
[6] siehe z.B: *Security Analysis of the PACE Key-Agreement* Protocol, Lecture Notes in Computer Science, Springer-December 18, 2009