Fraunhofer SmartCard-Preis 2009 für Bernd Kowalski

19. SIT-SmartCard Workshop am 3. Februar 2009 in Darmstadt Laudatio von Michael Hegenbarth

Lieber Bernd,
geschätzte Freunde des SIT-SmartCard Workshops,
verehrte Gäste!

Auch dieses Jahr freue ich mich wieder, der Bitte der SIT-SmartCard-Preisverleihungs-Jury folgen zu dürfen, dem Preisträger des SIT-SmartCard-Workshops 2009 unsere Glückwünsche und den SIT-SmartCard-Preis zu überreichen. Der diesjährige Preisträger heisst Bernd Kowalski.

Viele der Anwesenden kennen sich mit den facettenreichen Aspekten der Chipkarten bestens aus, was eigentlich nicht sonderlich nennenswert sein sollte, denn immerhin befinden wir uns ja auf dem SmartCard Workshop. Was ebenfalls kaum jemanden von Ihnen zum Staunen bringen könnte, ist die Fähigkeit einer Chipkarte, Authentikations- und Verschlüsselungsfunktionen gemäß international genormter Verfahren durchzuführen. Hört sich heutzutage alles ziemlich normal an, war es aber durchaus nicht vor fast 25 Jahren. Wie Einschneidendes zu diesem Thema damals begonnen hatte, ist ein besonderer Teil der beruflichen Lebensgeschichte unseres heutigen Preisträgers.

Nachdem Bernd Kowalski sein Studium der Elektrotechnik/Nachrichtentechnik an der Rheinisch-Westfälischen TH in Aachen mit Abschluss Diplom-Ingenieur absolviert hatte, trat er im Jahr 1982 in den Dienst der Deutschen Bundespost (DBP) ein. 1984 bewarb er sich beim Fernmeldetechnischen Zentralamt (FTZ) in Darmstadt um eine Referenten-Stelle im Bereich Text- und Datenübermittlungssysteme.

Die entscheidende Kick-off-Situation für ihn folgte gleich ein Jahr später. Das damalige Bundesministerium für das Post- und Fernmeldewesen (BPM) – woraus unter anderem in den 90'er Jahren Zug um Zug die Deutsche Telekom hervorgangen war – wies das FTZ im August 1985 an, sich um das Thema Sicherheit in der Datenkommunikation zu kümmern, mit dem Ziel, eventuell aus den künftigen FTZ-Untersuchungen und -Vorschlägen kommerziell verwertbare Produkte und Dienstleistungen abzuleiten.

Der Auftrag des BPM landete auf Bernd Kowalski's Schreibtisch und löste bei ihm eine Mischung von Faszination, Begeisterung, Innovationsfreude, Pioniergefühl und letztlich Unternehmergeist aus, von alledem er seit jeher nichts eingebüßt hat. Er stellte ein relativ kleines Team aus Kollegen zusammen, suchte sich relevante Berater von externer Seite (u.a. damalige Mitarbeiter der GMD Darmstadt) und packte das neue Thema zielgerecht an.

Sehr gelegen kam ihm dabei, dass das Forschungsinstitut des FTZ just im selben Jahr eine neue Mathematikgruppe gegründet hatte, die zwar vornehmlich die Aufgabe hatte, die GSM-Verschlüsselungsverfahren fachlich zu begleiten und innerhalb Europa zu harmonisieren, sich jedoch ab sofort auch für Kowalski's Projekt assistierend zur Verfügung stellte.

Einen ersten Meilenstein konnte Kowalski gleich im Folgejahr vorweisen, was auch einer guten Kooperation mit der GMD zu verdanken war. 1986 war die weltweit erste öffentliche Teletex-Übermittlung – Teletex war der komfortable und wesentlich schnellere Nachfolger des Telex - von digital signierten Nachrichten verfügbar, wofür das asymetrische RSA-Verfahren eingesetzt wurde. Die Kunden-Chipkarte nahm dabei die Rolle eines sicheren Speichers für den geheimen Schlüssel ein. Die Kombination aus dem öffentlich und international verfügbaren Teletex-Dienst und einem public-key-Verfahren war die Geburtsstunde der IT-Sicherheitsdienstleistungen der DBP, wohlgemerkt vor knapp einem Vierteljahrhundert!

Dieser Pionierschritt reichte Herrn Kowalski keineswegs. Im Jahr 1986 waren die CCITT-Normungsaktivitäten (Comité Consultatif International Télégraphique et Téléphonique) für den elektronischen Mitteilungs- und Auskunftsdienst (X.400- und X.500-Serien) in vollem Gange. Kowalski überzeugte die DBP, dass in die CCITT-Standardisierung die soeben von der DBP erfolgreich hochgefahrenen Techniken für sichere Textübertragung Einzug halten sollten. Die Idee war dabei so einfach, wie plausibel und bestechend, nämlich „go international" mit dem

aufkeimenden IT-Sicherheitspflänzchen der DBP. Kowalski machte sich im CCITT per Lobbying für seinen Teletex-Dienst eine gewisse Neidstimmung zunutze. Warum sollte nur Teletex mit neuesten Sicherheitsverfahren kombinierbar sein, und nicht auch die künftigen neuen „message-store-and-forward"-Dienste? Seine Taktik führte zum Erfolg! CCITT akzeptierte die Idee für einen gesicherten Zugang zu Verzeichnisdiensten (X.500-Serie) und die dafür erforderliche Schlüsselmanagementfunktion für Electronic Mail (X.400-Serie).
Um das Ziel X.509 zu erreichen, mussten noch zwei bedrohliche Hürden genommen werden. Eine erste kritische Situation kam in einem CCITT-Meeting in Ottawa auf. Man hatte zwar Sicherheitstechniken mittels Kryptoverfahren akzeptiert, man stritt aber darum, ob es public-key oder private-key Verfahren werden sollten. Der Streit eskalierte zu einer Kampfabstimmung um die Frage „DES oder RSA". Die Patt-Situation wurde dadurch aufgelöst, dass Kowalski für RSA votierte. Das Resultat dieser wenigen, sehr spannenden Abstimmungsminuten darf als Startpunkt für die de-facto-Normung eines ersten asymmetrischen Verfahrens und die Standardisierung der damit verbundenen Authentikations-, Signatur- und Verschlüsselungsverfahren interpretiert werden.

ISO/TC97/SC21 übernahm dann damals zeitgleich den vorliegenden Entwurf zu X.509, was zu einem weiteren kritischen Augenblick im Jahr 1987 führte. Auf Betreiben eines großen Mitgliedstaates mußte die Normung von Kryptoverfahren bei ISO ausgesetzt werden. Damit entstand die Diskussion, ob der Standard X.509, der sich kurz vor seiner Fertigstellung befand, überhaupt in der vorliegenden Form hätte weiterverfolgt werden können. Inzwischen war jedoch die Lobby für X.509 derart stark geworden, dass ein Stopp vermieden werden konnte.

X.400/X.500 wurde im Jahr 1988 am Ende der turnusgemäßen Studienperiode vom CCITT angenommen. Das Pendant zu X.509 bei ISO wurde als ISO 9594-8 im gleichen Jahr internationaler Standard.

Nennenswert bei den genannten Entwicklungen war die damals von Kowalski in Auftrag gegebene sogenannte GMD-Studie (1986-1987). Diese hatte die international lancierte Haltung der DBP zum Einsatz der asymmetrischen Kryptoverfahren bestätigt und sie bei ihren weiteren Überlegungen hinsichtlich Entwicklung dementsprechender Produkte bestärkt.

Ein solides Fundament war erreicht worden, so dass sich fortan das Engagement darauf konzentrierte, wie man die international genormten Sicherheitsverfahren in geschäftlich interessante Produkte und Dienstleistungen umsetzen kann.

Zur bestmöglichen Erreichung von IT-Sicherheit hatte man den Anspruch, dass die public-key-Algorithmen innerhalb der Chipkarte ablaufen sollten, damit der secret-key die Karte nicht verlassen muss. Kowalski kooperierte eng mit den Firmen VALVO und Siemens-Halbleiter, mit dem Ziel, so bald als möglich einen „RSA-fähigen" Chip auf die Beine zu stellen, welcher auch

den Dimensionsanforderungen einer standardkonformen Chipkarte genüge leisten sollte. 1992 war es dann so weit: der weltweit erste RSA-Chipkarten-taugliche Chip war verfügbar.

Inzwischen hatte Kowalski seine Aufgaben in Richtung Sicherheitsproduktentwicklung fokusiert. 1990 hatte die Deutsche Telekom das Produktzentrum TeleSec in Siegen gegründet und ihn mit der Leitung dieser Einrichtung beauftragt. Es erhielt die Aufgabe neue Dienstleistungen und Produkte im Bereich IT-Sicherheit bereitzustellen.

Als wesentliche Meilensteine der Telesec können genannt werden:

- **1993 entstand das erste TrustCenter, möglicherweise sogar weltweit erste, welches X.509-konform war und nicht nur Zertifikate erstellte, sondern auch die Personalisierung von Karten durchführen konnte,**

- **1994 wurde das erste X.509-konforme Chipkarten-Betriebssystem der Telekom (TCOS) verfügbar, und somit die erste marktreife SmartCard für digitale Signaturen,**

- **1998 wurde TCOS gemäß ITSEC E4 zertifiziert und als Signaturgesetz-konform bestätigt.**

Bernd Kowalski führte die Telesec-Geschäftseinheit bis 2002. Im gleichen Jahr wechselte er zum Bundesamt für Sicherheit in der Informationstechnik (BSI) und leitet seitdem die Abteilung 3 mit den Aufgabenbereichen Zertifizierung, Zulassung, Konformitätsprüfungen und Neue Technologien.

Ich habe nun die Ehre, lieber Bernd, Dir in Vertretung der Jury den SIT-SmartCard-Preis zu überreichen, für Deine Verdienste bei der internationalen Nutzbarmachung assymmetrischer Schlüsselverfahren für praktikable und marktmäßig interessante IT-Sicherheits-Techniken unter Miteinbeziehung von kryptosystem-verarbeitbaren Chipkarten.

Wir alle wünschen Dir für die bevorstehenden Jahre Deines Wirkens viel Freude, Gesundheit und Glück. Herzlichst alles Gute für Deine Zukunft!

Laudatio von Michael Hegenbarth, 03.02.2009