35. Infobrief 2008

Nachfertigung von Schlüsseln

Fleißige Leser des Info-Briefs werden sich jetzt die Frage stellen, kann es zu diesem Thema noch Neues geben? Wir wollen Ihnen aufzeigen, dass es dahingehend noch erheblich Neues, man könnte auch sagen, revolutionär Neues gibt. Das Schlüsselwort heißt: KEYMAX-ScanTower.

Zunächst ein paar Worte zum Hintergrund:

Bei einfachen Schließzylindern, die nicht mit dem Sicherungsmerkmal einer Sicherungskarte versehen sind, war es bisher möglich, bei einem Schlüsselfachgeschäft/Schlüsseldienst, unter Vorlage eines der zu dem Schließzylinder gehörenden Schlüssel, einen oder mehrere Nachfertigungen zu erlangen. Der Schlüssel wurde in einer Kopierfräsmaschine eingespannt (dabei entstanden Spannspuren), er wurde mit einem Abtastfinger abgetastet (mechanischer Abtastvorgang mit Abtastspuren), oder es erfolgte ein Abtasten mit einem gebündelten Lichtstrahl (Laserabtastung), parallel dazu wurden ein oder mehrere Nachschlüssel gefertigt. Auch bei der Laserabtastung musste der Schlüssel eingespannt werden, obwohl es dabei keine Abtastspuren mehr gab.

Zu Schließzylindern, die über eine Sicherungskarte verfügten, konnte auf diesem Wege in der Regel kein Nachschlüssel erlangt werden. Dies galt auch für Schließzylinder, die zu einer Schließanlage gehörten. Möglich war es jedoch aufgrund eines Gerichtsurteils, Schlüssel zu sogenannten Z-Anlagen (Zentralschließanlagen wie sie üblicherweise in Mietshäusern vorkommen, d.h. mit dem Wohnungsschlüssel konnte auch die Haustür, das Garagentor usw. betätigt werden) zu erhalten.

Grund dafür, dass die Schlüsseldienste zu Anlagen mit Sicherungskarte keine Schlüssel fertigen konnten, war, dass die Rohlinge auf dem Markt nicht zu erhalten waren.

Vor einigen Jahren kam aus dem Süddeutschen Raum eine Maschine auf den Markt, die auch derartige Rohlinge aus einem Messingblechstreifen (Smiley) fräste. Auch dazu gab es Widerstände aus den Reihen der Schlossindustrie, die jedoch nicht den gewohnten Schutzeffekt erbrachten. Um jeglichen weiteren Gerichtsprozessen und Attacken der Schlossindustrie zu entgehen, hat der Hersteller und Vertreiber dieser Maschinen sich kurzum nach Teneriffa abgesetzt. Von dort aus kann er ungehindert den deutschen und europäischen Markt beliefern.

Zum Hintergrund: Es handelt sich hier auch um eine Art Schlüsselkopierfräsmaschine, diese greift jedoch zunächst nur das Schlüsselprofil, d.h. den Rohling mit seinen Längsnuten ab und fräst dann, nicht wie der Hersteller mit speziellen Formfräsern, sondern mit einem ganz dünnen Scheibenfräser aus diesem Blechstreifen den Rohling heraus. Anschließend können mit einer normalen Kopierfräsmaschine oder auch einer programmierbaren Maschine nach Code die Schafteinschnitte gefräst werden.

Man erlangt so unter Vorlage eines Musterschlüssels einen Schlüssel zu einem Schließzylinder oder einer Schließanlage, der ansonsten nur mit einer Sicherungskarte zu erhalten wäre. Die Verantwortung evtl. Verletzungen von Schutzvorschriften hat der Hersteller der Maschine kurzum auf den Betreiber abgewälzt.

Die Problematik für den Hersteller und der Vorteil für die Kriminaltechnik waren, dass Spuren an dem Musterschlüssel entstanden, die nachgewiesen werden konnten.

Der Hersteller hat seine Maschine noch effektiv erweitert, in dem sie programmgesteuert aus einem Lichtbild (Handy), das den Schließzylinder bzw. den Schlüsselkanal und anschließend auch den Schlüssel abbildete, die Grundlage für die Herstellung eines Nachschlüssels nahm.

Nicht recht durchgesetzt hat sich dieses System wohl auch wegen des hohen Preises.

Nun hat der Hersteller einen neuen Vorstoß auf den Markt unternommen und anlässlich der Security Sept. 08 in Essen auch vorgestellt. Das KEYMAX-ScanTower-System kann einen Schlüssel „lesen“ in dem dieser in eine Haube hineingesteckt und eingescannt wird. Dies macht nicht mehr der Schlüsseldienst, sondern der Verbraucher an dem Tower selbst, der z.B. im Kaufhaus, der Fußgängerzone, im Baumarkt usw. aufgestellt sein wird. Er erhält danach eine Mail über die Erstellungskosten und kann dann entscheiden, ob er den Schlüssel haben will oder nicht. Bei Ablehnung entstehen keine Kosten (darauf wird ausdrücklich hingewiesen). Auf diese Art und Weise wird, so ist es ausdrücklich in der Homepage angegeben, ist es möglich, einen Schlüssel zu Schließanlagen zu erhalten.

Eine evtl. Maßungenauigkeit, die bei dem Scannen auftreten könnte, wird von dem Programm, indem sämtliche Profile, also auch die zu codierten Einzelschließungen und Schließanlagen gehören, kompensiert.

Versuche, die im Rahmen eines Probelaufs durchgeführt wurden, brachten eindeutige Ergebnisse. Der so erhaltene Schlüssel passte, ein Schließen war problemlos möglich.

Dieses Keymax-System wird auch den Schlüsseldiensten zum Kauf oder zum Leasing angeboten. Von uns durchgeführte Rückfragen bei verschiedenen Schlüsseldiensten brachten einerseits entrüstete Ablehnung (meist waren dies gut sortierte Fachgeschäfte), andererseits jedoch auch Zustimmung, meist bei kleinen Schlüsseldiensten die das auf Vorrathalten der Vielzahl von Rohlingen umgehen wollen.

Es wird also in Zukunft nicht mehr auszuschließen sein, dass vermehrt auch zu Schließzylindern mit Sicherungskarte, unkontrolliert erlangte Nachschlüssel existieren.

Dies stellt nach unserer Auffassung ein erhebliches Sicherheitsrisiko für die Betreiber der Schließanlagen dar, insbesondere, weil es nicht möglich ist, in kurzer Zeit die Vielzahl von mechanischen Schließanlagen, die sich in Tausenden von Gewerbeunternehmen, kleinerer bis größter Art befinden, auszutauschen.

Sicherheit lässt dieses System auch dort vermissen, wo wir sie uns alle mehr oder weniger wünschen, z.B. auf Flughäfen, Kernkraftwerken o.ä. Bereichen. Auch die Wirtschaft kann sich nicht mehr sicher sein, dass ihre Pläne für ein bestimmtes Produkt mit einem solchen Schlüssel „geklaut“ werden.

Die Industrie hat in Kenntnis dieser Entwicklung, dies hat auch die Security dieses Jahr gezeigt, massiv nachgelegt. Es gibt inzwischen von mehreren Herstellern zu bestehenden Schließanlagen Ergänzungen mit mechatronischen Zylindern, darüber hinaus können in relevanten Zugangstüren die mechanischen Schließzylinder auch gegen rein elektronische Schließsysteme ersetzt werden.

Handeln ist jedoch zwingend gefordert.

Vonseiten der Kriminaltechnik stellt sich die Sache insgesamt jedoch nicht problematisch dar.

Ein Schließzylinder, der mit einem derartigen Schlüssel zur Tatausführung geschlossen wurde, erhält an den Funktionsteilen ein abweichendes Spurenbild gegenüber dem Spurenbild, das mit den passenden und ständig verwendeten Schlüsseln erzeugt wird.

Die optimale kriminaltechnische Untersuchung erfordert jedoch den Einsatz eines Raster-Elektronen-Mikroskops um abweichende Spurenmerkmale z.B. auf den Kuppen der Kernstifte erkennen und bewerten zu können. In unserem Prüflabor werden alle Schließzylinder seit 10 Jahren mit dem REM untersucht.

KeeLoq-System

In den ersten Monaten des Jahres 2008 fand eine Veröffentlichung statt, dass unter der Leitung von Prof. Christoph Paar der Uni Bochum der Quellcode des KeeLoq-Systems geknackt sei.

Es war in der Presseveröffentlichung des Weiteren ausgeführt, dass eine Vielzahl von Fahrzeugfernbedienungen zum Öffnen und Schließen, Bediensysteme zu Einbruchmeldeanlagen und elektronischen Schließzylindern im Objektbereich, insbesondere auch zu Fernbedienungen für Garagentüröffner, nicht mehr sicher seien. Es war ferner ausgeführt worden, man könne das Signal bis zu einer Entfernung von 100 m auffangen und klonen. Das Abfangen von nur zwei Nachrichten erlaube es, einen Schlüssel (Signal) zu kopieren und sich den Zugang zum Haus oder dem Fahrzeug zu verschaffen. Ferner sei eine Manipulation möglich, sodass der „Schlüssel“ des Berechtigten nicht mehr funktioniere.

Zu der Technik war ausgeführt worden, dass ein Funktüröffner aus einem aktiven RFID-Sender, wie er typischerweise in Autoschlüssel eingebaut wird, und einem Empfänger, der sich in der Fahrzeugsteuerung befindet, besteht. Beide Seiten, Sender und Empfänger, verschlüsseln ihre Funk-Kommunikation mit der KeeLoq-Chiffre. Die Angriffe der Bochumer Gruppe ermöglichen die Rückgewinnung des geheimen Schlüssels (Quellcode) sowohl auf der Sender- als auch auf der Empfängerseite, durch die Messung der elektrischen Energie, die die Geräte verbrauchen. Unter Anwendung der sogenannten Seitenkanalanalyse konnten die Forscher den Herstellerschlüssel, eine Art Generalschlüssel, für sämtliche Produkte einer Serie aus dem gemessenen Stromverbrauch des Empfängers zurückgewinnen. Der Angriff der Seitenkanalanalyse und die spezielle Eigenschaft der KeeLoq-Chiffre kombiniert, kann auf alle bekannten Ausführungen der Chiffre, die in gängigen Systemen eingesetzt wird, angewandt werden. Das KeeLoq-System wird seit Mitte der 90er Jahre standardmäßig in Zugangskontrollsystemen eingesetzt. Es ist eines der am weitesten verbreiteten Verfahren in Europa und den USA. Neben der häufigen Verwendung in Garagentoröffnern und Gebäudezugangskontrollsystemen wird KeeLoq auch von mehreren Automobilherstellern wie Toyota, Lexus und andere Fahrzeuge als Diebstahlschutz eingesetzt.

Bisherige Recherchen haben ergeben, dass jedoch keine Geräte, die der Nutzer einsetzen könnte, (noch nicht) auf dem Markt angeboten werden. Weiterhin hat sich ergeben, dass eine Vielzahl von Fahrzeugherstellern, im Wesentlichen bei diebstahlrelevanten Fahrzeugen mit Ausnahme eines japanischen Herstellers der dort auch genannt ist, andere Systeme verwendet, so dass hier keine Gefahr besteht.

Fahrzeughersteller, die das KeeLoq-System eingesetzt haben, ließen mitteilen, dass man auf Alternativsysteme in den zukünftigen Baureihen zurückgreifen will. Damit ist jedoch die Gefahr bei bestehenden Fahrzeugen, bei denen diese Systeme verbaut wurden, nicht eliminiert.

Wesentlich erscheint jedoch insbesondere bei der Vielzahl von Torantrieben von Garagentoren, bei denen überwiegend das KeeLoq-System eingesetzt wird, dass hier ein echter Sicherheitsmangel vorherrscht, den der Garagenbesitzer eigentlich nur dadurch eliminieren kann, dass er entweder ein anderes Torantriebssystem einsetzt, in der Garage keine wertvollen Gegenstände lagert, sein Auto abschließt und, soweit eine Tür zwischen Garage und Wohnhaus existiert, diese ebenfalls verschließt.

Insoweit bringt das System für den Nutzer aufgrund der mangelnden Sicherheit den Effekt, um- oder nachzurüsten bzw. weitere Sicherheitsmaßnahmen zu ergreifen.

Problematischer sieht es bei Alarmanlagen aus, die mit diesem System arbeiten. Alarmanlagen im Objektbereich werden überwiegend dort eingesetzt, wo hochwertiges Gut, zusätzlich zur mechanischen Sicherung abgesichert werden muss. Dies stellt jedoch ein besonderes Angriffsziel für bestimmte Personengruppen dar. Hier muss mit geeigneten Systemen nach- bzw. umgerüstet werden.

Näheres zu diesem System kann im Internet unter www.ruhr-uni-bochum.de abgefragt werden.

Auslesen von Kfz-Schlüsseln

Als vor mehreren Jahren bekannt wurde, dass man aus dem Speicherbaustein des Schlüssels verschiedene Daten unter anderem auch den Kilometerstand des Fahrzeuges auslesen konnte, war für die Schadenregulierung ein weiteres Medium gefunden worden, möglichen Manipulationen des betrügerischen Versicherungsnehmers auf die Schliche zu kommen. Insbesondere der Hersteller BMW, der hier eine gewisse Vorreiterrolle eingenommen hatte, hat jedoch schon relativ frühzeitig in den Antwortschreiben aufgrund der Nachfrage mitgeteilt, dass diese ausgelesenen Daten nicht ohne weitere Überprüfung für gerichtliche Auseinandersetzungen eingesetzt werden können bzw. dürfen.

Schadenregulierer, die ihre Tätigkeit verantwortungsvoll ausgeführt haben, beherzigten dies und haben damit auch gute Erfolge gehabt bzw. mussten keine Negativurteile einfangen. Durch unsere Tätigkeit im Auftrag der Gerichte haben wir jedoch bedauerlicherweise festgestellt, dass oftmals auch leichtfertig mit den ausgelesenen Daten aus den Schlüsseln, die zwischenzeitlich bei einer Vielzahl von Fahrzeugherstellern zu erlangen sind, einfach nur anhand eines von uns oder einem anderen Sachverständigen überlassenen Prüfprotokolls oder Kurzgutachtens die Leistung an Versicherungsnehmer versagt wurde. Die Begründung dazu war lapidar, das Datum der letzten Benutzung und der angegebene Kilometerstand stimmen nicht mit den Feststellungen des Sachverständigen überein. Die „Bauchlandung“ war vorprogrammiert.

Der Sachbearbeiter hätte gut daran getan, seine Erkenntnisse von dem Sachverständigen zu hinterfragen, diese durch weitere Erkenntnis zu untermauern, statt lediglich mit der kurzen Mitteilung des Sachverständigen den Schaden abzulehnen und darüber hinaus noch in den Prozess zu gehen.

Zur Erklärung des Hintergrundes ist es erforderlich, die Datenablage in dem Schlüssel genauer zu analysieren. Einerseits haben nur sehr wenige Fahrzeuge eine Funkuhr zur Einstellung von Datum und Uhrzeit, d.h. bei der Fahrzeugübergabe an den Kunden wird das Datum und die Uhrzeit bei den meisten Fahrzeugen manuell eingestellt. Wird das Fahrzeug zur Inspektion gegeben oder liegt eine größere Reparatur an, kann es vorkommen, dass die Batterie abgeklemmt wird. Wenn die Daten nicht über einen Pufferspeicher gesichert sind, gehen sie verloren.

Jeweils liegt es an dem Geschick des Verkäufers/Monteurs das „richtige“ Datum und die Uhrzeit einzugeben, wobei er in der Regel seine eigene Armbanduhr benutzen wird. Handelte es sich dabei z.B. um eine Automatikuhr oder hat er vergessen, bei dem Vormonat, der nur 30 Tage hatte, die Armbanduhr nachzujustieren, dann wird er das falsche Datum eingeben, weil seine Uhr auch ein falsches Datum anzeigt.

Wir haben also bei diesen Systemen überhaupt keine Sicherheit, dass ein korrektes Datum und Uhrzeit eingestellt wurde. Der Mensch ist hier die Unsicherheit.

Die im Schlüssel abgespeicherte Kilometerlaufleistung wird in unterschiedlichen Varianten vorgenommen. Es wird bei dem Betrieb des Fahrzeuges vom Getriebe ein Signal an die Tachoeinheit gegeben (die Tachowelle gibt es schon lange nicht mehr). Somit ist die Tachoeinheit im Kombiinstrument der Baustein für die Versorgung der verschiedenen Speicher im Fahrzeug, die den KM-Stand hinterlegen. Dazu gehört auch der Schlüssel. Das Übertragen der Daten findet in unterschiedlichen Abständen und nach verschiedenen Parametern statt. Bei einem Fall in unserem Untersuchungsbereich wurde das Fahrzeug 24 Kilometer gefahren und es fand kein Übermitteln des neuen Kilometerstandes zum Schlüssel statt.

Der Speicherbaustein im Schlüssel und die weiteren im Fahrzeug, können bauartbedingt nur „nach oben“ überschrieben werden, es sei denn, sie werden komplett gelöscht, dann fangen sie bei Null an. Erhalten sie jedoch einen Datensatz zum Speichern von der Tachoeinheit, so findet das Niederschreiben dieses Km-Standes nur dann statt, wenn in der Speichereinheit kein höherer Km-Stand vorhanden ist, ansonsten wird dieser Km-Stand nicht verändert, nur das Datum angepasst. Dies ist auch an den unterschiedlichen Datensätzen bei einem Schlüsselsatz zu entnehmen.

Stellt sich die Frage, wie verhält es sich, wenn eine Tachojustierung stattgefunden hatte?

Die Speicherbausteine im Fahrzeug behalten in der Regel den ursprünglichen Kilometerstand, zumal es einerseits nicht äußerlich sichtbar ist und zum anderen einen relativ hohen Aufwand erfordert, den Kilometerstand dort zu korrigieren. Wenn z.B. ein Fahrzeug 100.000 km gelaufen hat, der Tacho um 40.000 km zurückgestellt wurde, zeigt der Tacho 60.000 km an. Das Fahrzeug hat jedoch 100.000 km in den weiteren Speicherbausteinen stehen. Wenn das Fahrzeug 10.000 km gefahren wird, zeigt der Tachostand 70.000 km an, im Speicherbaustein bleiben jedoch 100.000 km stehen. Erst dann, wenn der Tachostand auch den Speicherbausteinstand erreicht hat, findet auch das Fortschreiben im Speicherbaustein statt.

Wenn das Fahrzeug also seine 100.000 km wieder auf dem Tacho anzeigt, stimmen Tacho- und Speicherbausteindatensatz wieder überein, das Fahrzeug hat dann jedoch in Wirklichkeit 140.000 km gelaufen. Diese Mehrkilometer werden nicht angezeigt und sind auch in keinem Speicherbaustein hinterlegt.

Ebenso verhält es sich mit dem Speicherbaustein im Schlüssel. Dieser behält die 100.000 km auch dann, wenn das Fahrzeug auf dem Tacho 60.000 km anzeigt. Die Fortschreibung im Schlüssel findet auch erst dann statt, wenn das Fahrzeug wieder 100.000 km auf dem Tacho erreicht hat.

Dies ist auch so, wenn das Fahrzeug mehrfach eine Tachojustierung nach unten erfährt. Theoretisch wäre es so möglich, dass das Fahrzeug 200.000 km tatsächlich gelaufen hat, durch die Mehrfachjustierung jedoch einen Kilometerstand von 60.000 km anzeigt. Bisher kannten wir keine Fälle, bei denen der Tachostand auch im Schlüssel zurückgestellt wurde. Im Laufe des Jahres 2008 stellte uns jedoch ein Elektroniker ein Programm vor, mit dem es uns möglich wäre, ohne Unterstützung des Herstellers den Speicherbaustein im Schlüssel in allen Ebenen auszulesen. Gleichzeitig ist dieses Programm auch in der Lage den Tachostand im Schlüssel zu verändern. Einerseits aus Kostengründen, andererseits wegen der Problematik des Nachweises haben wir auf die Beschaffung dieses relativ teuren Programmes, insbesondere auch wegen der Erforderlichkeit permanent Updates zu ordern, verzichtet.

Programme zur Veränderung der EEPROM-Speicherbausteine

Fortführend der Mitteilung im Info-Brief 2007 bezüglich der Feststellungen und anlässlich unseres Besuches in Litauen wurden im Laufe des Jahres 2008 auch hierzu weitere Erkenntnisse erlangt. In Litauen konnten wir Geräte und Programme in Augenschein nehmen, die es ermöglichten, direkt in die Speicherstruktur des EEPROM einzugreifen. Hier wurde jedoch in der Regel „nur“ die vorhandene Wegfahrsperre ausgeschaltet. Dass dies möglich war, wussten wir bereits von einem Reparaturbetrieb, mit dem wir in Kooperation stehen, der zur Reparatur von Steuergeräten den Zugang auch dadurch schaffen muss, dass das „Sperrelement Wegfahrsperre“ vorübergehend ausgeschaltet wird.

Der gleiche Anbieter, der uns ein Programm zum Auslesen der Schlüsselspeicherbausteine anbot, führte uns vor, dass er über die OBD-Schnittstelle mit seinem Laptop die Speicherung des EEPROM darstellen und auch entsprechend verändern konnte.

Es besteht somit die Möglichkeit, dass er weitere Schlüssel dem Steuergerät anpasst und diese Schlüssel dort einprogrammiert. Es besteht so auch die Möglichkeit, ein entwendetes Fahrzeug, zu dem keine Originaltransponder der Schlüssel vorliegen, wieder in einen fahrfähigen Zustand zu bringen. Es stellt sich jetzt die Frage, in wieweit eine derartige Änderung nachvollzogen werden kann.

Der Anbieter des Programmes zeigte uns, dass bei einer Veränderung quasi ein Kontrolleintrag an weiterer Stelle im Speicher erfolgt. Dieser würde auch bestehen bleiben, wenn eine Rückprogrammierung zu den ursprünglichen Daten und den entsprechenden Schlüsseln vorgenommen werden würde.

Die Problematik ist hier jedoch, dass einerseits das Programm einen nicht unerheblichen Kostenaufwand erfordert und Folgekosten durch die Updates entstehen, sodass sich derartige Hilfsmittel nur dann für uns rentieren, wenn auch entsprechende Untersuchungsaufträge an uns herangetragen werden.

Letztlich ist jedoch auf diesem Wege die zentrale Frage, ob der letzte Halter, Fahrer oder Nutzer durch
seine Mitwirkung die Entwendung des Fahrzeuges unterstützt oder begünstigt hat, nicht zu klären.

Selbst wenn eine Hinterlegung des Datums, wann die Änderung vorgenommen wurde, erfolgt, stellt sich wiederum die Frage, wie auch bereits o.a. schon erörtert, nach der korrekten Einstellung von Datum und Uhrzeit. Aus kriminaltechnischer Sicht kann ausgeführt werden, dass der Nachweis der
Fahrzeugentwendung zwar möglich ist, der Aufwand sich jedoch sehr erheblich darstellt, sodass es in vielen Fällen zwar Hinweise geben kann, dass das Fahrzeug nicht ohne Mithilfe entwendet wurde, der letzte und sichere gerichtlich geforderte Beweis aber nicht mehr erbracht werden kann.

Die Mithilfe des Fahrzeugherstellers findet hier auch nicht wirklich statt. Dieser trägt auf zwei Schultern, einmal einen Schadenfall aufzuklären, anderseits sich jedoch seinem Kunden gegenüber loyal zu verhalten, um ihn nicht zu verlieren.

Letztlich werden durch die ungerechtfertigten Leistungen, die von der Versicherungswirtschaft erbracht werden müssen, auch die redlichen Versicherungsnehmer durch Erhöhung der Beiträge geschädigt. Daher erscheint es erforderlich, dass von der Versicherungswirtschaft Forderungen an die Fahrzeughersteller gerichtet werden, entsprechende Unterstützung zu leisten.

Ein wesentlicher Punkt dazu wäre auch, die vollkommene Freigabe sämtlicher fahrzeugrelevanter Daten im Falle einer Fahrzeugentwendung an den Versicherer.

Letztlich müsste auch darüber nachgedacht werden, dass das System „Wegfahrsperre“ seine ursprüngliche Forderung nicht mehr erfüllt und daher über Ersatzsysteme nachgedacht werden sollte.

- siehe Homepage: www.vag-info.com –

Manfred Göth

Kriminaltechnisches Prüflabor GÖTH, GmbH, Mayen

www.goeth.com