VERKEHRS KONGRESS 2014
SAARBRÜCKEN

Recht | Daten | Sicherheit

Die Dokumentation

ACE Auto Club Europa

e.consult Aktiengesellschaft

VUT Verkehr

INHALTSVERZEICHNIS

Verkehrskongress 2014

DATEN | RECHT | SICHERHEIT

Themen und Referenten

Hinweise in eigener Sache:

Im Folgenden handelt es sich um eine überarbeitete Transkription, es wurde versucht den Inhalt zu belassen und die Lesbarkeit zu verbessern. Die Diskussion wurde rausgelassen, da die Fragen auf der Audioaufnahme nicht verständlich waren. Original Transkription gerne auf Anfrag.

VERKEHRS KONGRESS 2015 - 05.06.2015 im Saarbrücker Schloss
(Kapazität max. 200 Teilnehmer!)

VORTRAG

Prof. Dr. Michael Backes, Professor für Informationssicherheit und Kryptographie an der Universität des Saarlandes

Datensicherheit – Fälschungssicherheit von digitalen Messdaten

Moderator

Jetzt gehen wir weiter ans Eingemachte, so wie wir es heute versprochen haben. Der nächste Referent Michael Backes ist Professor für Computersicherheit und Kryptografie an der Universität des Saarlandes. Professor Backes hat, ich glaube, das kann man genau so sagen, eine Karriere im absoluten Zeitraffer hingelegt. Er hat nach Mathematik und Informatik Studium in Saarbrücken, 3 Jahre lang im IBM Forschungszentrum geforscht und wurde dann im Alter von 27 Jahren in Saarbrücken zum Professor auf Lebenszeit ernannt, als jüngster Informatikprofessor Deutschlands.

Nach Professor Backes, hat Informatik sehr viel mit Kreativität zu tun. Deshalb freuen wir uns jetzt auch auf einen kreativen Vortrag und ich überlasse Ihnen sehr gerne die Bühne, Professor Backes.

Prof. Dr. Backes

Das mit der Kreativität hätte ich eventuell nicht im Interview sagen sollen, jetzt muss ich wahrscheinlich einfach liefern. Gut, versuchen wir es.

Ich wurde gebeten, über Datensicherheit von Geschwindigkeitsüberwachungsgeräten zu sprechen. Ich werde hier die technische Komponente beleuchten, daher komme ich, da kenne ich mich aus. Ich bin kein Anwalt, kein Jurist, werde mich auch nicht mit der Exekutive beschäftigen. Wie Sie das, was ich sage, interpretieren, überlasse ich Ihnen. Ich kann Ihnen nur sagen: Was ich sage ist korrekt. Was Sie damit machen ist Ihre Sache. Zunächst motiviere ich ganz kurz, um was es eigentlich geht, dann werden wir ein kleines bisschen technischer. Dann werde ich Ihnen möglichst einfach erklären, ob das was momentan draußen ist, gut ist, ob es nicht gut ist, was die Konsequenzen sind und was machen könnte, wenn man denn möchte.

Es geht im Wesentlichen um Messdaten und es geht generell um Echtheit dieser Daten. Zunächst möchte ich ganz kurz sagen, und das werden Sie zumindest besser wissen als ich, dass manipulierte Daten drastische, wirkliche Konsequenzen haben können.

Ich hab zwei Sachen zur Motivation herausgenommen. Der Stuxnet Virus, falls Sie ihn kennen, war ein Virus, der die Zentrifugen in Atomkraftwerken ein bisschen schneller drehen ließ. Das hat keiner gemerkt. Man hatte gedacht, die Daten wären korrekt, waren sie aber nicht. Und nachher hatte man echte Probleme oder echtes Glück, je nachdem von welcher Seite Sie es betrachten. Andere Sachen, z.B. wenn Sie nicht wissen, ob gewisse Informationen korrekt sind, können drastische Auswirkungen auf die Börse haben. Es gab eine Nachricht vor ein paar Jahren, die die Leute als korrekt, authentisch betrachtet haben, wo es im Wesentlichen hieß, das Weiße Haus ist gerade nieder gebombt wurden. Das hatten Leute als korrekt erachtet. An diesem ist die Börse komplett gecrasht, Verluste von ungefähr 150 Milliarden Dollar. Wegen einer Sache, die nicht korrekt war. Klarer Weise haben wir hier ein kleineres Szenario. Trotzdem müssen wir sehen, dass die Korrektheit von Daten generell gegeben sein muss, wenn wir daraus Schlussfolgerungen ziehen wollen oder wenn wir etwas als Beweis, Indiz oder Ähnliches benutzen möchten.

In dem Fall haben wir uns klassische Geschwindigkeitsüberwachungsgeräte angesehen. Diese Informationen hier habe ich im Wesentlichen aus öffentlichen Quellen, da dies nicht mein primäres Gebiet ist. Ich habe mir nur die Sicherheitskomponente davon angeschaut. Die Informationen, die man bekommt, sagen, es gibt etwa 3100 fest installierte Geräte. Die Funktionsweisen und die Eichung sind nicht, ich sage mal, zwangsweise öffentlich dokumentiert, oft Herstellergeheimnis. Messdaten und Fotos werden digital aufgenommen und sollen als primäre Eigenschaft vor Manipulationen selbstverständlich geschützt werden. Dass das nicht immer

ganz so geht, sieht man bei sehr interessanten Bildern, die manchmal tatsächlich auftauchen. Bei diesen darf man sich ein bisschen die Frage stellen darf, ob das ein wahnsinniger Fahrer war oder, ob diese Daten eventuell manipuliert werden können. Das heißt hier geht es einerseits um die Echtheit des Bildes, ansonsten werden Sie jemanden Falschen anklagen, und andererseits um die Echtheit der Messdaten, ansonsten haben Sie falsche Geschwindigkeiten und das was Sie gemacht haben ist im Wesentlichen wertlos. Das muss sichergestellt werden, ansonsten können Sie es einerseits selbst anfechten, wenn Sie beschuldigt werden. Das ist eine Sache. Wobei ich eine andere Sache schlimmer finde: Wenn Sie fälschen können, können Sie auch Ihren Nachbarn anschwärzen, dass er auf irgendeiner Autobahn angeblich zu schnell war. Wenn Sie nicht nachprüfen könnten, dass dies wirklich korrekt ist, können Sie sich natürlich selbst schützen und andere fälschlicherweise anklagen unter der Annahme, dass dieser Schutz nicht gewährleistet ist.

Kommen wir kurz dazu, was diese Systeme gemäß dem öffentlichen Anforderungsprofil eigentlich können sollen. Im Wesentlichen werden wir besprechen, was diese Begriffe eigentlich bedeuten und dann schauen wir uns mal an, ob das funktioniert oder nicht.

Die Anforderungen sind von der Physikalisch Technischen Bundesanstalt definiert. Diese sagt, Daten dürfen nicht manipuliert werden. Ein bisschen konkreter sagen sie, die gesamte Datei, das sind das Bild und die echten Messdaten, sind mit einer digitalen Signatur zu versehen. Eine Signatur ist intuitiv, aber ich komme gleich dazu, ein Schutzmechanismus, der es jedem Menschen verhindert oder unmöglich macht Daten zu ändern, ohne dass der Empfänger es merkt. Quasi das Gegenstück von einer handgeschriebenen Signatur, um eine Unveränderbarkeit herzustellen. Das ist auch genauso spezifiziert. Durch die Signatur, deshalb lese ich es ab, kann die Unversehrtheit des Inhalts der Datei verifiziert werden. Zusätzlich ist die Authentizität der Datei zu bestätigen. Das bedeutet, dass sie auch in der Tat vom richtigen Ursprung gesendet wurde, die Datei also vom richtigen Absender stammt. Das ist die offizielle formale Vorgabe, die wir erfüllen müssten. Ich werde nachher überprüfen, ob das stimmt oder ob das nicht stimmt und auch zu welchem Maße.

Ich gehe ganz kurz auf ein paar Begriffe ein. Elementare Einführung in Computersicherheit auf drei bis vier Folien. Was ist Vertraulichkeit? Wir brauchen es. Was ist Integrität? Was ist Authentizität? Wir müssen uns im Prinzip die Begriffe, die gerade in diesem Text vorkamen, anschauen. Wir müssen wissen, was sie eigentlich bedeuten, um zu wissen, ob sie gelten oder nicht.

Vertraulichkeit ist eigentlich klar. Auf Informationen dürfen ausschließlich durch befugte Personen zugegriffen werden. Wenn Sie sich die technische Seite anschauen, ist das eigentlich ein völlig gelöstes Problem. Es gibt Verschlüsselungen, was bedeutet, Sie verschlüsseln Ihre Daten und schicken sie unter gewissen Annahmen über einen sicheren Kanal zum Empfänger und die Geheimhaltung ist im Wesentlichen gewährleistet. Was Sie in der Praxis haben, ist ein gesicherter Kanal. Das kennt jeder von Ihnen, obwohl sie es vielleicht nie explizit wahrgenommen haben: Wenn Sie Online-Banking machen, haben Sie genau das. Aus genau diesen Gründen, weil Sie nicht wollen, dass jemand mitbekommt wie viel Geld Sie gerade wohin überweisen. Und andere Leute sollen auch nicht Geld von Ihrem Konto überweisen. Dieser Kanal ist wohl etabliert. Was er macht, er verbindet zwei Komponenten, man könnte sich jetzt vorstellen es wäre ein Blitzgerät und die entsprechende Stelle die Daten aufnimmt. Könnte man machen, würde funktionieren. Was Sie hier haben: Sie haben Dateiverschlüsselung; Sie können sicherstellen, dass die Daten korrekt geschützt sind. Aber es gibt eine Grundannahme. Und die Grundannahme ist, Sie müssen sicherstellen, dass die Schlüssel, die zum Verschlüsseln und Entschlüsseln benutzt werden, auch nur den Personen zugänglich sind, die diese Daten sehen dürfen. Diese Annahme müssen wir im Kopf behalten, weil das genau der Punkt ist, an dem es nachher Probleme geben wird. Das heißt, es ist sicher, wenn die Schlüssel nur dort liegen, wo sie hingehören. Es gibt zwei Varianten davon. Es gibt symmetrische Sachen, das ist relativ einfach: Das sind zwei Leute, die haben denselben Schlüssel. Wenn ich den Schlüssel habe, kann ich verschlüsseln und entschlüsseln, gleicher Schlüssel. Und es gibt asymmetrische Verfahren. Da kann im Prinzip jeder, der einen sogenannten öffentlichen Schlüssel besitzt verschlüsseln. Aber nur der eine Mensch, der den geheimen Schlüssel hat, kann entschlüsseln.

Integrität.

Integrität bedeutet, Daten, in diesem Fall Messdaten, wurden nicht verändert. Also sie wurden in der Tat so aufgenommen und sie wurden unverändert an den Server geschickt, der sie im Endeffekt bearbeitet. Sie kommen bei der entsprechenden Autorität korrekt und unverändert an und Sie wissen, dass sie nicht verändert wurden. Korrektheit heißt, keine Übertragungsfehler, das ist relativ klar und relativ trivial, aber auch keine Möglichkeit der Manipulation. Also es ist nicht möglich, diese Daten zu verändern, ohne dass der Empfänger es merkt.

Wenn Sie ein bisschen technisch versiert sind, wissen Sie: Da gibt es einige triviale Maßnahmen. Es gibt zum Beispiel Checksummen. Wenn Sie relativ viele Daten schicken, haben Sie hinten so ein dediziertes Element, wo Sie so etwas wie eine Quersumme berechnen. Dies dient dazu, dass Sie nachprüfen können, ob das alles irgendwie zusammenpasst. Das wird benutzt, damit keine Übertragungsfehler passieren. Da geht es gut, bringt Ihnen aber Nichts gegen böswillige Veränderungen. Aber darüber reden wir natürlich hier gerade. Schauen wir uns ein Beispiel an. Ich weiß nicht, ob es so einleuchtend ist, bei meinen Studenten würde ich es nicht einmal so bringen. Im Endeffekt stellen Sie sich vor, Sie schicken folgende Zahlen und die Prüfsumme ist einfach die Summe. Wenn Sie jetzt das ganze betrügen wollen und wollen diese Zahlen verändern, zum Beispiel aus Geschwindigkeiten, die Ihnen nicht gefallen, anderen Geschwindigkeiten machen. Dann hilft Ihnen die Checksumme nicht viel, Sie würden einfach da unten das Ding genau so anpassen. Der Empfänger wird einfach denken, das hat mir nichts gebracht, weil diese Checksumme nicht geschützt ist. Dafür haben Sie Signaturen. Signaturen haben folgende Eigenschaft und daran müssen wir uns genau halten: Es gibt zwei Schlüssel. Es gibt einen privaten Schlüssel, der wird genutzt zum Signieren. Den müssen Sie wirklich geheim halten, denn wer diesen Schlüssel hat, kann in Ihrem Namen unterschreiben. Dieser Schlüssel würde in diesem Fall in den entsprechenden Geschwindigkeitsmessgeräten sitzen, da das Gerät die Daten entsprechend signieren soll. Das ist auch so! Auf der anderen Seite ist der öffentliche Schlüssel. Der öffentliche Schlüssel wird benutzt, um die Korrektheit der Signatur zu testen. Jetzt gibt es zwei Eigenschaften, die erste ist trivial, die zweite ist nicht minder wichtig, wird aber oft übersehen. Die erste ist: Der privaten Schlüssel muss geheim gehalten werden. Auf dieses Szenario mit den Blitzgeräten übertragen heißt das: Stellen Sie sicher, dass niemand Ihren Blitzer stiehlt, das Ding auseinander schraubt und Ihren Schlüssel klaut. Nicht unmöglich, aber lassen wir mal weg. Das andere ist aber noch interessanter: Die andere Partei, die die Signatur prüfen will, muss sicher sein, dass dieser öffentliche Schlüssel der richtige öffentliche Schlüssel ist, ansonsten wird es schwierig. Was würde ich tun? Ich generiere mir selber einen privaten und öffentlichen Schlüssel, gebe Ihnen meinen öffentlichen Schlüssel. Sie können ja nicht prüfen, ob das meiner ist oder von jemanden sonst. Und dann signiere ich munter mit meinem eigenen Schlüssel und Sie glauben, alles super. Deshalb gehen wir mal einen Schritt zurück. Im Prinzip ist es folgendes Szenario: Sie wollen eigentlich mit einem Server kommunizieren, aber es könnte einen anderen Server geben, irgendeinen bösartigen Angreiferserver, der genau das mit Ihnen macht. Er schickt Ihnen einen öffentlichen Schlüssel. Wenn Sie keine Vorsichtsmaßnahmen treffen, wissen Sie nicht, welcher welcher ist. Sie zertifizieren, signieren und Sie prüfen und Sie können nicht auseinanderhalten, woher es kommt, alles ist gültig. Dafür gibt es Zertifikate und so weiter und so fort, darauf komme ich nachher noch einmal zurück.

Wie läuft das in der Praxis? Ich sage vorab, die Analyse dieser Geräte ist nicht besonders kompliziert. Es ist nicht so, dass es nachher unglaublich kompliziert wird. Es ist ein sehr elementarer Fehler drin, den wir auch alle gemeinsam sehen werden, vielleicht auch interaktiv, mal schauen.

Wie wird man es machen? Wenn Sie eine Nachricht signieren wollen haben Sie die Nachricht, Ihren geheimen Signatur-Schlüssel und Sie machen eine Signatur. Das ist die mit diesem roten Kreis. Sie schicken diese signierte Nachricht an den entsprechenden Empfänger. Der Empfänger muss den korrekten öffentlichen Schlüssel kennen. Er kann es prüfen und sagen, stimmt oder stimmt nicht, je nachdem, ob es korrekt war oder nicht. Damit lösen Sie intuitiv auch das Problem, was man mit Blitzgeräten hat: Sie nehmen ein Bild, machen die Messdaten, signieren das ganze geschickt, Sie schicken es rüber. Die andere Partei nimmt den korrekten öffentlichen Schlüssel verifiziert das, das kann keiner fälschen und Sie sind fertig. Soweit die Theorie. Zur Praxis. Ganz kurz noch: Es gibt viele Probleme, die man beachten muss, wenn das ganze juristisch oder exekutiv betrachtet.

Einerseits gibt es Probleme beim Prüfen der Integrität. Es ist Software, die diese Prüfung durchführt. Das heißt, es ist nicht klar, ob die Software das korrekt macht. Oftmals ist es so, dass der Algorithmus in Ordnung ist, aber er ist schlecht implementiert, die Software macht nicht, was sie soll, sie zeigt eventuelle falsche Daten an. Darauf muss man weiterhin aufpassen. Sehr oft ist die fehlerhafte Anwendung der kryptografischen Methoden das Paradebeispiel: Die Algorithmen sind in Ordnung, aber sie werden so benutzt, dass sie gar nicht die Eigenschaften haben, die Sie möchten. Das ist das, was hier passiert ist. Letzter Punkt ist: Sie wollen, dass es automatisch funktioniert, Sie wollen nicht, dass Sie manuell später alles noch einmal auf Korrektheit prüfen müssen. Wenn Sie das pro Transaktion wollen, dann bräuchten Sie diesen ganzen Aufwand nicht zu treiben. Und dann hätten Sie unglaublichen Overhead durch human Manpower. Das geht, aber das will natürlich kein Mensch. Sie wollen es automatisch haben und nicht so.

Was haben wir gemacht? Wir haben uns die Messdateien von zwei große Herstellern genommen und haben uns angeschaut, wie diese Sachen im Sinne vom Schutz der Integrität umgesetzt werden. Wir haben uns die anderen, die es gibt, nicht angeschaut. Ich kann keine Aussage treffen, ob die ähnliche Fehler machen. Es würde mich nicht beliebig überraschen, aber ich kann es nicht ausschließen. Die ersten waren die Messdateien der ESO GmbH und ich zeige Ihnen kurz, was passiert ist. Und dann können Sie mir nachher sagen, sagen wir mal interaktiv, ob wir das hinkriegen, was da nicht so ganz läuft wie es soll. Das hier ist die Messdatei, die dieses Gerät wegschickt oder zumindest auf Festplatte speichert oder jemand kommt es abholen, das spielt keine Rolle. Das ist die Messdatei, die nachher in der entsprechenden Behörde oder Institution ankommt. Sie hat im Wesentlichen zwei Teile. Sie hat, den öffentlichen Signaturschlüssel, der ist drin, damit der Empfänger prüfen kann. Sie brauchen ja als Empfänger einen öffentlichen Schlüssel, sonst können Sie nicht überprüfen, ob das stimmt. Das grüne ist die Signatur von dem, was drunter ist. Das Gelbe und das Blaue sind die Messdaten. Der Unterschied ist jetzt, die Gelben sind die, die man jetzt nicht extra noch verschlüsselt hat, die Blauen sind verschlüsselt. Im Endeffekt stehen unten die Daten, Sie wurden geknipst mit der und der Geschwindigkeit, das Grüne ist die Signatur und das Rote ist das, was Sie haben, um die Signatur zu verifizieren. Das ganz kleine Stück Blau oben ist Teil des Schlüssels, das ist öfter so: Der öffentliche Schlüssel besteht halt aus zwei. Ich gehe mal eins weiter und dann sagen Sie mir mal, warum das nicht so die beste Idee ist. Ganz vorsichtig ausgedrückt: Das erste ist, wir haben uns die Verschlüsselung angeschaut. Verschlüsselung habe ich gesagt, ist ein sehr gelöstes Problem. Sie werden keinen Forscher finden, der an Verschlüsselungen forscht, außer an noch effizienteren. Aber das ist klar wie das geht. Hier war es so, dass der Verschlüsselungsalgorithmus selbst sehr proprietär waren, also man konnte herausfinden, wie verschlüsselt wurde. Das ist nicht schlimm unter der Annahme, dass der Schlüssel zur Verschlüsselung geheim ist und gut gewählt. Hier war es so, dass man den Schlüssel einfach auslesen konnte. Es war so verschlüsselt, dass man durch einmaliges scharfes Hinschauen und es war in der Tat einmaliges scharfes Hinschauen, das entschlüsseln kann. Das heißt, die Vertraulichkeit ist hier nicht gegeben. Das war jetzt gar nicht unser Hauptziel. Ich sage auch gleich, das wäre einfach zu lösen, nehmen Sie sich einen besseren Schlüssel, nehmen sich ein besseres Verschlüsselungsverfahren, wir würden nie wieder drüber reden. Deshalb bin ich aber nicht hier. Wir wollten über Integrität reden. Schematisch sieht es so aus: Die Datei, die geschickt wird, hat drei Teile: Öffentlicher Signaturschlüssel, die Signatur, die Daten. Was macht der Empfänger? Er nimmt die Daten und testet, ob die Signatur mit diesem öffentlichen Signaturschlüssel korrekt ist für die Daten. Und jetzt sagen Sie mir, ob das Sinn macht? Stellen Sie sich vor, dass sind Daten, die Sie nicht möchten. Einverstanden? Sie möchten Sie nicht! Sie sind gerade geblitzt worden, es war ein nicht so schöner Tag. Sie wollen die Daten ändern. Also mal angenommen, ich habe mal Zugriff auf die Hardware oder auf das Wireless, das spielt keine Rolle. Ich ändere die Daten. Dann stimmt die Signatur aber nicht mehr, das ist ja die Eigenschaft. Was mache ich jetzt? Jetzt brauche ich aber eine Signatur, die für diese Daten gilt, wie mache ich das? Richtig. Der private Schlüssel der zu diesem Schlüssel gehört, das Gegenstück, den haben Sie nicht. Was machen Sie? Sie machen sich einen eigenen privaten Schlüssel und Ihren öffentlichen Schlüssel hängen Sie hier an. Würde ich jetzt nicht als den kompliziertesten Angriff auf dieser Erde bezeichnen. Kurzform: Sie machen sich einen neuen Schlüssel, das kann jeder privat und öffentlich, Sie signieren veränderte Daten, hängen die neue Signatur in die Mitte und hängen aber auch Ihren öffentlichen Schlüssel an.

Was passiert? Die andere Seite wird dieses Ding kriegen, die Signatur ist gültig, Sie haben sie für die geänderten Daten ja gerade erzeugt. Warum wird es nicht auffallen? Es wird nicht auffallen, weil keiner weiß, dass dieser öffentliche Schlüssel nicht der öffentliche Schlüssel des Blitzgerätes ist. Das kann man machen, das kann man implementieren. Man bräuchte so etwas wie eine Public Infrastructure gibt es aber nicht. Das heißt, so haben Sie es ausgehebelt.

Damit können Sie auch ganz etwas Anderes machen, wenn wir es auf die Spitze treiben. Das könnte ich Ihnen, wenn es nicht illegal wäre, innerhalb einer Stunde problemlos demonstrieren: Ich kann einfach für eins von Ihren Autos Daten machen. Ich sage, Sie waren 100km/h zu schnell und schwärze Sie an. Und das würde funktionieren, es sei denn Sie gehen vor Gericht und beweisen, dass Sie zu der Zeit physisch woanders waren und lösen es im Dialog. Aber technisch hätten Sie keine Chance. Simpelster Angriff: Öffentlicher Schlüssel ausgetauscht, Daten verändert, Signatur angepasst, geht technisch durch, kein Schutz dagegen.

Hier sehen Sie ein kleines Beispiel, wie wir es gemacht haben mit der echten Software und dem originalen Messfoto. Natürlich haben wir die Nummernschilder usw. aus Datenschutzgründen ausgeschwärzt. Sie sehen links unten dieses Schlosssymbol, was signalisieren soll: Alles korrekt, zertifiziert, die Signatur stimmt und so weiter. Die Software sagt Ihnen: Es ist ein original Messfoto und es ist korrekt. Weiterhin haben wir aus Spaß das Firmenlogo genommen, haben es in die Messdatei reingemacht und die Software sagt, es ist ein ganz akkurates Messfoto von der A8, das ich um 14.00 Uhr aufgenommen habe. Mir ist klar, das sieht für einen Menschen nicht realistisch aus, aber die Technik sagt: Kein Problem.

Bei dem zweiten Hersteller sieht es eigentlich nicht so viel anders aus. Wie wir gleich sehen werden, ist das Ganze initial etwas anders aufgesetzt, hat aber eigentlich auch das gleiche Problem.

Die Messdatei sieht etwas anders aus. Sie haben die Daten, Sie haben die Signatur, Sie haben aber nicht den öffentlichen Schlüssel, sondern Sie haben einen Link zu einer Datei, die den öffentlichen Schlüssel enthält, die aber der Messdatei angehangen ist.

Gut. Ich bin froh, dass Leute schmunzeln, das heißt Sie haben verstanden, dass der Angriff genauso funktioniert. Die Datei ist optional verschlüsselt. Wir haben da eine interessante Sache gemacht. Sie könnten jetzt wieder hingehen und sagen, Sie extrahieren den Verschlüsselungsalgorithmus. Das kann man machen. Das ist manchmal aufwendig, manchmal geht es schnell. Hier gibt es aber eine interessante Alternative wie Sie es machen können: Sie machen einfach das Auswertungsprogramm auf: Die Software entschlüsselt für Sie. Während Sie damit arbeiten legt das Ding eine eigene temporäre Datei an, in der alle diese Sachen unverschlüsselt drin liegen. Sie benutzen die Software, damit sie für Sie entschlüsselt. Die Datei können Sie auslesen und ändern und das Programm verschlüsselt dann auch wieder für Sie. Das kommt vor, da will ich auch gar nicht bösartig sein. Ich kenne viele Leute, bei denen so etwas vorkommt. Das sind so Dinge, die kann man korrigieren. Wenn man Sicherheit nicht so im Blut hat, passiert das häufiger. Was viel ärgerlicher ist: Die Integrität geht ähnlich verloren wie im ersten Verfahren. Eigentlich haben Sie hier die Daten, Sie haben die Signatur, Sie haben nicht den öffentlichen, sondern den Namen der Schlüsseldatei, die aber angehangen ist. Der Angriff: Klar! Sie machen sich ein neues Schlüsselpaar, Sie verändern Ihre Daten, Sie verändern die Signatur, Sie lassen den Link auf die Datei genau gleich und Sie legen den neuen öffentlichen Schlüssel in diese Schlüsseldatei. Geht genau gleich. Was machen Sie mit den Bildern? Hier haben wir es so gemacht: Wir haben das original Bild mal genommen und jetzt sieht man da oben 74 km/h, ist wirklich ein original Bild was wir freundlicherweise zur Verfügung gestellt bekommen haben. Wir haben das Bild geändert, wir hätten es aber auch einfach lassen können, das Bild ist ja da. Und wir verändern jetzt mal einfach die Geschwindigkeit auf 999 km/h. Ich hätte das Bild auch lassen können, ich hätte es runter machen können auf 54 km/h, das ist relativ egal. Alles was wir eben gesagt haben trifft zu. Die Software sagt logischerweise: Es ist korrekt. Das können Sie nur dann verhindern, wenn Sie einen extra Check beim Empfänger haben, der Ihnen irgendwie sagt, das war nicht der richtige Schlüssel.

Fazit: Momentan ist es so: Die Versionen, die wir uns angeschaut haben, erkennen Manipulationen nicht. Ich kann Ihnen nicht sagen, ob es vielleicht Änderungen oder Updates gibt, aber unsere Untersuchung ist nicht lange her. Die Signatur wird in der Tat geprüft, aber das bringt Ihnen nichts. Ein typischer Fall von einer

Anwendung von Kryptografie, die nicht das Ergebnis liefert, was Sie möchten. Die Signatur wird geprüft, aber da die Authentizität des Signaturschlüssels nicht klar ist, wissen Sie nur: Irgendjemand hat da eine gültige Signatur erzeugt, aber nicht ob das der Blitzer war, das wissen Sie nicht. So wie ich die Anforderungen der PTB verstehe, erfüllt es diese Anforderungen nicht. Das sind natürlich juristische Fragen, das werden Sie besser wissen als ich. Den Schutz im Sinne von „keine Manipulation möglich“ verstehe ich damit als nicht erfüllt. Aber das wissen Sie besser als ich.

Ich gebe Ihnen nur eine mögliche Lösung. Sie brauchen eigentlich irgendeine globale Instanz, meistens hierarchisch also eine Public Infrastructure, die die Herkunft des öffentlichen Schlüssels irgendwie zertifiziert, benennt, prüfbar macht. Das heißt, Sie wollen, dass fremde Schlüssel als solche erkannt werden können. Es gibt viele Mechanismen, beim Online Banking ist das gang und gäbe. Es gibt Zertifikate, das könnten wir auch benutzen, das wäre keine Problem, Sie könnten Fingerprints haben, Sie können sogar die öffentlichen Schlüssel speichern. So viele sind es ja nun auch nicht. Das würde aber andere Probleme mit sich führen: Stellen Sie sich vor, jemand klaut so einen Blitzer. Und der nimmt dann diesen Schlüssel wirklich raus. Ich weiß nicht, ob so etwas passiert. Doch wenn es passiert, müssten Sie Ihre Listen immer aktuell halten, das kann es schwierig machen. Aber generell ist so etwas mit sehr moderatem Aufwand technisch relativ einfach lösbar. Sodass ich einfach dafür werben würde, dass man diesen letzten Schritt noch einbaut, er ist wirklich nicht zu schwer.
Das war es im Prinzip schon.

Vielen Dank.

VORTRAG

Prof. Dr. Michael Backes, Professor für Informationssicherheit und Kryptographie an der Universität des Saarlandes

Datensicherheit – Fälschungssicherheit von digitalen Messdaten

Zusammenfassung und Fazit der VUT

Aktuell sind in Deutschland ca. 3100 fest installierte „Blitzer“ in Betrieb. Die Aufzeichnung von Messdaten und Fotos erfolgt heute durchgehend digital. Intuitiv ist leicht nachvollziehbar, dass diese digitalen Daten vor Manipulation geschützt sein sollen: Nur, wenn die Messdaten auch tatsächlich den Geschwindigkeitsverstoß dokumentieren, ist auch eine entsprechende Ahndung geboten. Dennoch bleiben Funktionsweise und Eichung ein Herstellergeheimnis.

Die physikalisch-technische Bundesanstalt (PTB) als zulassende Behörde fordert folgerichtig die Korrektheit digitaler Messdateien:

*„[Die Gesamtdatei ist] mit einer **digitalen Signatur** zu sichern. [...]*

*Durch die Signatur kann die **Unversehrtheit des Inhalts** der Datei verifiziert werden.*

*Zusätzlich ist die **Authentizität** der Datei zu bestätigen, d.h. es muss [...] sichergestellt sein, dass die Datei vom richtigen Absender stammt.“*

Bei den Messgeräten der Firmen Jenoptik ROBOT GmbH und eso GmbH wird zur Umsetzung dieser Anforderungen eine digitale Signatur eingesetzt. Problematisch daran ist jedoch, dass eine Signatur alleine keine Authentizität, also keine Informationen über die Herkunft der signierten Daten, liefern kann. Erst eine zweifelsfreie Zuordnung der Schlüssel des Signaturverfahrens ermöglicht die Erkennung der Urheberschaft von Daten.

Auf diesen Aspekt der Zuordnung der Schlüssel bei der Überprüfung der Signatur verzichten die Auswerteprogramme der vorgenannten Firmen. Somit ist es bei beiden Herstellern problemlos und automatisiert möglich veränderte Messdateien zu erstellen, die von den jeweiligen Auswerteprogrammen als korrekt erkannt werden. Hierzu werden veränderte Messdateien mit einem eigenen Signaturschlüssel neu signiert. Da eine Prüfung der Schlüssel nicht umgesetzt ist, erkennt die Auswertesoftware diese geänderten Signaturen als korrekt an. Eine manuelle Überprüfung der Schlüssel mag zwar möglich sein, jedoch ist eine manuelle Prüfung digitaler Daten nicht praktikabel.

Zusammenfassend können weder eso Digitales II noch BiffProcess Manipulationen erkennen. Zwar wird die digitale Signatur geprüft, nicht jedoch die Authentizität des Signaturschlüssels. Die Anforderungen der PTB sind somit nicht erfüllt. Dabei ist die Frage des Authentizitätsnachweises bei Signaturen seit Jahren technisch einwandfrei lösbar, beispielsweise durch den Einsatz einer sogenannten PKI.

Das Fazit in Kurzform ist:

„[...] wenn sie in der Forschung bei uns einen öffentlichen Signaturschlüssel mit an die Nachricht hängen würden, würde man ihnen den Kopf abreißen.“

Kontakt:

VUT Sachverständigen GmbH & Co.KG
Matthias-Nickels-Str. 17a
66346 Püttlingen

Tel. 0 68 06 / 30 05 - 0
Fax 0 68 06 / 30 05 - 180

info@verkehrskongress.de
www.verkehrskongress.de

VUT Verkehr