Versteckte RFID-Chips unter der TÜV-Plakette zur totalen Überwachung

von: Christof Windeck

Drahtlose Kollekte - RFID-Tags überwachen den Autoverkehr
TÜV-Plaketten mit drahtlos auslesbaren Identifikationschips ermöglichen nicht nur die Maut-Abrechnung, sondern auch flächendeckende Geschwindigkeitsüberwachung.

Weitgehend unbemerkt von der Öffentlichkeit erobern drahtlose digitale Kennzeichen unser tägliches Leben. Radio Frequency Identification (RFID) löst nicht nur die Strichcodes auf Verpackungen ab [1], sondern lässt sich auch unsichtbar in Produkte, Tiere und Menschen einbauen. Passende Lesegeräte erfassen die winzigen Smart Tags unbemerkt auch auf größere Entfernung - im Supermarkt der Zukunft braucht man die Waren an der Kasse gar nicht mehr aus dem Einkaufswagen (oder der Manteltasche) zu nehmen, und die Kasse erkennt die Rabattkarte mit RFID-Chip auch, wenn der Kunde sie im Portemonnaie stecken lässt. Die RFID-Technik ist standardisiert und kommt weltweit zum Einsatz, sodass Lesegeräte bald sehr preiswert zu haben sein dürften.

Eher zufällig stießen wir auf eine offenbar schon vor Monaten eingeführte RFID-Anwendung. Dank rigoroser Geheimhaltung lief unbehelligt von Kritikern und Datenschützern ein sorgfältig vorbereitetes Überwachungsprogramm an, ob dessen Umfangs man kaum noch von einem "Feldversuch" sprechen kann. Arglose Autobesitzer stellen dabei die Versuchskaninchenschar, ohne das Geringste davon zu ahnen. Schlimmer noch: Die Zeichen deuten darauf hin, dass die Karnickel demnächst zur Jagd freigegeben werden.

Reporter Zufall

Während eines Tests von Navigationssystemen wunderten sich die c't-Redakteure über sporadische Knacksgeräusche des billigen PMR446-Handfunkgeräts, die reproduzierbar vor allem in der Nähe des Fahrzeughecks auftraten. Ein EMV-Messgerät aus dem c't-Labor entlarvte dann Unglaubliches: Ein in der TÜV-Plakette verborgener RFID-Chip war die Störquelle. Für die Smart Tags ist in Europa neben 13,56 MHz und 2,446 GHz auch der Bereich um 435 MHz (ISM SRD) vorgesehen; dieser liegt nur 2,5 Prozent unter dem PMR446-Band, die zweite Oberwelle kommt nahe an 890 MHz heran, die untere Grenzfrequenz für D-Netz-Handys. Offenbar antwortet die Auto-Wanze auf starke Hochfrequenzfelder, wenn diese in der Nähe der eigenen Frequenz liegen, und die Antwortsignale wiederum scheinen die Empfänger zu verwirren.

Beim vorsichtigen Abziehen entlarvt sich die unscheinbare TÜV-Plakette als Funk-Wanze.

Doch wie kommt der Funk-Chip in die TÜV-Plakette - und was hat er dort zu suchen? Eine Internet-Recherche liefert erste Hinweise. Die mittlerweile liquidierte Nemesys GmbH aus Essen, eine Tochterfirma der RWTÜV AG [2], erhielt bereits 1996 ein europäisches Patent [3] auf ein automatisiertes System zur Geschwindigkeitsüberwachung auf Basis von Lasermessung und Fahrzeugidentifikation per Digitalkamera. Das Funktionsprinzip ließe sich viel einfacher mit RFID-Chips realisieren, denn über den Doppler-Effekt ist die Geschwindigkeit eines mit einem Sender versehenen Fahrzeugs sehr präzise messbar - daran

arbeitet unter anderem die TU Clausthal [4]. Dient als HF-Sender ein RFID-Etikett, bekommt man die automatische Identifikation als Dreingabe dazu.

Nicht mit mir: Ein HF-Kondensator hinter dem Nummernschild verstimmt die Antenne des RFID-Chips.

Die nötigen Funk-Chips für den automobilen Einsatz sind indes längst verfügbar. Der Autoschilder-Spezialist Utsch [5] hat in Kooperation mit Schreiner ProSecure [6] und Infineon den IL-Tag entwickelt, eine serienreife RFID-Kennzeichnung für Kraftfahrzeuge. Dieselbe Firma Schreiner ProSecure stellt auch TÜV-Plaketten her - kann das alles Zufall sein?

Speed Correct

Es gibt natürlich keine Beweise für den Einstieg der genannten Firmen in die flächendeckende Verwanzung deutscher Autos. Der Einsatz dieser Technik liegt aber auf der Hand. Drahtlos auszulesende Fahrzeugkennzeichen ermöglichen eine simple und preiswerte Mauterfassung; das ist in Frankreich [7] und den USA [8, 9] gängige Praxis. Smart Tags wären also eine Alternative für die geplante LKW-Maut, falls das technisch aufwendige und teure Toll-Collect-System endgültig scheitert. Auch die Maut für Autos und Motorräder - von Insidern längst erwartet - ließe sich mit kleinen RFID-Plaketten leicht und preiswert einführen. Die bereits von Toll Collect [10] entlang deutscher Autobahnen aufgebauten Mautbrücken könnte man leicht mit RFID-Lesern nachrüsten. Auch andere Infrastruktur ließe sich weiternutzen, etwa das im Raum Hannover zur Expo 2000 installierte Move-System zur Verkehrsbeeinflussung [11].

Toll-Collect-Mautbrücke: bald Basis für Speed Correct?

Zur flächendeckenden Erfassung ist eine große Zahl von Lesestationen nötig, aber diese sind billig und eröffnen gerade durch ihre große Anzahl völlig neue Möglichkeiten für die Verkehrsüberwachung und Strafverfolgung, etwa die Entlarvung chronischer Raser. Dazu reicht es, die Zeit zu messen, in der ein Fahrzeug einen bestimmten Streckenabschnitt zwischen zwei Mautbrücken zurücklegt. Anschließend vergleicht man das Ergebnis mit der kürzest möglichen Fahrtdauer, die sich unter Beachtung der entlang der gefahrenen Strecke geltenden Geschwindigkeitsbeschränkungen erzielen lässt. Kam das Fahrzeug schneller an der zweiten Messstation an, als es die Polizei erlaubt, erhält der Halter automatisch eine Verwarnung. Bürgerrechtsorganisationen schienen den Braten bereits gerochen zu haben und forderten schon im Februar den unverzüglichen Abbau der Mautbrücken. Doch anscheinend ist das Kind bereits in den Brunnen gefallen.

Totale Kontrolle

Anders als in den USA oder in Frankreich, wo Maut-Autobahnen in privater Hand sind, hätten deutsche Behörden unmittelbaren Zugang zu RFID-Daten. Und selbst wenn Datenschützer die Maut-Abrechnung vor direktem Polizeizugriff schützen: Über die große Zahl alltäglicher Erfassungsvorgänge und durch die Einbeziehung anderer Daten aus polizeilichen Routinekontrollen oder der in einigen Bundesländern "erprobten" automatischen Kennzeichenerfassung per Videokamera [12] (übrigens erleichtert durch den merkwürdigen Schriftschnitt der neuen Kennzeichenlettern) wird die Zuordnung des Funk-Etiketts zum Fahrzeughalter per Data-Mining eine leichte Übung.

Die billige Handgurke dient als Anti-Spionage-Waffe.

Durch zwangsweise Verwanzung mit strahlenden TÜV-Plaketten wären alle in Deutschland zugelassenen Autos innerhalb kürzester Zeit drahtlos zu orten. Autobahnauffahrten und Innenstadt-Kreuzungen ließen sich schnell mit Lesegeräten ausstatten. RFID-Handys ermöglichen mobilen Greiftrupps Geschwindigkeitsmessung und Fahrzeugidentifikation gleichzeitig. Per UMTS-Anbindung ist auch die Halterfeststellung am Tatort kein Problem.

Bürgerwehr

Doch die drahtlose Fahrspaß-Bremse lässt sich aushebeln. Der enttarnte RFID-Chip versteckt sich in einer aufgenieteten TÜV-Plakette; anscheinend sind unauffällig verwanzte Klebe-Etiketten noch nicht serienreif. Nach einigen Versuchen konnten wir den Transponder kaltstellen, ohne die Plakette zu zerstören.

Ein übliches Nummernschild mit seinen 52 cm Länge bildet einen exakt abgestimmten 3/4-Lambda-Strahler für das 435-MHz-Signal (70 cm Wellenlänge!); nur durch Einsatz dieser Hilfsantenne kann der RFID-Chip die geforderten Reichweiten zur Fahrzeugerfassung überbrücken. Belastet man die exakt abgestimmte Antenne - also das Nummernschild - an geeigneter Stelle kapazitiv mit einem Lambda-Achtel-Kondensator, bricht der Antennengewinn um mehr als 10 dBµV zusammen, und aus ists mit dem Lauschangriff.

Das hört sich kompliziert an, ist aber sehr einfach zu realisieren: Sie benötigen ein auf 86,1 Millimeter Kantenlänge zugeschnittenes Quadrat aus Aluminiumfolie, das als Gegenelektrode dient. Als Dielektrikum und Klebstoff reicht Kerzen-Paraffin (relative Dielektrizitätszahl 2,2). Die Paraffinschicht muss möglichst dünn und gleichmäßig ausfallen, das Folienquadrat pappt man rückwärtig dort aufs Nummernschild, wo vorne der Speed-Correct-Sender, sprich die Plakette, sitzt. Noch ist das nicht verboten, aber zur Not geht es auch rückstandsfrei wieder ab.

Zur Erfolgskontrolle lässt sich hervorragend ein bezüglich EMV-Konformität noch "undichtes" D-Netz-Handy der ersten Generationen verwenden: Kommt eine damit in der Nähe des Nummernschildes versendete SMS verstümmelt an, hat das RFID-Tag dazwischengefunkt. Die Störungen werden umso wahrscheinlicher, je länger die SMS ist und je höher die Buchstaben im ASCII-Alphabet angesiedelt sind; hoch geeignet erscheint uns eine SMS aus 143 großen Üs, die man an sich selbst sendet. Zur Komplettierung unserer geografischen Verbreitungsübersicht freuen wir uns über Positiv- und Negativmeldungen an die eigens dafür eingerichtete E-Mail-Adresse rfidtuev@ctmagazin.de - eine anonyme Mitteilung mit Angabe der Postleitzahl und des Handy-Typs genügt.

Stand-Ort Deutschland

Es ist absehbar, dass Vater Staat seine Big-Brother-Anwandlungen mit hehren Zielen verbrämen wird. Als Vorwand zur Gängelung freier Bürger dürften wieder einmal die Absenkung der Unfallzahlen und der Umweltschutz herhalten, wobei man aber den RFID-Elektrosmog geflissentlich übersieht. Genau wie Microsoft sein Trusted-Computing-Konzept zur Beschneidung von Nutzer-Rechten als Sicherheitssystem zum Schutz privater Daten und vor Viren verkaufen will, wird man den Autobesitzern die Funk-Kennzeichnung als Diebstahls- und Missbrauchschutz andrehen wollen. Dazu ist direkter staatlicher Druck gar nicht nötig: Es reicht, wenn die Versicherungen unmarkierte Fahrzeuge nicht mehr akzeptieren - wie bei der Wegfahrsperre. Deutschland ist auf dem besten Wege zum

buchstäblichen Stand-Ort. (ciw)

Literatur

[1] Jürgen Kuri, Angela Meyer, Peter Schüler, Im Fadenkreuz, Verbindungsdatenspeicherung, Biometrie, DRM, RFID: die Aushöhlung des Datenschutzes, c't 6/04, S. 138
[2] RWTÜV AG: www.rwtuev.de
[3] Digitale Geschwindigkeitsmessung mit Lasern der Firma Nemesys: Europäisches Patent EP 0 741 377 von 1996, www.depatisnet.de
[4] Geschwindigkeitsmessung mit aktivem Transponder: www.iei.tuclausthal.de/methods/projekt_seite?project_id=radarpositioning
[5] Schreiner Group (ProSecure, LogiData): www.schreiner-online.com
[6] IL-Tag der Utsch AG: www.utsch.com/iltag
[7] Liber-T, drahtlose Mauterfassung in Frankreich (Télépéage): www.saprr.fr
[8] Automatische Mauterfassung in Virginia: https://smart-tag.com
[9] Automatische Mauterfassung in New Jersey: www.ezpass.com
[10] Detlef Borchers, Verursacherbedingt verspätet, Das "fortschrittlichste Mautsystem der Welt" und die Realität, c't 22/03, S. 92
[11] move GmbH: www.move-info.de
[12] Kennzeichen-Erfassung in Thüringen und an der bayerischen Grenze www.heise.de/newsticker/meldung/43046