

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

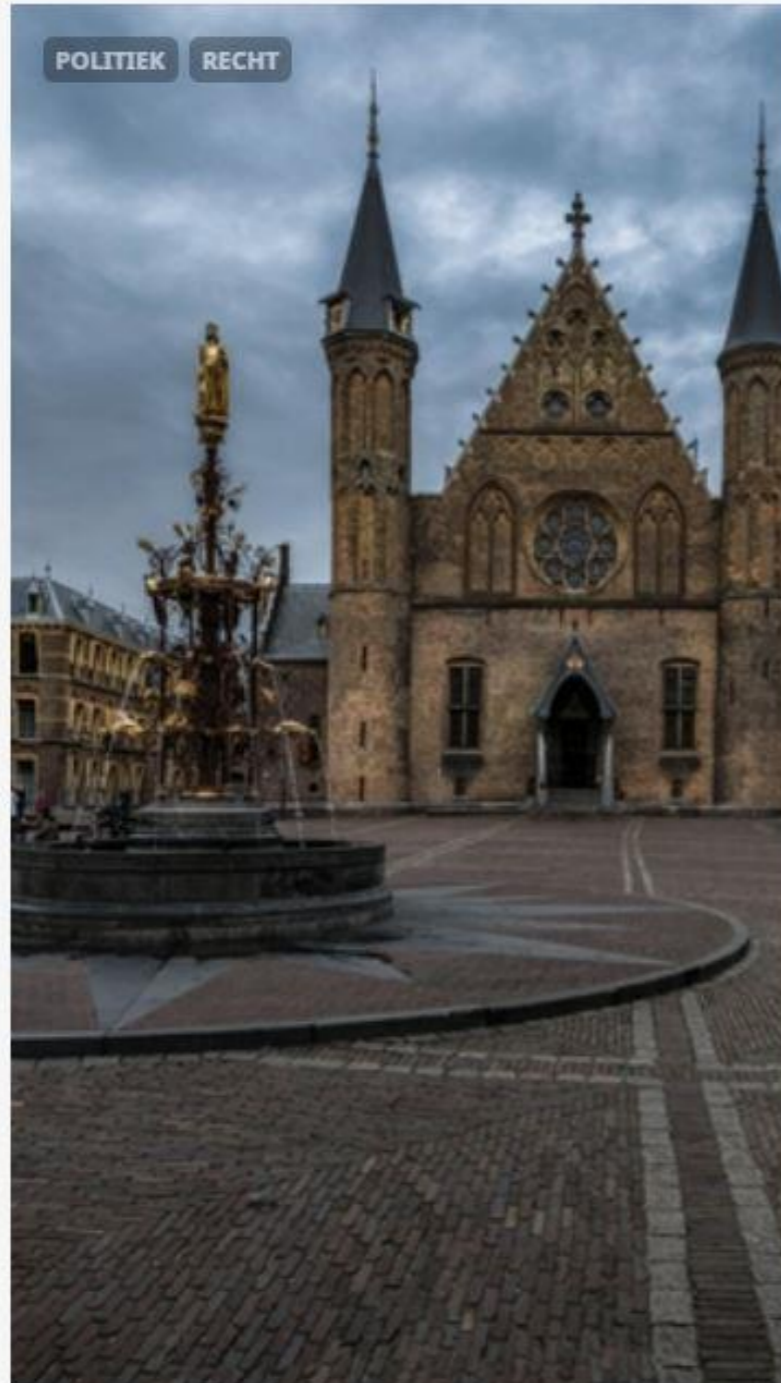
For additional information about this publication click this link.

<http://hdl.handle.net/2066/196298>

Please be advised that this information was generated on 2020-09-25 and may be subject to change.

Jouw interessegebieden worden getoond

Recht ([aanpassen](#))

[AGENDA](#)[INTERESSES](#)

POLITIEK RECHT

De Grondwet rigide? Dat valt te bezien

02



ACTUALITEITEN ETHIEK RECHT

Cartoonwedstrijd: neem de grenzen van de grondrechten in acht

03



ETHIEK MAATSCHAPPIJ RECHT

Waarom Martha Nussbaum ons moet blijven boeien

03



ACTUALITEITEN RECHT

Zaak Nicky Verstappen: doorbraak door Nijmeegse DNA-software

02



DIVERSITEIT ETHIEK RECHT

De duivelse dilemma's van een rechter

03

Cybersecurity en de verplichting tot het bijwerken van onveilige software in het Nederlandse privaatrecht

P.T.J. Wolters

p.wolters@jur.ru.nl

Radboud Recharge 6 oktober 2018

Wired – 7 maart 2017

ANDY GREENBERG SECURITY 03.07.17 04:03 PM

HOW THE CIA CAN HACK YOUR PHONE, PC, AND TV (SAYS WIRILEAKS)

Wired – 21 juli 2015

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

Roel Verdult

*Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.*

rverdult@cs.ru.nl

Flavio D. Garcia

*School of Computer Science,
University of Birmingham, UK.*

f.garcia@cs.bham.ac.uk

Bariş Ege

*Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.*

b.ege@cs.ru.nl

Abstract

The Megamos Crypto transponder is used in one of the most widely deployed electronic vehicle immobilizers. It is used among others in most Audi, Fiat, Honda, Volkswagen and Volvo cars. Such an immobilizer is an anti-theft device which prevents the engine of the vehicle from starting when the corresponding transponder is not present. This transponder is a passive RFID tag which is embedded in the key of the vehicle.

In this paper we have reverse-engineered all proprietary security mechanisms of the transponder, including

1 Introduction

Electronic vehicle immobilizers have been very effective at reducing car theft. Such an immobilizer is an electronic device that prevents the engine of the vehicle from starting when the corresponding transponder is not present. This transponder is a low-frequency RFID chip which is typically embedded in the vehicle's key. When the driver starts the vehicle, the car authenticates the transponder before starting the engine, thus preventing hot-wiring. In newer vehicles the mechanical ignition key has often been removed and replaced by a start button, see Figure 1(a). In such vehicles the immobilizer transponder is the only anti-theft mechanism that prevents a hijacker from driving away.

Telegraph.co.uk – 30 juli 2013

HOME » FINANCE » NEWS BY SECTOR » INDUSTRY

Volkswagen sues UK university after it hacked sports cars

Volkswagen has sued the University of Birmingham to stop it revealing how to hack anti-theft systems on luxury cars such as Porsches, Audis, Bentleys and Lamborghinis.



Researchers were able to hack the anti-theft system on Lamborghinis

Grondslagen in het Nederlandse privaatrecht

- 7:17 BW – Conformiteit. Een afgeleverde zaak moet
 - De eigenschappen bezitten die de koper mag verwachten.
 - Geschikt zijn voor normaal gebruik.
- 6:248 lid 1 BW – redelijkheid en billijkheid.
- 7:401 BW – goed opdrachtnemer.
- 7:206 lid 1 BW – verhelpen gebreken door verhuurder.
- 6:162 BW – ongeschreven recht.

Grondslagen

- ‘Open normen’.
- Geen expliciete cybersecurityverplichting.
- Het bestaan en de omvang van de verplichting hangt af van de omstandigheden van het geval.

Juridische argumenten voor het aannemen van een verplichting tot updaten

- Security updates worden regelmatig uitgebracht. Consumenten mogen ze daarom ook verwachten.
- Kun je een slecht beveiligde smartphone 'normaal' gebruiken?

Economische argumenten voor het aannemen van een verplichting tot updaten

- Samsung kan beveiligingslekken relatief gemakkelijk repareren.
- *Een* update kan *alle* telefoons beveiligen.
- Samsung verkoopt nog steeds telefoons met Android.
- Vertrouwen koper.

Wet bescherming persoonsgegevens/Algemene verordening gegevensbescherming

- Verplichting tot het beveiligen van de verwerkte persoonsgegevens.
- Wat is de relatie tussen de beveiliging van de telefoons en de verwerking door Samsung?

Vordering Consumentenbond

III. Samsung te bevelen alle smartphones in Nederland gedurende een periode van vier jaar na de introductie op de markt en/of twee jaar na het moment van verkoop door Samsung of via een retailkanaal te voorzien van updates die kwetsbaarheden in de software repareren, althans updates die een door Google als “kritiek” aangemerkt beveiligingslek in het Android besturingssysteem repareren, steeds binnen een maand nadat de update door Google beschikbaar is gesteld, althans een door de rechtbank in goede justitie te bepalen bevel;

Kortgezegd:

- Samsung dient de beveiliging van de telefoons bij te werken.
- Twee jaar na de verkoop, en vier jaar de introductie.
- In het bijzonder kwetsbaarheden die door Google als ‘kritiek’ zijn aangemerkt en waarvoor Google een update beschikbaar heeft gesteld.
- Binnen een maand.

De rechter erkent de verplichting tot het bijwerken van de beveiliging

4.14.

- “Niet ter discussie staat dat in dit verband van Samsung kan worden verwacht dat zij voldoende adequaat en doeltreffend optreedt tegen de hiervoor omschreven veiligheidsrisico’s van door Google als critical aangemerkte kwetsbaarheden.”
- “Wat voldoende en adequaat en doeltreffend is, wordt mede bepaald door de aard en de ernst van de zich daadwerkelijk/reëel voordoende veiligheidsrisico’s.”
- “Voor toewijzing van de vorderingen is alleen plaats als de conclusie luidt dat Samsung feitelijk te weinig doet ter bestrijding van de veiligheidsrisico’s door niet **in alle gevallen** gedurende de door de Consumentenbond genoemde periode en binnen de door de Consumentenbond genoemde termijn upgrades en updates door te voeren.”

De rechtbank wijst de vordering af

- Niet-ontvankelijk voor zover de vordering betrekking heeft op de toekomst.
- Niet ieder 'kritiek' beveiligingslek lijdt tot onaanvaardbare risico's.
- Het bijwerken van software is complex.
- Samsung mag prioriteiten aanbrengen.
- Conclusie: Samsung is *niet altijd* verplicht om de telefoons bij te werken.

Een concrete vordering - complicaties

- Samsung kan een specifiek beveiligingslek alsnog wegnemen.
- Geen belang in de zin van 3:303 BW bij een verklaring voor recht.

Conclusie

- Het Nederlandse privaatrecht creëert cybersecurityverplichtingen.
- De precieze omvang van deze verplichting is niet duidelijk.
- Het is niet eenvoudig om deze verplichting in de rechtspraak te concretiseren.