Senator Mike Kowall
S-309, Capitol Building
100 N. Capitol Ave.
Lansing, MI 48933

May 16, 2016

RE: Car Hacking Legislation – S.B. 0927 (2016)

Dear Senator Kowall:

We the undersigned cybersecurity companies, organizations, and professionals write to express our concern with S.B. 0927 (2016).[1] The legislation would amend MCL 752.794 to create a new crime that forbids, among other things, intentionally accessing or causing access to an electronic system of a motor vehicle to willfully alter or gain unauthorized control of a motor vehicle. The legislation would punish violations with a potential life sentence. Although we appreciate the goal of protecting motorists from cyber threats, we are concerned that – as written – the bill would hinder valuable independent security research. Blocking independent research to uncover vehicle software flaws would undermine cybersecurity and put motorists at greater risk. We respectfully urge reconsideration or amendment of this legislation.

Independent computer researchers frequently access electronic systems to assess and report flaws in the software. This research strengthens cybersecurity because the researchers call attention to software vulnerabilities that manufacturers may have missed or even ignored, which encourages manufacturers to make timely, appropriate fixes to keep people safe. For example, in Jul. 2015, researchers found serious security flaws in Jeep software, prompting a recall of 1.4 million vehicles.[2] Another example: in Sep. 2015, researchers found Volkswagen software was designed to skirt emissions laws.[3]

Motorists are safer as a result of such independent research. However, future research would be hindered by S.B. 0927 since the bill neither protects researchers nor requires any unlawful purpose as a prerequisite for prosecution.[4] By prohibiting "causing access" to vehicle software, S.B. 0927 may even chill academics publishing technical assessments of gaps in vehicle security, since they may be held to have "caused" access if their work is used as a basis for unauthorized access to vehicle software.

In addition, S.B. 0927 does not explicitly permit vehicle owners to access the software of their own vehicles, nor to authorize researchers or repair shops to access vehicle software on the owners' behalf, to fix cybersecurity flaws. Several vehicle manufacturers claim that vehicle owners only license – and do not own – the software in their vehicles, and that vehicle owners need the manufacturers' permission to access the software in their own vehicles.[5] Manufacturers that do not support independent research and repair, or that may have something to hide (as in the case of Volkswagen), could simply deny the owner permission to access vehicle systems – and owners that access, or hire security research or repair services to access, their own vehicles may then be liable under S.B. 0927. This can leave more cybersecurity vulnerabilities undiscovered and motorists at greater risk.

It is unclear why S.B. 0927 is necessary. Michigan law – at MCL 752.795 – already broadly forbids accessing a computer to acquire or alter property "or otherwise use" the computer without

[1] https://www.legislature.mi.gov/documents/2015-2016/billintroduced/Senate/pdf/2016-SIB-0927.pdf
[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[3] http://www.autoblog.com/2015/09/23/researcher-how-vw-got-caught/?ncid=edlinkusauto00000015
[4] Compare, for example, to MCL 752.794 and 752.796.
[5] http://www.copyright.gov/1201/2015/comments-032715/class%2021/Auto_Alliance_Class24_1201_2014.pdf

authorization.[6] Violations are punished as felonies.[7] The existing definition of "computer" in Michigan law encompasses computers embedded in vehicles.[8] Other Michigan laws forbid the use of computers to defraud or commit any crime.[9] If the intent of the bill is to make clear that vehicle computers are protected under Michigan law, this could be achieved with a minor alteration to the existing definition of "computer" to explicitly include computers and computer systems integrated in vehicles.

To avoid negative consequences to researchers and consumers, we respectfully urge reconsideration of the legislation. The bill could also be amended to mitigate these issues through the following revisions:

1. Make clear that neither MCL 752.794(2) nor 752.795 apply to access solely for the purpose of good faith testing, investigating, correcting, or repairing known or potential security flaws, vulnerabilities, or broken or degraded components of a computer program, computer, computer system, or computer network, carried out in a manner designed to avoid harm to individuals or the public.

2. Make clear that, for purposes of MCL 752.794.2, authorized individuals can access vehicle electronic systems, and that "authorization" includes grant of permission by both lawful owners and licensees of the vehicle electronic systems.

We appreciate that S.B. 0927 is aimed at protecting motorists from cyber attack. As modern vehicles are built with more software and autonomy, strengthening vehicle cybersecurity should be a high priority. However, independent security research is a catalyst for better cybersecurity, and regulations should avoid chilling this increasingly important activity that has already made us safer. We hope you will consider revising your legislation to reflect these concerns. If you have any questions, or if we can be of any assistance, please do not hesitate to contact us.

Sincerely,

Rapid7
Bugcrowd
Duo Security
Grimm
HackerOne
I Am The Cavalry
Kryus
Luta Security
Nmap Project
Open Garages
Veracode
Virta Laboratories, Inc.

[6] MCL 752.795. "A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following: (a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network. (b) Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network."
[7] MCL 752.797(2).
[8] MCL 752.792(3).
[9] MCL 752.794 and 752.796.

Kevin Fu, Associate Professor, Electrical Engineering and Computer Science, University of Michigan
Robert Graham, CEO, Errata Security
J. Alex Halderman, Associate Professor, Computer Science and Engineering, University of Michigan
Peter Honeyman, Research Professor of Computer Science and Engineering, University of Michigan
Dan Kaminsky, Chief Scientist and Cofounder, White Ops
Zachary Lanier, Director of Research, Cylance, Inc.
Art Manion
HD Moore, Principal, Special Circumstances, LLC
Atul Prakash, Professor, Electrical Engineering and Computer Science, University of Michigan
André Weimerskirch, Association Research Scientist, University of Michigan Transportation Research Institute

Cc:
Senator Ken Horn
Senator Wayne A. Schmidt
Senator Rebekah Warren
Senator Rick Jones
Senator Tonya Schuitmaker
Senator Steven M Bieda
Senator Tory Rocca
Senator Patrick Bolbeck