

Right to Repair

## O) repair.org

## Fix, or Toss? The 'Right to Repair' Movement Gains Ground

Both Republicans and Democrats are pursuing laws to make it easier for people to fix cellphones, cars, even hospital ventilators. In Europe, the movement is further along.



#### Right to Repair is a Growing Movement





#### 88% of Voters

in Massachusetts overrode the car companies and passed the automobile owners' Right to Repair law in November, 2012.

#### 114,322 Americans

signed a petition to legalize cell phone unlocking. The White House supports cell phone unlocking—but your voice is still needed to convince Congress.

## Monopoly Strategies Copyright on Service Manuals



31st July 2012

Dear Mr Hicks,

Toshiba copyright Repair Manuals.

We understand that you are the owner and editor of a website that is found at <a href="http://tim.id.au">http://tim.id.au</a> and that your ABN is

On your website we are able to read and see that you are distributing, by download, copyright repair manuals (the Manuals) that are proprietary to Toshiba (Australia) Pty Limited and its parent company, Toshiba Corporation of Japan (Toshiba).

The Manuals are only available to Toshiba authorised service providers under strict confidentiality agreements. You are not a Toshiba authorised service provider and therefore you have no rights to have any of the Manuals that are listed and linked under the heading "Toshiba" that appears on your website.



## TOSHIBA

Leading Obsolescence

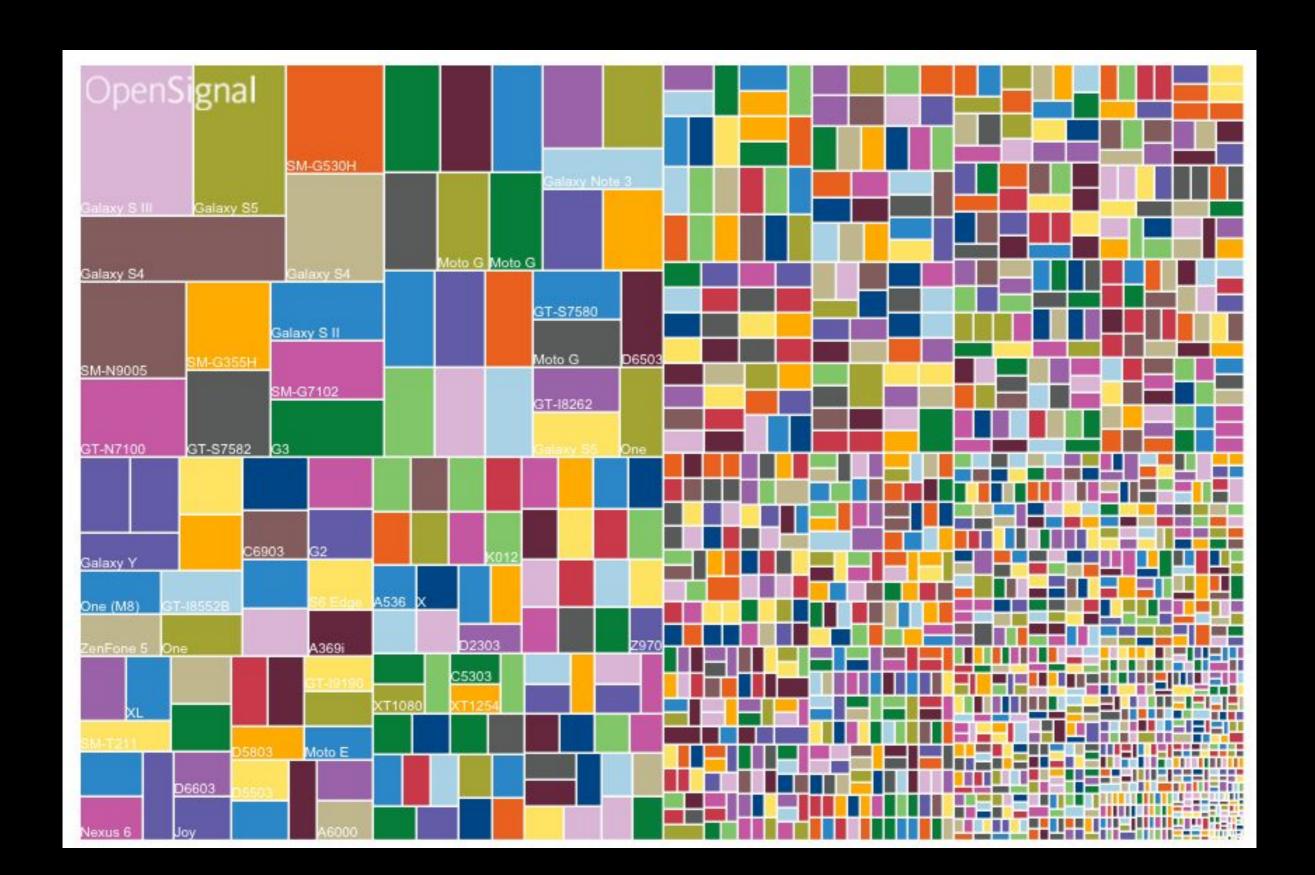


| Localytics | CS |
|------------|----|
|------------|----|

| ■ iPhone XR         | 13.54% |
|---------------------|--------|
| iPhone 7            | 11.61% |
| iPhone 8            | 11.4%  |
| ■ iPhone X          | 10.68% |
| ■ iPhone 8 Plus     | 9.26%  |
| ■ iPhone 7 Plus     | 6.8%   |
| ■ iPhone 6S         | 6.8%   |
| iPhone XS Max       | 6.65%  |
| iPhone XS           | 5.63%  |
| iPhone 11           | 4.28%  |
| iPhone 6            | 3.97%  |
| ■ iPhone 11 Pro Max | 3.25%  |
| ■ iPhone 6S Plus    | 2.62%  |
| iPhone 11 Pro       | 2.49%  |
| iPhone 6 Plus       | 1.02%  |

Source: Localytics December 2019

#### **Android Fragmentation**

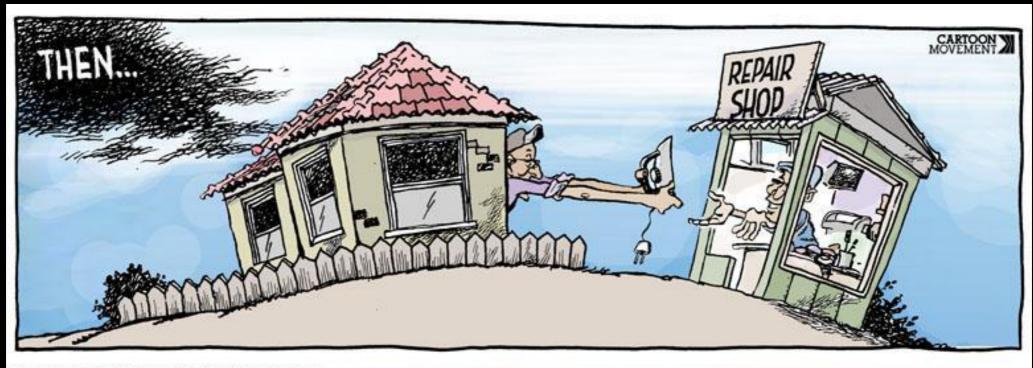




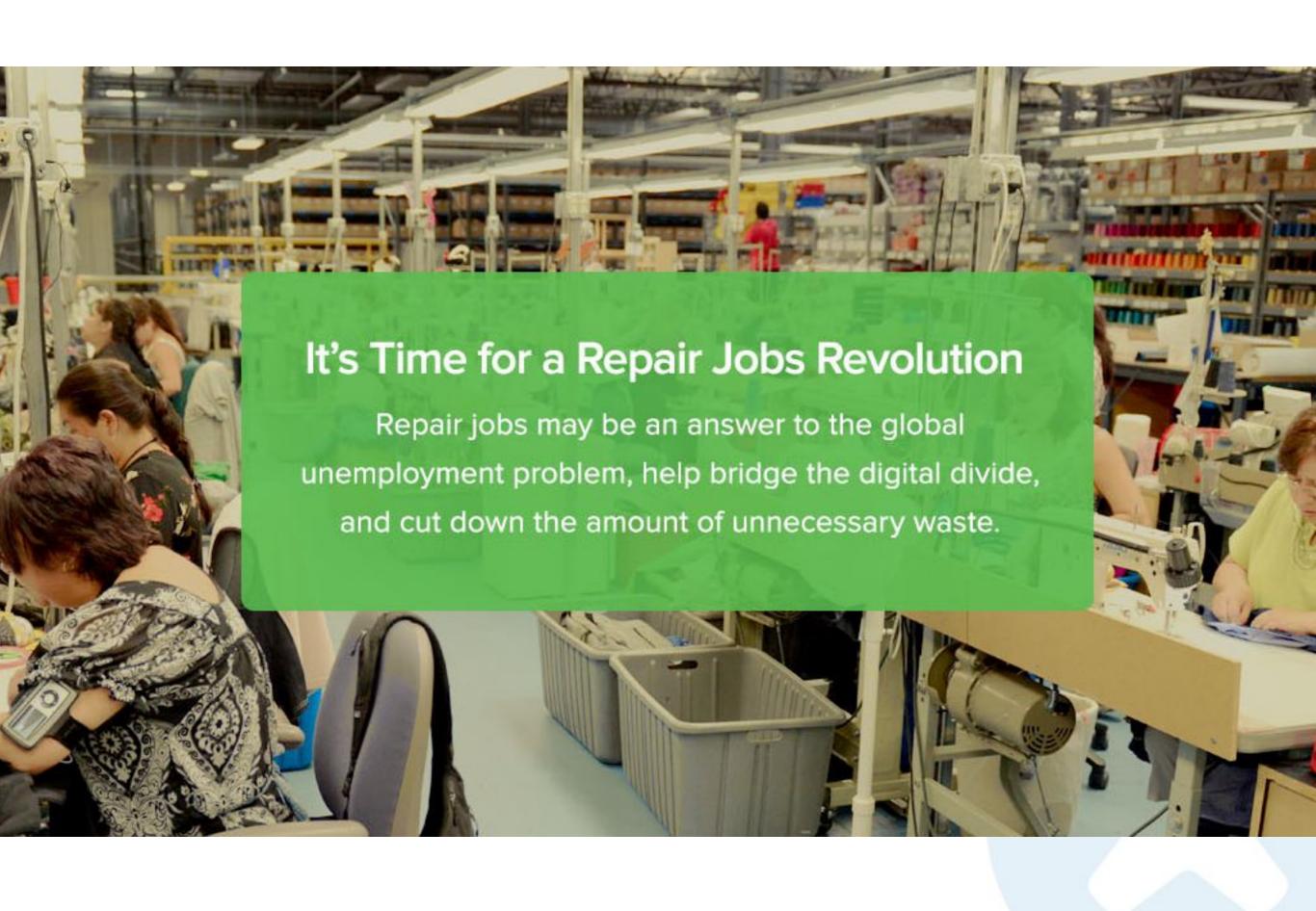
#### Right to Repair Legislation

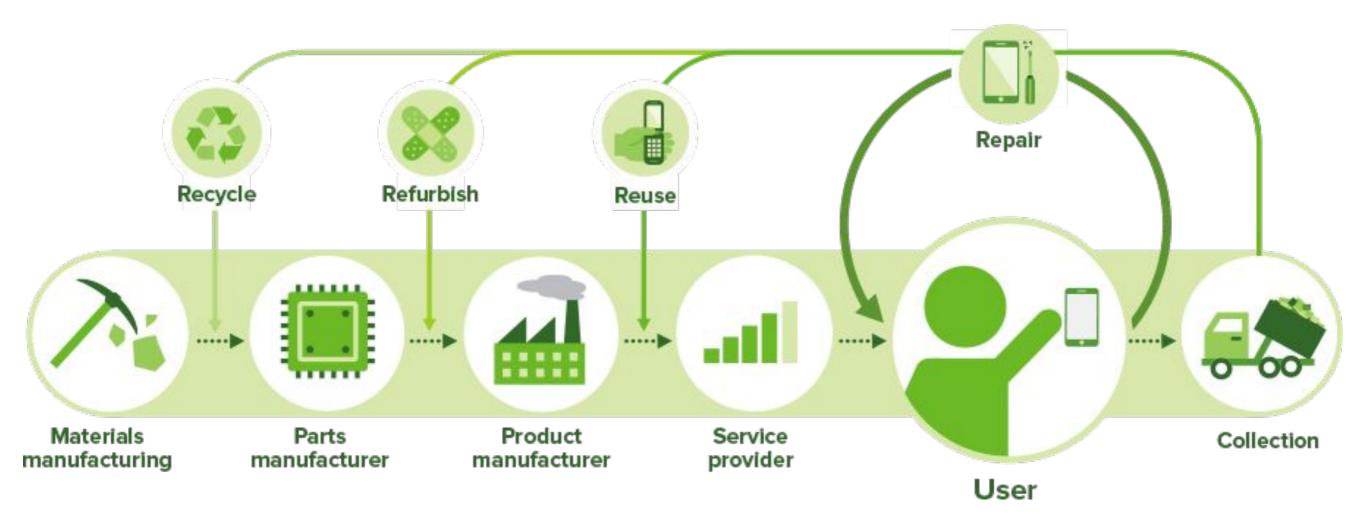
Parts + Tools + Know-how

2020 – State Legislative Activity "Heat Map" (forecast) MT ND MN OR ID WI MI SD СТ WY DE IA ОН NE IL NV UT KY co CA KS MO SC High Risk (14) OK AR ΑZ NM GA Medium Risk (5) AL Low Risk TX









## Repair is a cornerstone of our environmental and economic future.

| 7 | т    | $\sim$ | ы | c |
|---|------|--------|---|---|
|   | - 10 | u      | - |   |

#### Los Angeles Times

START TRIAL 10 FREE wks

Tammie Jo Shults, who calmly landed Southwest Flight 1380, broke barriers as a fighter pilot



Attention women: Your choice of blood pressure medicine may affect your risk of pancreatic...



East Bay fault is 'tect bomb,' more da Andreas, new s

BUSINESS

LA TIMES

### Those stickers warning that repairs will void your warranty are nonsense, FTC says



By WASHINGTON POST APR 11, 2018 |

8:45 AM



**ABOUT THE FTC** 

**NEWS & EVENTS** 

**ENFORCEMENT** 

POLICY

**TIPS & ADVICE** 

44

Home » News & Events » Events Calendar » Nixing the Fix: A Workshop on Repair Restrictions

#### Nixing the Fix: A Workshop on Repair Restrictions

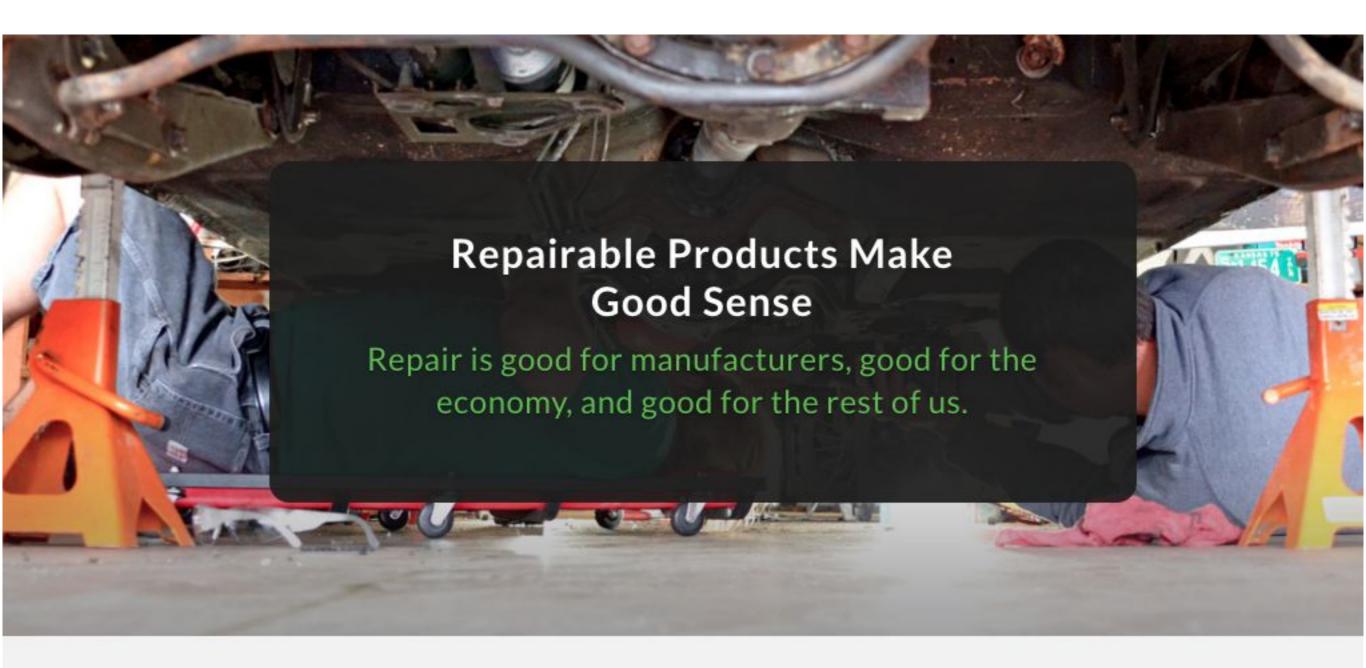


JUL 16, 2019 12:30PM

#### CONSTITUTION CENTER

400 7th St SW, Washington, DC 20024 I Directions & Nearby





We rate the latest products to make it easy to buy repairable hardware.

**Smartphones** 





#### iPhone 12 Pro

2020

- Display and battery replacements remain a priority in the new iPhones' design.
- Most other important components are modular and easy to access or replace.
- Glass on front and back doubles the likelihood of drop damage—and if the back glass breaks, you'll be removing every component and replacing the entire chassis.





#### Microsoft

#### Surface Duo

2020

- Batteries are glued and require extensive disassembly to service.
- The USB-C port is soldered directly to the main board.
- Uncommon tri-point screws secure key components.



### Samsung Galaxy Note 20 Ultra

2020

- Battery replacement remains far too difficult for a consumable component.
- Screen repairs are tedious, poorly prioritized, and unnecessarily expensive.
- \* You'll only need one screwdriver, a standard Phillips.



#### iPhone SE 2020

2020

- The two most commonly replaced components, display and battery, remain straightforward to access with the proper knowledge and tools.
- Most components are modular and independently replaceable, including many that are cross-compatible with iPhone 8.
- The fragile glass back is impractical to replace.

















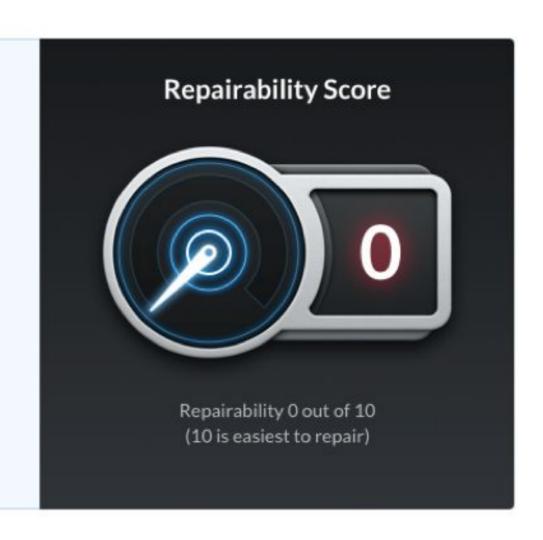






#### **Final Thoughts**

- This laptop is not meant to be opened or repaired; you can't get inside without inflicting a lot of damage.
- The CPU, RAM, and onboard storage are soldered to the motherboard, making upgrades a no-go.
- The headphone jack, while modular, can only be accessed by removing the heat sink, fan, display, and motherboard.
- The battery is difficult and dangerous to replace, giving the device a limited lifespan.



# Microsoft Surface Laptop 3 15"





## TEARDOWN



#### **Final Thoughts**

- The opening procedure is straightforward, with a clever design that represents a *dramatic* improvement over its predecessors.
- The M.2 SSD is fully modular and easy to access.
- Torx Plus screws call for relatively rare drivers, but our standard Torx drivers worked in a pinch.
- Display access is well-prioritized, but must be replaced as an (expensive) complete unit—subcomponents aren't modular.
- While many components are modular, intricate layered construction makes them difficult to service.
- The firmly glued-down battery will be very difficult to service when it inevitably goes kaput.

#### Repairability Score



Repairability 5 out of 10 (10 is easiest to repair)

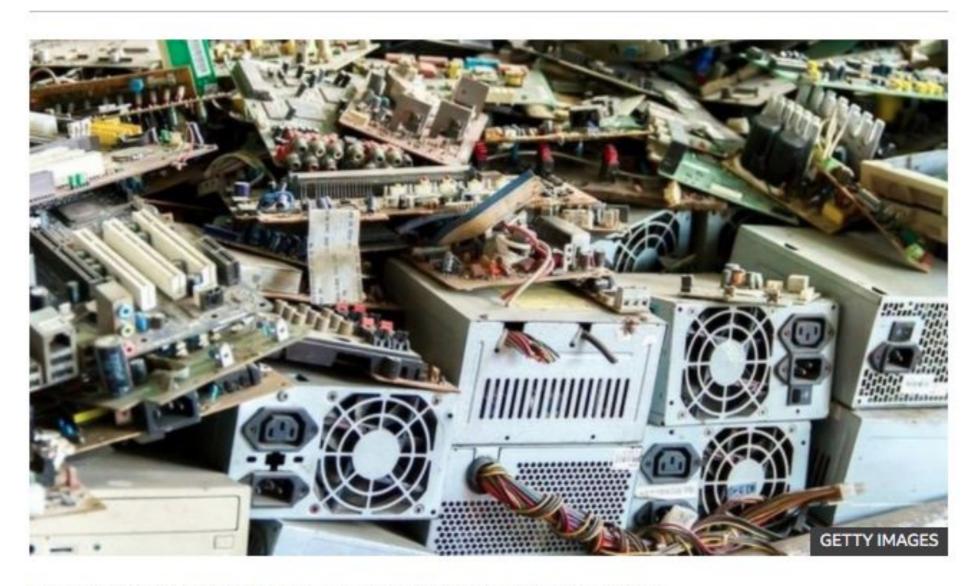
#### NEWS

Home US Election | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories

#### Electric goods 'should have repairability rating'

By Justin Parkinson Political reporter, BBC News

3 days ago



The government must look at forcing manufacturers to put "repairability" scores on electric devices, opposition parties have said.



# Right to Repair Legislation

Parts + Tools + Know-how





The Massachusetts "Right to Repair" Initiative, also known as Question 1, was on the November 6, 2012 general election ballot in the state of Massachusetts as an initiated state statute, where it was approved. The measure, originally filed four times with the Massachusetts Attorney General, was filed by Arthur W. Kinsman, and was assigned initiative numbers 11-17. The proposal required automobile manufacturers to provide non-proprietary diagnostic directly to consumers and also the safety information needed to repair their cars. [1][2]

According to reports, on the last day of session, a legislative compromise was confirmed. Although the compromise was enacted, Question 1 remained on the ballot. The measure became a law as well when voters approved it.<sup>[3]</sup>

# Type State statute Origin Right to Repair Coalition Topic Business regulation Status

#### Election results

See also: 2012 ballot measure election results

The following are official election results:

| Massachusetts Question 1 |           |            |
|--------------------------|-----------|------------|
| Result                   | Votes     | Percentage |
| ✓ Yes                    | 2,353,603 | 87.7%      |
| No                       | 392,562   | 12.3%      |

Results via the Massachusetts Secretary of State ...



**ABOUT THE FTC** 

**NEWS & EVENTS** 

**ENFORCEMENT** 

POLICY

**TIPS & ADVICE** 

44

Home » News & Events » Events Calendar » Nixing the Fix: A Workshop on Repair Restrictions

#### Nixing the Fix: A Workshop on Repair Restrictions



JUL 16, 2019 12:30PM

#### CONSTITUTION CENTER

400 7th St SW, Washington, DC 20024 I Directions & Nearby



# **DMCA 1201**

# 17 U.S. Code § 1201 - Circumvention of copyright protection systems

U.S. Code Notes

prev | next

- (a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES.—
  (1)
  - (A) No person shall <u>circumvent a technological measure</u> that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.



kylewiens.com @kwiens

# Hacking Tractors for Repair

Using MITM Brute Force



#### Motivation

 Companies are locking diagnostics and commands behind proprietary code.

- https://www.wired.com/story/john-deere-farmers-right-to-repair/
- https://ifixit.org/blog/7192/john-deere-mess/
- https://www.wired.com/2015/04/dmca-ownership-john-deere/
- Without access to information, repair becomes difficult.
- Tractor commands aren't encrypted. We can view and copy them.
  - With a library of possible commands we can create our own tools.



#### Progress

- The CAN "language" has an open source handbook to help figure out commands
  - http://opengarages.org/handbook/
- Previous students have captured data packets and parsed some of them
  - https://tractorhacking.github.io/documentation/ has their results and instructions for how to pickup where they left off.
  - The last group improved data collection with **PolyCAN**

#### Car Hacker's Handbook by OpenGarages

#### Download the book for free!

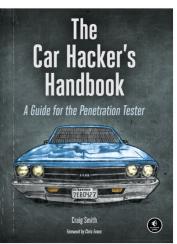
Below you can download the book in several different formats. The license of the books is under a <u>Creative Commons</u>. <u>Noncommercial-Share Alike license</u>, which lets you share it, remix it, and share your remixes, provided that you do so c

The Car Hacker's Handbook will give you a deeper understanding of the computer systems and embedded software in modern Âvehicles It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and Âbetween devices and

Then, once you have an understanding of a ÂvehicleA∈<sup>∞</sup>s communication network, youâ∈<sup>∞</sup> II learn how to Âintercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source has tools such as Metaspoliol, Wireshark, Kayak, can-utile, and AChipWhipperer, The Car Hackerde<sup>™</sup>s Handbook will show you how to:

- Build an accurate threat model for your vehicle
  Reverse engineer the CAN bus to fake engine signals
  Exploit vulnerabilities in diagnostic and data-logging systems
  Hack the ECU and other firmware and embedded systems
  Feed exploits through infotainment and vehicle-to-vehicle communic

View Book Onlin



#### **Documentation**

Documentation of our efforts to reverse engineer the John Deere CAN bus protocol can be found here. This documents work performed from September 2017 - March 2018.

- · Connecting to a Live System
- Connecting to the ECU
- Benchtop ECU Internals
- Future Reverse Engineering Work
- Processing Script
- Proprietary CAN IDs
- Technical Notes CAN
- Technical Notes J1939

Documentation of individual CAN-BUS IDs extracted from the tractor can be found below

**CAN-Bus ID Format Explanation** 

- 0 Torque/Speed Control 1
- 000C7802 Electronic Engine Controller 16
- 000C7803 Electronic Engine Controller 16
- 000C7EBE Electronic Engine Controller 16
- 000C7F65 Electronic Engine Controller 16
- 000C7F78 Electronic Engine Controller 16

#### General Goals

- Define John Deere Tractor CAN commands
  - Expand on existing library



- Attempt to get a bench ECU (Engine Control Unit) working.
  - We bought one. Record signals from live tractor, play back on ECU



## Required Skills

- Minor knowledge of electronics
- Knowledge of oscilloscope & function generators
- Programming



### **Implications**

- Help farmers around the world save time and money
- Learn how "Security through Obscurity" can be brute forced



#### **Deliverables**

- More CAN library commands
- Create oscilloscope symbol table
  - https://about.keysight.com/en/newsroom/backgrounders/CANdb 18FD 1000 Diesel Particulate Filter Control 1 https://about.keysight.com/en/newsroom/backgrounders/CANdb 18FD 18FD 1000 Diesel Particulate Filter Control 1 https:
  - http://socialledge.com/sjsu/index.php/DBC\_Format



Documentation of individual CAN-BUS IDs extracted from the tractor can be found below: CAN-Bus ID Format Explanation 0 - Torque/Speed Control 1 000C7802 - Electronic Engine Controller 16 • 000C7803 - Electronic Engine Controller 16 • 000C7EBE - Electronic Engine Controller 16 000C7F65 - Electronic Engine Controller 16 • 000C7F78 - Electronic Engine Controller 16 000C7F7E - Electronic Engine Controller 16 • 000C7FFD - Electronic Engine Controller 16 0C000006 - Torque/Speed Control 1 • 0CF00300 - Electronic Engine Controller 2 • 0CF00400 - Electronic Engine Controller 1 18F00503 - Flectronic Transmission Controller 2 • 18FE6900 - Engine Temperature 3 • 18FED500 - Alternator Information 18FEDF00 - Electronic Engine Controller 3 18FEE706 - Vehicle Hours • 18FEEE00 - Engine Temperature 1 • 18FEEF00 - Engine Fluid Level/Pressure 1 18FEF147 - Cruise Control/Vehicle Speed 1 • 18FEF200 - Fuel Economy (Liquid) 18FEF500 - Ambient Conditions • 18FEF600 - Intake/Exhaust Conditions 1 • 18FEF700 - Vehicle Electrical Power 1

18FEFC47 - Dash Display 11CFDDF47 - Front Wheel Drive Status



kylewiens.com @kwiens