Letting the Air Out of Tire Pressure Monitoring Systems

Mike Metzger - Flexible Creations
mike@flexiblecreations.com

History

- Porsche - First implemented on the 959 in 1986 (Thanks Wikipedia)
- A bunch of various styles used in luxury cars
- TREAD act - Basically, the Firestone / Ford Explorer problems in the 90's instigated legislation mandating use

TPMS Types

- Direct - This is used in most vehicles
  - Battery / Battery-less
- Indirect - Uses ABS and various calculations instead of a sensor
- Focus on battery-powered Direct TPMS

Direct TPMS Description

- Typically 4 sensors, possibly 5 w/ spare, mounted on wheel (behind the valve stem)
- Receiver is built into car, often collocated with the keyless entry components
- Car ECU / PCM processes info - behaves differently depending on car

Annoying TPMS Light

Sensor Description

- Most are a combination of an ASIC (ie, a microcontroller - Atmel / Freescale / Microchip, etc), a pressure sensor, and some RF components
- Typically part of the valve stem and sits in a recessed area of the rim, inside the tire
- RF transmits in 315MHz band (US) or 433MHz (EU)

Sensor Description

- Can be woken up by:
  - Rotation
  - Low frequency transmission (125kHz - modulated or continuous)
  - Magnets
- Transmission system varies by manufacturer but is typically once per minute unless there's a problem (meaning, significant pressure variation)
- Transmissions can overlap, requiring retransmits

Sensor Internals

- Siemens VDO (From a Mazda 3, 6, or RX-8)
- Uses an ATMEL AT092 chip (4-bit microprocessor)
- A MEMS style pressure sensor
- Simple RF transmission components
- Battery (CR2302)
- Assorted passive components

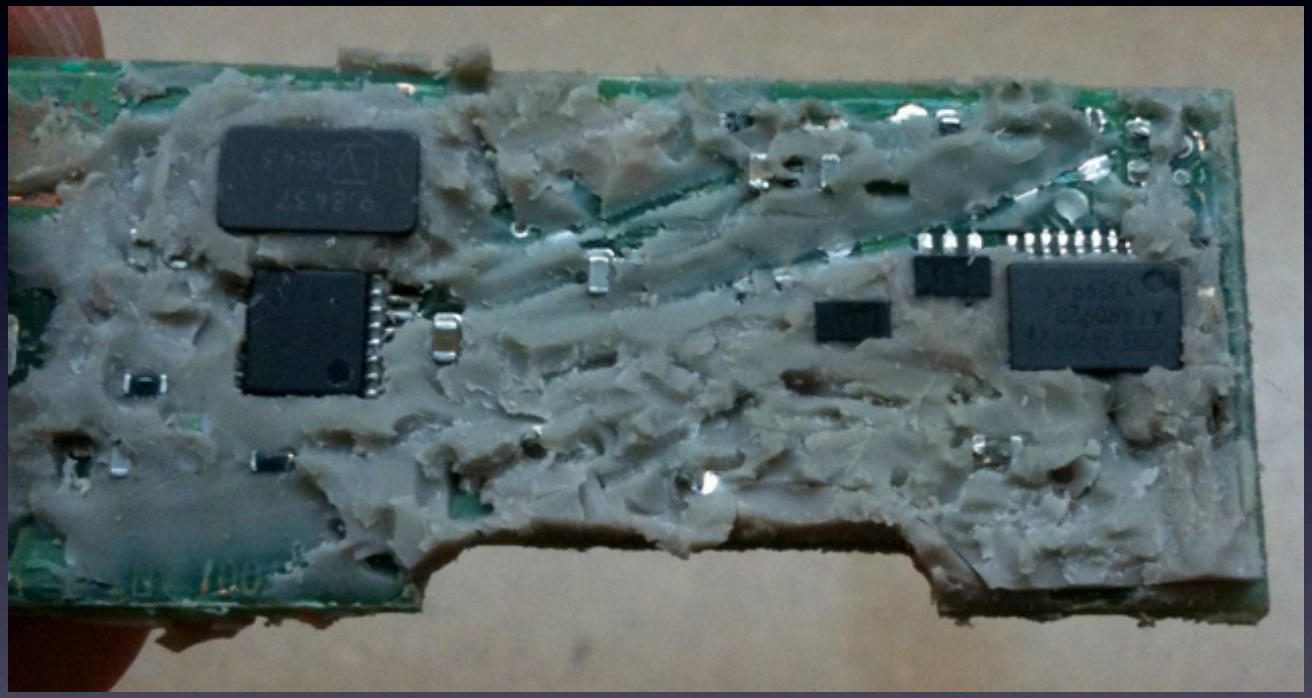
Before...


SIEMENS
S120092001A
>PA 6.6 GF30<
FE01-37140
3/10425/652506065
00984ABB
05164
FCC ID:
KR5S120092001

During...


SIEM
S120092001A
>PA 6.6 GF30<
FE01-37140
/10425/652506065
00984ABB
05164
FCC ID:
KR5S120092001

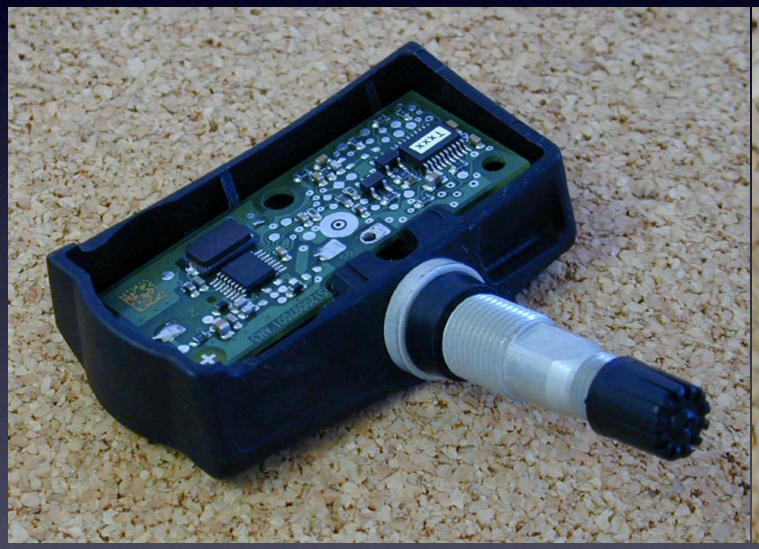
After...

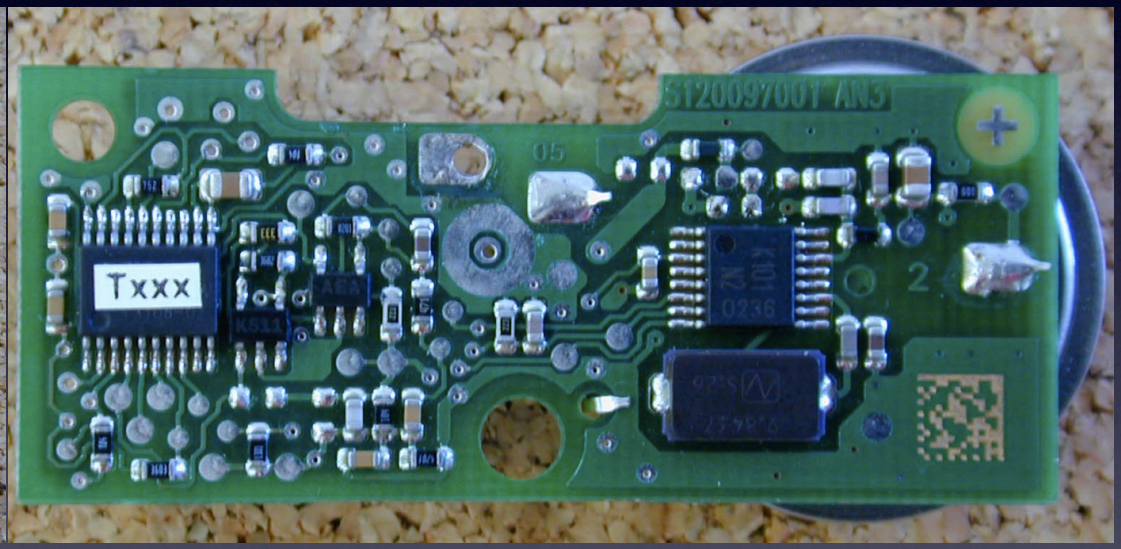


And then...

- A discovery...
- http://www.fcc.gov/oet/ea/fccid/
- Enter in the Grantee & Product code

FCC Testing Documents





Including...

- Spectrum Analyzer output
- General description of operation
- Often a build of materials
- etc...
- But how to find all the FCC IDs?

eBay...

eBay Motors Hello! Sign in or register. Go eBay Hor

Cars & Trucks | Parts & Accessories | Motorcycles | Powersports | Boats | Other Vehicles

Back to Search Results | Listed in category: eBay Motors > Parts & Accessories > Car & Truck Parts > Wheels, Tires & Parts > Valve Stems & Caps

RX8 TPMS OEM-USED

Enlarge

Item condition:	Used
Compatibility:	This information is not available.
Time left:	5d 18h (Jul 05, 2010 09:36:43 PDT)
Bid history:	0 bids
Starting bid:	US $14.99
Your maximum bid:	US $ [ ] Place bid (Enter US $14.99 or more)
Price:	US $25.00 Buy It Now
	Watch this item
Returns:	3 day money back | Read details
Shipping:	$5.00 Standard Flat Rate Shipping Service | See all details Estimated delivery time varies.

eBay Buyer Protection NEW
eBay will cover your purchase price plus original shipping.
Learn more

Receiver Description

- Typically in trunk or behind glove box
- May have multiple receiver elements
- Receiver will typically remember 4-10 sensors at once (summer, winter wheels)
- Most require special tools / operations to go in "Learning Mode"

Sensor RF Details

- Varies considerably based on sensor
- Using a Siemens VDO FE01-37140
- Uses a combination of ASK/FSK transmission
- 12 pulses of ASK "wakeup"
- 3 pulses of FSK transmission containing actual sensor data
- Repeats 1/min over 20mph, or every 5s with pressure problem

Sensor Transmission Details

- Each transmission consists of pressure level, battery level, and...
- A sensor ID (which exists to identify each wheel)
- BUT - the ID is usually way too precise - 32-108 bits
- Encoded, but completely unencrypted
- Combine w/ 4-5 sensors per car and it's very easy to identify a car by tires alone

Dealer / Tire Repair Shop Tools

- "Universal" tools - Cost from $150-$3000
  - Can usually generate the 125kHz signals to activate most TPMS
  - Often contain a special "tool", aka a magnet, to activate older ones
  - Upscale models will decode transmissions based on make, model, year, etc.
  - Others simply indicate reception of signal

DIY Tools

- Didn’t want to overpay for ridiculous tools
- Some practical, some nefarious purposes
- Based on commodity parts

DIY Receiver

- Mostly complete
- RF receiver element (C1110, Microchip options, etc)
- Arduino for simplicity, but could be any given chip
- LCD Display (if needed)
- Magnet & 125kHz transmitter
- Open source & database for transmission methods

Using Receiver

- Can store multiple IDs
- Great for CarPCs for vehicles with limited TPMS (ie, RX8 says it's low, but not which one or by how much)
- Easy way to verify TPMS sensors
- Walk around parking lot and get TPMS IDs of interesting vehicles

DIY Transmitter

- Still in development
- Not really a TPM sensor, rather a spoofer
- RF Transmitter element
- Arduino again for simplicity, could be reduced to any given RF chip (ie, RFPIC)
- Also open & database of transmission

Using Transmitter...

- Certain wheels cannot accept TPM sensors. Use transmitter to send expected TPMS IDs
- Get IDs then send spoofed messages confusing the ECU (ie, low pressure, high pressure, etc)
- Near a stoplight, setup a sensor with a good antenna to grab the IDs/Formats of TPM sensors nearby. Setup deal with nearby service station / car dealer for cut of tire related services. Send out spoofed messages...

More ideas...

- Setup a network of receivers tied to loggers at given locations and track interesting vehicles going nearby
- Start fuzzing the TPM formats and see what it does to various ECUs (Remote Exploit...?)

Future

- Need to drastically build out the database for TPM communication formats
- Ideally build a single device capable of acting in send / receive configuration

Thanks & References

- Ed Paradis: Dallas Makerspace & radio transmission ideas
- Travis Goodspeed: GoodFET, software fix & IM-ME flashing guide
- Michael Ossmann: IM-ME Spectrum Analyzer
- Barrett Canon: First blog regarding idea of TPMS tracking (April 08)