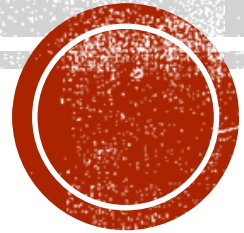
THREAT MODELING MY WIFE



Brian Knopf

IEEE Computer Society, Buenaventura, Nov 2014

brian@brksecurity.com

@DoYouQA

ABOUT ME

- Director of Application Security, Belkin International (owners of WeMo & Linksys)
- Security researcher focused on IoT
- Previously Principal Test Architect, Office of the CTO at Rapid7
- 20+ years of experience in IT, QA, Development and Security
- Programming, disassembling and reverse engineering since age 5

OUTLINE

- The Accident
- CRPS
- Why would you Threat Model your wife?
- Why is IoT security important?
- Anatomy of Neurostimulators
- The Threat Model
- Other Threat Models
- Conclusion

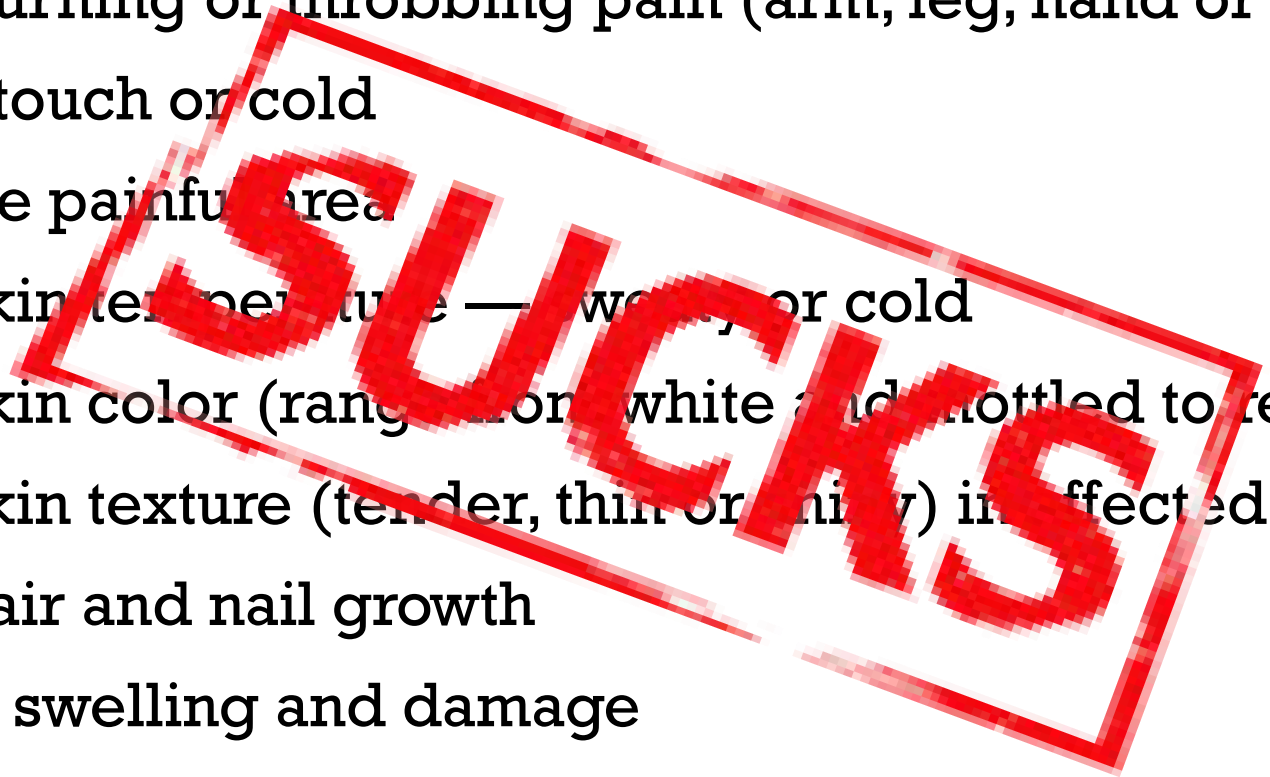
THE ACCIDENT

- My wife was injured when a sign fell on her foot
- She suffered nerve damage, fractured bone, damaged tendons & ligaments, and…
- Complex Regional Pain Syndrome (CRPS)
- Uncommon form of chronic pain that usually affects an arm or a leg
- Typically develops after an injury, surgery, stroke or heart attack
- Pain is out of proportion to the severity of the initial injury

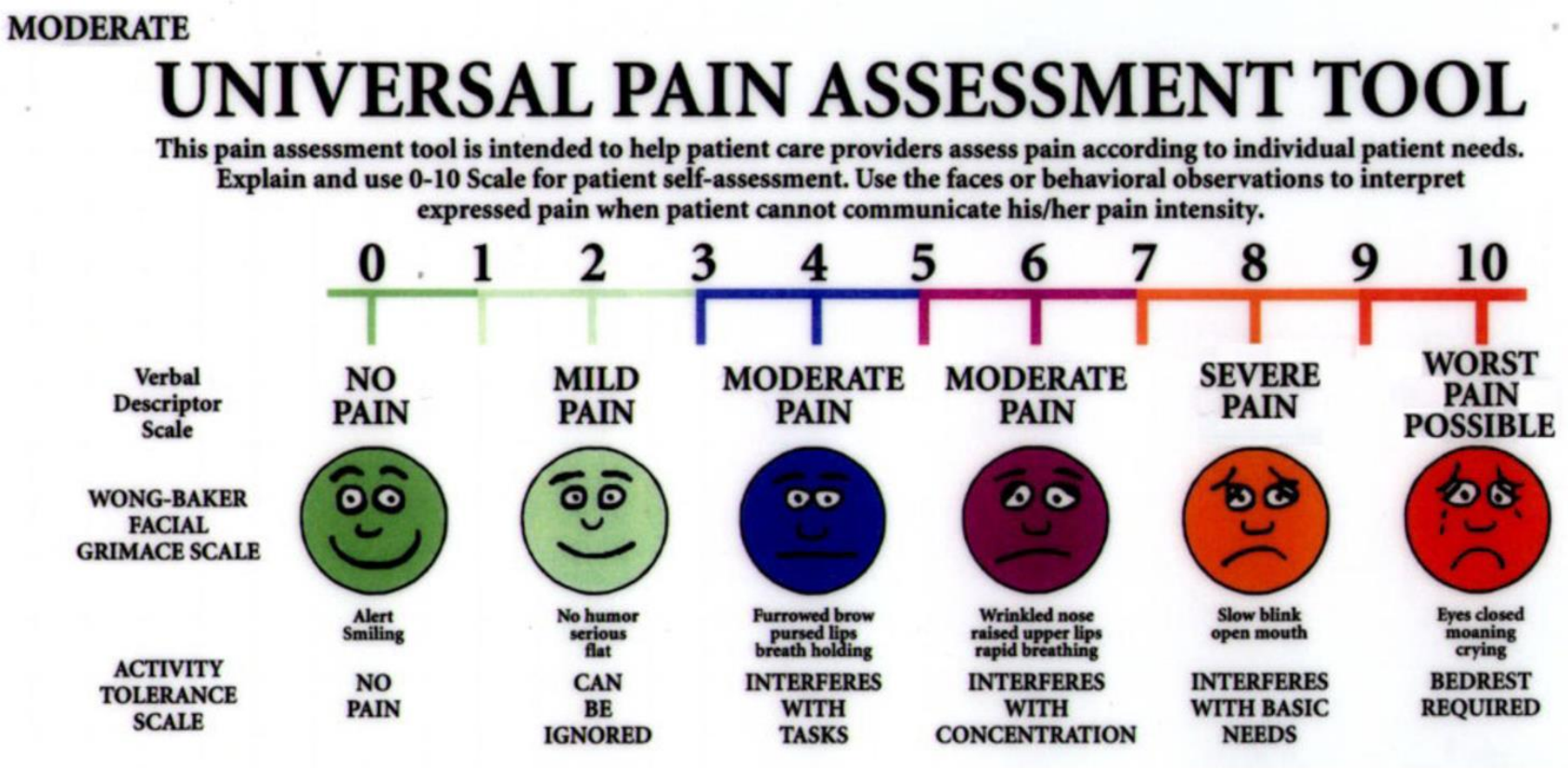
Source: Mayo Clinic http://www.mayoclinic.org/diseases-conditions/complex-regional-pain-syndrome/basics/definition/con-20022844

CRPS SYMPTOMS

- Continuous burning or throbbing pain (arm, leg, hand or foot)
- Sensitivity to touch or cold
- Swelling of the painful area
- Changes in skin temperature — warmth or cold
- Changes in skin color (ranging from white and mottled to red or blue)
- Changes in skin texture (tender, thin or shiny) in affected area
- Changes in hair and nail growth
- Joint stiffness, swelling and damage
- Muscle spasms, weakness and loss (atrophy)
- Decreased ability to move the affected body part



Source: Mayo Clinic http://www.mayoclinic.org/diseases-conditions/complex-regional-pain-syndrome/basics/definition/con-20022844



HOW MUCH PAIN?

Before implant – constant 8-10

After implant – 7 (spikes to 9 or 10)

WHY THREAT MODEL YOUR WIFE?

- She needed a medical device implanted in her back
- All other treatment options exhausted
- No manual alternative
- My job is to assess products for security risks
- Paranoia based on previous medical device exploits
- Programmers still do not focus on securing code
- Specialize in IoT security

"WE CAN IMPLANT A PAIN MANAGEMENT DEVICE IN YOUR BACK THAT YOU CONTROL AND CHARGE WIRELESSLY."

Doctor explaining options to my wife

FIRST THOUGHT

Android or cyborg?

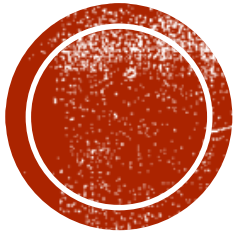
SECOND THOUGHT

My wife, the bionic woman

Third Thought

Pentesting this is a **BAD** idea.

Stick with the Threat Model



The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Source: Gartner http://www.gartner.com/newsroom/id/2636073

IoT Industry Growth

- Asset Management

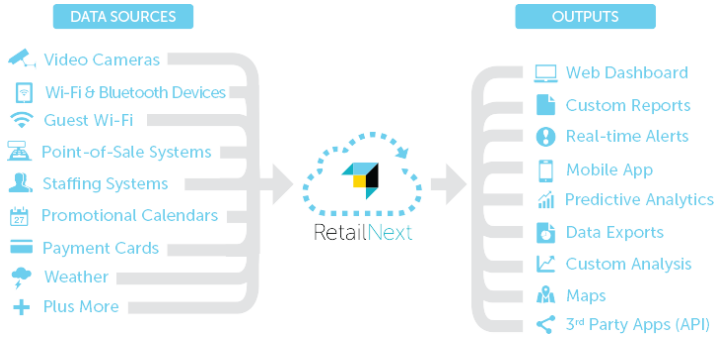
- Health & Fitness

- Insurance

- Medical

- Banking

- Retail

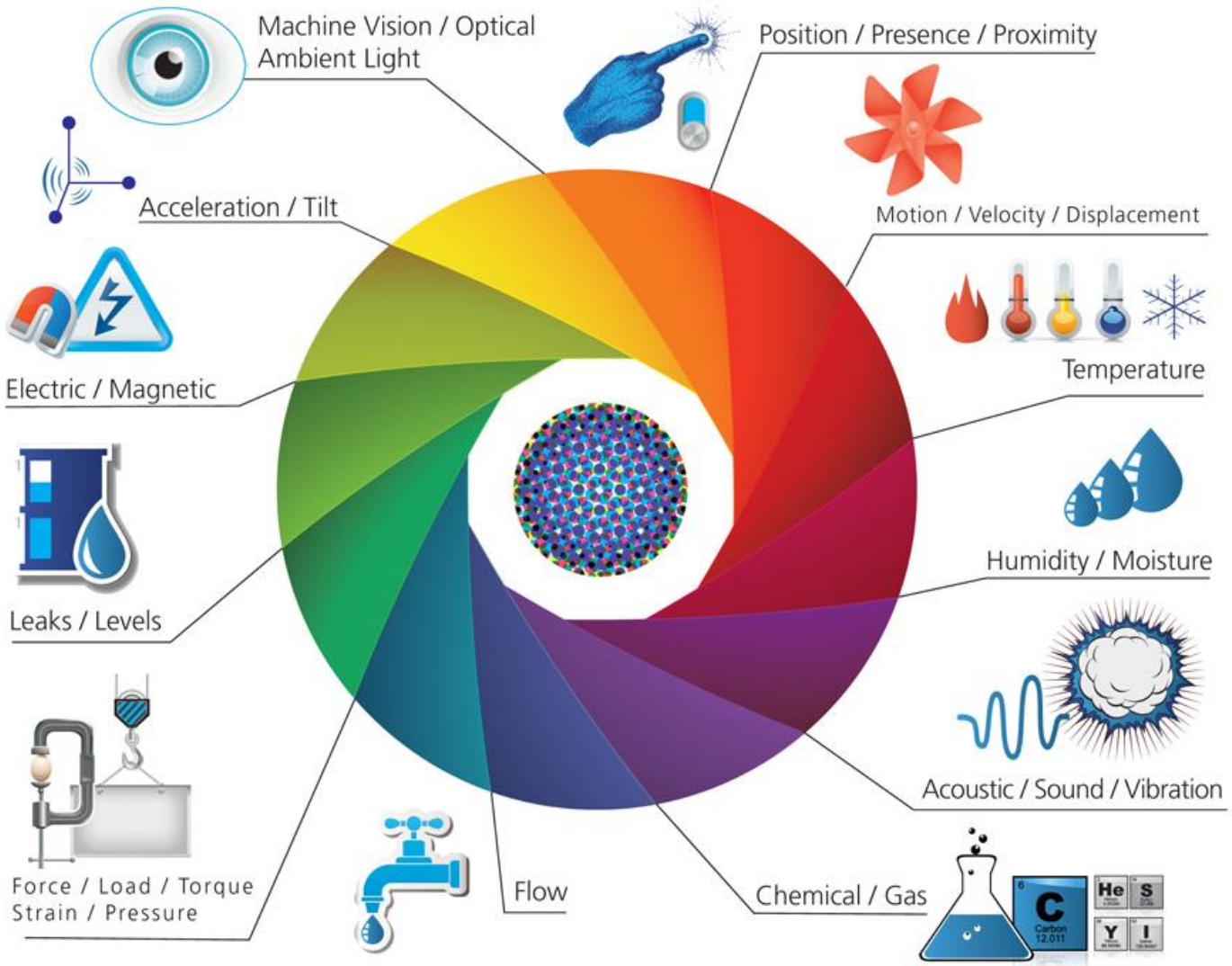


- Entertainment

Sources: http://www.vizualiiz.com, http://professional.medtronic.com, http://www.nike.com, http://www.progressive.com, http://retailnext.net, http://www.skylanders.com, https://onlycoin.com

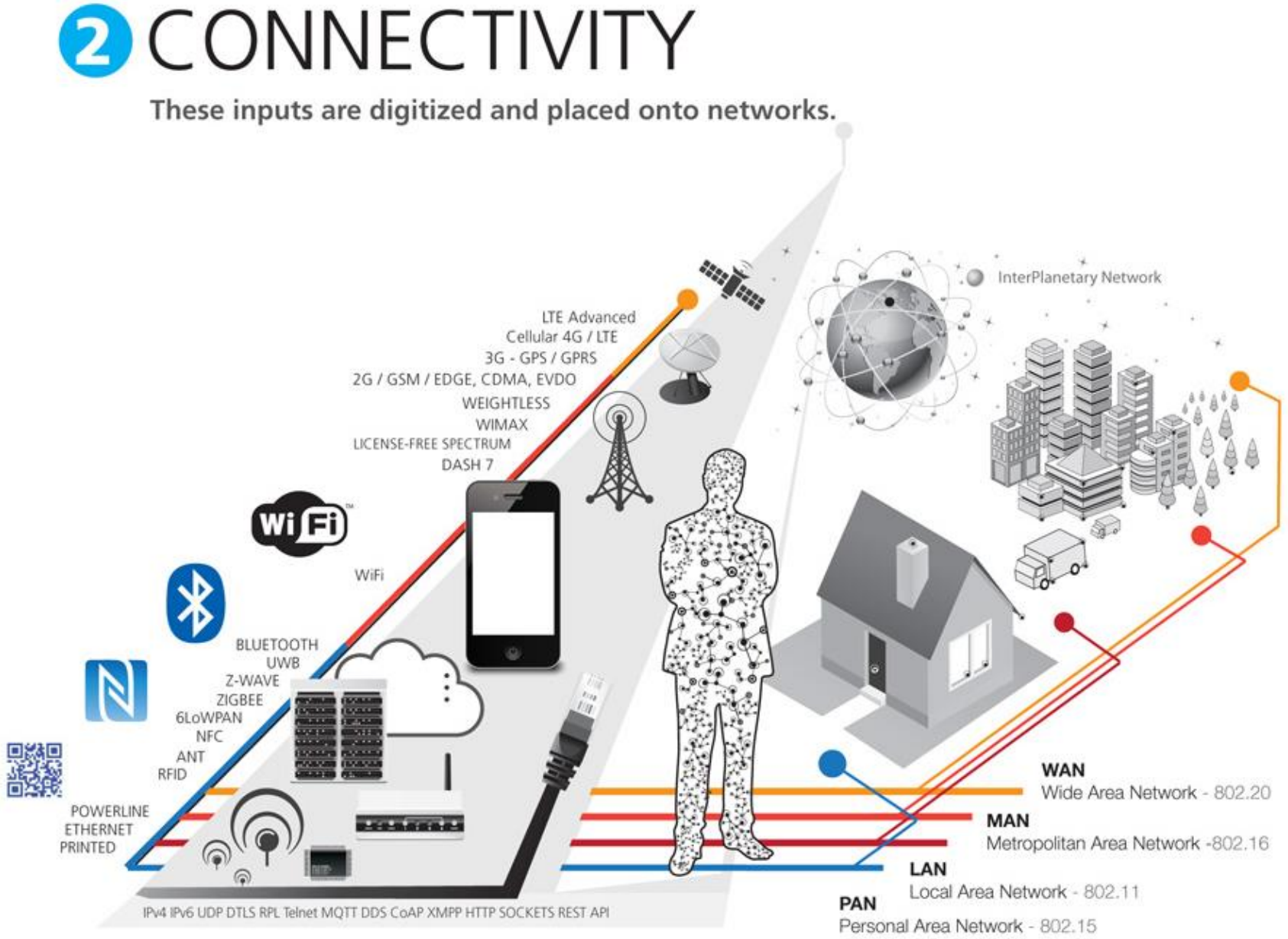
1 SENSORS & *ACTUATORS*

We are giving our world a digital nervous system. Location data using GPS sensors. Eyes and ears using cameras and microphones, along with sensory organs that can measure everything from temperature to pressure changes.



Source: Postscapes http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

COLLECT & MEASURE DATA



Source: Postscapes http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

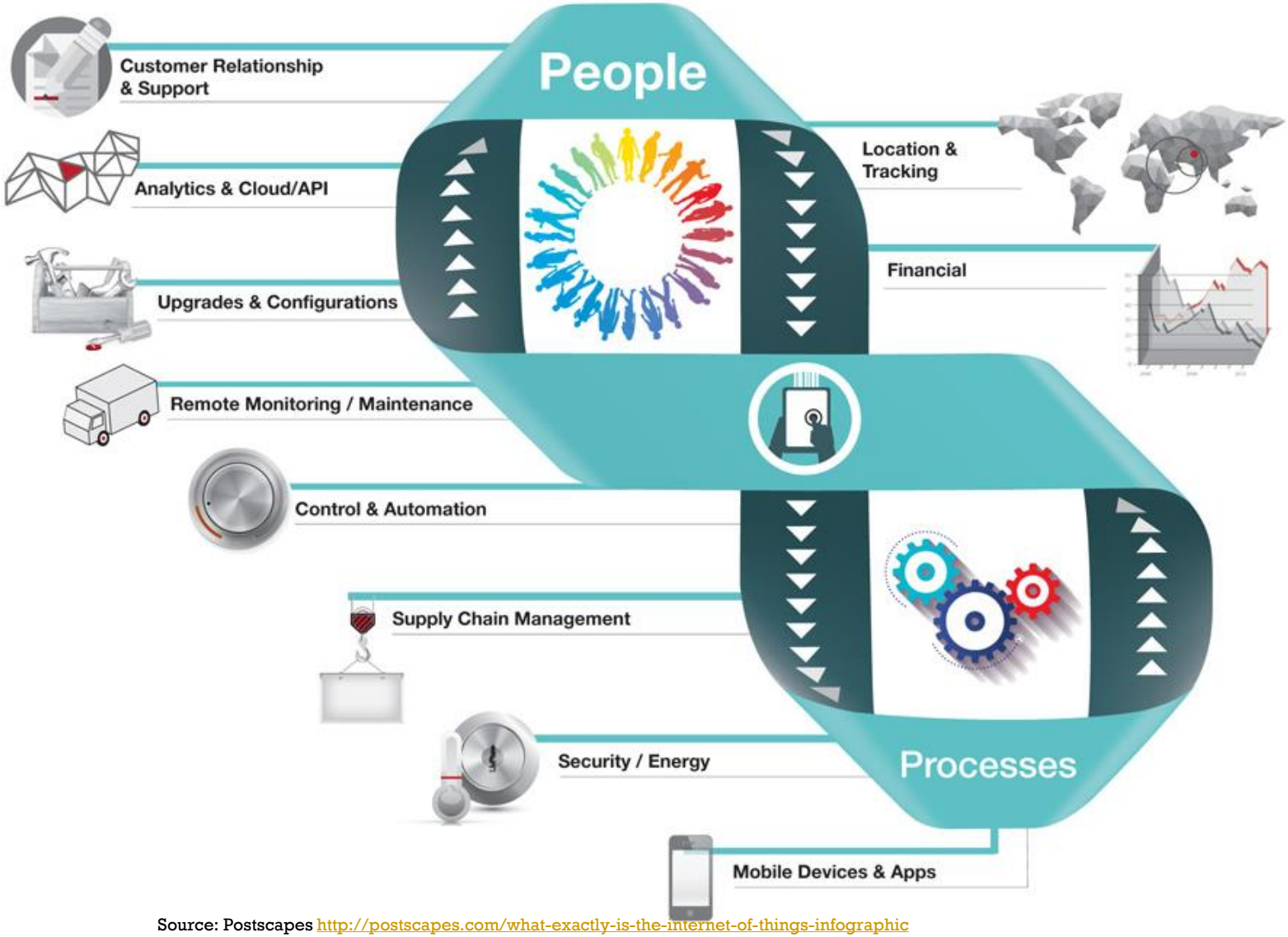
CONNECT & COMMUNICATE

Protocols

- ZigBee
- Z-Wave
- 6LoWPAN
- NFC
- RFID
- Bluetooth
- Bluetooth Low Energy
- INSTEON
- Lutron
- MQTT
- Thread

3 PEOPLE & *PROCESSES*

These networked inputs can then be combined into bi-directional systems that integrate data, people, processes and systems for better decision making.

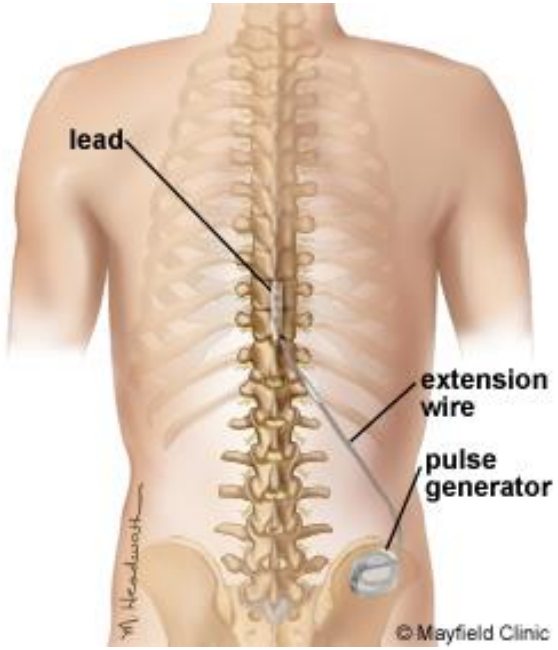


Source: Postscapes http://postscapes.com/what-exactly-is-the-internet-of-things-infographic

INTEGRATE & INNOVATE

IOT MAKES LIFE EASIER

Pain Management 1970's



Pain Management 2010's

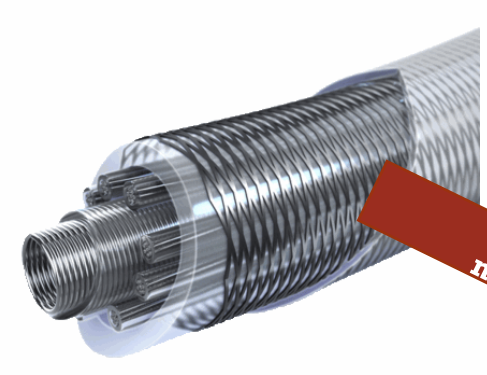
WHY IS IOT SECURITY IMPORTANT?

- Hundreds of IoT devices across every vertical
- Manufactures lack control of entire stack
- Devices not easily updated
- Focus on features and usability, not security
- Exploit hardware easy to buy

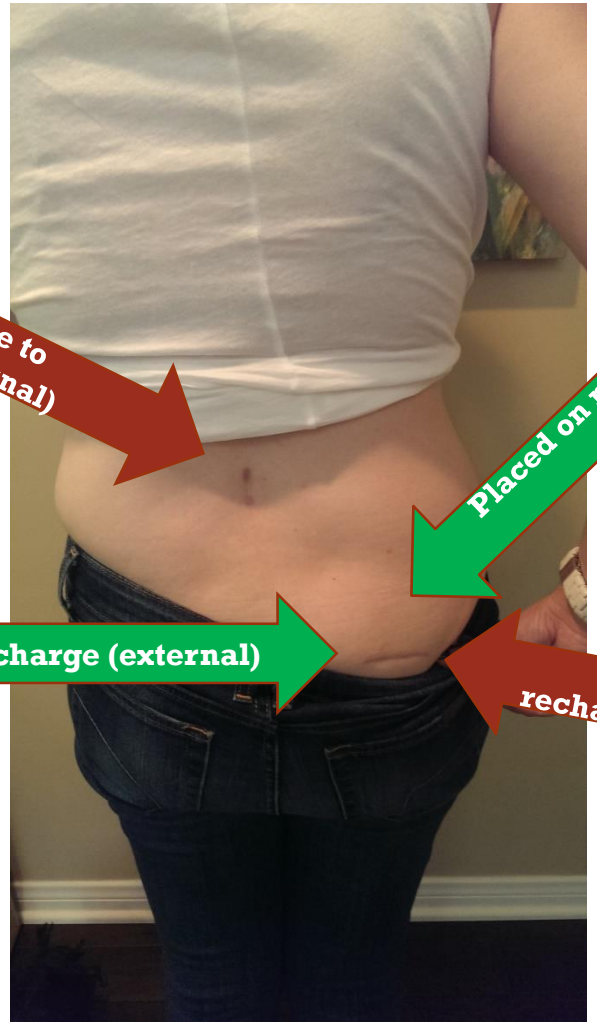
WHY IS IOT DIFFERENT?

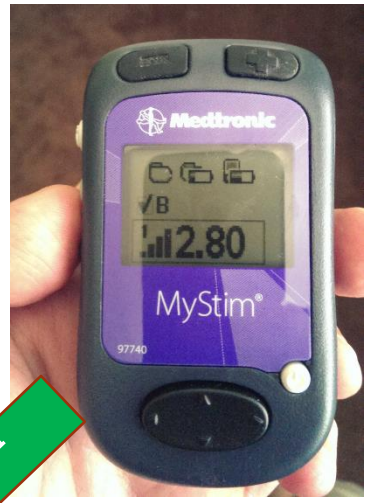
- Access to personal information
- Can be used to protect physical location
- Share some technology with traditional networked devices
- Updates are mostly manual if available
- Some endpoint devices are not updateable at all (ZigBee, Z-Wave)
- Consumers rarely think about patching
- Consumers are dependent on manufacture updates
- Many built on SDKs from chip vendors and manufactures with no security expertise
- Use 3rd Party libraries as black boxes

ANATOMY OF NEUROSTIMULATORS



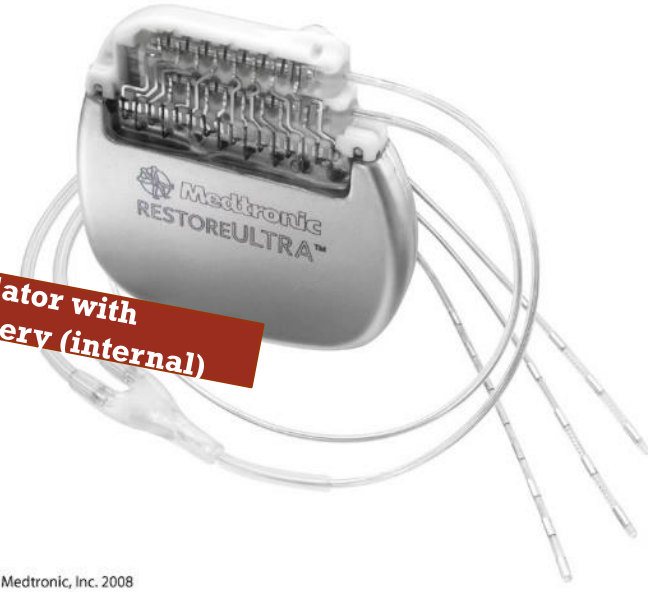
Leads connect spine to neurostimulator (internal)





Placed on neurostimulator to control (external)

Placed on neurostimulator to charge (external)



Neurostimulator with rechargeable battery (internal)

NEUROSTIMULATOR SPECS

- **Programmable parameter: Operating range and resolution**
- Remotes communicate in 400 MHz range
- Amplitude: **0 to 10.5 V** with 0.05-V or 0.1-V resolution
- Amplitude – upper patient limit: Tracking limit: programmed value **+0 to +4 V** (0.5-V resolution)

Custom limit: programmed value **up to 10.5 V** (same resolution as amplitude)

- Amplitude – lower patient limit: Custom limit: 0 V to the programmed value (same resolution as amplitude)
- Pulse width: 60 to 1000 μs (10-μs resolution)
- Pulse width – upper patient limit: Tracking limit: programmed value +0 to +300 μs (60-μs resolution)

Custom limit: programmed value up to 1000 μs (10-μs resolution)

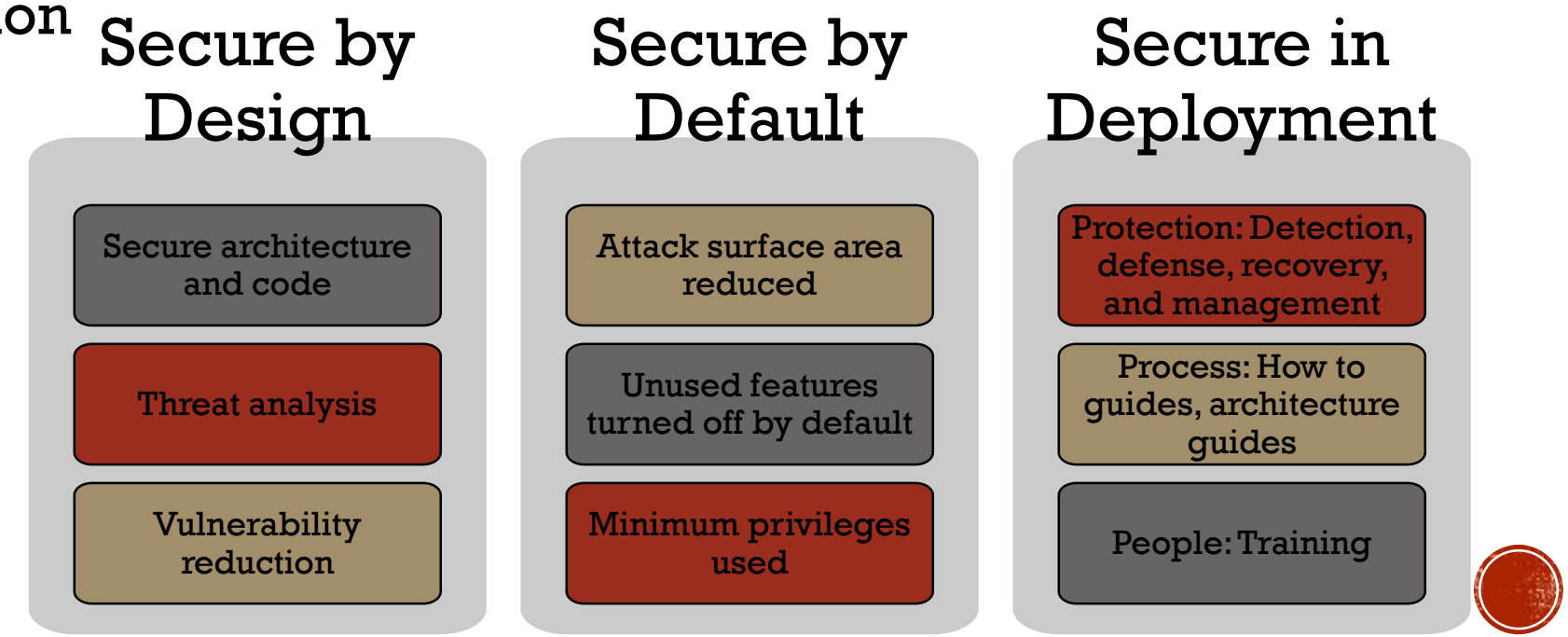
- Pulse width – lower patient limit: Custom limit: 60 μs to the programmed value (10-μs resolution)
- Rate: 2 to 1200 Hz (resolution: 1 Hz from 2 Hz to 10 Hz; 5 Hz from10 Hz to 250 Hz; 10 Hz from 250 Hz to 500 Hz; 20 Hz from 500 Hz to 1000 Hz; 50 Hz from 1000 Hz to 1200 Hz)
- Rate – upper patient limit Tracking limit: programmed value +0, +10, +20, +50, +100 Hz
- Custom limit: programmed value to 1200 Hz (same resolution as rate)
- Rate – lower patient limit Custom limit: 2 Hz to the programmed value (same resolution as rate)
- SoftStart/Stop Off, On: 1, 2, 4, or 8 second ramp duration

MANUFACTURES

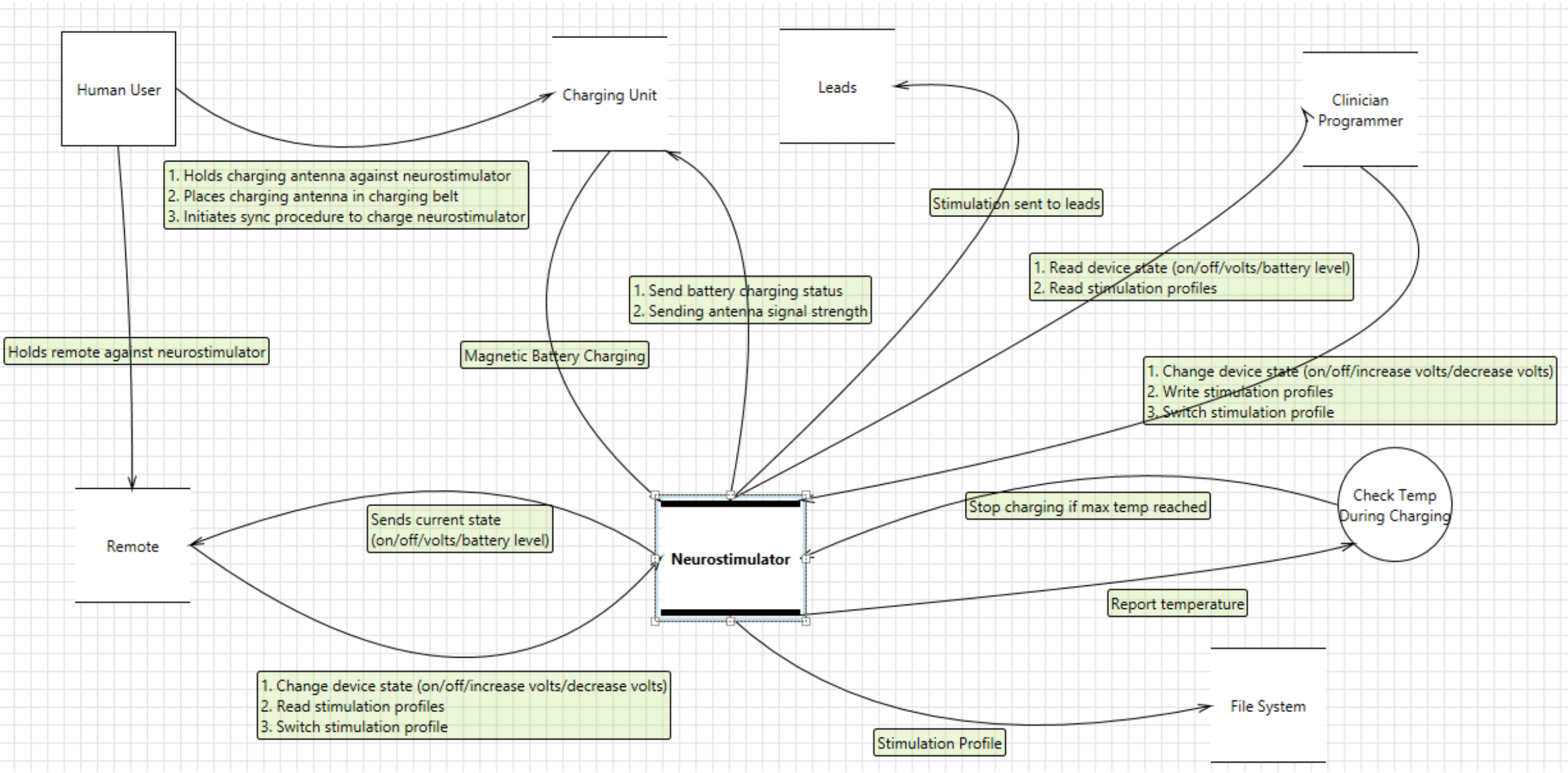
- Medtronic
- St. Jude
- Boston Scientific

BENEFITS OF THREAT MODELING

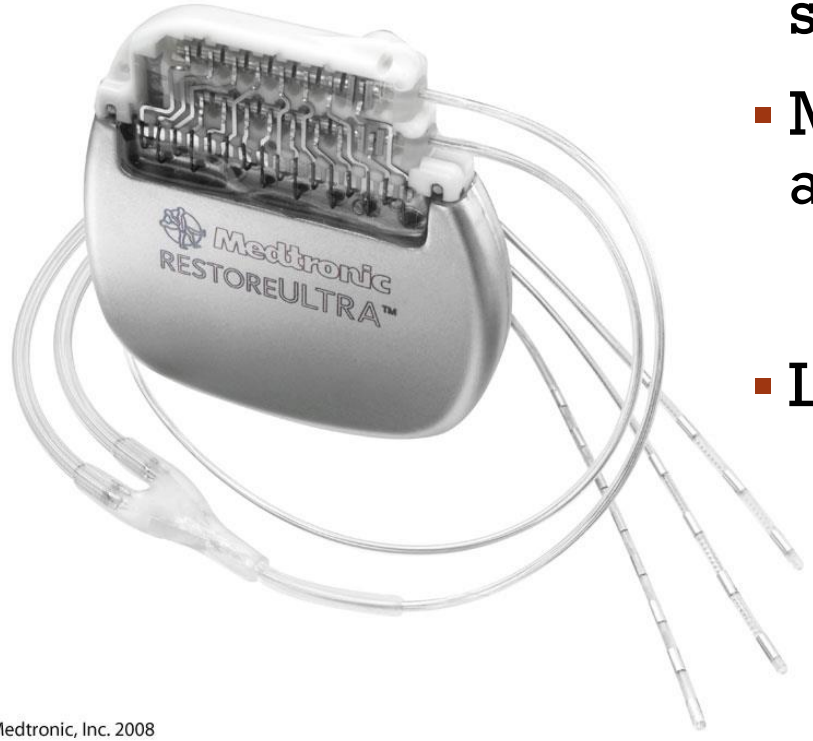
- Threat Model critical to identifying risks
- Focuses security audit effort correctly
- Documents risk assumptions made before audit
- Used to aid in estimation of audits
- Roadmap for mitigation
  - Microsoft 3S+C
  - Communication



THREAT MODEL



POTENTIAL RISKS



- Risk: Damage to neurostimulator caused by strong EMI interference
- Mitigation: Neurostimulator has EMI shielding and is MRI safe under specific conditions
- Likelihood of attack: **highly unlikely**

POTENTIAL RISKS

- Risk: Changing programming on neurostimulator via wireless signal
- Mitigation: Remote only works when directly against skin or over very thin clothes.
- Remote does not work when going through jeans and a shirt
- External antennas do not change this

- Likelihood of attack: **highly unlikely**

POTENTIAL RISKS

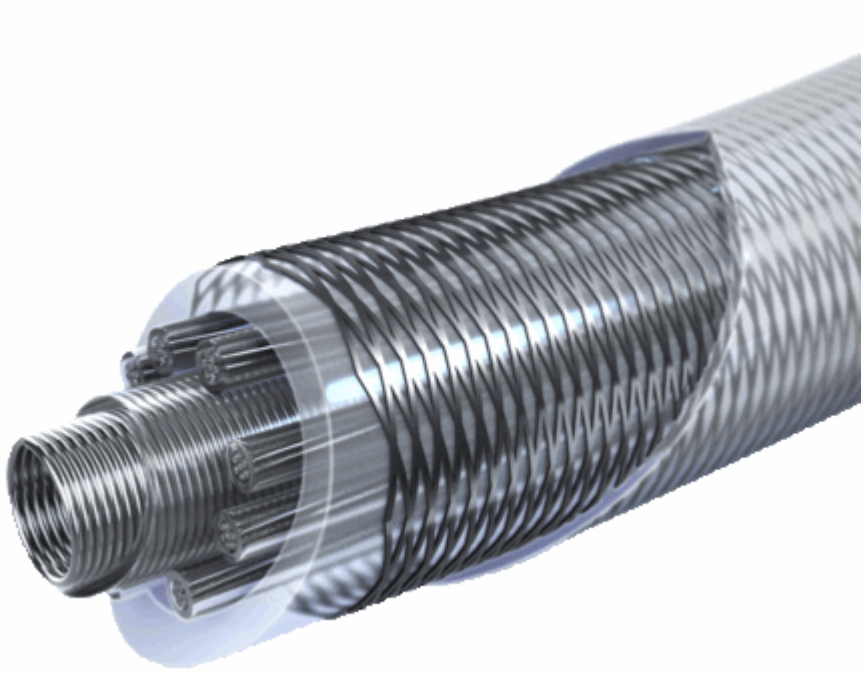
- Risk: Attacker turns on stimulation at high voltage
- Mitigation: Remote only works when directly against skin or over very thin clothes.
- Likelihood of attack: **highly unlikely**

POTENTIAL RISKS

- Risk: Overheating the skin during charging causing burns
- Mitigation: Neurostimulator monitors skin temperature and its temperature
- Stops charging if unit or skin overheat

- Likelihood of attack: **highly unlikely**

POTENTIAL RISKS



- Risk: Damaging leads with high RF causing electrocution, shock, death
- Mitigation: New leads disperse RF across the entire length of the lead
- Likelihood of attack: **highly unlikely**

WHY STOP THERE?

- Device cost was **$30,000**
- Not willing perform penetration test on device inside my wife
- Willing to continue research if I receive enough donations to purchase another device

HOW WOULD YOU TEST IT?

- HackRF
- 10 MHz to 6 GHz operating frequency
- Half-duplex transceiver
- Compatible with GNU Radio, and Software Defined Radio (SDR)
- Software-configurable RX and TX gain baseband filter
- Open source hardware
- Lots of applications already written to decode wireless using this
- Cost: $330

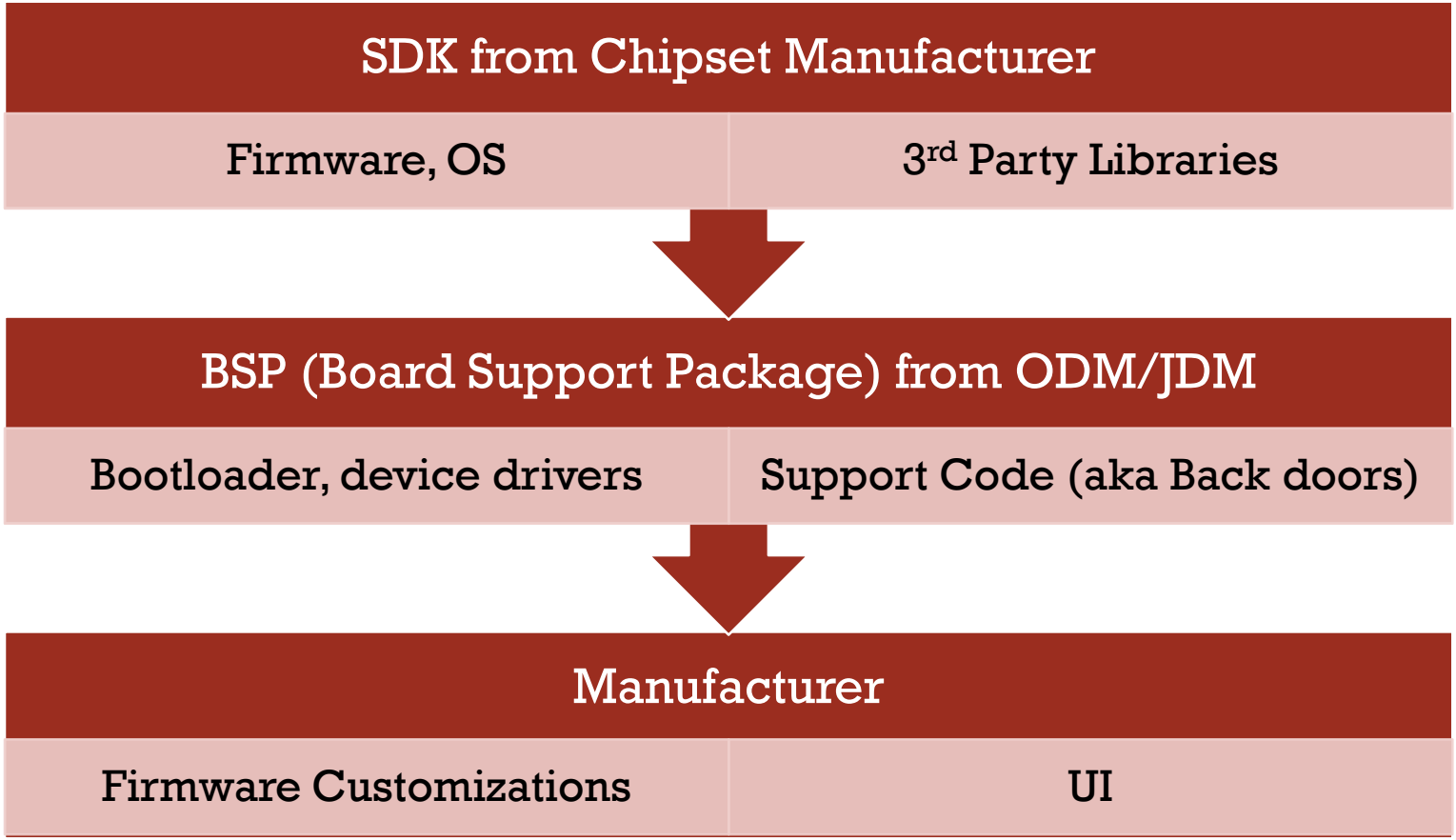
Source: https://greatscottgadgets.com/hackrf/, http://www.sharebrained.com/2014/05/28/portapack-h1-imminent/

TARGET & HOME DEPOT

- POS systems compromised by Malware
- Attackers exfiltrated data using HVAC service accounts
- HVAC accounts captured by phishing attack on HVAC company
- Why would HVAC accounts have access to POS and financial systems?
- Variant of that malware then used on Home Depot 5 months later

Source: Target image http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/

OTHER EMBEDDED DEVICES



CONCLUSION

- Threat Modeling is critical to understanding risk
- Threat Models should be refreshed regularly
- Risk needs to be balanced with probability of being exploited
- **Most consumers could not do this – They deserve to know**
- Researchers scare people into not using devices that could improve quality of life
- I Am The Calvary – Working on rating system (iamthecalvary.com)
- Build It Securely (builditsecure.ly) focused on IoT security
- Every device should be tested and published publicly

THANKS

- Huge thanks to my wife for putting up with this
- Thank you for attending
- Contact brian@brksecurity.com for additional information on IoT & Security
- Questions?