IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

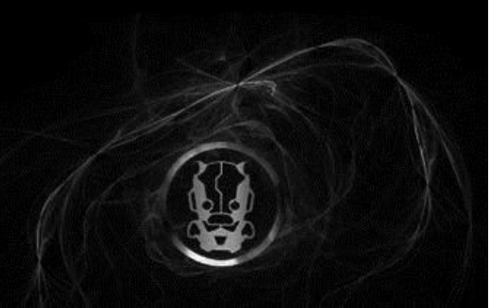
Hacking US Traffic Control Systems

Cesar Cerrudo
@cesarcer
CTO at IOActive Labs

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

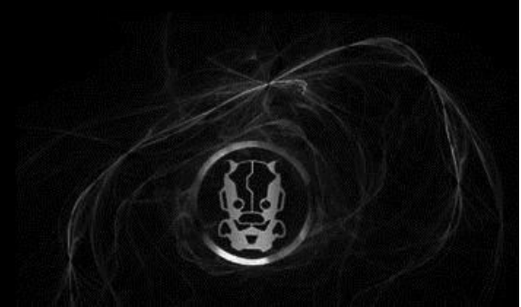
About me

- ***Hacker, vulnerability researcher, created novel exploitation techniques, dozens of vulnerabilities found (MS Windows, SQL Server, Oracle, etc.).***
- ***Developed, sold exploits and 0day vulnerabilities (7-10 years ago)***
- ***Run research and hacking teams, etc.***
- ***CEO of software company***
- ***CTO at IOActive labs***
- ***Live in small city in third world country, far away from everything***
  - ***–but I can hack US traffic control systems ☺***

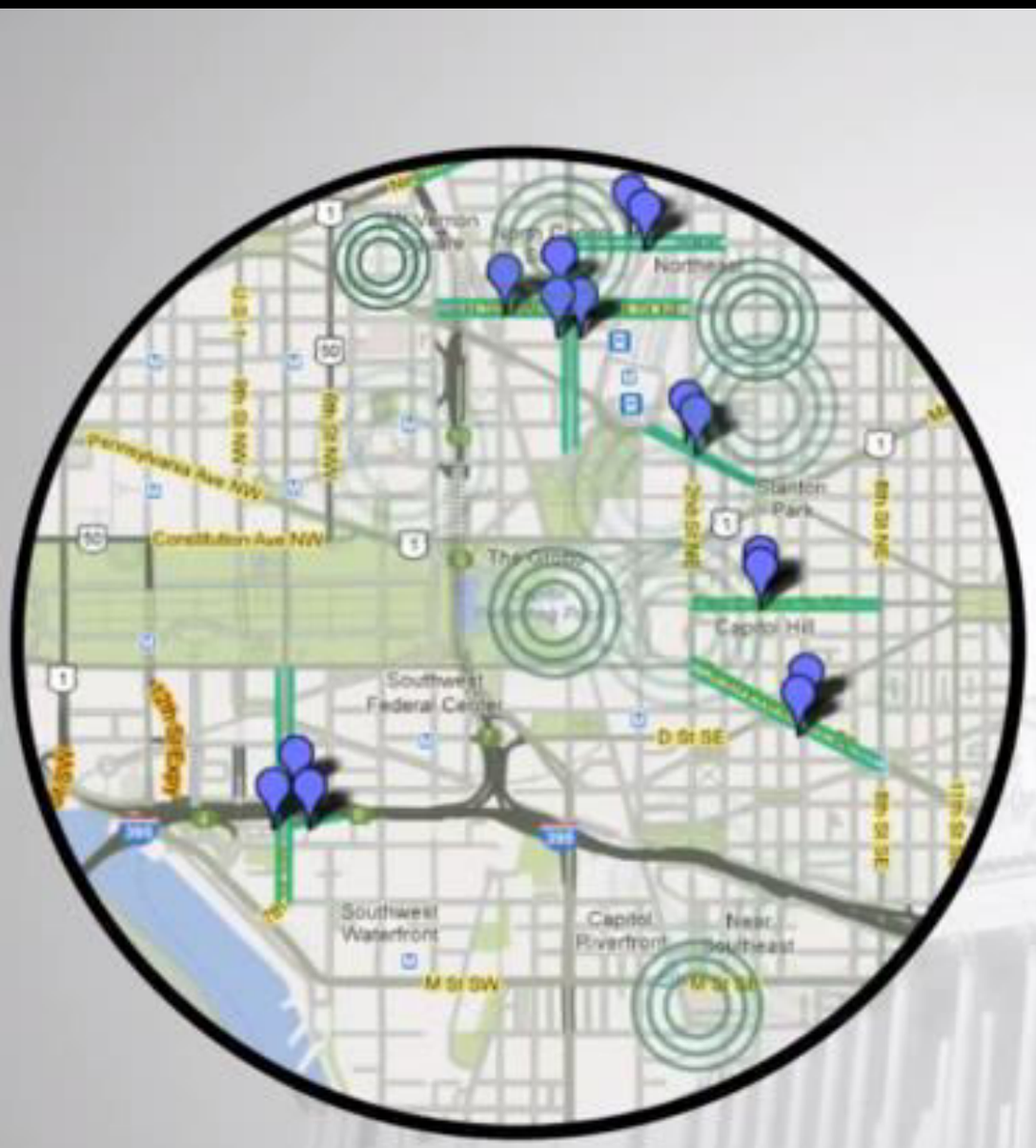


Thanks

- *Barnaby Jack*
- *Ruben Santamarta*
- *Mike Davis*
- *Mike Milvich*
- *Susan Wheeller*
- *Ian Amit*
- *Robert Erbes*



How all started



1300+

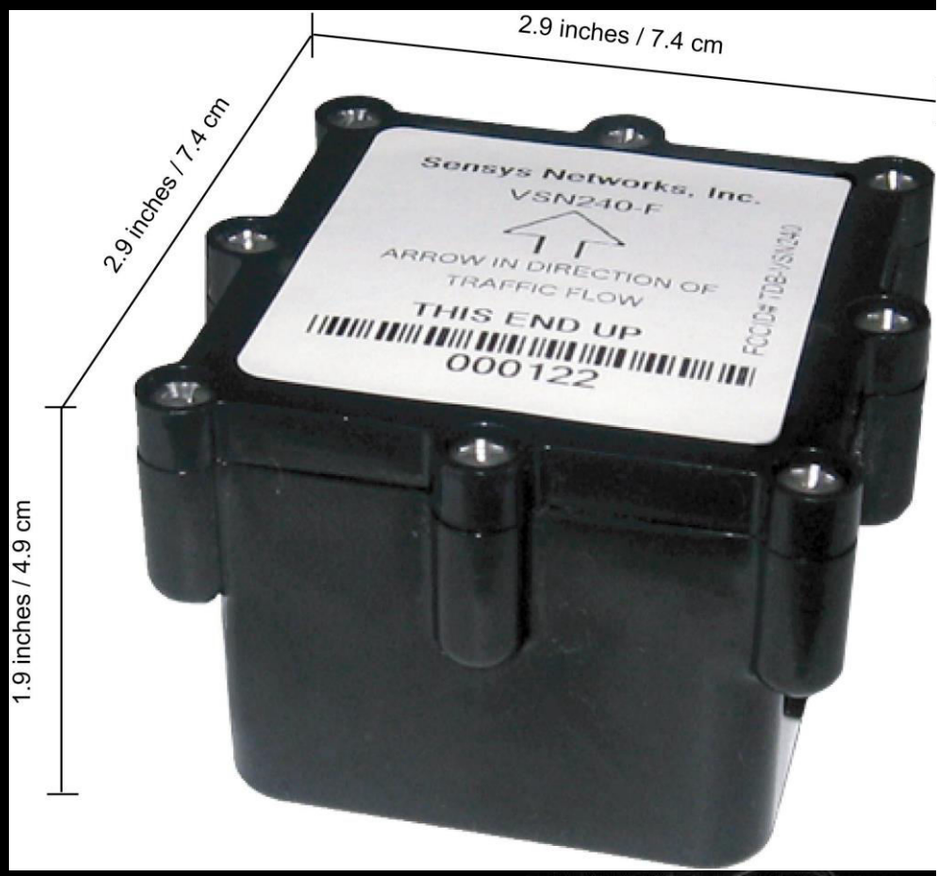
Wireless Sensors

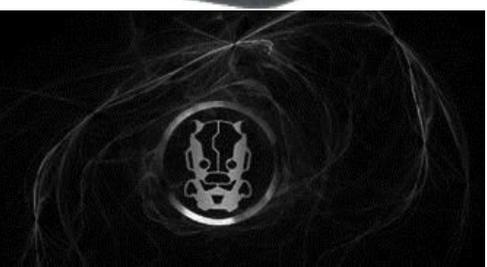
How all started

- Getting the devices
  - –Social engineered vendor
  - –Ship them to Puerto Rico and traveled with them back and forth to the US from Argentina several times without any problems

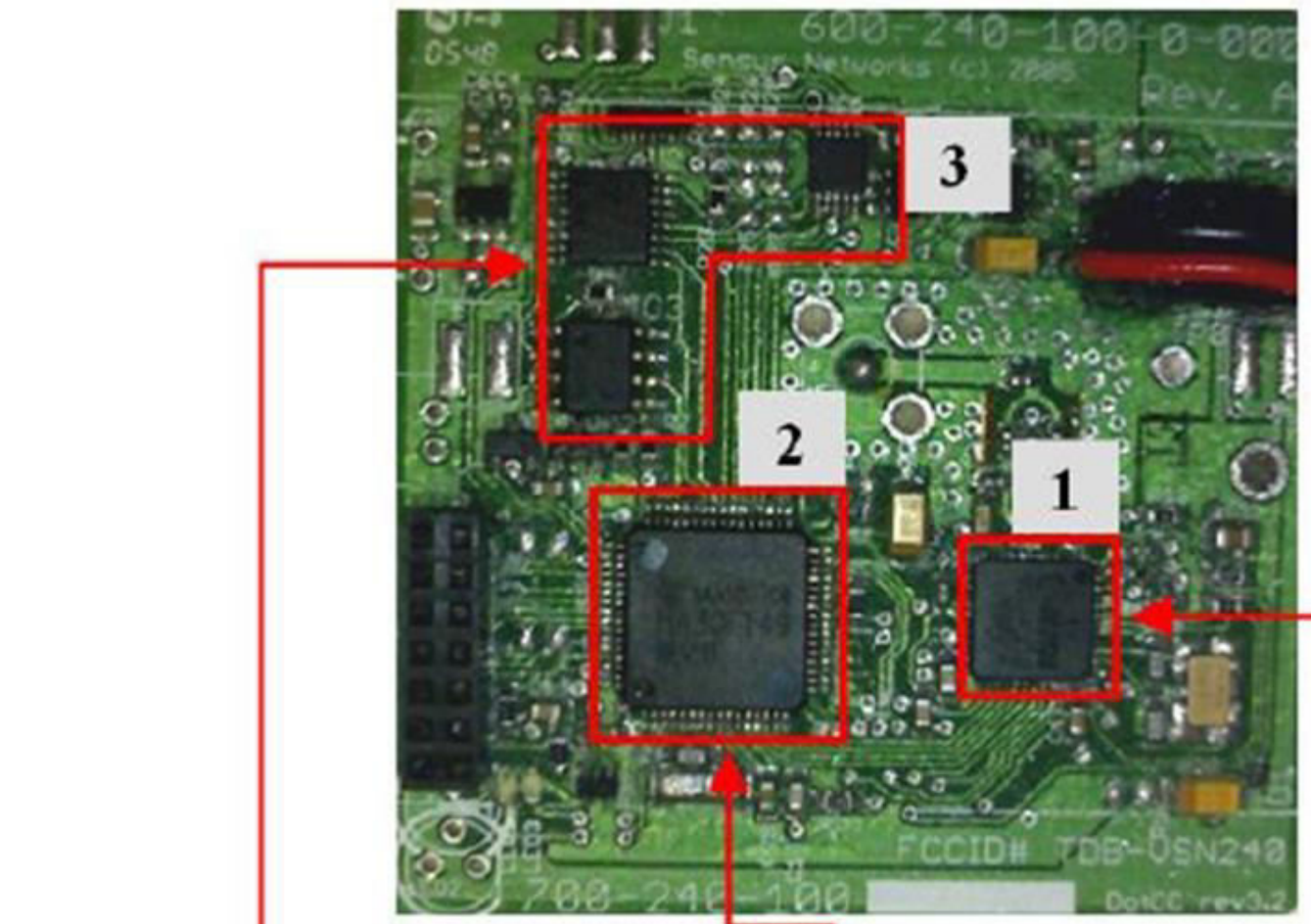
The devices: Wireless Sensors

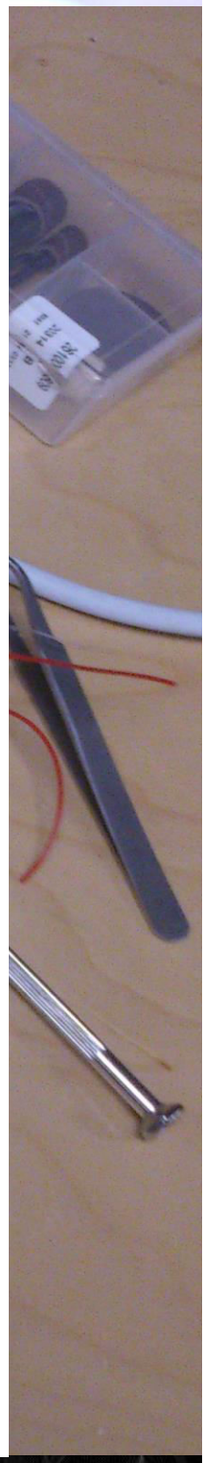
- Installs in small hole using hammer or core drill in less than 10 minutes
- Rugged mechanical design, 10 years of battery life
- TI CC2430 RF transceiver IEEE 802.15.4 system-on-chip 2.4-GHz
- TI MSP430 MCU (microcontroller) 16-bit RISC CPU , i386 Linux (probably TinyOS RTOS)





The devices: Wireless Sensors





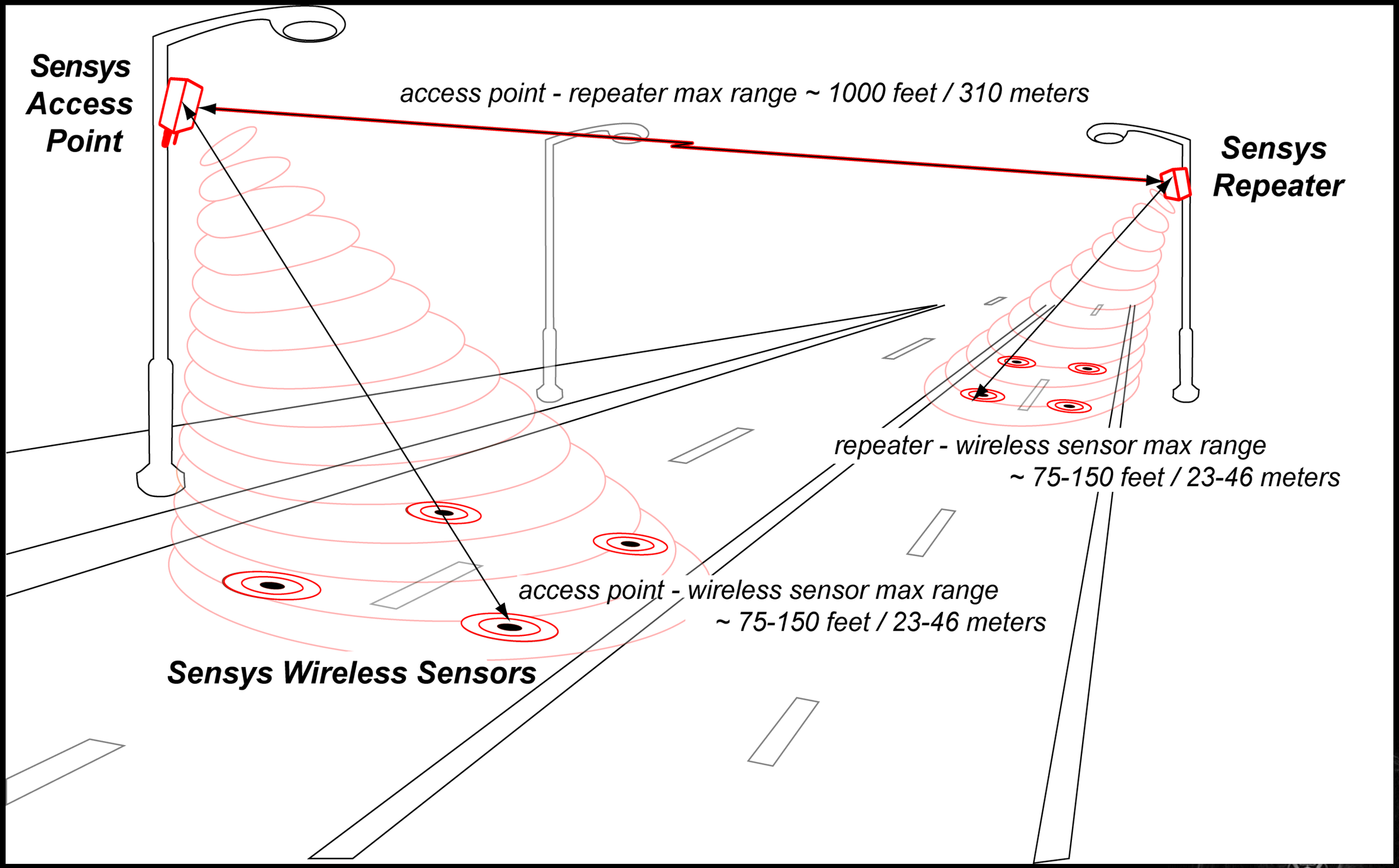
The devices: Access Point

- Processes, stores, and/or relays sensor data (uCLinux)
  - –66 MHz 5272 Coldfire processor 4 MB of flash memory, and 16 MB of DRAM.
  - –Contact closure to traffic controller, IP (fiber or cellular) to central servers, PoE
- Supports as many sensors as necessary, Can serve as IP router for peripherals (video cams, etc.)

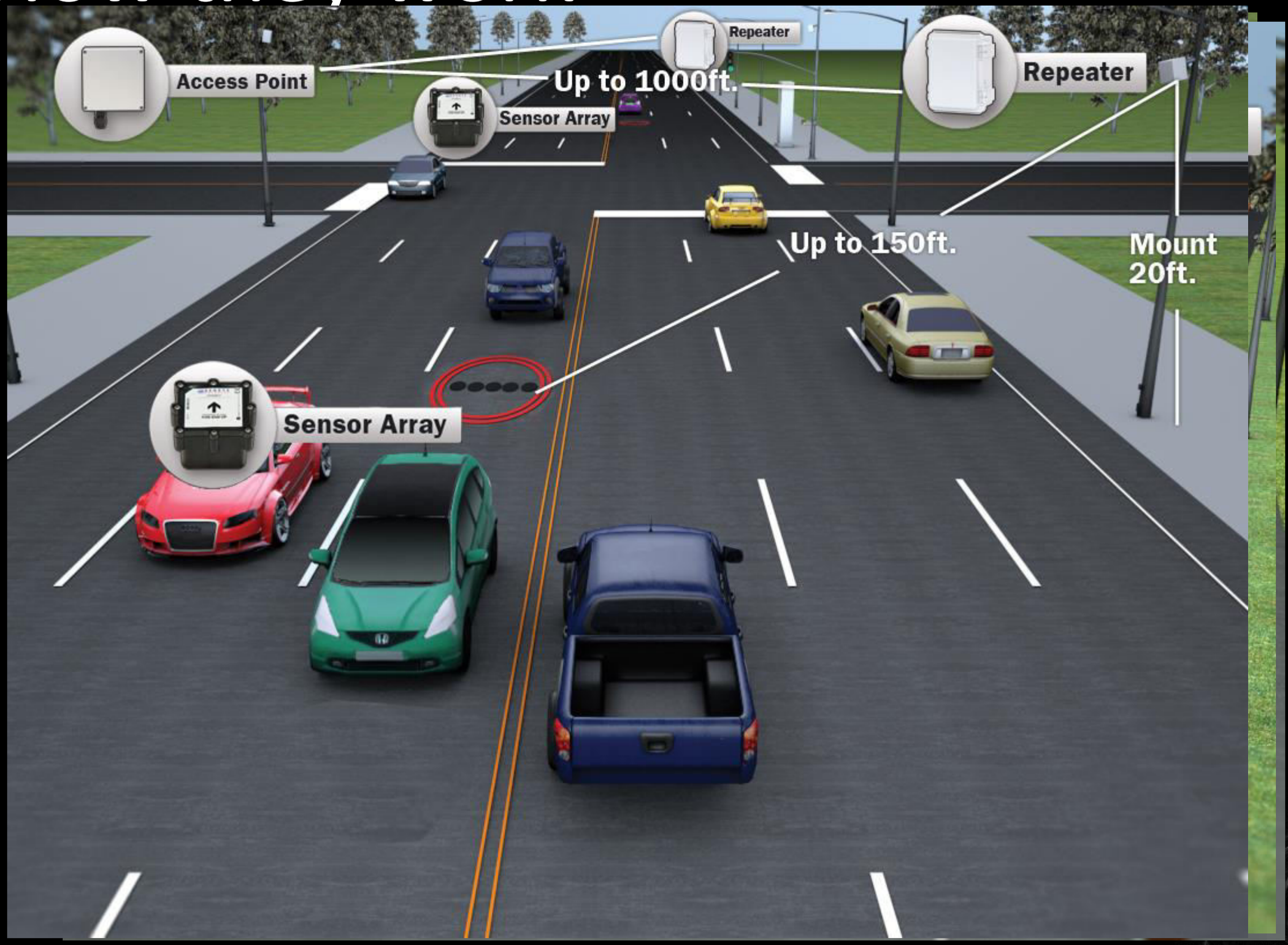
The devices: Repeater

- Battery-powered unit
- Supports up to 10 wireless sensors
- Relays detection data back to access point, extending range

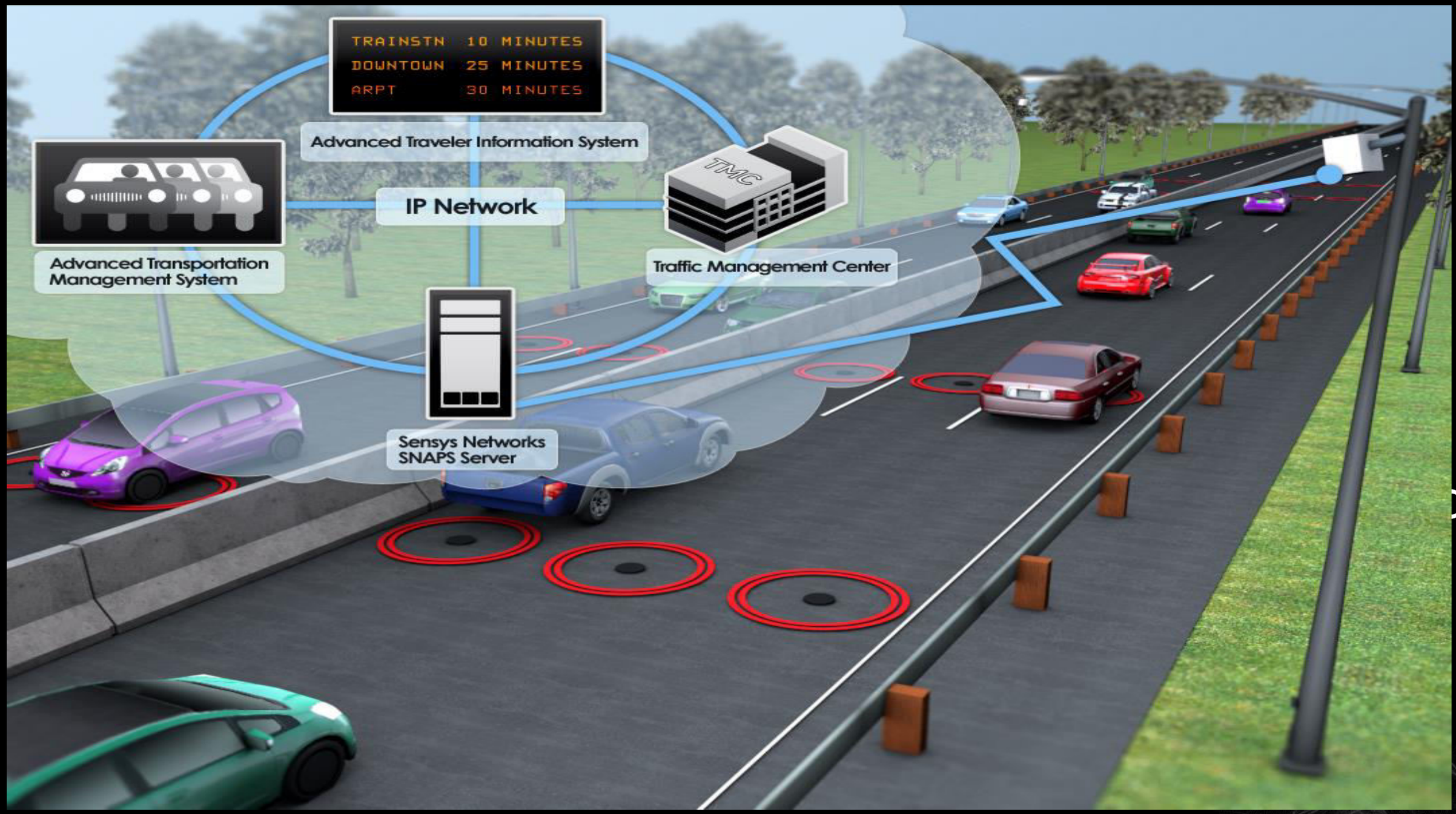
The devices: Radio Ranges



How they work



Software


TRAINSTN 10 MINUTES
DOWNTOWN 25 MINUTES
ARPT 30 MINUTES
Advanced Traveler Information System
IP Network
TMC
Traffic Management Center
Advanced Transportation Management System
Sensys Networks SNAPS Server

Vulnerabilities

- No encryption, all wireless communication in clear text.
- Vendor claims:
- *"Security: SNP **radio transmissions never carry commands**; only data is transmitted. Therefore, while RF communications may be subject to local interference**, there is no opportunity to embed malicious instructions to a network device or upstream traffic system**."*

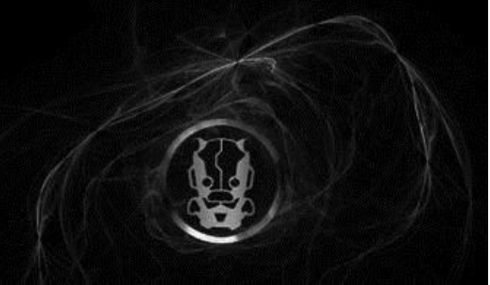
*"The option for encrypting the over the air information was removed early in the product's life cycle based on customer feedback. **There was nothing broken on the system as we did not intend the over the air information to be protected.** Firmware updates are encrypted AES."*

Vulnerabilities

- No authentication
  - –Sensors and repeaters can be accessed and manipulated over the air by anyone, including firmware updates
  - –AP doesn't authenticate sensors just blindly trust wireless data
- Firmware updates not encrypted nor signed
  - –Anyone can modify a firmware and get it updated on sensors and repeaters
- Vendor claims:

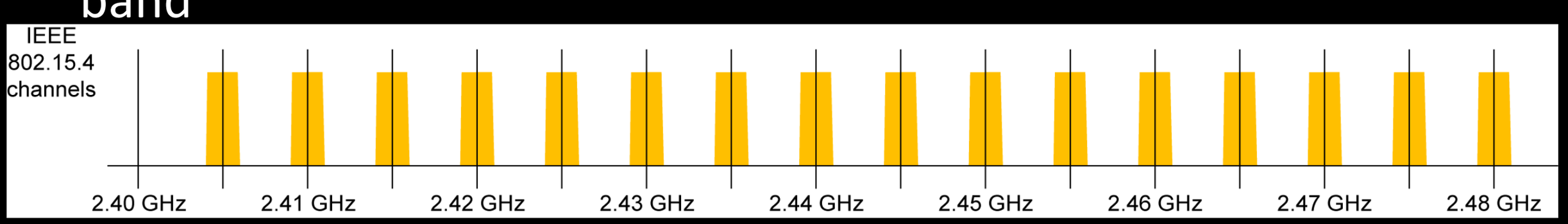
"We are encrypting/signing firmware in new sensor version" (just forgot a little and insignificant detail…)

"Security: Proprietary protocol – hacker safe"



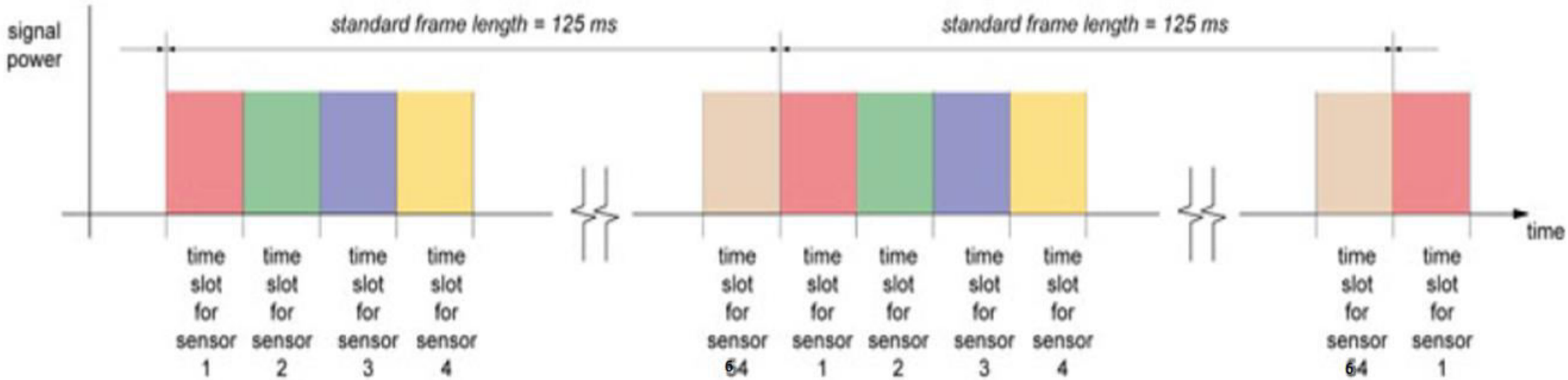
Protocol

- IEEE 802.15.4 PHY, used by ZigBee and other wireless systems
  - –Data rate of 250 kbps, 16 frequency channels in the 2.4 GHz ISM band



- Sensys NanoPower (SNP) protocol
  - –On top of 802.15.4 PHY as Media Access Protocol (MAC)
  - –The MAC layer is TDMA based and uses headers very similar to IEEE 802.15.4 MAC layer.

Protocol



Simplified representation of the Sensys NanoPower TDMA scheme

Protocol

- Packet structure: 80 80 55 AA BB 55 55 55 55 55 55

[frame header (2 bytes)] + [sequence # (1 byte)] + [address (2 bytes)] + [data]

- Frame header is used to specify the type of packet
- Sequence # from sensor packets is used by AP to acknowledge them
- Address is used to identify sensors by the AP and 2nd byte in address is ”colour code” used by sensors to identy the AP
- Data can be 4 bytes to 50 bytes long, first 2 bytes is data type
  - –Sensor data: mode, version, battery level, detection (presence or not of traffic), etc.
  - –AP data: Commands, synchronization, sensor and repeater firmware updates, etc.

Protocol

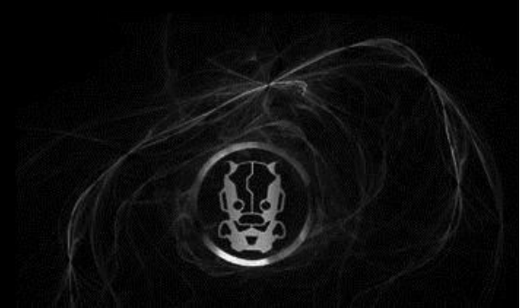
- Sample packets

80 41 69 CA B6 65 00 FF 7F -> sensor to AP, no detection event, count mode

80 41 67 CA B6 65 00 CE E7 -> sensor to AP, detection event, count mode

80 41 C0 CA B6 02 00 4C 00 03 00 03 BA 00 00 00 00 65 00 00 00 00 02 CA B6 FF 00 -> sensor to AP, sensor info

80 80 89 F0 FF 01 00 07 1E 40 07 C0 01 1A 00 00 00 00 00 00 40 40 20 01 00 ->AP to sensor



Protocol

- Firmware file, ldrect proprietary format

l0012AF10DADA***AAE1E60C***5A00006A020030133013 6C19021B3013A461D030301330142

l0088AF10DADA***AA6FC60D***5A00006A020030893089 6C8F02913089A4D7D0A6308930893 7

l2012301330133013301330131C17001300120300030 04C00FFFFFFFFFFFFFFFFFFFDF

l2088308930893089308930891C8D00890088030003004C00FFFFFFFFFFFFFFFFFFFB9…

- Firmware update packet

80 00 45 F0 F4 D2 00 ***00 12 AF 10 DA DA AA E1 E6 0C 5A 00 00 6A 02 00 30 13 30 13 6C 19 02 1B 30 13 A4 61 D0 30 30 13 30 13***

  – AP firmware broadcast, data part except first two bytes is a exact line from firmware file without the checksum byte

The tools

Attack impact

- –+50,000 sensors and ? repeaters worldwide that could be compromised
- –Traffic jams at intersections, at ramps and freeways
  - Rest in green (exceeds max. green time), Red rest (all red until detection), flashing, wrong speed limit display, etc.
- –Accidents, even deadly ones by cars crash or by traffic blocking ambulances, fire fighters, police cars, etc.
- –US DOT Federal Highway Administration (Traffic Detector Handbook):

"…sensor malfunctions and associated signal failures increase motorists' time and delay, maintenance costs, accidents, and liability."

Onsite passive testing

- Made AP portable
  - –USB powered instead of PoE with USB battery charger
  - –WiFi portable router battery powered, connect notebook to AP by WiFi
- Put AP in my backpack and went to Seattle, NY and Washington DC
  - –Took out notebook and start sniffing around in the sidewalk while pointing my backpack in the right directions
  - –Saw some spooks at DC but got no problems
  - –Video

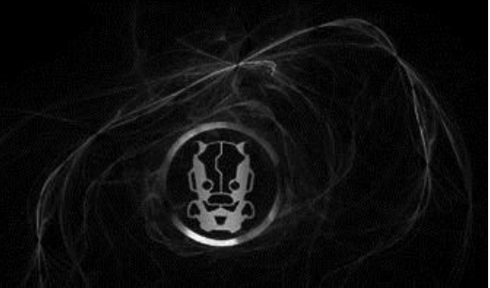
The Attacks

- DoS
  - –By disabling sensors/repeaters by changing configuration or firmware
  - –By making sensors/repeaters temporary (maybe permanently) unusable by changing firmware
  - –By flooding AP with fake packets
- Fake traffic detection data
  - –Send lots of car detections when there is no traffic (intersections, ramp meters and highways, etc.)
  - –Send no detection on stop bar at exit ramps
  - –Disable sensors/repeaters and send no detection data when there is a lot of traffic

The Attacks

The Attacks

- Sensor malicious firmware update worm
  - –Just need to compromise one sensor with malicious firmware and it can replicate later on other sensors
  - –Impossible to know if there are already compromised sensors since firmware version is returned by firmware itself
- NSA/Gov/Special forces/terrorist/etc. style attacks
  - –Locate persons in real time, hack Smartphone, launch attack
  - –Use sensor car identification data to trigger bomb when car target is near, no need to track car, just sniff sensor wireless packet (Cadillac One fingerprint?)



Conclusions

- Any third world guy can easily get devices used by US critical infrastructure, hack them and then attack the US
- Anyone can build a $100 worth device to cause traffic problems on most important cities on US (some other world cities too)
- Smart cities are not so smart when data that feeds them is blindly trusted and can be easily manipulated
- Cyberwar is cheap

BuildItSecure.ly

Our Goals for the "Internet of Things"

BUILDITSECURE.LY

- 👁 FOCUS effort towards crowd-funded, small commercial and bootstrapped vendors
- ❤ BUILD partnerships and goodwill between IoT vendors and the security community
- ✔ COORDINATE efforts to incentivize security researchers for reporting vulnerabilities
- 📝 CURATE informational resources to help educate vendors on security best practices
- 🧍 PRESENT research at relevant events and be a point of contact for press inquiries

Fin

"Battles can be won being smart not just with a great attack power. We need to focus more on ideas, on innovation, trying to do things in different ways as hackers usually do"

- Questions?

- Gracias.
- E-mail: ccerrudo@ioactive.com
- twitter: @cesarcer