Park This

Yet Another Parking Meter Talk
Who’s Paul Moreno?

- EMEA Security Engineering Lead for Uber BV
- Advisory Board Member for Bugcrowd and Nanosec
- Former Head of Security for Pinterest
- Sound to Light Artist and likes long walks on the beach etc.
What?
We will discuss a variety of techniques by walking through the reverse engineering of an electronic parking meter. The embedded device includes a cashless payment system and a wireless (infrared) auditing system, which he analyzed without access to the other half of the communication system. The presentation's highlights include retrieving the read-only memory (ROM) directly from the silicon chip (via electron microscope with the aid of neural-network image processing), using electronically erasable programmable read only memory (EEPROM) limitations to gain advantages, breaking a payment system through statistical black-box crypto-analysis, determining block-cipher keys with careful current measurements of a running device, and ultimately achieving remote code execution through the infrared communication channel.
"Smart" Parking Meter Implementations, Globalism, and You

Black Hat USA 2009

Joe Grand aka Kingpin, Grand Idea Studio, Inc.
Jacob Appelbaum, Noisebridge
Chris Tarnovsky, Flylogic Engineering
• IPS Group Inc.
• The hardware
  ○ Capabilities
  ○ Identified chips and bits
  ○ Funny business
• What’s next...
IPS Group Inc.

- Based in Sunny San Diego
- Founded in 1994
- Private, venture backed ~$2.8m
- PCI Level 1 certified
- No CSO?

Not to be confused with The IPS Group, Group IPS, IPS Group BV, IPS Group Limited, or I-P-S Group
IPS Group Inc.

@IPSsmartmeter Does IPS Group Inc have a security bug bounty program or responsible disclosure?

10:43 PM - 8 Feb 2016
Conversation started February 9

Paul Moreno
Do you happen to have a security bug bounty program?

IPS Group, Inc.
Hi Paul, I don't know if we are the company you are speaking about. We are a smart parking technology company. There is another IPS Group that does security.

Please let us know if you have any other questions.

Thank you,
IPS Group
M5™ Single-Space Smart Parking Meters

IPS Group, Inc. provides customers and their patrons with an intuitive and convenient parking experience which is more cost-effective, customer-friendly, and reliable than alternatives. The patented IPS Smart Meter retrofits into current on-street parking meter housings, and offers multiple payment options (coins, credit/debit card, smart card, tokens, pay-by-phone, and optional NFC/contactless payment). The IPS single-space Smart Meter boasts unparalleled power efficiency and utilizes solar-power technology. Each Smart Meter is wirelessly networked to a state-of-the-art Data Management System which provides customers with a wealth of real-time data. Click here for a demonstration of how to use IPS parking meters.

Key Features:

- Patented meter mechanism accepts payment by coins, credit/debit card, smart card and tokens, pay-by-phone and optional NFC/contactless payment
- Wirelessly networked to a web-based, SaaS management system—no additional communications infrastructure required
- Retrofits into existing meter housings/poles, and maintains all current meter enforcement and collection processes
- Solar powered with rechargeable battery pack
- PA-DSS and Level 1 PCI-DSS Certified
The M5

- Costs $485-$515 retail, per online proposals
- $5.75 per month in license and wireless fee’s
- $.08 per credit card transaction
- Takes your money... via coins, chip cards, smart cards, NFC?

“Cloud” managed WCGW?
The M5

Made in San Diego?

- Costs $485-$515 retail, per online proposals
- $5.75 per month in license and wireless fee’s
- $.08 per credit card transaction
- Takes your money… via coins, chip cards, smart cards, NFC?

“Cloud” managed WCGW?
Parky McParkface
Parky McParkface Teardown

- Main Processing Board
- Modem / Solar Panel
- Display / Reader Assembly

Also...

- Coin Validator
- Other parts: Batteries, antennas, LEDs, buttons and shit
Parky McParkface Teardown

- Main Processing Board
Parky McParkface Teardown

- Main Processing Board
- Rechargeable battery
- RFID chip, TRF7960
- 2.4gmhz LAIRD wireless chip (not enabled)
- I2C, other ports
- Mixed Signal Controller
Parky McParkface Teardown

- Main Processing Board
- Texas Instruments M430F5438A
  - Ultra low voltage
  - JTAG interface
  - Hella UARTS
Parky McParkface Teardown

- Modem / Solar Panel
Parky McParkface Teardown

- Modem / Solar Panel

Telit CE910-DUAL

- CDMA / 1xRTT
- Verizon Networks
- USB Port?
Parky McParkface Teardown

- Display / Reader Assembly
Parky McParkface Teardown

- Coin Validator
Parky McParkface Teardown

- Other parts: Batteries, antennas, LEDs, buttons and shit
Parky McParkface Teardown

- Rechargeable battery?
Parky McParkface Teardown

- Rechargeable battery?

Lithium Thionyl Chloride (Li-SOCl2)

Not rechargeable…

Found online for ~$1 a piece in quantity possibly less in mass
What’s Next?

- Attempt to read the firmware off the FPGA
- Get it back online, using a Samsung Network Extender
- Take a look at the modem AT Commands
- Replace firmware

Free Parking?
Thank You