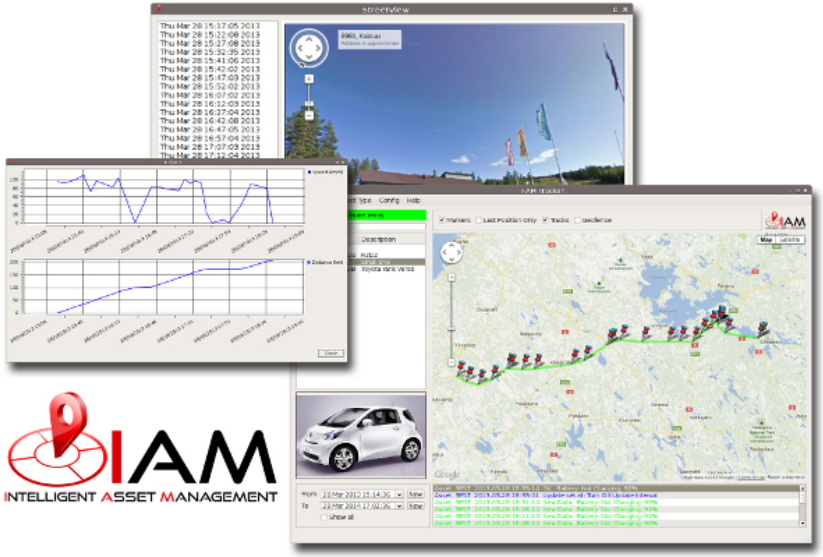
Design and Deployment of Security Sensitive, Networked Embedded Systems

Johan Dams

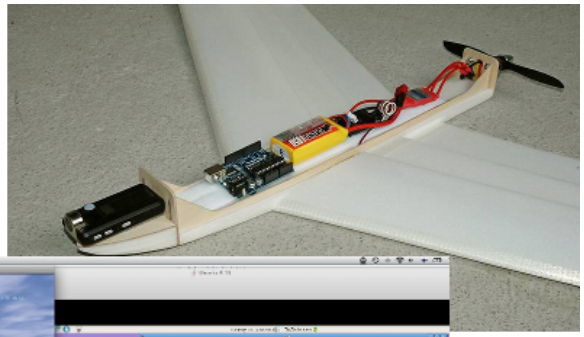
24-26/09/2015
www.wrdsystems.co.uk

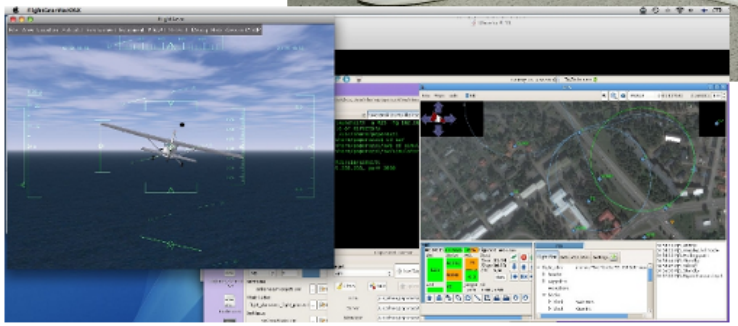
WRD Systems

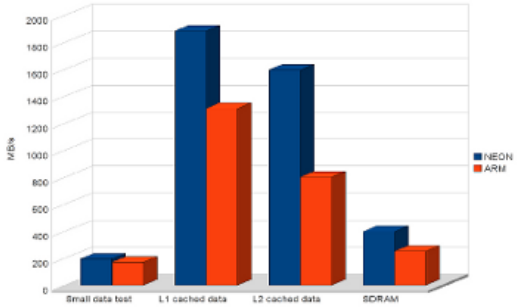
Innovation Excellence

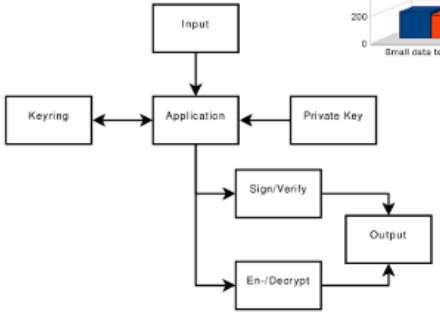


PROJECT ARGUS









WRD Systems
Innovation Excellence

Some discovered issues

Smart Meters

- No tamper protection
- No encryption of the data sent or received by the meter
- No authentication procedure between meter and local / remote reader
- Potential to read and write (modify) the program code stored in the meter Electronics (JTAG not disabled, etc.)

The AnonaBox

- Default password, stock hardware (after claiming it was custom), etc.
- Kickstarter funding frozen
  - → restarted on IndieGogo and funded again!

Lots of other stuff, see for example recent car hack, LIFX Smart light bulbs hack (yes, really: http://thehackernews.com/2014/07/smart-led-lightbulbs-can-be-hacked-too.html), baby monitors, etc...

Some of the Major Current Security Challenges

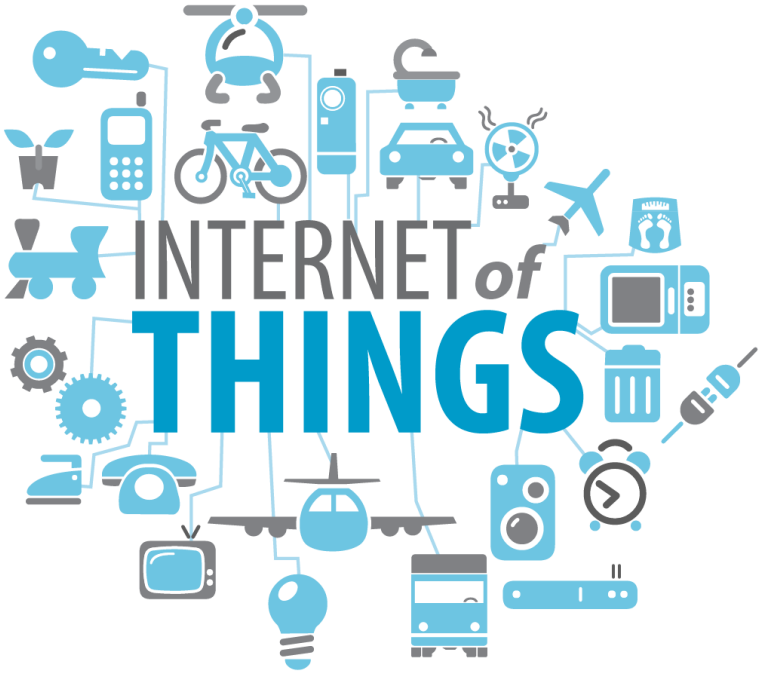
The Cost Issue
- Security is expensive
- Needs dedicated people
- Features over all else

The (Lack of) Knowledge Issue
- Security is hard
- Seems to work, but really isn't
- Not part of the design from the beginning
- Too Much Data (correct example: Estonia age check)

→ Lots of, especially, managers are in denial
“There are no security issues”
“We have good engineers, they can handle it”
“It's too expensive at this stage in our product, we'll get to it later”
“The V.C. won't fund new people and doesn't want any outsiders on it”

WRD Systems
Innovation Excellence

The Hype...



WRD Systems
Innovation Excellence

Possible Solution

Solving the trust issue, using proof of work

→ Byzantine fault tolerance

→ Borrow heavily from Bitcoin, BitMessage and BitMask

→ Decentralized, trust-less, peer-to-peer protocol over IP

→ No need for central authorities, certificates, etc.

→ Key management forms a central part of the protocol without separate key management infrastructure
  - → node address == hash(public_key)
  - → ephemeral addresses for perfect forward secrecy

WRD Systems
Innovation Excellence

Needs lots of hashing…
→ dedicated ASIC
→ use old Bitcoin miners

Parameters

Payload (encrypted)	Target: 2^64/(payload length * difficulty)	Initial Hash: hash(payload)

Perform POW

```
while trial > target
    nonce = nonce + 1
    result  = hash(hash(nonce + initial hash))
    trial    = first 8 bytes of result
```

Send message, prepend 8 byte result from POW

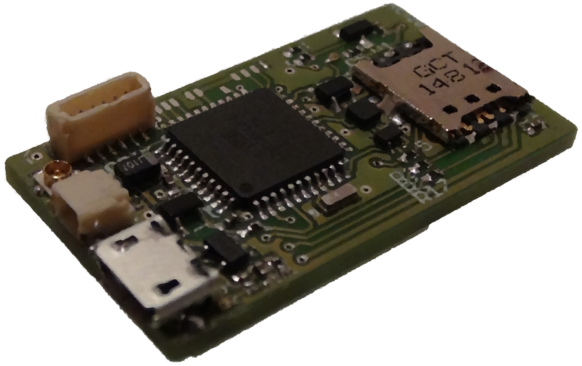
Verify POW

Nonce: (first 8 bytes of received)
Data: (message – first 8 bytes)
Initial hash: hash(data)
Result hash: hash(hash(nonce + initial hash))
POW value: (first 8 bytes of result hash)
Target: 2^64 / (payload length * difficulty)

If POW Value <= target, POW check passes

Initial version shows promise, but needs more work… and <cough>funding</cough>

WRD Systems
Innovation Excellence



Project: 5000 GPS trackers deployed in major UK city

→ Implemented with higher security standards than required by government

- → All data encrypted at all times (in transit and at rest)
- → U.K. data centre, dedicated servers, block all access from outside U.K., etc.
- → 256-bit encryption as minimum (WRD Systems internal requirement)

- → All development (software, hardware, firmware) done internal at WRD
- → Manufactured in the U.K. with U.K. component suppliers

- → Actually cheaper than competition, with much faster turnaround between demo and final product

Questions?