Internet Of Things (IOT) InSecurity

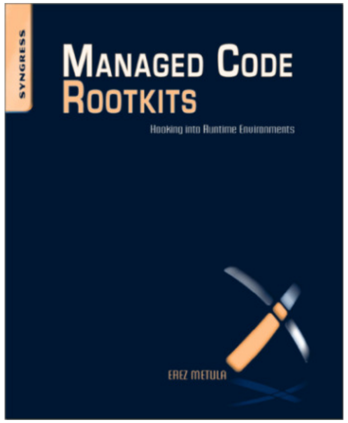
Erez Metula
Chairman & Founder, AppSec Labs
ErezMetula@AppSec-Labs.com

Israel Chorzevski
CTO, AppSec Labs
Israel@AppSec-Labs.com

About us

Erez Metula

- Chairman and Founder of AppSec Labs
- Book author
- World renowned Speaker & Trainer



Israel Chorzevski

- CTO of AppSec Labs
- Security consultant and trainer
- Security enthusiast
- Manager of Mobile and IoT research

AppSec R&D expertise

- 2010 focus – Mobile (Android, IOS) security
  - Special tools & VMs was developed
  - Dedicated courses in mobile app security (three peat appearance at blackhat USA)

- 2015 focus – IoT security
  - New attack vectors
  - Mitigations and solutions
  - Customized security trainings

Agenda

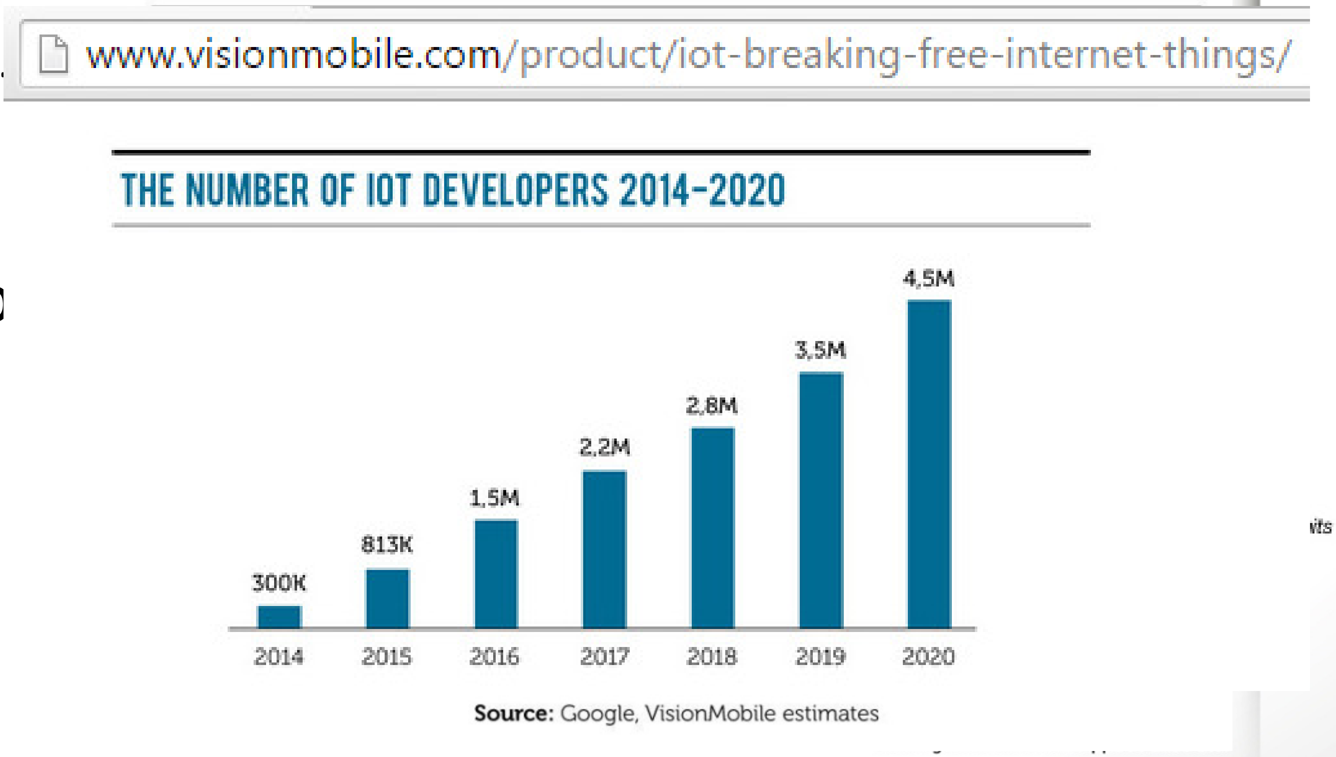
- Introduction to IoT
- IoT technologies
- IoT architecture
- Common vulnerabilities
- Demos & Videos

What's common to all..?

- [OXFORD] A proposed development of the Internet in which **everyday objects have network connectivity**, allowing them to send and receive data.

Industries & Consumers

- Connected homes – appliances, locks
- Smart cars (Automotive)
- Wearables
- Connected ci
- Health care
- Transportatio
- Oil & Gas



www.visionmobile.com/product/iot-breaking-free-internet-things/

THE NUMBER OF IOT DEVELOPERS 2014-2020

Source: Google, VisionMobile estimates

Standards war

Hyper/Cat
intel
SAMSUNG
BROADCOM
WIND RIVER
OPEN INTERCONNECT CONSORTIUM
AllJoyn
QUALCOMM
Microsoft
cisco
Panasonic
ALLSEEN ALLIANCE
IEEE Internet of Things
Google

debian
ubuntu
redhat
CentOS
fedora
Mandriva
slackware linux
FreeBSD
PC-BSD
solaris 10
opensolaris
suse
ARM mbed
RTOS

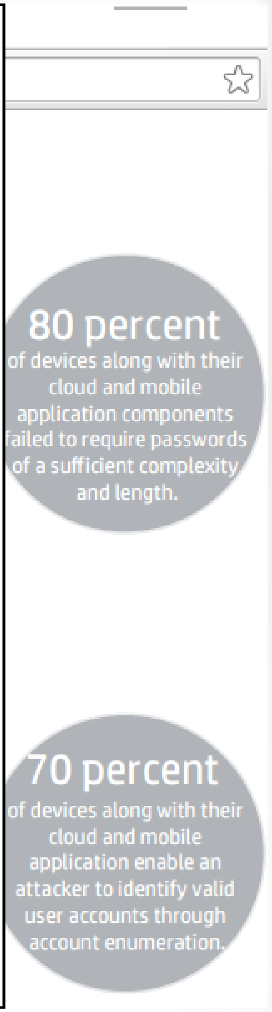
- Zigbee
- 6LoWPAN
- Z-Wave
- Sigfox
- Weightless

- BLE
- oneM2M
- LTN
- Thread
- 802.11ah

- Clean -Slate
- 2G
- 3G
- 4G
- 5G?

IoT Security Fail Examples

- 10/10 security systems accept ‘123456’
- 10/10 security systems with no lockout
- 10/10 security systems with enumeration
- SSH listeners with root/“” access
- 6/10 web interfaces with XSS/SQLi
- 70% of devices not using encryption
- 8/10 collected personal information
- 9/10 had no two-factor options
- Unauthenticated video streaming
- *Completely flawed* software update systems

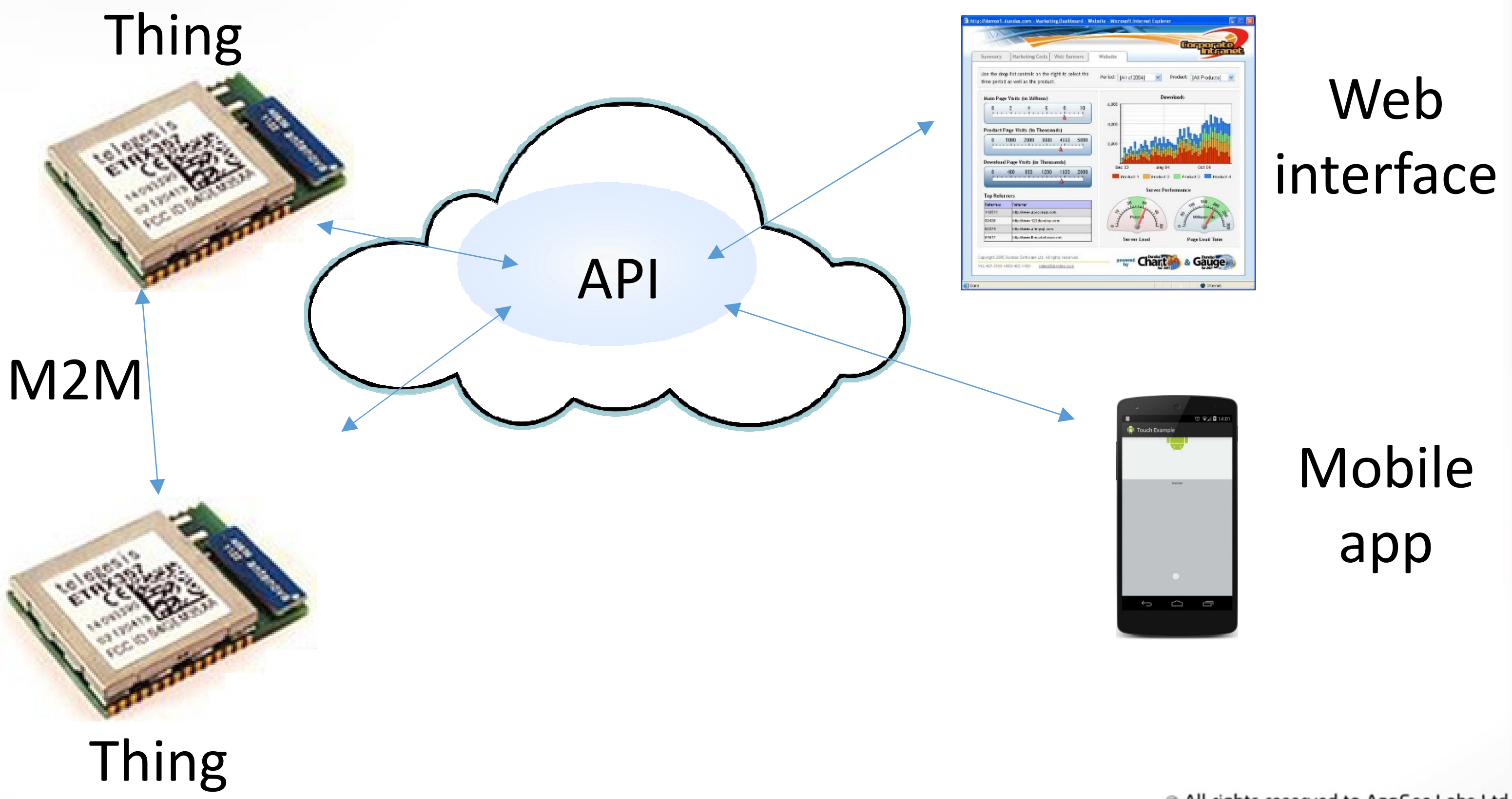


80 percent
of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.

70 percent
of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

IOT architecture

- IoT layers: Device (sensor / controller), Network, Application, Mobile, Cloud (API / Web)



Thing

M2M

Thing

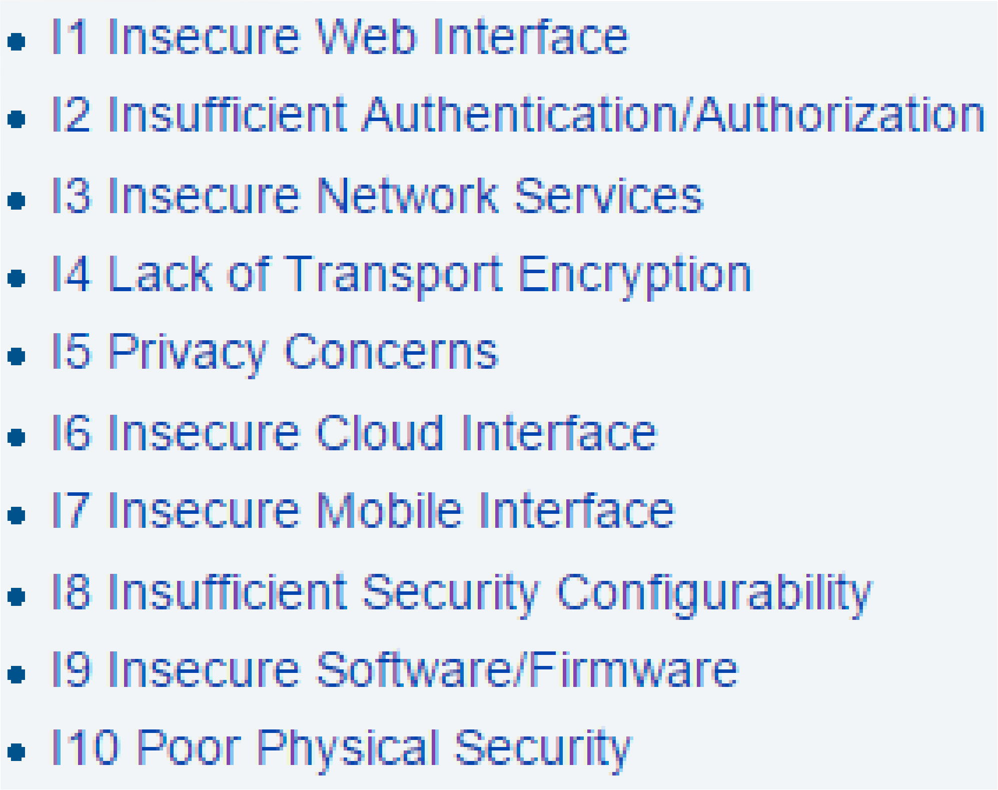
API

Web interface

Mobile app

OWASP IoT TOP TEN

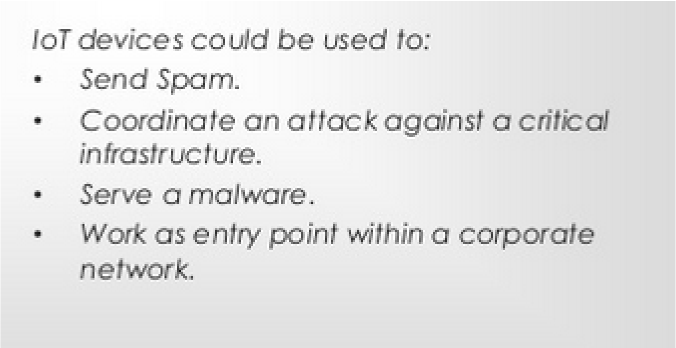
IoT top ten vulnerabilities



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

levels

- **Hardware Based Security:** open it up, dump firmware, etc
- **Web Dashboard/Mobile Apps** - Vulnerabilities in the web/mobile apps could lead to the compromise of security for the entire device network.
- **M2M - Communication between the components:**



IoT devices could be used to:

- *Send Spam.*
- *Coordinate an attack against a critical infrastructure.*
- *Serve a malware.*
- *Work as entry point within a corporate network.*

We are a node of a global network

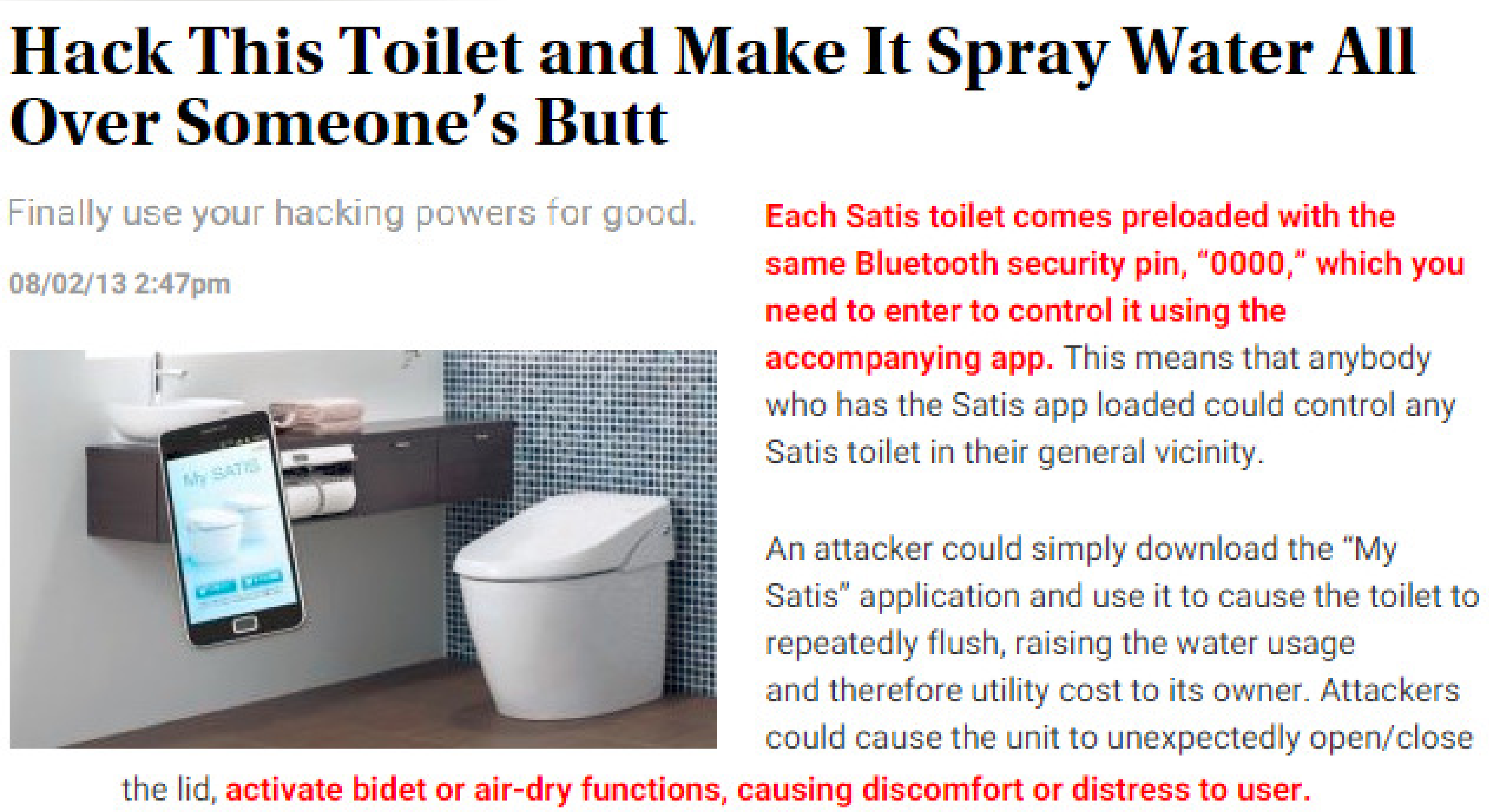
Why this happens and what's the risk

- Why there are so much of vulnerabilities
  - Focusing on product-to-market
  - A number of products based on prototypes
  - Failure to provide OTA and update mechanisms
  - Micro-controllers have limited CPU / RAM
  - Existing libraries are not optimized for embedded
  - Hardware developers become software developers
- What's the damage?

Story Time

From weird to scary

From weird to scary



Hack This Toilet and Make It Spray Water All Over Someone's Butt

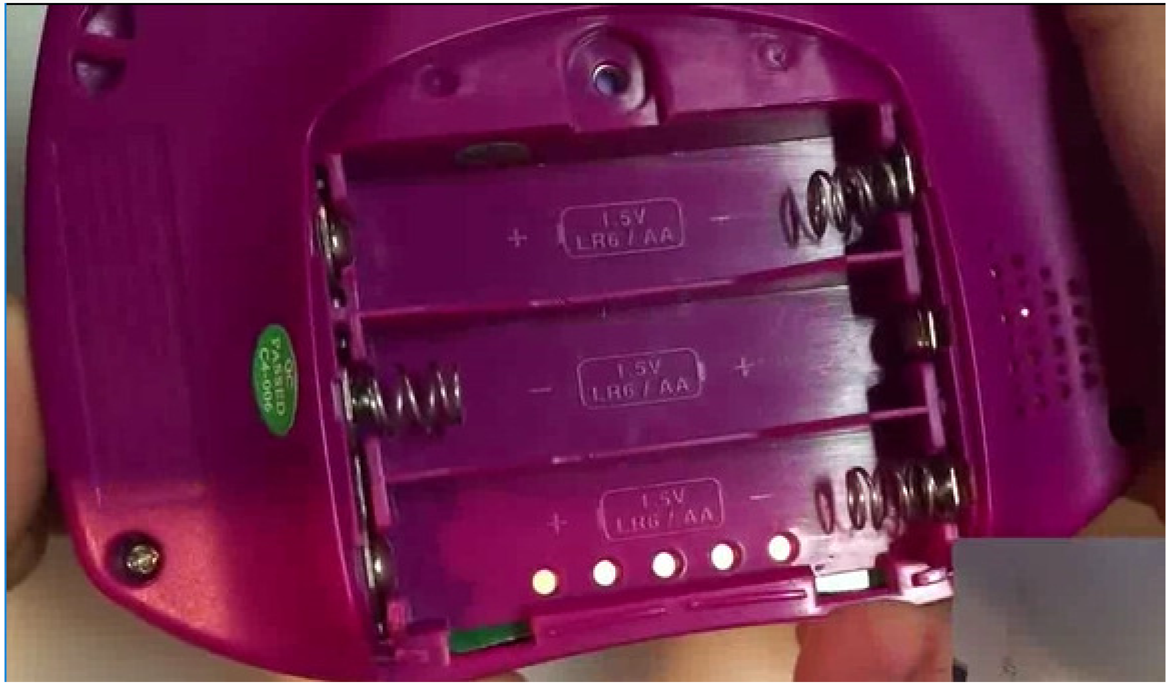
Finally use your hacking powers for good.

08/02/13 2:47pm

Each Satis toilet comes preloaded with the same Bluetooth security pin, "0000," which you need to enter to control it using the accompanying app. This means that anybody who has the Satis app loaded could control any Satis toilet in their general vicinity.

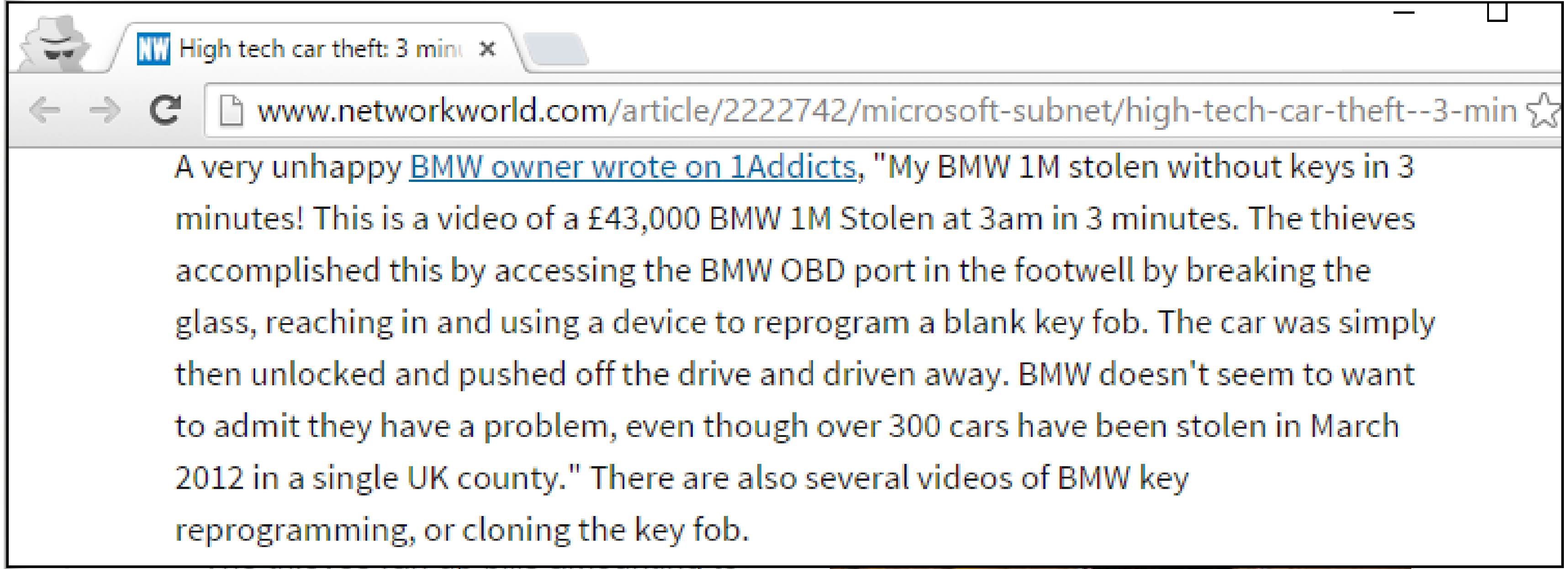
An attacker could simply download the "My Satis" application and use it to cause the toilet to repeatedly flush, raising the water usage and therefore utility cost to its owner. Attackers could cause the unit to unexpectedly open/close the lid, **activate bidet or air-dry functions, causing discomfort or distress to user.**

From weird to scary

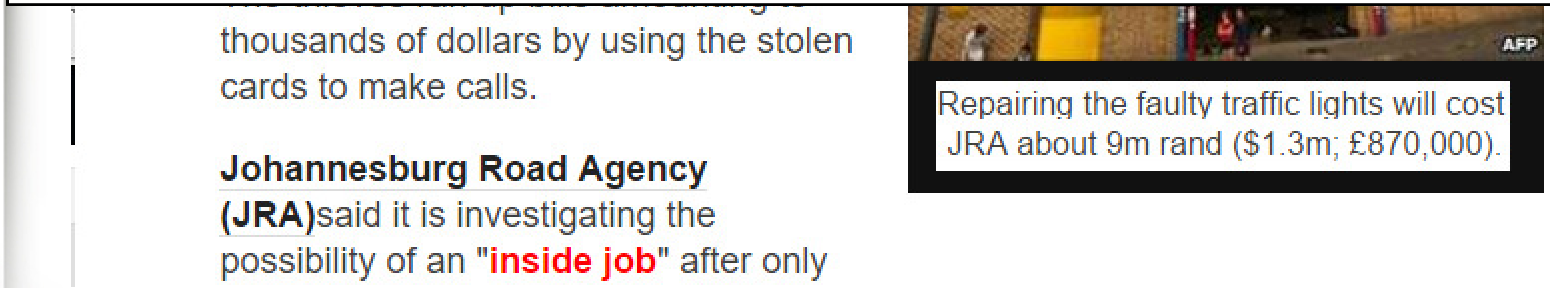


From weird to scary

From weird to scary


High tech car theft: 3 min
www.networkworld.com/article/2222742/microsoft-subnet/high-tech-car-theft--3-min

A very unhappy BMW owner wrote on 1Addicts, "My BMW 1M stolen without keys in 3 minutes! This is a video of a £43,000 BMW 1M Stolen at 3am in 3 minutes. The thieves accomplished this by accessing the BMW OBD port in the footwell by breaking the glass, reaching in and using a device to reprogram a blank key fob. The car was simply then unlocked and pushed off the drive and driven away. BMW doesn't seem to want to admit they have a problem, even though over 300 cars have been stolen in March 2012 in a single UK county." There are also several videos of BMW key reprogramming, or cloning the key fob.



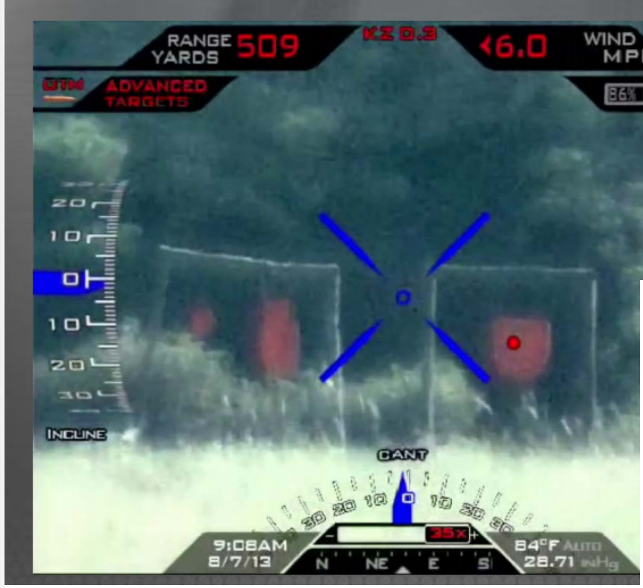
thousands of dollars by using the stolen cards to make calls.

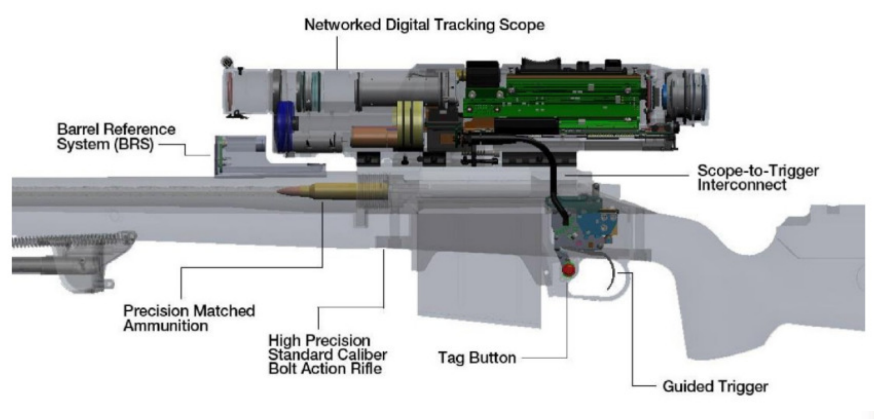
Johannesburg Road Agency (JRA)said it is investigating the possibility of an "**inside job**" after only

Repairing the faulty traffic lights will cost JRA about 9m rand ($1.3m; £870,000).

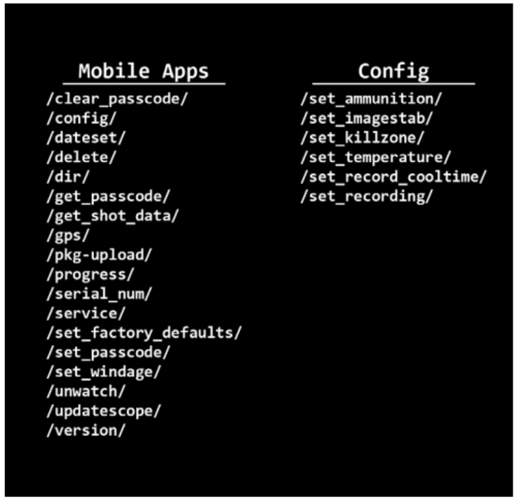
WIFI Gun – BlackHat 2015

ShotView App



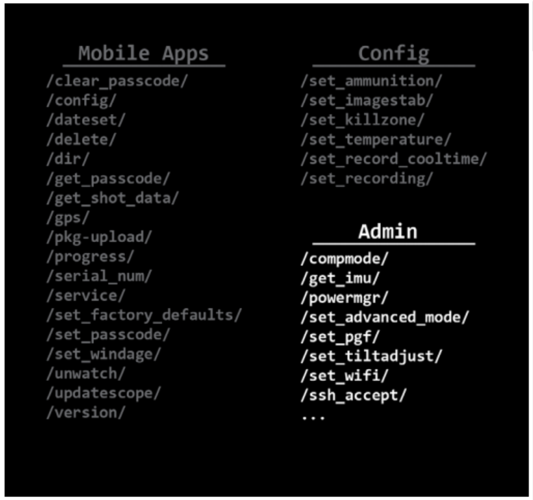

Networked Digital Tracking Scope
Barrel Reference System (BRS)
Scope-to-Trigger Interconnect
Precision Matched Ammunition
High Precision Standard Caliber Bolt Action Rifle
Tag Button
Guided Trigger

Public API



```
  Mobile Apps                    Config
/clear_passcode/              /set_ammunition/
/config/                      /set_imagestab/
/dateset/                     /set_killzone/
/delete/                      /set_temperature/
/dir/                         /set_record_cooltime/
/get_passcode/                /set_recording/
/get_shot_data/
/gps/
/pkg-upload/
/progress/
/serial_num/
/service/
/set_factory_defaults/
/set_passcode/
/set_windage/
/unwatch/
/updatescope/
/version/
```

Admin API



```
  Mobile Apps                    Config
/clear_passcode/              /set_ammunition/
/config/                      /set_imagestab/
/dateset/                     /set_killzone/
/delete/                      /set_temperature/
/dir/                         /set_record_cooltime/
/get_passcode/                /set_recording/
/get_shot_data/
/gps/                            Admin
/pkg-upload/                  /compmode/
/progress/                    /get_imu/
/serial_num/                  /powermgr/
/service/                     /set_advanced_mode/
/set_factory_defaults/        /set_pgf/
/set_passcode/                /set_tiltadjust/
/set_windage/                 /set_wifi/
/unwatch/                     /ssh_accept/
/updatescope/                 ...
/version/
```

Special IOT attacks

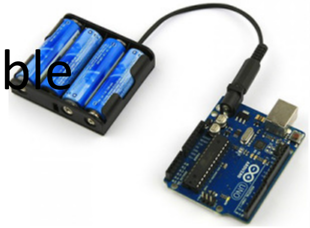
- Transport attacks
  - Bluetooth/LBE (e.g. “Just work” mode)
  - SMS (spoofing, 2g, new sim inssuance)
  - Etc.
- Electronic “screening”
- Timing based attack
  - Reveal data
  - Disabling other commands
- Power attack
  - Delayed disabling detection
  - Battery abuse
- Thing “relocation”

NSA: Never use standard commercial Bluetooth headsets.
https://www.**nsa**.gov/ia/_files/factsheets/i732-016r-07.pdf

- Physical threats (fire, explosion, etc.)
- Lack of CPU power (encryption, etc.)
- M2M
- And more…

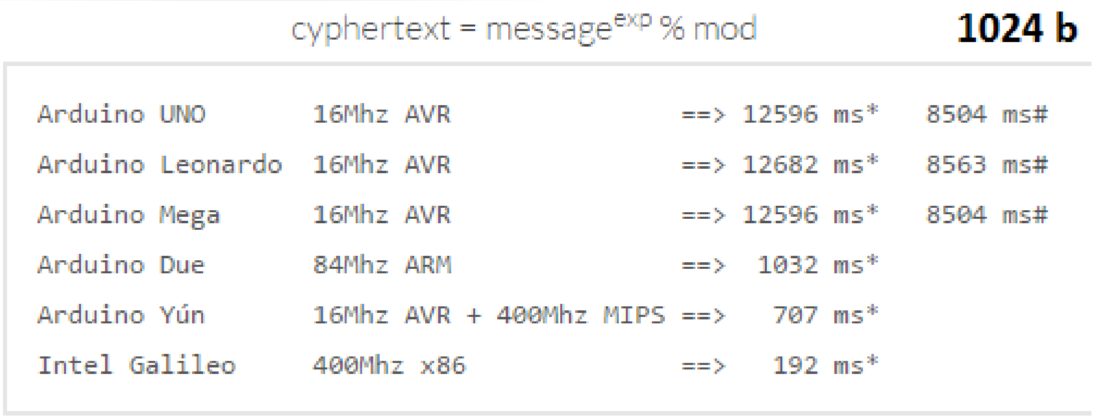
Example – power attack

- Some attacks are against the power source of the device
- No power = DoS
- Leds, thought innocent looking, can be a source of trouble



- Example – calculation of led power consumption
- AA batteries: 2700 mAh
- Leds consume between 5 -20 mA when on
- can easily eat a battery in less than a week
- two AA batteries, using 6mA Arduino current
- LED (20mA) on all day: 4 days [avg current = 26mA]
- LED on/off (1s/1s): 7 days [avg current = 16mA]
- LED on/off (0.5s/1.5s): 17 days [avg current = 6.5mA]

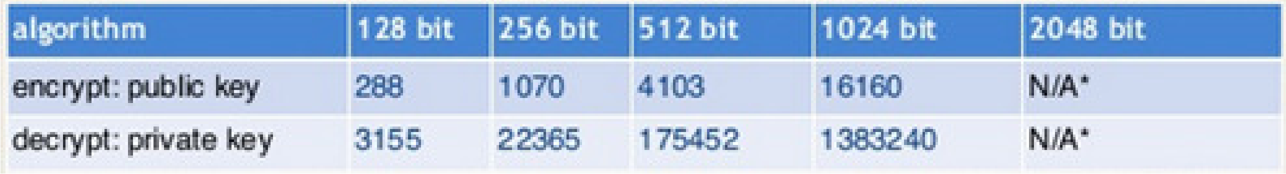
Example – Lack of CPU power



cyphertext = message^{exp} % mod **1024 b**

```
Arduino UNO       16Mhz AVR                ==> 12596 ms*   8504 ms#
Arduino Leonardo  16Mhz AVR                ==> 12682 ms*   8563 ms#
Arduino Mega      16Mhz AVR                ==> 12596 ms*   8504 ms#
Arduino Due       84Mhz ARM                ==>  1032 ms*
Arduino Yún       16Mhz AVR + 400Mhz MIPS ==>   707 ms*
Intel Galileo     400Mhz x86               ==>   192 ms*
```

Apple is requiring device makers using both WiFi and Bluetooth LE to use complicated encryption with 3072-bit keys

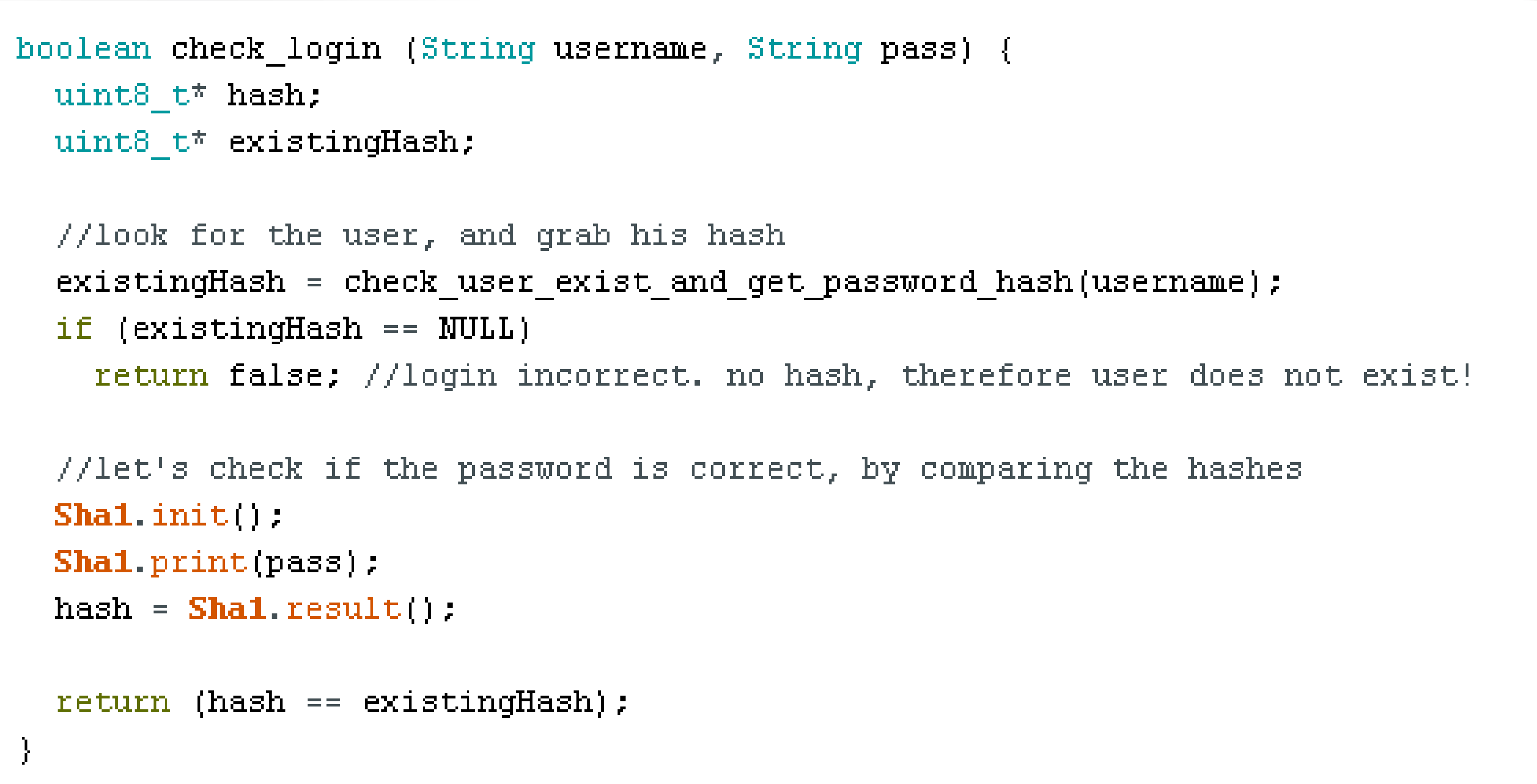


algorithm	128 bit	256 bit	512 bit	1024 bit	2048 bit
encrypt: public key	288	1070	4103	16160	N/A*
decrypt: private key	3155	22365	175452	1383240	N/A*

“Just figuring out if a door was opened or closed took 40 seconds”, said Lars Felber, a spokesman for Elgato

Example - Timing attacks

- Demo (if time permit)



```
boolean check_login (String username, String pass) {
  uint8_t* hash;
  uint8_t* existingHash;

  //look for the user, and grab his hash
  existingHash = check_user_exist_and_get_password_hash(username);
  if (existingHash == NULL)
    return false; //login incorrect. no hash, therefore user does not exist!

  //let's check if the password is correct, by comparing the hashes
  Sha1.init();
  Sha1.print(pass);
  hash = Sha1.result();

  return (hash == existingHash);
}
```

Many ways to attack IOT devices…

- White box is recommended
- Take it apart, read the flash memory
- Disassemble the firmware from the manufacturer
- MITM attack exposed most of the traffic
- Upgrade to a "custom" version
- Exploit shitty embedded C
- Fuzzing
- Logic errors
- RF
- Most of the standard network security errors are present too:
  - Random open ports
  - Old and vulnerable OS/application code
  - Etc.

Many ways to attack IOT devices…

- All elements need to be tested
  - The Internet of Things Device
  - The Cloud
  - The Mobile Application
  - The Network Interfaces
  - The Software
  - Physical Security
  - USB ports
- For each entry/exit point
  - Authentication
  - Authorization
  - Encryption
  - Input validation

Summary

- IoT security is NOT device security
- IoT have a lot of special vulnerabilities and attacks
- IoT requires a wide range of tests to cover all of the interfaces
- Testing IoT requires special expertise

- We at AppSec Labs invest time and research to investigate and improve IoT security

QUESTIONS ?

THANK YOU !

Erez Metula

Chairman & Founder, AppSec Labs

ErezMetula@AppSec-Labs.com

Israel Chorzevski

CTO, AppSec Labs

Israel@AppSec-Labs.com

…and last thing: we're hiring !!!