Linux Day 2017

Giornata nazionale a favore della diffusione del software libero e del sistema operativo GNU/Linux

28 ottobre

Università degli Studi di Palermo
Viale delle scienze - Edificio 7
Aula Magna di Ingegneria
INGRESSO LIBERO

09.00	Registrazione dei partecipanti
09.30	Saluti e inizio dei lavori

Sessione mattutina
Moderatore: Marcello Masotto

10.00	Introduzione al Free software Lorenzo Faletra
10.30	GDPR 2016/679: conformi entro il 2018, cosa bisogna sapere? Adriano Bertolino
11.00	Blockchain, bitcoin e altro Daniele Mondello
11.30	Coffee Break
12.00	Introduzione alla crittografia Nanni Bassetti
13.00	Dibattito
13.30	Pausa Pranzo

Sessione pomeridiana
Moderatore: Marcello Masotto

14.30	(in)Sicurezza nella videosorveglianza Davide Ammirata
15.00	IoT: Internet of Things? Internet of Thieves! Giovanni Pullarà
15.30	Resistenza digitale: consigli per la privacy Mariano Graziano
16.30	Hacks, Data breach e Cyber Warfare Girolamo Daniele Bruneo
17.00	Dibattito e chiusura dei lavori
17.30	Rilascio degli attestati di frequenza

FREE CIRCLE

A.S.I.

SPONSOR

CENTRAL
COMPUTER, GAME...AND MORE

linuxday.thefreecircle.org/2017

LINUX DAY ITALIA

Col patrocinio di:

Città di Palermo

In collaborazione con:

udu unione degli universitari · fsfe · FAB LAB PALERMO · OLOMEDIA · Parrot Security · Viral digital strategies

Iniziativa realizzata nell'ambito del programma dell'Università degli studi di Palermo per la promozione delle attività culturali e sociali degli studenti

Internet Of Things?
Internet Of Thieves!

Pullarà Giovanni Battista [IT Engineer&DevOps]

Powered By GNU/Linux

GNU

powered by: FreeBSD

28/10/2017
Palermo

http://fablabpalermo.org

info@fablabpalermo.org

Who am I

**Sistemista/DevOps da sempre appassionato all'hacking.
La sua passione nasce accostandosi a realtà come il FreakNet e co-fondando l'hacklab a Palermo.
Con alle spalle un passato da IT Specialist presso Unicredit, attualmente si occupa dell'automazione di reti&sistemi e sviluppo per Viral Digital Strategies.
Socio del Fablab Palermo, FreeCircle GLUG, e del Museo dell'Informatica Funzionante, crede fermamente nell'opensource e nel "codice sorgente come mezzo di evoluzione personale e sociale".
Il suo motto?**

- **"Talk is cheap. Show me the code."
(Linus Torvalds)**

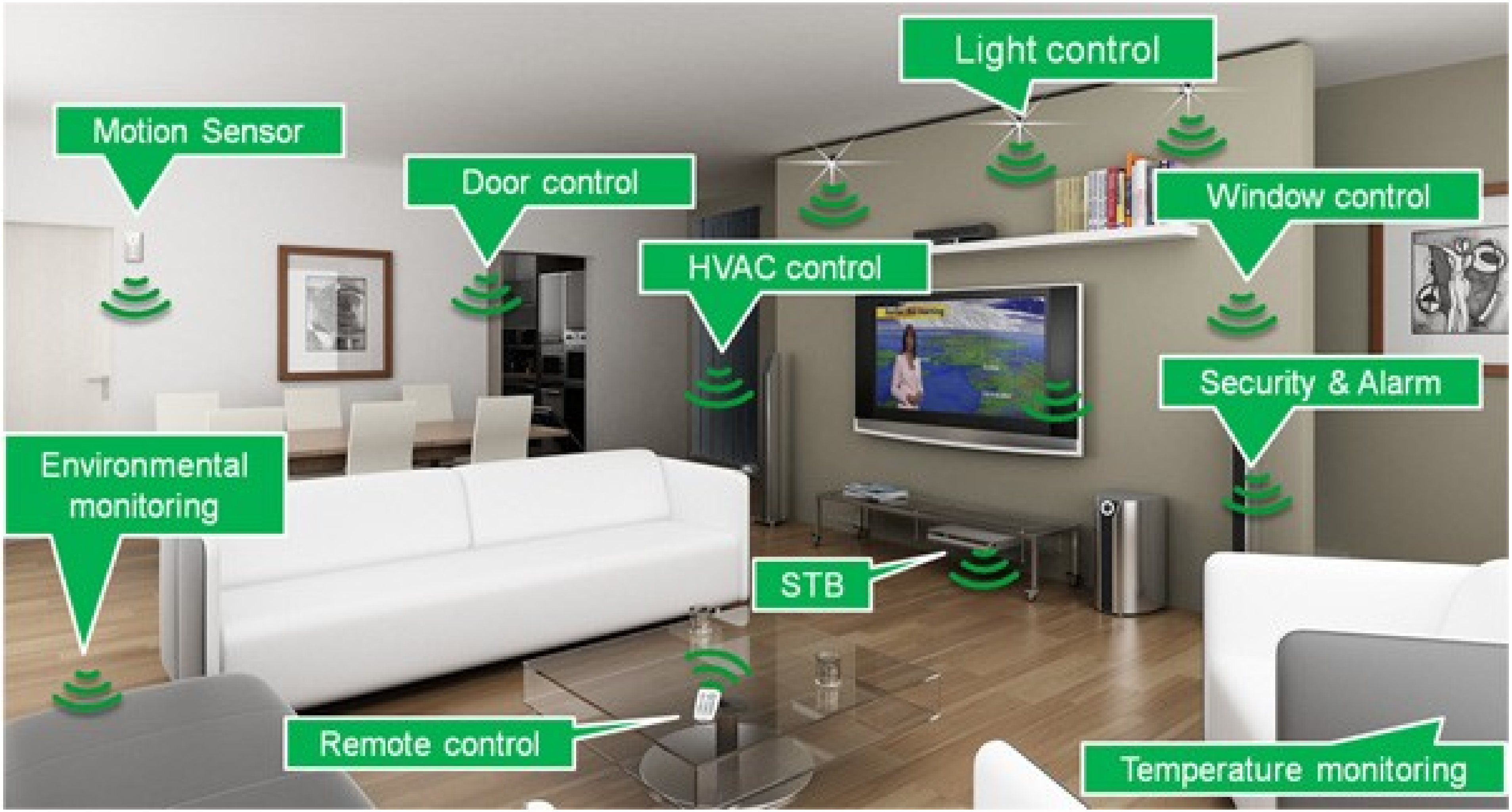
IOT DEVICE

IOT Device

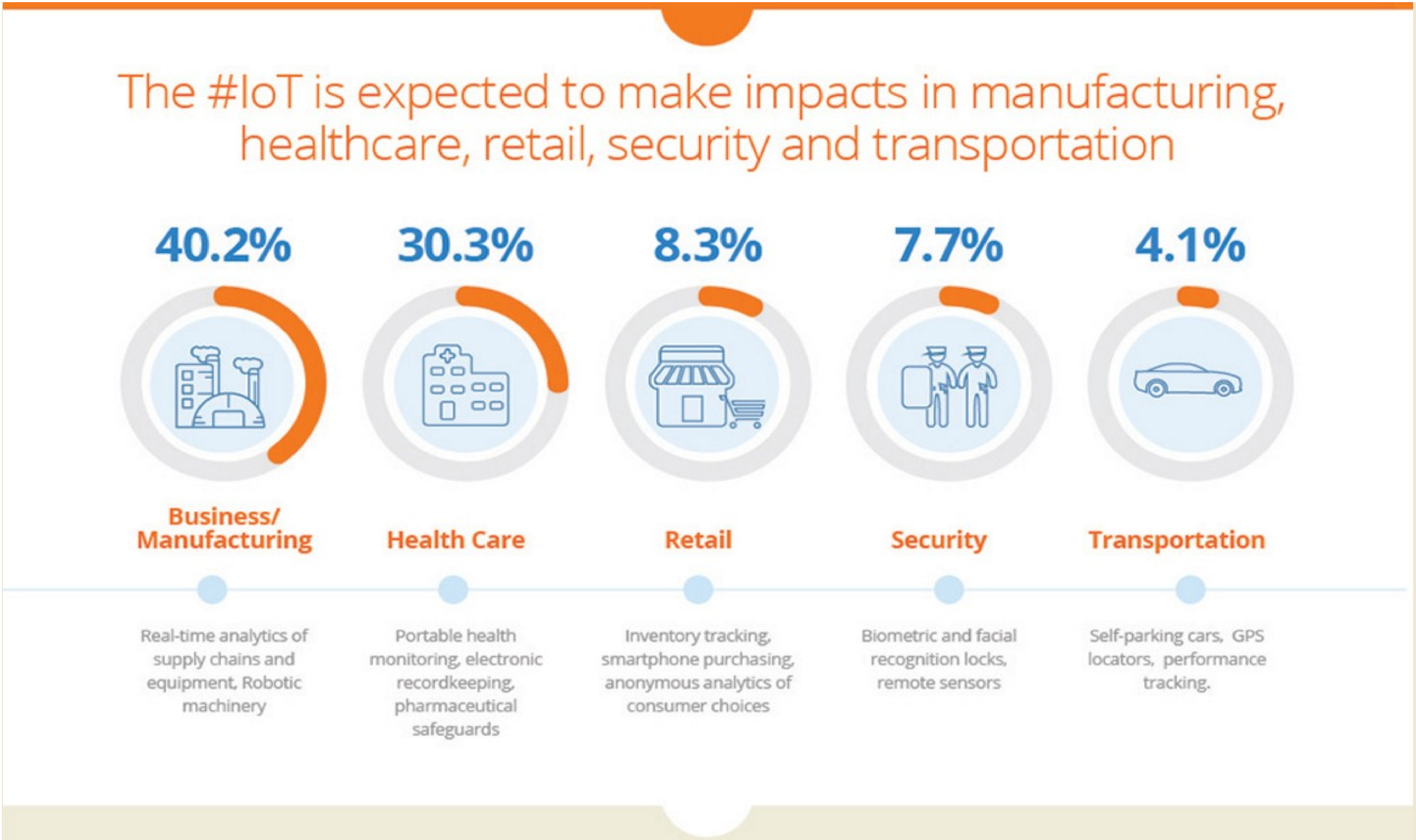
- Domotic [HVAC, SAC, FA, FLS, Lights&E.Appliance]
- Robotic
- Intelligent transportation system
- Biomedical
- Industrial Monitoring
- Telemetry
- Surveillance
- Smart Grid
- Smart City
- Embedded system
- Agricolture
- Zootechnics
- And more ...

IOT Device

IOT Device


Light control
Motion Sensor
Door control
Window control
HVAC control
Security & Alarm
Environmental monitoring
STB
Remote control
Temperature monitoring

IOT Device



The #IoT is expected to make impacts in manufacturing, healthcare, retail, security and transportation

40.2%

Business/ Manufacturing

Real-time analytics of supply chains and equipment, Robotic machinery

30.3%

Health Care

Portable health monitoring, electronic recordkeeping, pharmaceutical safeguards

8.3%

Retail

Inventory tracking, smartphone purchasing, anonymous analytics of consumer choices

7.7%

Security

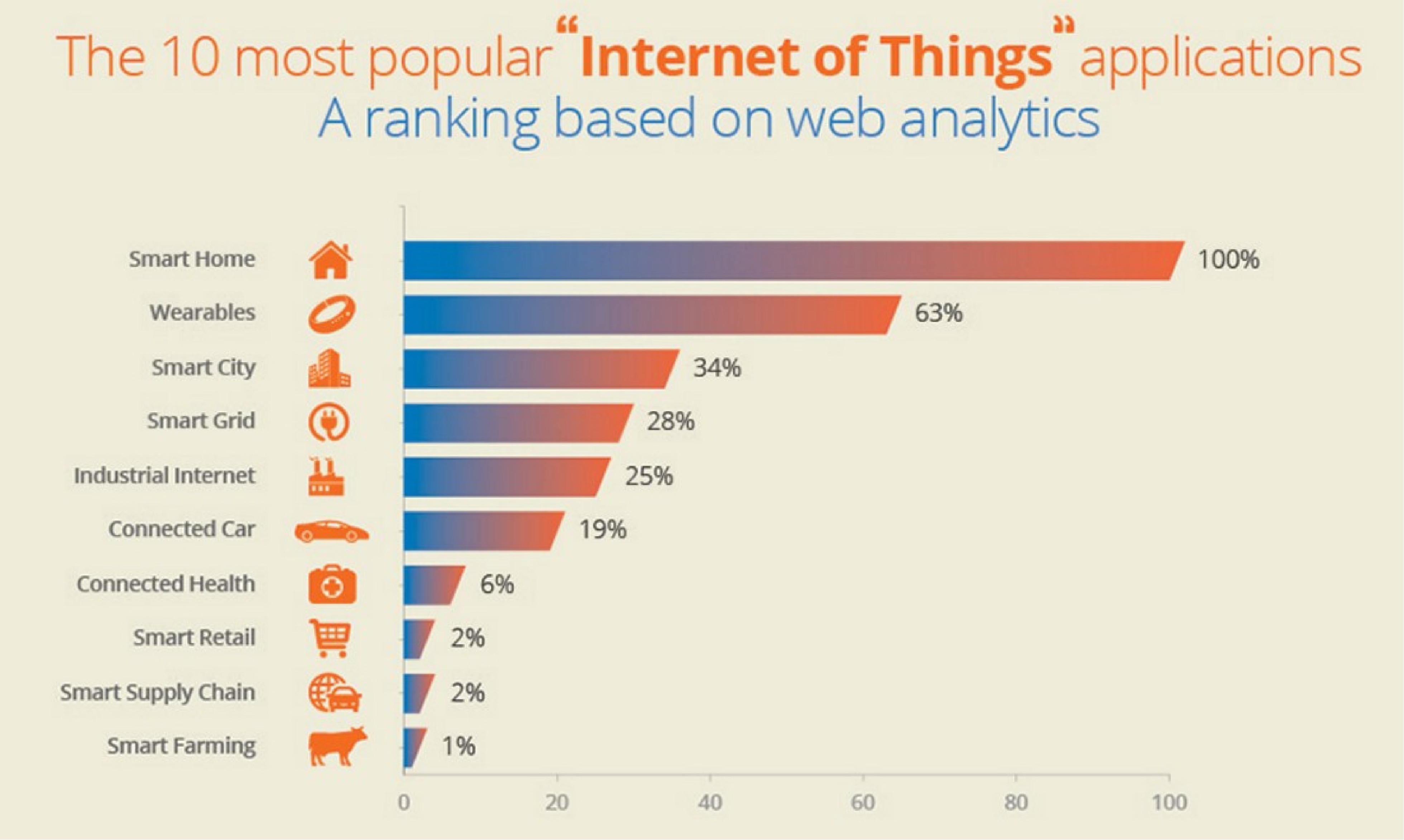
Biometric and facial recognition locks, remote sensors

4.1%

Transportation

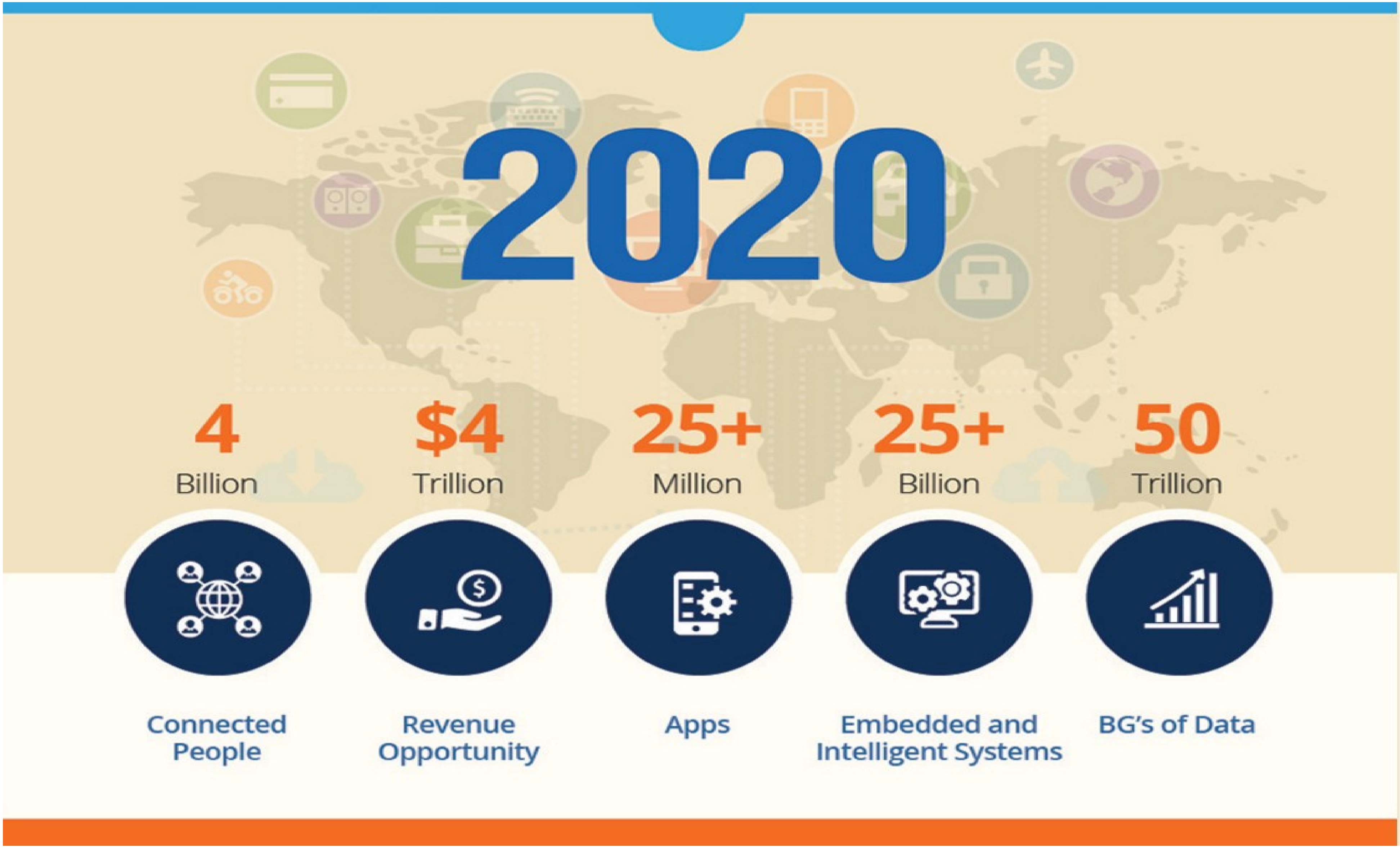
Self-parking cars, GPS locators, performance tracking.

IOT Device



The 10 most popular "Internet of Things" applications
A ranking based on web analytics
Smart Home
Wearables
Smart City
Smart Grid
Industrial Internet
Connected Car
Connected Health
Smart Retail
Smart Supply Chain
Smart Farming
100%
63%
34%
28%
25%
19%
6%
2%
2%
1%
0
20
40
60
80
100

IOT Device



2020

4 Billion Connected People

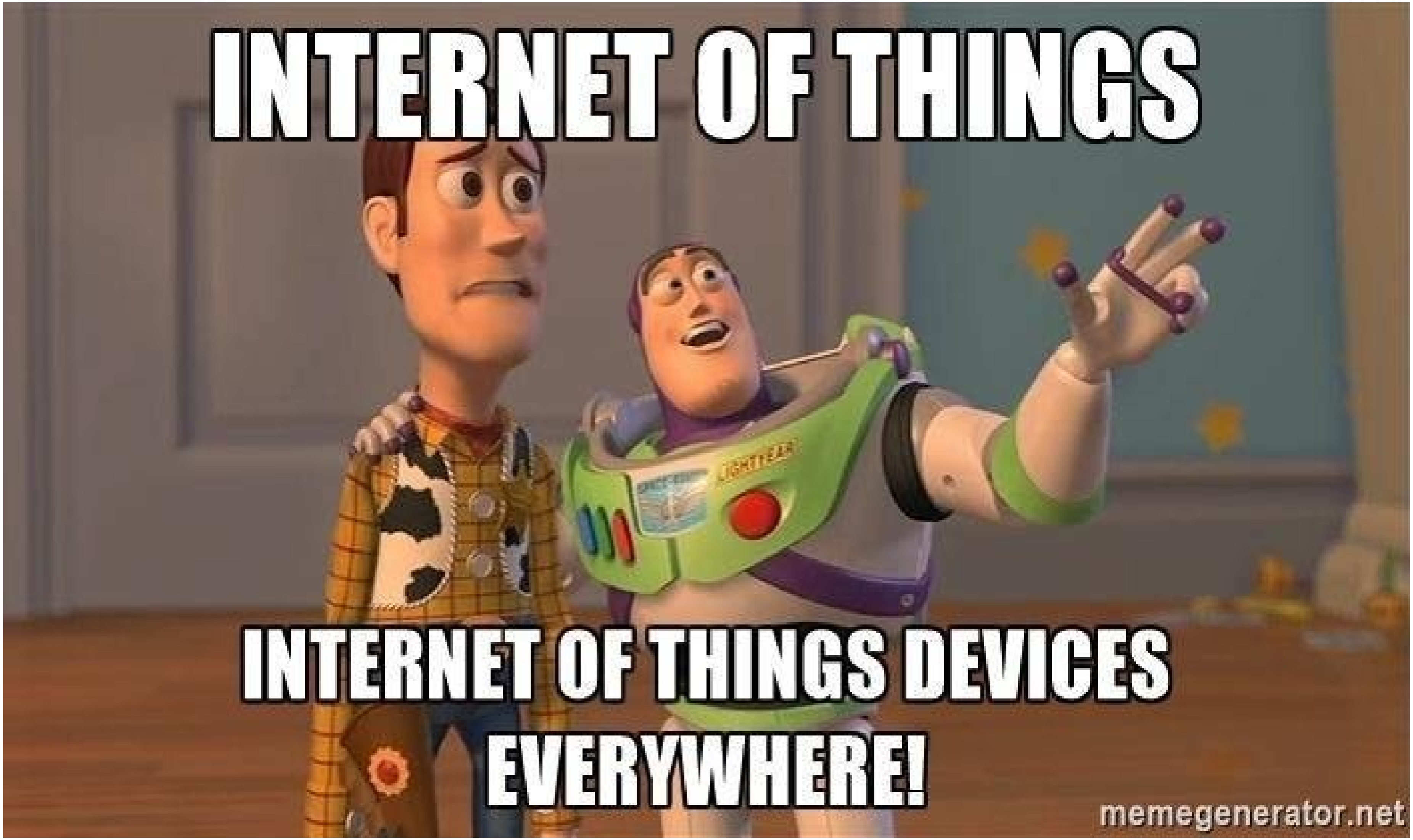
$4 Trillion Revenue Opportunity

25+ Million Apps

25+ Billion Embedded and Intelligent Systems

50 Trillion BG's of Data

IOT Device


INTERNET OF THINGS
INTERNET OF THINGS DEVICES EVERYWHERE!
memegenerator.net

IOT {in}Security

IOT inSecurity

THE S IN IOT
STANDS FOR SECURITY

IOT inSecurity

Kill a Jeep on the Highway !

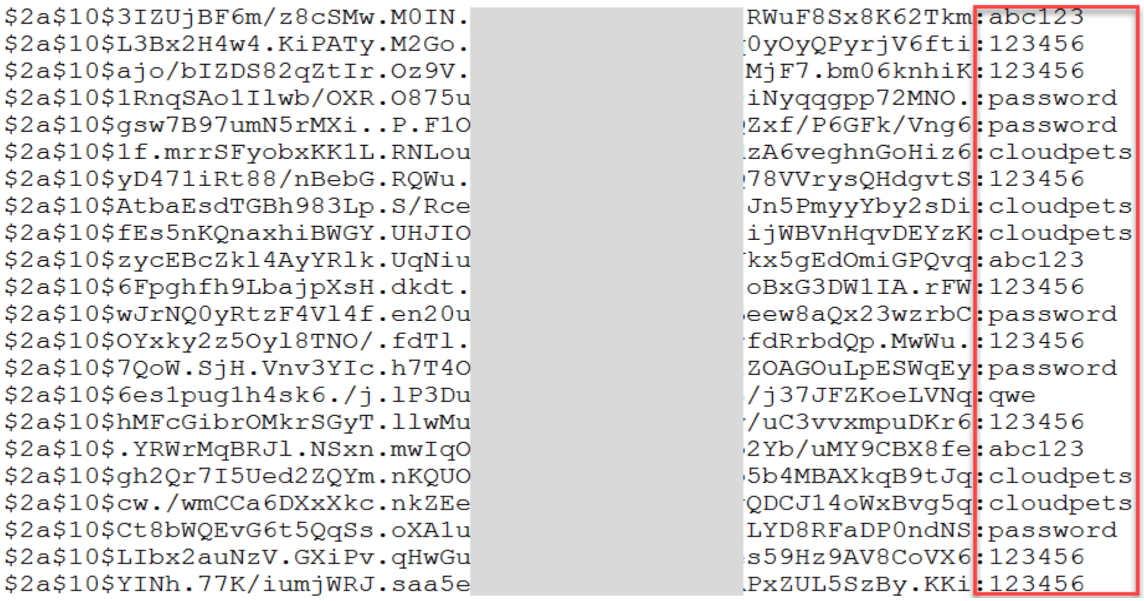
+ 500.000 hackable automobiles

Total Remote Control from Internet

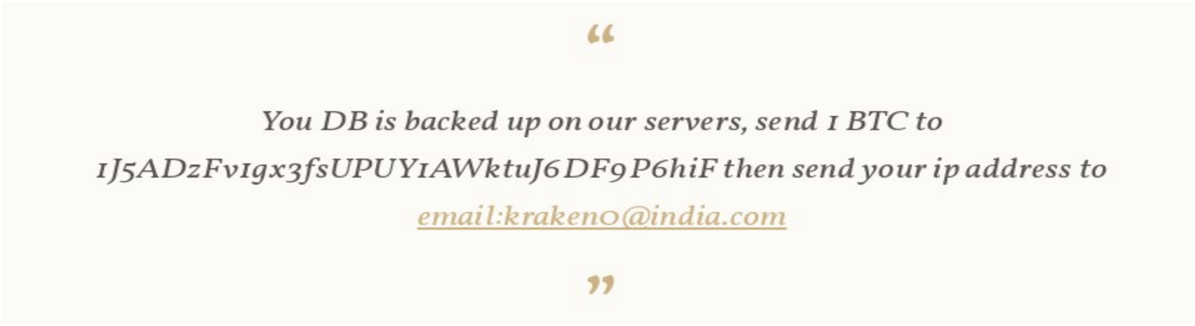
Chris Valasek's and Charlie Miller's pivotal research on hacking into Jeep's presented at DEFCON in 2015.

IOT inSecurity

Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages



```
$2a$10$3IZUjBF6m/z8cSMw.M0IN.[redacted]RWuF8Sx8K62Tkm:abc123
$2a$10$L3Bx2H4w4.KiPATy.M2Go.[redacted]0yOyQPyrjV6fti:123456
$2a$10$ajo/bIZDS82qZtIr.Oz9V.[redacted]MjF7.bm06knhiK:123456
$2a$10$1RnqSAo1Ilwb/OXR.O875u[redacted]iNyqqgpp72MNO.:password
$2a$10$gsw7B97umN5rMXi..P.F1O[redacted]Zxf/P6GFk/Vng6:password
$2a$10$1f.mrrSFyobxKK1L.RNLou[redacted]zA6veghnGoHiz6:cloudpets
$2a$10$yD471iRt88/nBebG.RQWu.[redacted]78VVrysQHdgvtS:123456
$2a$10$AtbaEsdTGBh983Lp.S/Rce[redacted]Jn5PmyyYby2sDi:cloudpets
$2a$10$fEs5nKQnaxhiBWGY.UHJIO[redacted]ijWBVnHqvDEYzK:cloudpets
$2a$10$zycEBcZkl4AyYRlk.UqNiu[redacted]kx5gEdOmiGPQvq:abc123
$2a$10$6Fpghfh9LbajpXsH.dkdt.[redacted]oBxG3DW1IA.rFW:123456
$2a$10$wJrNQ0yRtzF4Vl4f.en20u[redacted]eew8aQx23wzrbC:password
$2a$10$OYxky2z5Oyl8TNO/.fdTl.[redacted]fdRrbdQp.MwWu.:123456
$2a$10$7QoW.SjH.Vnv3YIc.h7T4O[redacted]ZOAGOuLpESWqEy:password
$2a$10$6es1pug1h4sk6./j.1P3Du[redacted]/j37JFZKoeLVNq:qwe
$2a$10$hMFcGibrOMkrSGyT.llwMu[redacted]/uC3vvxmpuDKr6:123456
$2a$10$.YRWrMqBRJl.NSxn.mwIqO[redacted]2Yb/uMY9CBX8fe:abc123
$2a$10$gh2Qr7I5Ued2ZQYm.nKQUO[redacted]5b4MBAXkqB9tJq:cloudpets
$2a$10$cw./wmCCa6DXxXkc.nkZEe[redacted]QDCJ14oWxBvg5q:cloudpets
$2a$10$Ct8bWQEvG6t5QqSs.oXA1u[redacted]LYD8RFaDP0ndNS:password
$2a$10$LIbx2auNzV.GXiPv.qHwGu[redacted]s59Hz9AV8CoVX6:123456
$2a$10$YINh.77K/iumjWRJ.saa5e[redacted]PxZUL5SzBy.KKi:123456
```



> “
>
> *You DB is backed up on our servers, send 1 BTC to 1J5ADzFv1gx3fsUPUY1AWktuJ6DF9P6hiF then send your ip address to email:kraken0@india.com*
>
> ”

IOT inSecurity

Hackers Can Disable a Sniper Rifle - Or Change Its Target

Security researchers Runa Sandvik, left, and husband Michael Auger have figured out how to hack into a Tracking Point TP750 rifle to disable it or control the trajectory of its bullets

Changing a single number in the rifle's software made the bullet fly 2.5-feet to the left, bullseyeing an entirely different target.

Thankfully TrackingPoint rifles are designed not to fire unless the trigger is manually pulled.

IOT inSecurity

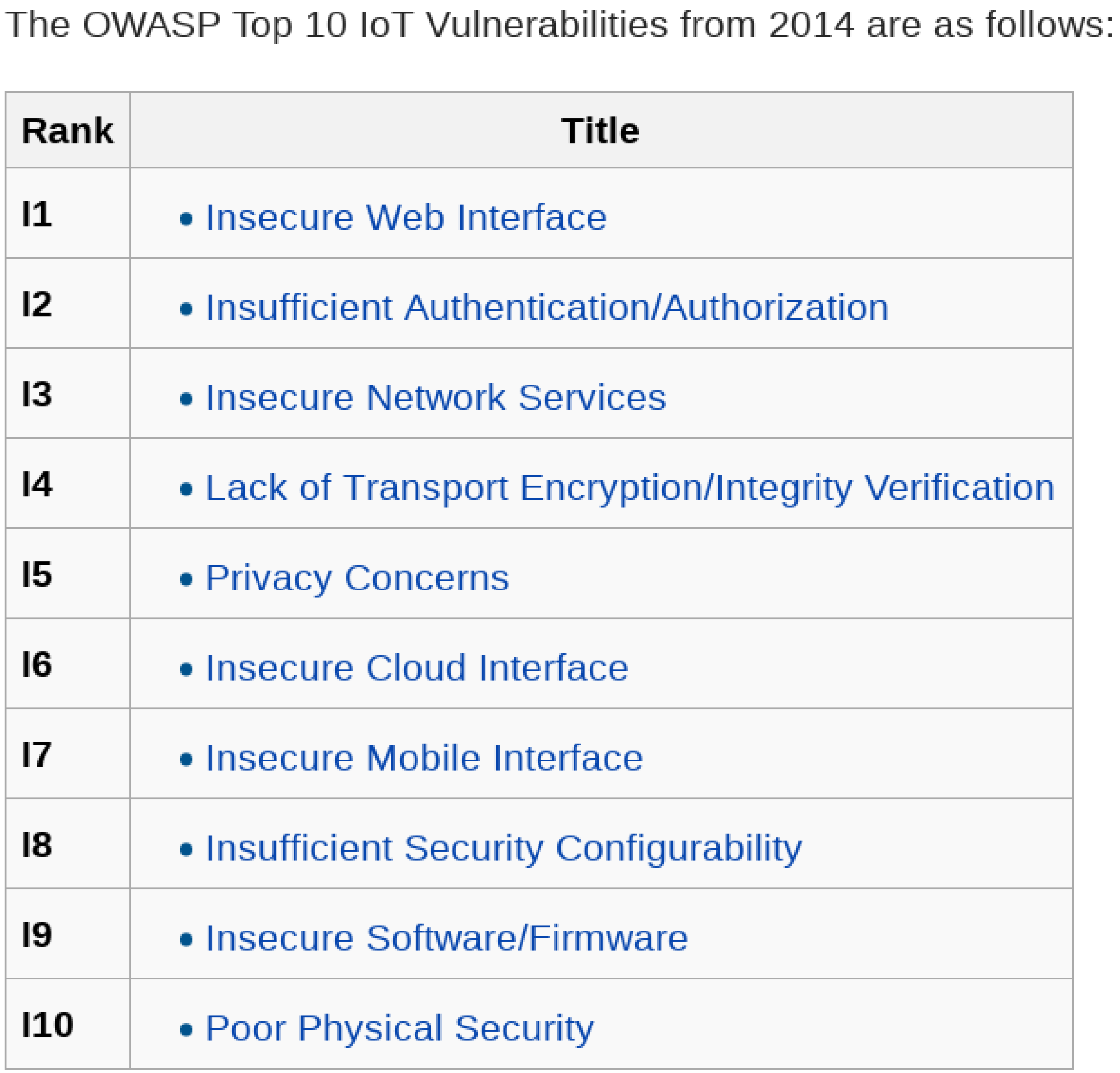
IOT inSecurity

NEED MORE PWNING STORY???

https://github.com/nebgnahz/awesome-iot-hacks
https://github.com/jaredthecoder/awesome-vehicle-security

A curated list of awesome resources, books, hardware, software, applications, people to follow, and more cool stuff about vehicle security, car hacking, and tinkering with the functionality of your car.

IOT inSecurity



The OWASP Top 10 IoT Vulnerabilities from 2014 are as follows:

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

IOT inSecurity

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

IOT inSecurity

IOT Security

IOT Security

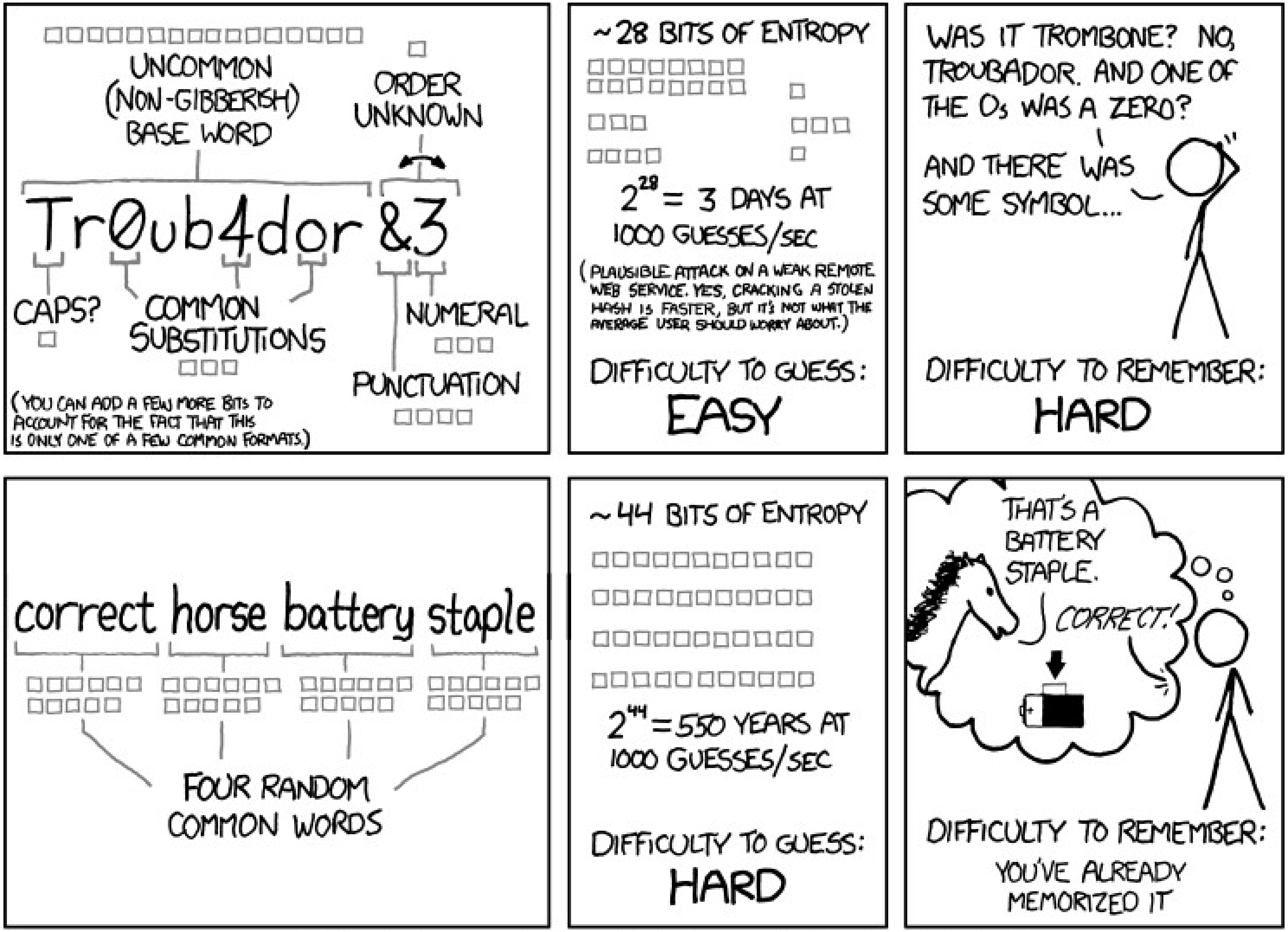
CHALLENGES

- IoT devices have less resource such as less processing power, storage space, memory etc.
- Firmware upgrade are not straight forward.
- Not easy to apply security patches.
- Current antimalware, endpoint security software can’t be installed on all IoT’s.
- Data on cloud, hard to self hosted.
- Too much {in}Security.
- Too much mobile.
- OWASP topten and more.

IMPROVING

- Users should download software’s and updates only from vendors and trusted source, and always verify the integrity of downloaded software with SHA.
- Product vendors/developers and customers are all responsible for improving IoT device security.
- Implement and enable 2-factor authentications by default.
- Follow secure coding methods and always perform input validation to avoid. Cross-site scripting (XSS), SQL injection and Buffer Overflow (BoF) vulnerabilities
- Enforce an effective passphrase policy, not short and hard, but long and easy to memorize.
- Always use encryption for communication.
- Vendors should think on ease of use vs security.
- People should think that, too.
- Network Isolation and Monitoring [vlan, firewall, IDS/IPS, NMS].
- Isolated Mobile.
- Complex but possible: selfhosted service. Not public/private cloud.
- Remember OWASP iot top ten.

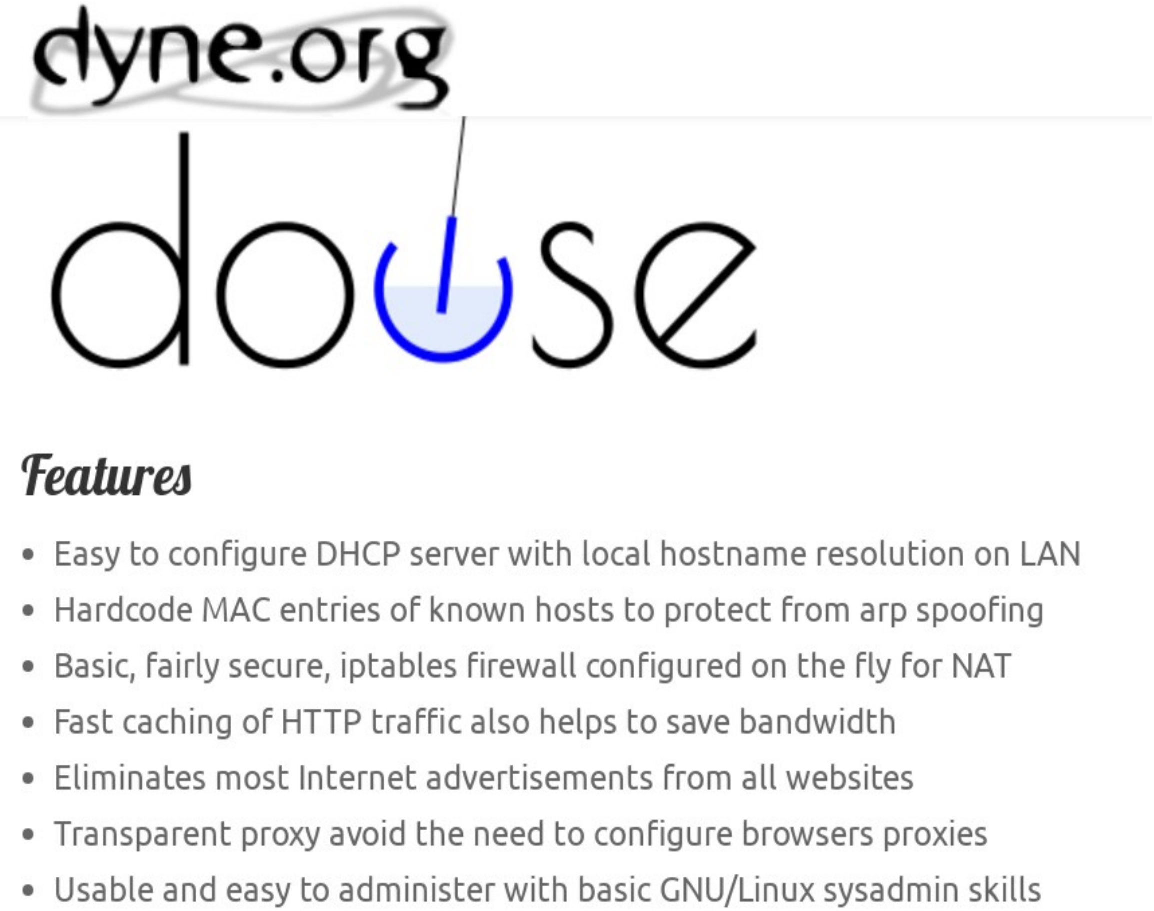
IOT Security


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

IOT Security

Dowse :: local area network rabdomancy

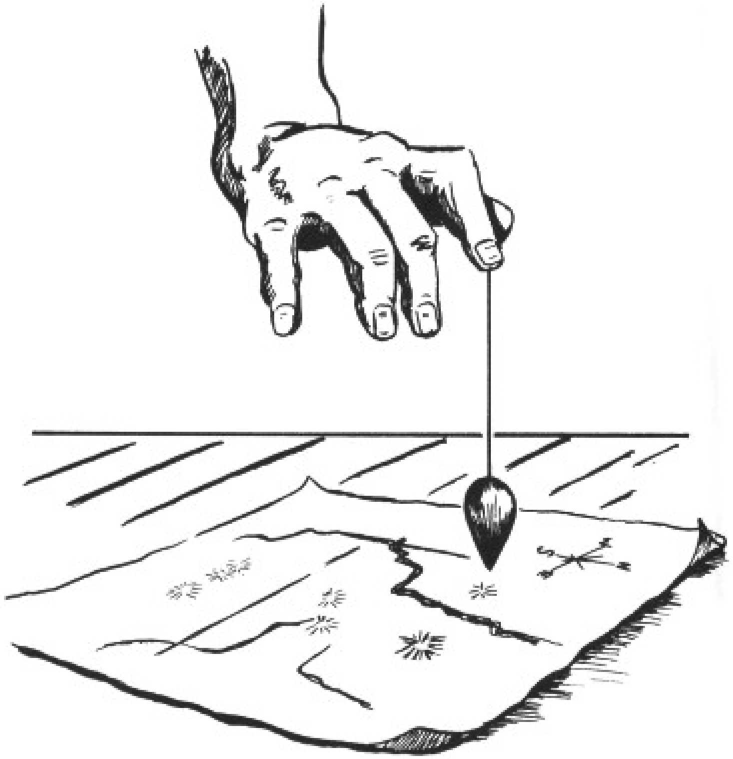


dyne.org

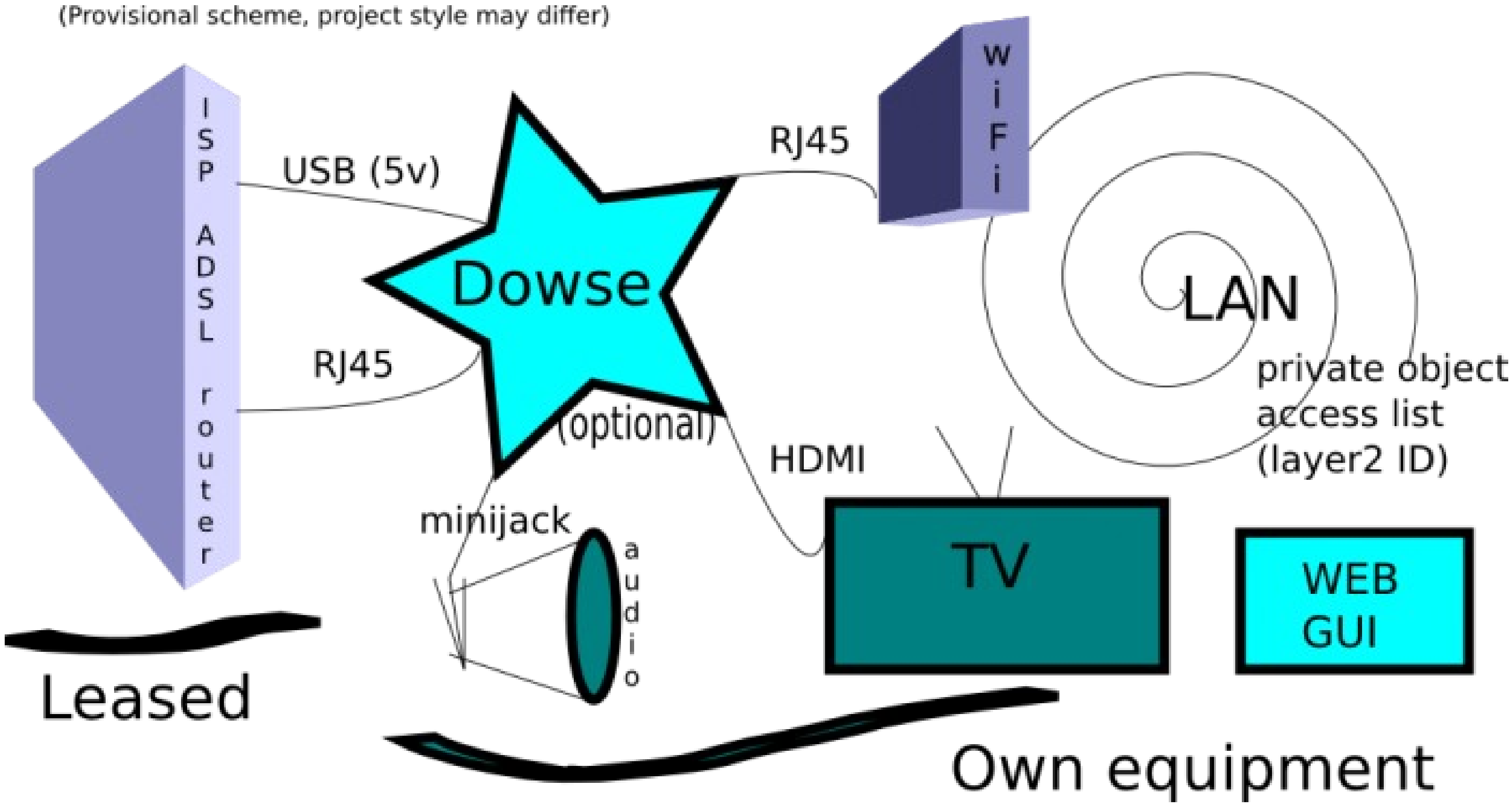
dowse

Features

- Easy to configure DHCP server with local hostname resolution on LAN
- Hardcode MAC entries of known hosts to protect from arp spoofing
- Basic, fairly secure, iptables firewall configured on the fly for NAT
- Fast caching of HTTP traffic also helps to save bandwidth
- Eliminates most Internet advertisements from all websites
- Transparent proxy avoid the need to configure browsers proxies
- Usable and easy to administer with basic GNU/Linux sysadmin skills



IOT Security



Dowse is a transparent proxy facilitating the awareness of ingoing and outgoing connections from and to a local area network.

Provides a central point of soft control for all local traffic: from ARP traffic (layer 2) to TCP/IP (layer 3) as well application space, by chaining a firewall setup to a trasparent proxy setup. A core feature for Dowse is that of hiding all the complexity of such a setup.

IOT Security

Dowse takes control of a LAN by becoming its DHCP server and thereby assigning itself as main gateway and DNS server for all clients. It keeps tracks of assigned leases by MAC Address. DNSMasq is the DHCP and DNS daemon.

All network traffic is passed through NAT rules for masquerading. HTTP traffic (TCP port 80) can be filtered through a transparent proxy using an application layer chain of Squid2 and Privoxy.

All IP traffic is filtered using configurable blocklists to keep out malware, spyware and known bad peers, using Peerguardian2 and Iptables.

All DNS traffic (UDP port 53) is filtered through Dnscap and analysed to render a graphical representation of traffic. It is also possible to tunnel it via DNSCrypt-proxy, encrypting all traffic (AES/SHA256) before sending it to DNSCrypt.eu or other configurable servers supporting this protocol.

In the future, traffic of all kinds may be transparently proxied for monitoring, filtering, and transformation by other applications loaded on the Dowse device.

All daemons are running as a unique non-privileged UID. The future plan is to separate them using a different UID for each daemon.

Final thoughts

Final Thoughts

Reference

Reference

https://github.com/nebgnahz/awesome-iot-hacks

https://github.com/jaredthecoder/awesome-vehicle-security

http://www.iotcrimes.com

http://illmatics.com/Remote%20Car%20Hacking.pdf

https://blog.codinghorror.com/password-rules-are-bullshit/

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

https://shodan.io

https://www.dyne.org/software/dowse/

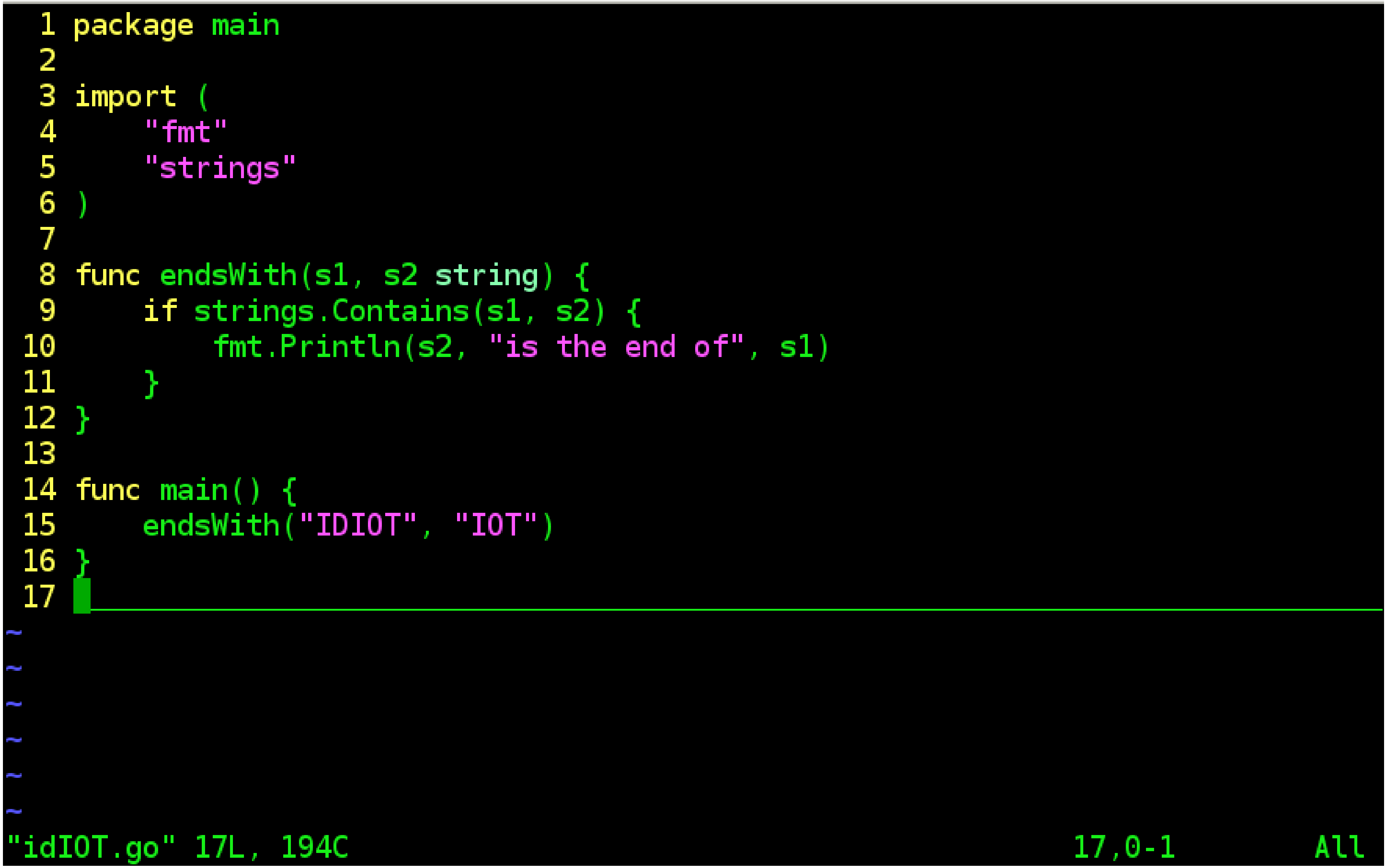
https://senseiserver.io

http://www.fablabpalermo.org

http://thefreecircle.org

http://viralds.it

The Truth



```
package main

import (
    "fmt"
    "strings"
)

func endsWith(s1, s2 string) {
    if strings.Contains(s1, s2) {
        fmt.Println(s2, "is the end of", s1)
    }
}

func main() {
    endsWith("IDIOT", "IOT")
}

~
~
~
~
~
~
"idIOT.go" 17L, 194C                                          17,0-1        All
```

Thanks and goodbye

Fablab&Free Circle - Palermo