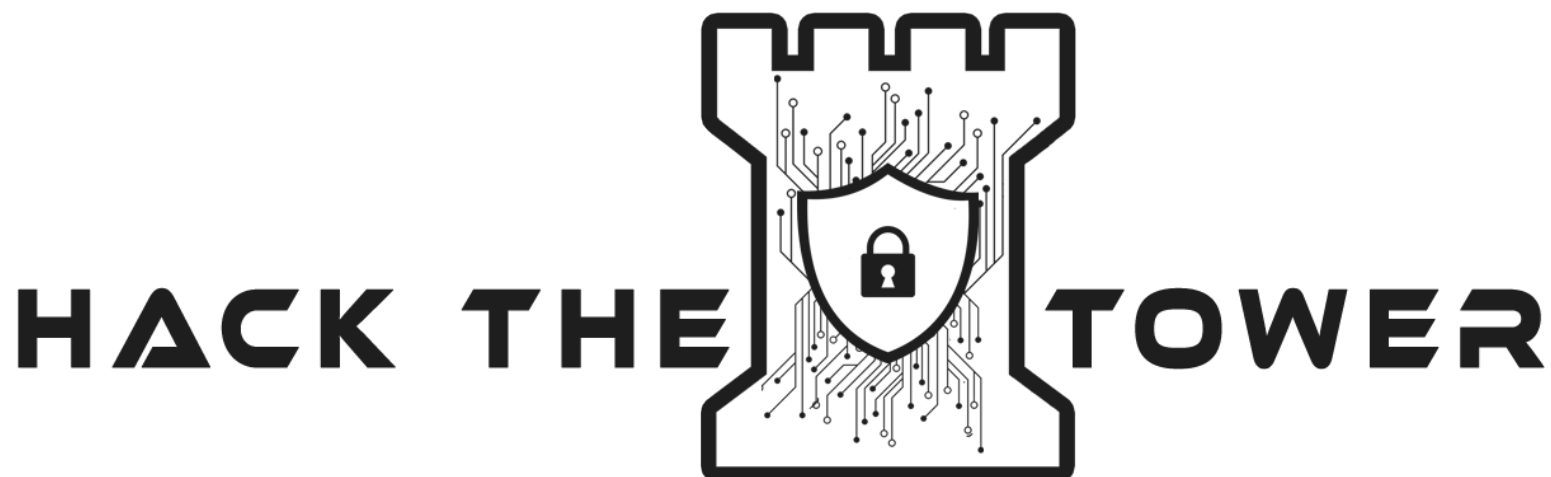


IoT: utile di sicuro. Ma sicuro?



Relatore:

19 giugno 2020



Igor Falcomatà, CEO
ifalcomata@enforcer.it



<https://creativecommons.org/licenses/by-nc/4.0/>

\$ whoami

- **attività professionale:**
 - **analisi delle vulnerabilità e penetration testing**
 - **security consulting**
 - **formazione**
- **altro:**
 - **sikurezza.org**
 - **(f|er-|bz-)lug**

free advertising >



Agenda

- **Introduzione a IoT**
- **IoT, IoE, IoM, M2M, IoS, CCS, ..**
- **Utilizzi e utilizzatori**
- **IoT e sicurezza**
- **Come fare?**
- **Riferimenti**
- **Q&A**



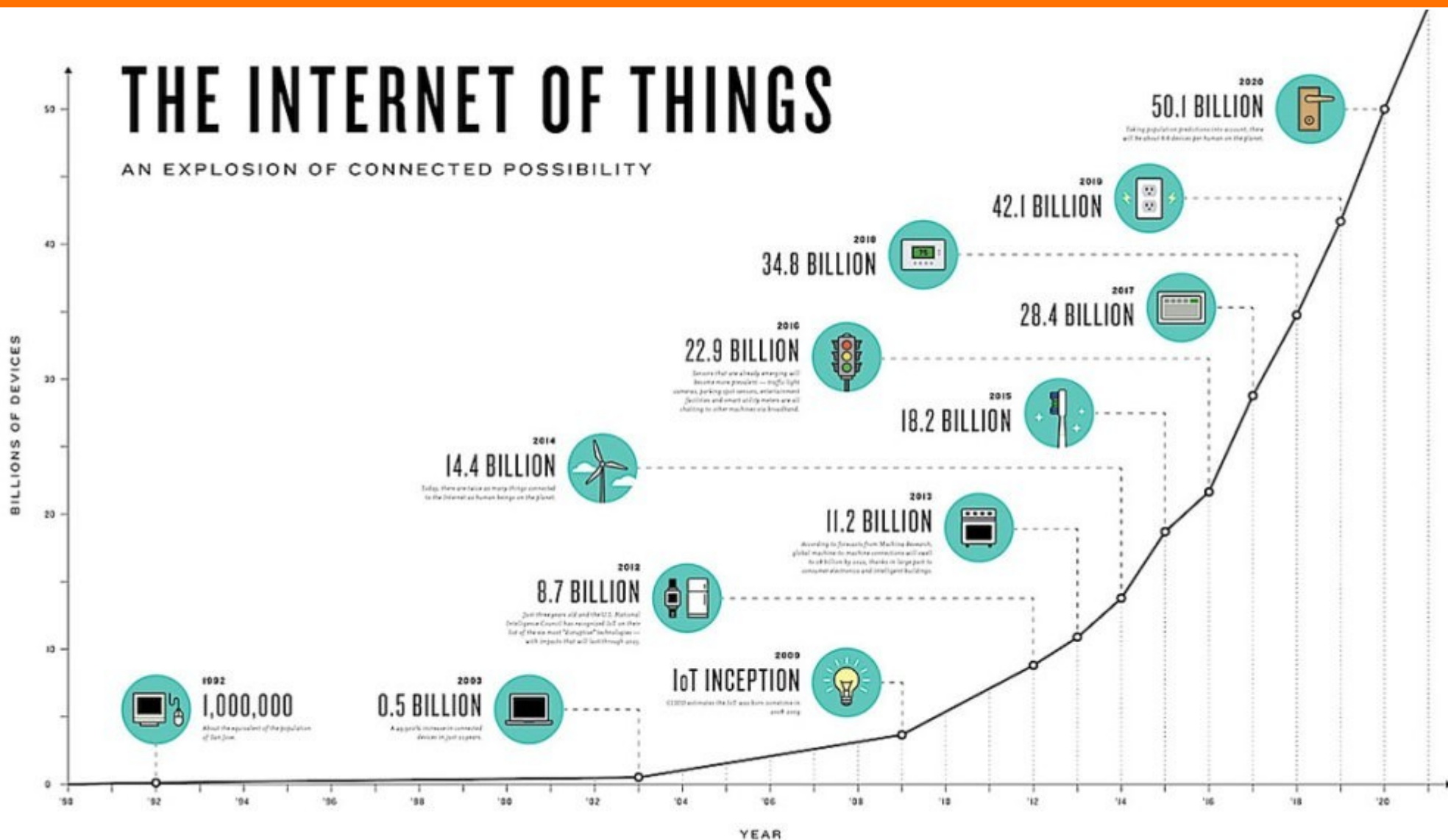
Introduzione a IoT

The **Internet of Things (IoT)** is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.^{[1][2][3]} Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

https://en.wikipedia.org/wiki/Internet_of_things



Crescita esponenziale..



<https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bfc>

Dispositivi..

Home & Building Automation

- Bringing intelligence, convenience and lifestyle



Smart Energy

- Adding power awareness to products and helping to save energy



Multimedia

- Wireless audio streaming and advanced remote controls



Security and Safety

- Improving remote control and home monitoring



Industrial M2M Communication

- Internet enhanced M2M communication using existing Wi-Fi infrastructure



https://theiotlearninginitiative.gitbooks.io/amazonwebservicesiot/content/iot_devices.html

Agenda

- Introduzione a IoT
- **IoT, IoE, IoM, M2M, IoS, CCS, ..**
- Utilizzi e utilizzatori
- IoT e sicurezza
- Come fare?
- Riferimenti
- Q&A

IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of Things

IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of Everything

IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of Machines

IoT, IoE, IoM, M2M, IoS, CCS, ..

Machine to Machine

IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of S..

IoT, IoE, IoM, M2M, IoS, CCS, ..

Servers?
Security?
Skynet?


IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of S it (@internetofs it) | Twitter - Mozilla Firefox

Internet of Shit (@int... x +

Twitter, Inc. (US) | https://twitter.com/internetofs it

Home About Search Twitter Have an account? Log in



Tweets 4,316 Following 157 Followers 265K Likes 3,293 Moments 2 Follow

Internet of S it
@internetofs it
whatever, put a chip in it. say hello:
internetofs it@gmail.com
In your stuff
facebook.com/internetofs it
Joined July 2015
1,051 Photos and videos

Tweets Tweets & replies Media

Internet of S it Retweeted

Casey Newton @CaseyNewton · Mar 7
I would never have guessed that a short-term problem with AI would be 'how do we get it to stop laughing at us'
18 389 1.0K
Show this thread

Internet of S it @internetofs it · Mar 7
You had literally one job: not make your home assistant laugh like an evil maniac

Techmeme @Techmeme
Amazon confirms some Alexa devices are randomly laughing and says it's working on a fix, after multiple users posted about it on social media (@shannon_liao / The Verge)

New to Twitter?
Sign up now to get your own personalized timeline!
Sign up

You may also like · Refresh

- SwiftOnSecurity** @SwiftOnSecurity
- briankrebs** @briankrebs
- Spectre Server** @sadserver



IoT, IoE, IoM, M2M, IoS, CCS, ..

The image shows a screenshot of a Twitter profile for 'Internet of Shit (@internetofshit)'. The profile header features a blue banner with the text 'Internet of' in large orange font. Below the banner, the profile name 'Internet of Shit' and handle '@internetofshit' are visible. The bio reads 'whatever, put a chip in it. say hello: internetofshit@gmail.com'. The profile statistics are: Tweets 4,316, Following 157, Followers 265K, Likes 3,293, and Moments 2. A 'Follow' button is present. The main content area shows a tweet from 'Internet of Shit' with a photo of a circuit board and the text 'You had literally one job: not make your home assistant laugh like an evil maniac'. Below this is a retweet from 'Techmeme' with the text 'Amazon confirms some Alexa devices are randomly laughing and says it's working on a fix, after multiple users posted about it on social media (@shannon_liao / The Verge)'. On the right side, there is a 'New to Twitter?' section with a 'Sign up' button and a 'You may also like' section with three suggested accounts: 'SwiftOnSecurity', 'briankrebs', and 'Spectre Server'. Large orange text 'Sh*t' is overlaid on the tweet area.



IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of things - Wikipedia - Mozilla Firefox

Internet of things - W... x +

https://en.wikipedia.org/wiki/Internet_of_things#Confusing_terminology 133% Search

Confusing terminology [\[edit \]](#)

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a "terminology zoo".^[196] The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user".^[196] A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics.^[196] According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and **technological convergence**: Internet of things, Internet of everything (IoE), industrial Internet, **pervasive computing**, pervasive sensing, **ubiquitous computing**, **cyber-physical systems** (CPS), **wireless sensor networks** (WSN), smart objects, cooperating objects, **machine to machine** (M2M), ambient intelligence (Aml), **Operational technology** (OT), and **information technology** (IT).^[196] Regarding IIoT, an industrial sub-field of IoT, the **Industrial Internet Consortium's** Vocabulary Task Group has created a "common and reusable vocabulary of terms"^[197] to ensure "consistent terminology"^{[197][198]} across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert^[199] to be notified when a new term is published. As of March 2017, this database aggregates 711 IoT-related terms,^[200] however, without any attempts to reduce terminological ambiguity and complexity.^[citation needed]

IoT adoption barriers [\[edit \]](#)

IoT, IoE, IoM, M2M, IoS, CCS, ..

Internet of things - Wikipedia - Mozilla Firefox

Internet of things - W... x +

https://en.wikipedia.org/wiki/Internet_of_things#Confusing_terminology 133% Search

Confusing terminology [edit]

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a "terminology zoo".^[196] The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user".^[196] A company operating in the IoT space could be working in anything related to sensor technology, networked embedded systems, or analytics.^[197] According to Lonergan, the term IoT was coined before smartphones, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of things, Internet of everything (IoE), industrial Internet, pervasive computing, pervasive sensing, ubiquitous computing, cyber-physical systems (CPS), wireless sensor networks (WSN), smart objects, cooperating objects, machine to machine (M2M), ambient intelligence (AMI), Operational technology (OT) and information technology (IT).^[196] Regarding IoT, the industrial sub-field, the Industrial Internet Consortium's Vocabulary Task Group has created a common and usable vocabulary of terms.^[197] To ensure consistent terminology,^[197] cross-publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert^[199] to be notified when a new term is published. As of March 2017, this database aggregates 711 IoT-related terms,^[200] however, without any attempts to reduce terminological ambiguity and complexity.^[citation needed]

IoT adoption barriers [edit]

Cosa Cavolo
Significano?

IoT: Dispositivi, computer, software

Oggetti e' il termine giusto.

Il vostro telefonino, il tablet, il computer, l'automobile, il televisore, la lavatrice ed il ferro da stiro non sono **dispositivi**, sono **oggetti di uso comune**, dei quali conosciamo la funzione, di cui siamo proprietari, che hanno spesso un'unica funzionalità e che usiamo quando opportuno per fare quello che desideriamo.

La soprastante affermazione e' divenuta **totalmente e tragicamente errata**; questa chiacchierata spera di fornirvene in maniera intuitiva la percezione; questa forse vi permettera' una meno pericolosa navigazione nell'infido oceano dell'**Internet delle Cose**.














(credits)

e-privacy XXI — Parole (ostili) contro la Rete - Mozilla Firefox

e-privacy XXI — Parole (... x +

e-privacy.winstonsmith.info/e-privacy-XXI.html

Chairman: [Marco Calamari](#), [Nabaztag](#) Progetto Winston Smith


Ora	Relatore	Titolo
14:30	Apertura lavori pomeridiani	
14:30	 Pasquale Annicchino (Lex Digital)	La sorveglianza delle minoranze religiose nell'era del terrorismo globale
14:55	  Giovambattista Vieri	Il giuoco nell'occhio
15:20	 Stefano Vignera (Bislab)	Industria 4.0, libertà del lavoratore e controllo della prestazione lavorativa
15:45	  Fabio Carletti	Cyberbullismo giovani e adulti in pericolo
16:10	   Diego Giorio (SEPEL Editrice)	Panem et circenses l'ha detto Zuckerberg?
16:35	   Marco Calamari e Igor Falcomata'	Internet of Thing: istruzioni per l'uso
17:00	Introduce e modera: Marco Calamari Partecipano:  Massimo Bozza , Fabio Carletti , Igor Falcomata' , Andrea Palumbo	Tavola Rotonda: Quali diritti con la IOT
18:00	Chiusura lavori	

Sabato 24 Giugno 2017 - mattina

Email address:

Donazione:

EUR

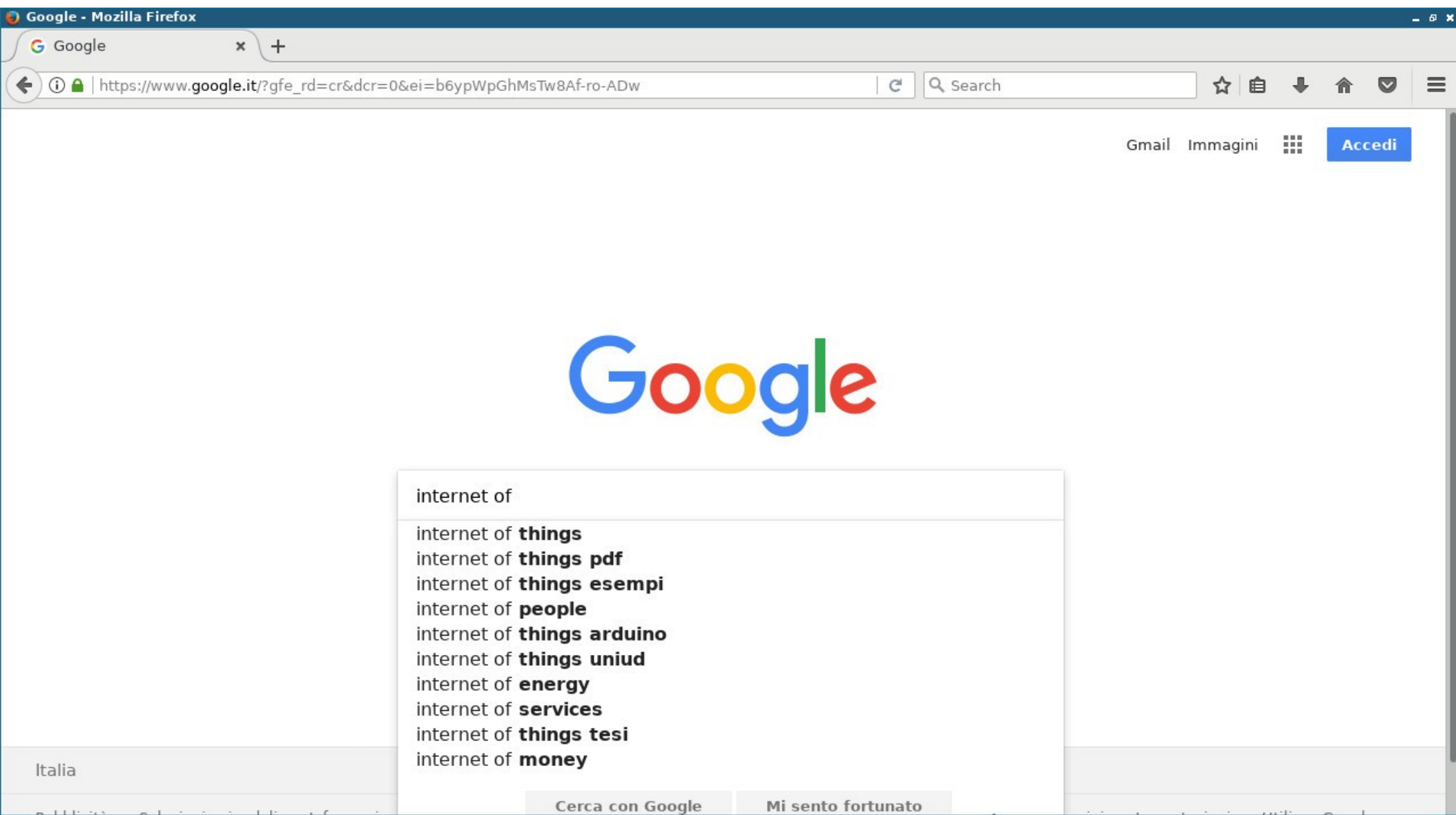


<http://e-privacy.winstonsmith.info/e-privacy-XXI.html>

Agenda

- Introduzione a IoT
- IoT, IoE, IoM, M2M, IoS, CCS, ..
- **Utilizzi e utilizzatori**
- IoT e sicurezza
- Come fare?
- Riferimenti
- Q&A

Utilizzi di IoT



Utilizzi di IoT

internet of things - Cerca con Google - Mozilla Firefox

internet of things - C... x +

https://www.google.it/search?dcr=0&source=hp&ei=b6ypWtGBOcWxsAGD2ovvDg&q=interr 120% Search

Google internet of things


Tutti Immagini Notizie Video Libri Altro Impostazioni Strumenti

Circa 37.900.000 risultati (0,57 secondi)

Articoli accademici per **internet of things**

- Internet of things** - Xia - Citato da 396
- Internet of things** - Kopetz - Citato da 239
- Internet of things** - Wortmann - Citato da 139

In telecomunicazioni **Internet** delle cose (o, più propriamente, **Internet** degli oggetti o **IoT**, acronimo dell'inglese **Internet of things**) è un neologismo riferito all'estensione di **Internet** al



Internet delle cose

Internet delle cose è un neologismo riferito all'estensione di Internet al mondo



Utilizzatori di IoT

- **Nessun utilizzo**
- **Utente / consumer (privato)**
- **Utente / consumer (business)**
- **Rivenditore / integratore**
- **Sviluppatore / vendor**

E il vostro rapporto con IoT?

Nessun utilizzo?!

- ~~Nessun utilizzo~~
- **utilizzo passivo e/o inconsapevole**

IoT è nella vostra automobile, nel vostro telefono, nella vostra TV, nel vostro router, nel vostro impianto d'allarme, nel vostro contatore, nel semaforo sotto casa, ...



Altri utilizzi?

- **vittima?!**

“internettizzazione” e
miniaturizzazione degli apparati di
tracciamento, spionaggio, law
enforcement, remote access, ..



Agenda

- Introduzione a IoT
- IoT, IoE, IoM, M2M, IoS, CCS, ..
- Utilizzi e utilizzatori
- **IoT e sicurezza**
- Come fare?
- Riferimenti
- Q&A

The **S** in IOT
stands for **Security**

Internet of Threats?

Internet of Things? More Like the Internet of Attack Vectors - Mozilla Firefox

File Edit View History Bookmarks Tools Help


www.infosecisland.com/blogview/23178-Internet-of-Things-More-Like-the-Internet-of-Attack-Vect

Front Page | Blog Posts | Resources | Media | Whitepapers | Visit SecurityWeek.com

Internet of Things? More Like the Internet of Attack Vectors

Wednesday, May 29, 2013

Contributed By:
Allan Pratt, MBA



Everyone is excited about the “Internet of Things,” also known as, IoT. Imagine, cars able to talk to other cars, devices able to contact repair facilities when repairs are needed, cars able to connect to the traffic grid, and refrigerators able to alert you when your milk or orange juice is running low.

According to Dr. Stefen Ferber of Bosch Software (@Stefferber on Twitter), “The Internet of Things is a place where technology and business meet, leading to the creation of new disruptive business models.”

But here’s how I see the situation. Cars may become mobile data-gathering devices. When an unsuspecting driver passes by, the attacker can grab your personal information including your name, address, vehicle identification number (VIN), and any other pertinent automotive information they can get away with in order to steal your identity.

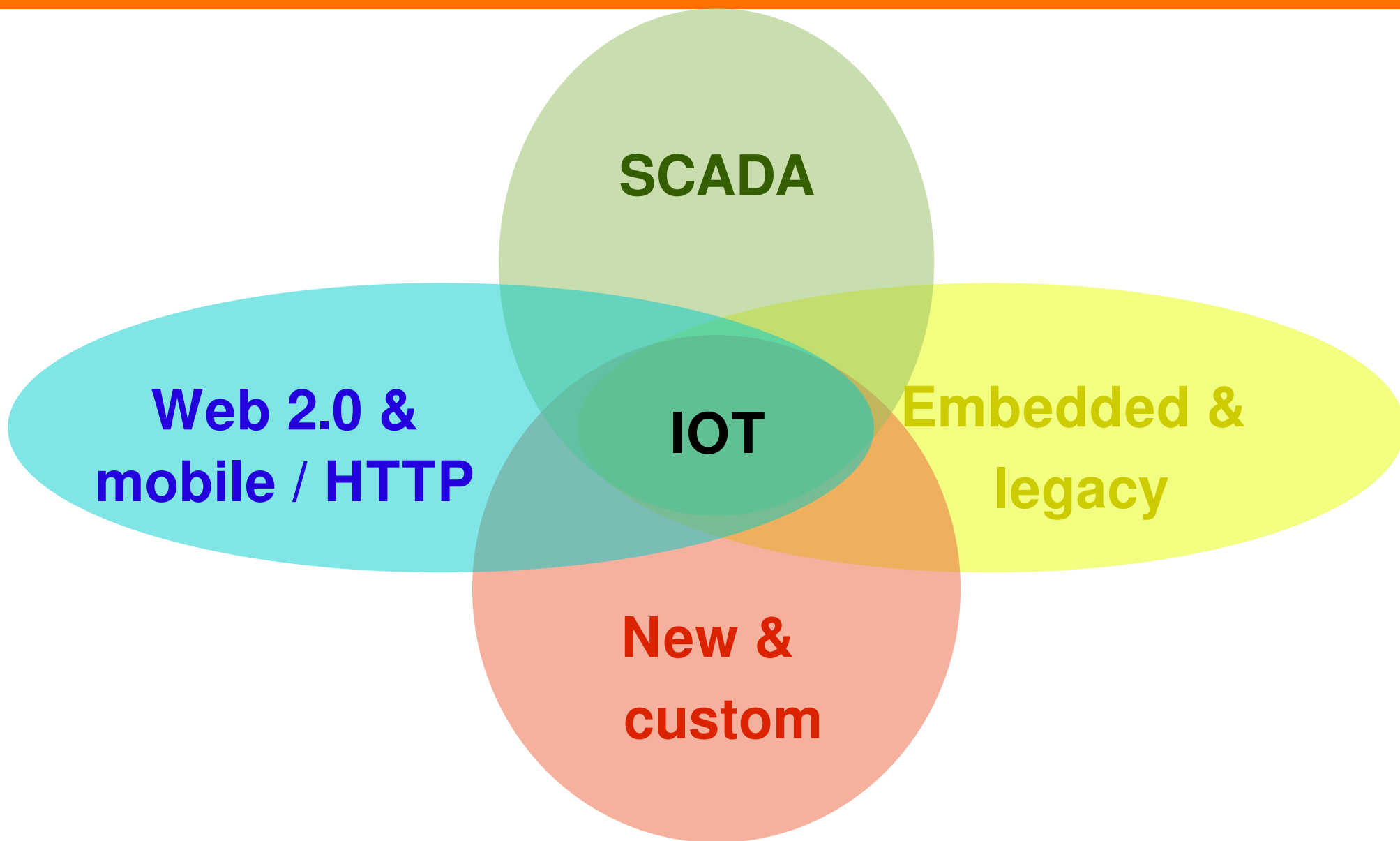
Consider this scenario: a fast driver could have his or her vehicle connect with the traffic grid, so that whenever his or her car approaches an intersection, the light immediately turns green.

Since your home and devices will be able to communicate, an unscrupulous repair person could discover your home

<http://www.infosecisland.com/blogview/23178-Internet-of-Things-More-Like-the-Internet-of-Attack-Vectors.html>



Tecnologia



SCADA?!

ma non sono quei grossi “così” che si usano negli impianti industriali? Che c’entrano con IoT?

Ci sono ovviamente differenze tra SCADA, IIOT, IOT, .. ma anche molte analogie.

1. Complessità (vs TTM)

Quanto software ?

- Nel 1969 siamo andati sulla Luna con meno di 10.000 linee di software, e per lo Shuttle negli anni '90 ne sono bastate 400.000.
- Un pacemaker ci salva la vita con 100.000 linee, tante quante ne aveva Photoshop 1.0 che oggi e' cresciuto a 3.500.000.
- Nel 1971 la prima versione di Unix aveva 10.000 linee, mentre Debian 5.0 (Lenny) nel 2009 ne aveva 65.000.000 (incluse le applicazioni disponibili).
- Nel 1991 Windows 3.1 contava 2.000.000 di linee, nel 2001 Windows XP 43.000.000
- Un "vecchio" caccia supersonico F22 "Raptor" si contentava di 2.000.000, mentre un aereo da trasporto Boeing 787 ne vuole 9.000.000 ed il famigerato F35 45.000.000

1. Complessità (vs TTM)



Fiat 500.

Dal 1960 ad ora: da zero a 50.000.000 di linee

1. Complessità (vs TTM)

- **K o M linee di codice**
- **oggetti “poco costosi” / ciclo di vita**
- **Time to Market / startup / outsourcing**
- **spesso in C (memory mangling, ..)**

**che cosa mai potrà
andare storto?**

1. Complessità (vs TTM)

Quindi il problema e' "troppo software"?

No, il problema e' anche che **il software degli oggetti IoT ~~fa schifo~~ e' di cattiva qualita'**, e viene prodotto in questo modo non per cattiveria, ma a causa del **modello di business degli oggetti IoT**.

Gli oggetti contenenti software non lo rivelano direttamente, e quindi **il software di per se non e' un "valore"**; rimpiazzarli con un nuovo modello e' sempre il desiderio primario di ogni produttore.

Pensate ancora che il software contenuto nel tipico oggetto IoT (ma anche nel vostro router ADSL) sia accuratamente sviluppato ed amorevolmente testato?

Pensate davvero che per il vostro braccialetto fitness, la vostra telecamera sorvegliabambini od il **Furby** incautamente regalato a vostro figlio usciranno le patch?

Pensate infine che i vostro oggetti IoT ed il vostro impianto di domotica non finiranno listati su **Shodan**?

2. Hardware / OS (micro)

- **No memory protection (flat MM)**
- **No DEP/NX/XN/..**
- **No CPU mode / Protection ring**
- **spesso in C (memory mangling, ..)**

**che cosa mai potrà
andare storto?**

2. Hardware / OS (embedded)

- **Tecnologie anti-exploiting carenti o assenti**
- **Tecniche attacco “comuni”**
- **Protezione carente/assente comunicazioni di rete**
- **Interfacce/API web based**

che cosa mai ..



Tecniche anti-exploiting?

Easy Feature Comparison | HardenedBSD - Mozilla Firefox

Easy Feature Compar... x +

https://hardenedbsd.org/content/easy-feature-comparison

Feature	HardenedBSD	FreeBSD	OpenBSD	NetBSD
Address Space Layout Randomization (ASLR)	<input checked="" type="checkbox"/>	<input type="checkbox"/> *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Base compiled as Position-Independent Executables (PIEs)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Base compiled with RELRO + BIND_NOW	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> *
Ports tree compiled with PIE, RELRO, and BIND_NOW	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Static PIE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ASLR brute force protection (SEGVGUARD)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> *
Prevention of the creation of writable and executable memory mappings (W^X part one)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> *
Restrictions on mprotect to prevent switching pages between writable and executable (W^X part two)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> *
sysctl hardening	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network stack hardening (IP ID randomization, use IPv6 temporary addresses)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Executable file integrity enforcement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Boot hardening	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
procfs/linprocfs hardening	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>
LibreSSL in base as the default cryptography library	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SROP mitigation	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Most of base sandboxed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Trusted Path Execution	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Donate

BTC:
1FmbSRvZK4yC1b6aj
eZWSvYXV2nmvwdWQq

BCH:
1PbGHPPmdNqSmh4L
3SbvPdaPzSL9kZ5H6f

ETH:
0x9Ea8E44736AC8Ed
806ef57f7F174a14D93689775

**2018 Sprint 1
Donation Status**

We've raised \$1437.00
out of \$10,500 USD.

Navigation

- [Home](#)
- [About HardenedBSD](#)
- [Stable Builds](#)
- [Packages](#)

2018 Sprint 1 Donation Status

We've raised \$1437.00 out of \$10,500 USD.

Navigation

- Home
- About HardenedBSD
- Stable Builds
- Packages

<https://hardenedbsd.org/content/easy-feature-comparison>



OS IoT più diffuso?

The kernel of the argument over Linux's vulnerabilities | The Washington Post - Mozilla Firefox

tp The kernel of the arg... x +

www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument/?utm


Search

Sections **The Washington Post** Share Net of Insecurity

NET OF INSECURITY

THE KERNEL OF THE ARGUMENT

Fast, flexible and free, Linux is taking over the online world. But there is growing unease about security weaknesses.



<http://www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument>

IOT: utile di sicuro. Ma sicuro? - Hack The Tower – 19 giugno 2020



3. Aggiornamenti

Internet of (billion of)
Things (to patch)

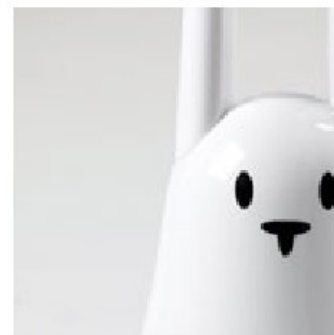
3. Aggiornamenti

- **Dispositivi non aggiornabili**
- **o solo “on-site”**
- **o solo “manualmente”**
- **aggiornamenti non rilasciati**

Buon lavoro..

Case study: nabaztag

Համառոտ պատմություն: Կարելի Բաներ - 4



2005: Nasce **Nabaztag**

e' la traslitterazione dall'armeno "նապաստակ" di "coniglio"; creato da **Rafi Haladjian** e **Olivier Mével**.

Prodotto complessivamente in oltre 100.000 esemplari dalla compagnia francese **Violet**, poi fallita ed incorporata da **Mindscape**, poi chiusa ed i cui asset sono stati acquistati da **Aldebaran Robotics** e dimenticati.

Il mio coniglio e' l'unica cosa informatica che in 30 anni di convivenza mi abbia fatto fare bella figura e guadagnare punti con la mia compagna.

Motto: "*if you can even connect rabbits, then you can connect anything*" (credit: @inakivazquez)

Case study: nabaztag

Breve storia: fatti importanti – 4



Ha un pulsante sulla testa, due orecchie mosse da motorini passo-passo e con encoder per rilevarne la posizione, 4 LED multicolori, un lettore RFID, una scheda audio con microfono ed una scheda WiFi.

E' controllato da un server remoto su cui si possono caricare plugin ed azioni. Puo' muovere le orecchie e fare coreografie con i LED, leggervi oroscopi e quotazioni azionarie.

Si possono "Sposare" due conigli, in modo che se si muovono le orecchie ad uno, l'altro si mette a suonare e lampeggiare, e le muove nello stesso modo. Non banale spiegarlo ad un cliente in ufficio!

Case study: nabaztag

Nabaztag: network protocol

Nabaztag:tag (v2) + OpenJabNab

Due to lack of documentation, the network protocol was sniffed & partially reverse engineered.

All client/server communications use the XMPP Jabber protocol (TLS encrypted).

However, when blob need to be transferred, Base64 encoded objects are transferred using HTTP cleartext protocol.

Because the lack of client side computing power, when a text message need to be read by the rabbit, is sent to the server that rasterize it in a MP3 file, then transferred during the XMPP session using plain HTTP.



http://www.cassandracrossing.org/documents/sha2017_calamari_an_autopsy_in_iot_nabaztag_the_hare.pdf

Case study: nabaztag

Nabaztag: network protocol

Nabaztag:tag (v2) + Openjabber
TLS sì,

Due to lack of documentation, the network protocol was sniffed & partially reverse engineered.

ma soggetto a MITM

All client/server communications use the XMPP (a Jabber protocol) (TLS encrypted).

(non verifica cert)

However, when blob need to be transferred, Base64 encoded objects are transferred using HTTP cleartext protocol.

Because the lack of client side computing power, when a text message need to be read, the application is sent to the server that rasterize it in a Mp3 file, then transferred during the XMPP session using plain HTTP.



XMPP

Case study: nabaztag

Nabaztag: simple attack - 2

`Nabaztag:tag (v2) + OpenJabNab`

The content of server rendered MP3 file was easily readable in the HTTP stream.



Using `ARPspoofer` to poisoning again the router, `Iptables` to mount a local MITM, and `BURPsniffer proxy`, a setup was prepared to intercept the server -> client communication side, and to replace the HTTP object containing the rasterized MP3 with a different one.

That way, the bunny is served with a modified MP3 saying *"I'm possessed, to have me back pay a Bitcoin"*

The session was repeated, and the rabbit give a quite different "Hello" to his master.

Case study: nabaztag

- **Traffico (comandi) cifrato senza verifica dei certificati**
- **Traffico (contenuti) in chiaro**
- **Utilizzo di risorse in cloud (storage/cpu limitati)**
- **“Orfano” (prodotto abbandonato)**



Design del 2005..

..siamo nel 2020..

..come siamo messi?

Welcome > Blog Home > Hacks > IoT Insecurity: Pinpointing the Problems

IoT INSECURITY: PINPOINTING THE PROBLEMS

by **Tom Spring** July 21, 2016 , 7:00 am

Internet Connected and Insecure

The IoT fridge threat is not theoretical. In fact, it was last year when researchers uncovered a flaw in Samsung's RF28HME1RSP smart fridge that attackers could exploit.

threatpost
We value your feedback
Help us exceed your expectations...
TAKE OUR BRIEF SURVEY

Top Stories

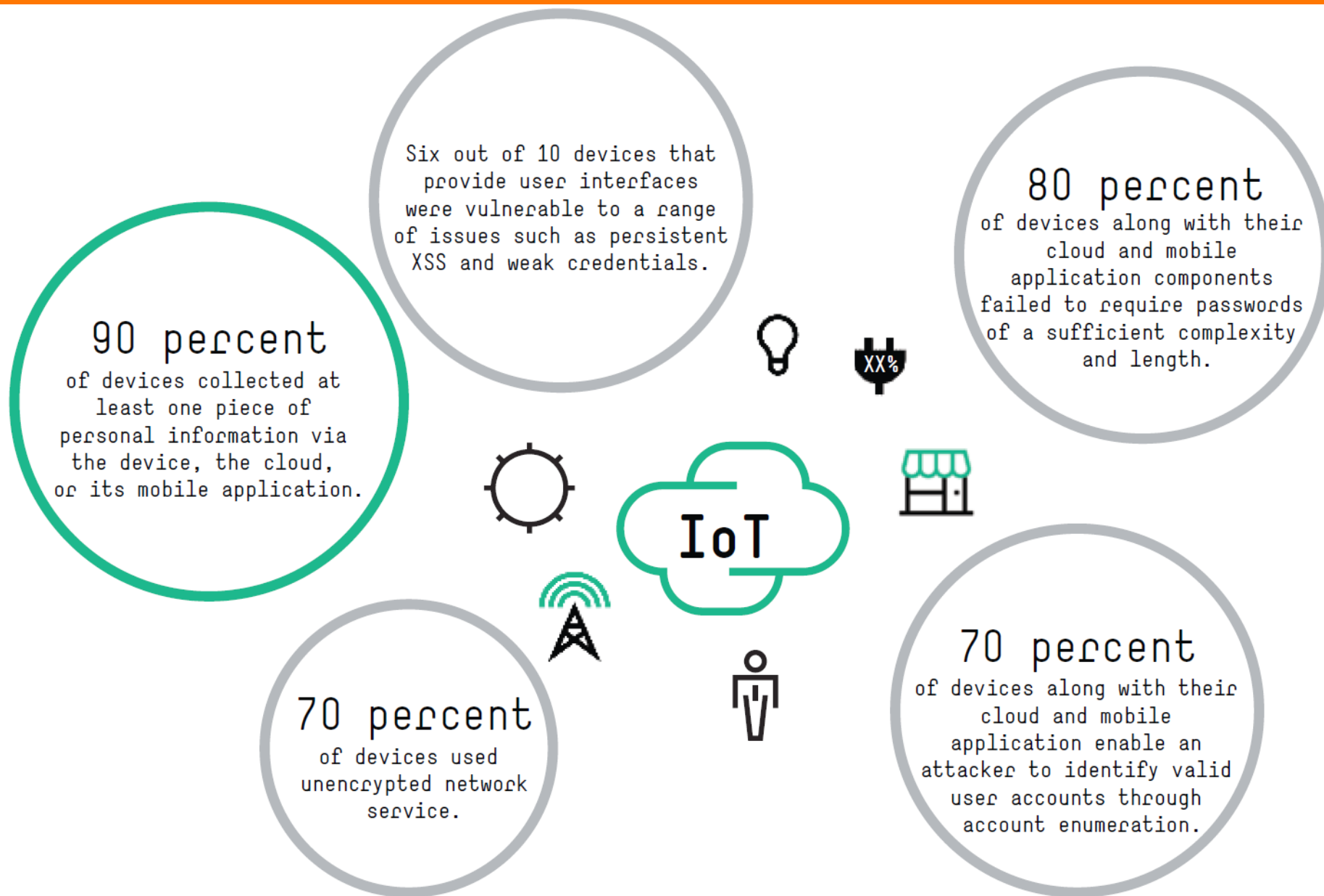
AMD Investigating Reports of 13 Critical Vulnerabilities Found in Ryzen, EPYC Chips
March 13, 2018 , 4:04 pm

Lookout: Dark Caracal Points To APT Actors Moving To Mobile Targets
March 8, 2018 , 11:59 am

<https://threatpost.com/iot-insecurity-pinpointing-the-problems/119389/2/>



(o almeno nel 2016)



Chiudete Internet..

INTERNET OF DILDOS: A LONG WAY TO A VIBRANT FUTURE - FROM IOT TO IOD - Mozilla Firefox

INTERNET OF DILDOS: A ... x +

www.securitynewspaper.com/2018/02/03/internet-dildos-long-way-vibrant-future-iot-iod/ 120% Search

Vibratissimo Panty Buster product, Image source: vibratissimo.com

VULNERABILITIES

The following vulnerabilities, describe issues in the iOS/Android application and the corresponding backend as well as hardware related issues.

1. Customer Database Credential Disclosure
2. Exposed administrative interfaces on the internet
3. Cleartext Storage of Passwords
4. Unauthenticated Bluetooth LE Connections
5. Insufficient Authentication Mechanism
6. Insecure Direct Object Reference
7. Missing Authentication in Remote Control
8. Reflected Cross-Site Scripting

1) CUSTOMER DATABASE CREDENTIAL DISCLOSURE

In the webroot of the host vibratissimo.com a .DS_STORE file was found. Those files are always a

<http://www.securitynewspaper.com/2018/02/03/internet-dildos-long-way-vibrant-future-iot-iod/>

Case study: IP Cam

Rai 3 HD



VOGLIO PIANGERE

di GIULIANO MARRUCCI

REPORT

<http://www.report.rai.it/dl/Report/puntata/ContentItem-7907d06c-adcf-4f60-8edd-90aca383e535.html>

IOT: utile di sicuro. Ma sicuro? - Hack The Tower – 19 giugno 2020



Case study: IP Cam

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# telnet 217.133. 81  
Trying 217.133. ...  
Connected to 217.133. .  
Escape character is '^]'.  
GET login.cgi HTTP/1.0  
  
HTTP/1.1 200 OK  
Date: Tue May 9 21:54:56 2017  
Server: GoAhead-Webs  
Last-modified: Thu Jan 1 00:00:00 1970  
Content-type: text/html  
Cache-Control: no-cache  
Content-length: 66  
Connection: close  
  
var loginuser="report";  
var loginpass="rai3";  
  
var pri=255;  
  
Connection closed by foreign host.  
root@kali:~#
```

Case study: IP Cam

Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server - IT Security Research by Pierre - Mozilla Firefox

Multiple vulnerabilities f... x +

https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

IT Security Research by Pierre


[Home](#) • [About](#) • [Feed](#)

Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server

TL;DR: by analysing the security of a camera, I found a pre-auth RCE as root against 1250 camera models. Shodan lists 185 000 vulnerable cameras. The "Cloud" protocol establishes clear-text UDP tunnels (in order to bypass NAT and firewalls) between an attacker and cameras by using only the serial number of the targeted camera. Then, the attacker can automatically bruteforce the credentials of cameras.

Product Description

The Wireless IP Camera (P2P) WIFICAM is a Chinese web camera which allows to stream remotely.



<https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html>



Case study: IP Cam

- **Decine di prodotti “diversi”** (derivati dallo stesso firmware/produttore)
- **UPnP**
- **Credenziali default (Mirai) [*]**
- **Auth bypass noto dal 2004**
- **Traffico cloud in chiaro**
- **No aggiornamenti (firmware) [**]**



to the internet while they enjoy a cheeky pint.

As the gallery of snapshots shows below, every facet of our lives can be recorded for the viewing of the Internet at large. *(Faces and identifiable markers have been blurred by ZDNet to protect identities.)*

The most shocking of Shodan

SEE FULL GALLERY



1 - 5 of 9

NEXT >

But why does this happen?

Shodan scours the Web for devices which use Real Time Streaming Protocol (RTSP port 554) which are left open without basic password protection -- or only the default password settings -- in place. Luckily for those with vulnerable webcams, Shodan trawls the web for open feeds but only takes a snapshot before moving on.

build a chain of trust

White Papers from IBM

READ NOW

The State of Container-Based App Development

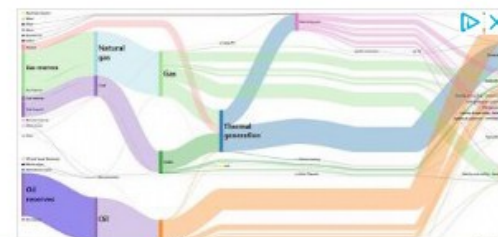
White Papers from IBM

READ NOW

The dZone Guide to Microservices: Breaking Down the Monolith

White Papers from IBM

READ NOW



http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/



OWASP IoT Attack Surface Areas

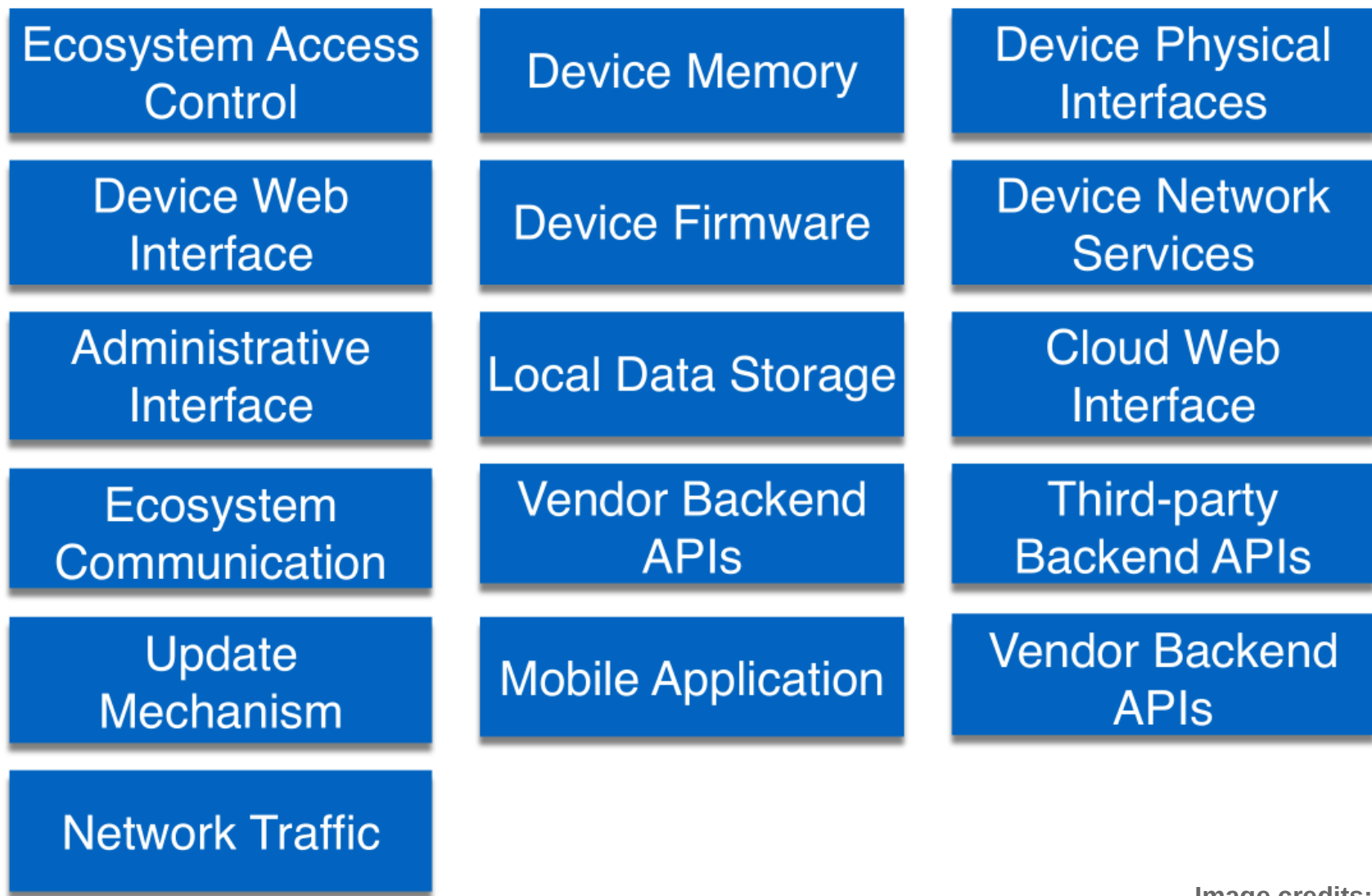


Image credits: Dan Miessler

<https://hackaday.com/2016/06/13/iot-security-is-an-empty-buzzword/>

Agenda

- Introduzione a IoT
- IoT, IoE, IoM, M2M, IoS, CCS, ..
- Utilizzi e utilizzatori
- IoT e sicurezza
- **Come fare?**
- Riferimenti
- Q&A

Come fare?

- **Awareness: I stands for Internet**
- **Security** by Design
- **Privacy** by Design
- **Secure** SDLC
- **Usare piattaforme, framework e protocolli standard e sicuri**
- **Security review / PT**

Agenda

- Introduzione a IoT
- IoT, IoE, IoM, M2M, IoS, CCS, ..
- Utilizzi e utilizzatori
- IoT e sicurezza
- Come fare?
- **Riferimenti**
- **Q&A**

Riferimenti

OWASP Internet of Things Project

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

CIS Critical Security Controls

<https://www.sans.org/critical-security-controls>

NIST Cybersecurity for IoT Program

<https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>

IoT Security Foundation

<https://www.iotsecurityfoundation.org/>

GOV.UK - Secure by Design

<https://www.gov.uk/government/publications/secure-by-design>

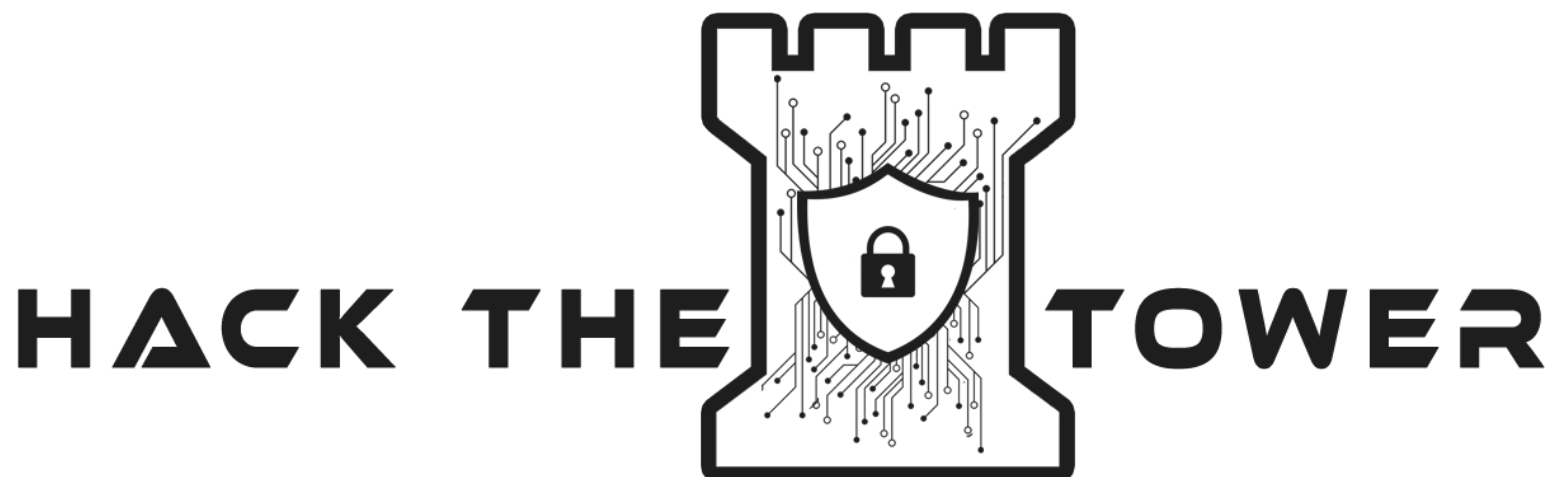
Shodan - The search engine for Security ..

<https://www.shodan.io/>

Thinkst ConCollector (ricerca slid, econferenze di sicurezza informatica)

<http://cc.thinkst.com/> (es. “zigbee”)

IoT: utile di sicuro. Ma sicuro?



Domande?

(grazie dell'attenzione)

Relatore:



Igor Falcomatà, CEO
ifalcomata@enforcer.it



<https://creativecommons.org/licenses/by-nc/4.0/>