IoT: utile di sicuro. Ma sicuro?

HACK THE TOWER

Relatore:

19 giugno 2020

easynet group

enforcer SECURITY

Igor Falcomatà, CEO
ifalcomata@enforcer.it

$ whoami

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

free advertising >

Agenda

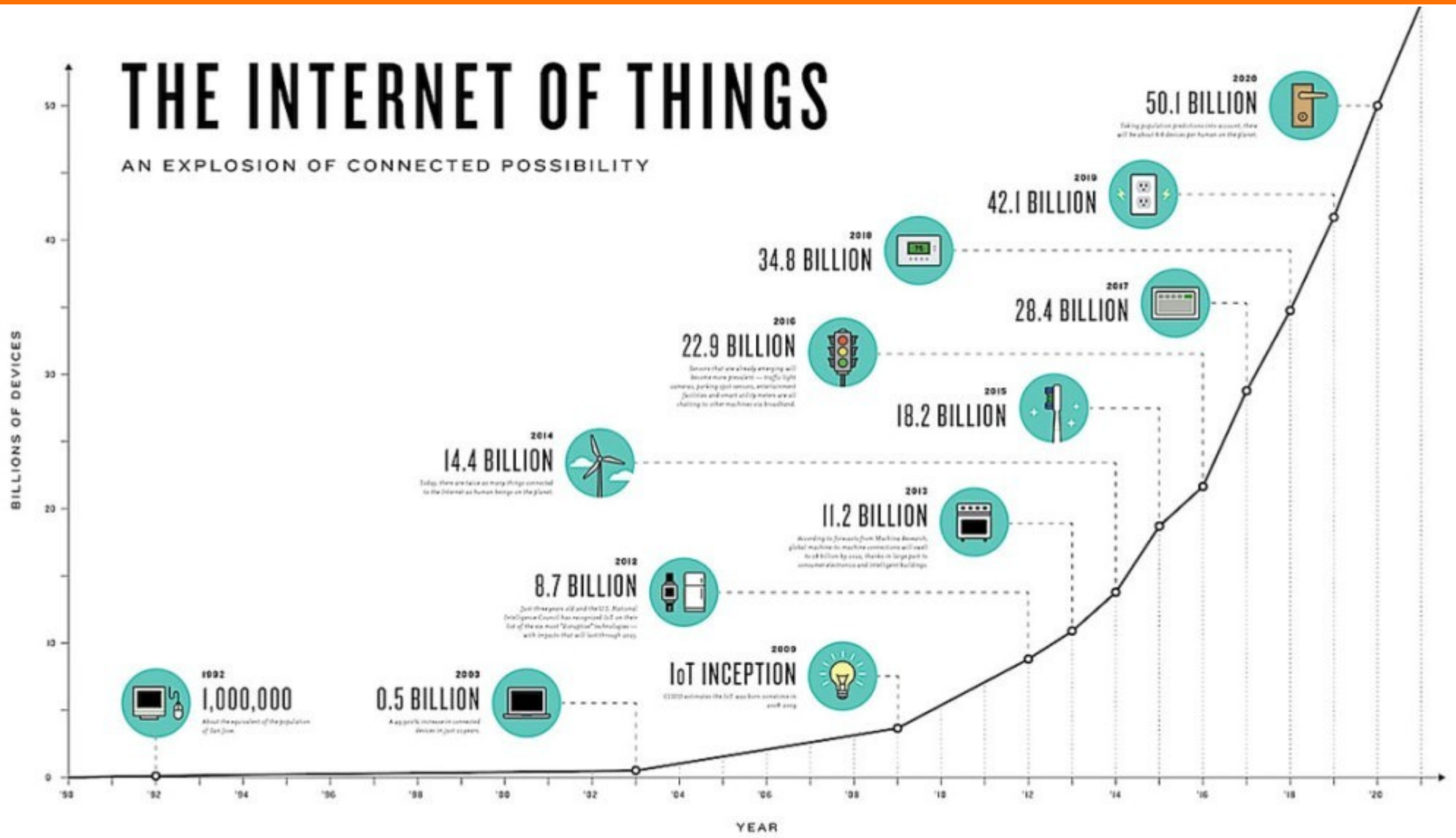
- Introduzione a IoT
- IoT, IoE, IoM, M2M, IoS, CCS, ..
- Utilizzi e utilizzatori
- IoT e sicurezza
- Come fare?
- Riferimenti
- Q&A

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-2017-2023-175f845c2bcf

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



2

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...

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

Search

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

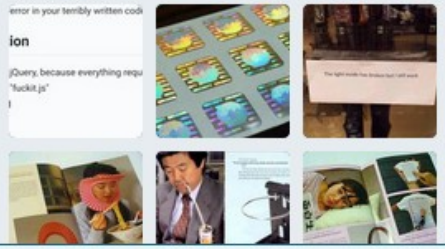
whatever, put a chip in it. say hello: internetofs it@gmail.com

In your stuff

facebook.com/internetofs t

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

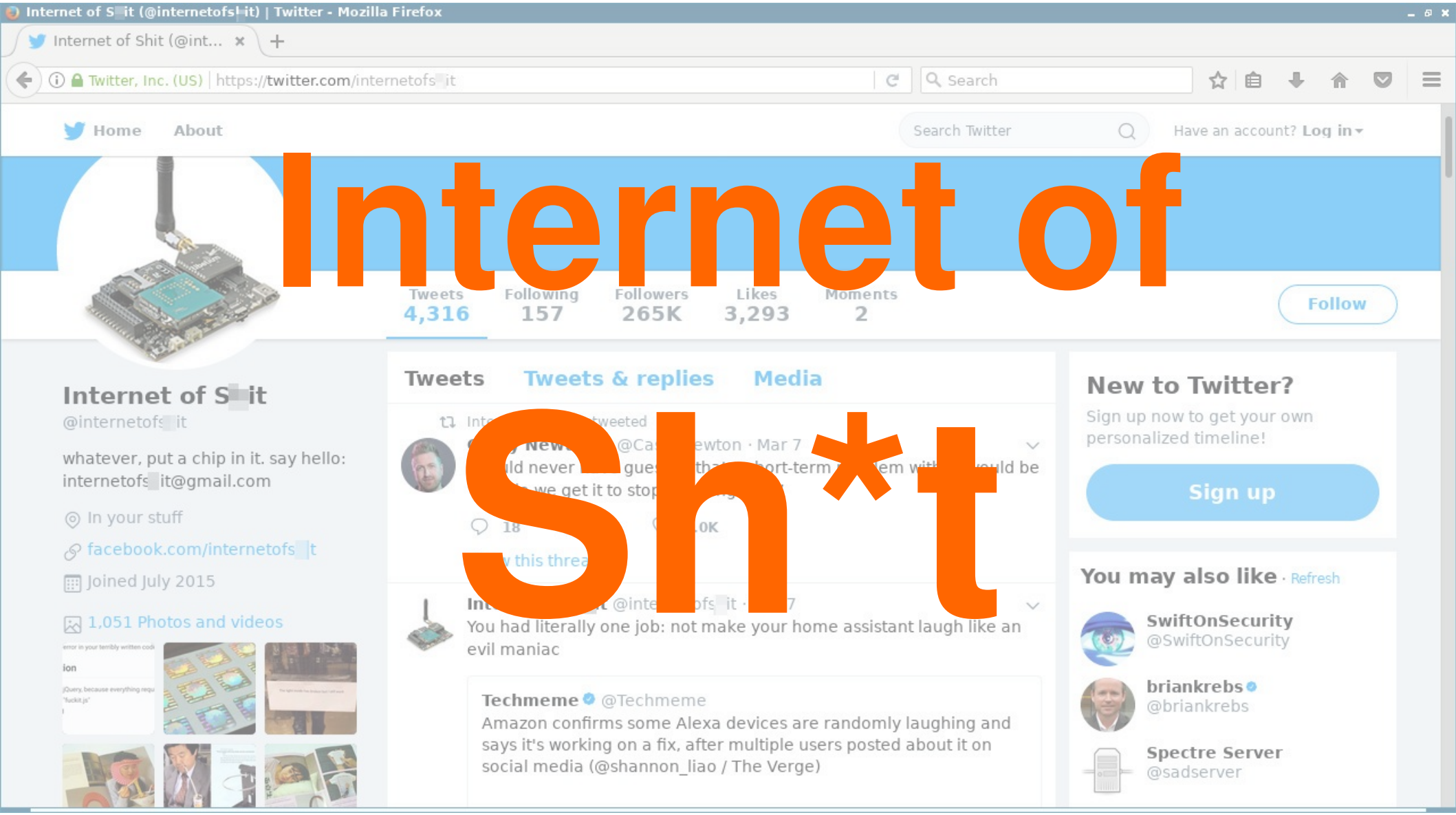
You may also like · Refresh

SwiftOnSecurity @SwiftOnSecurity

briankrebs @briankrebs

Spectre Server @sadserver

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



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

Internet of things - Wikipedia - Mozilla Firefox

Internet of things - W...

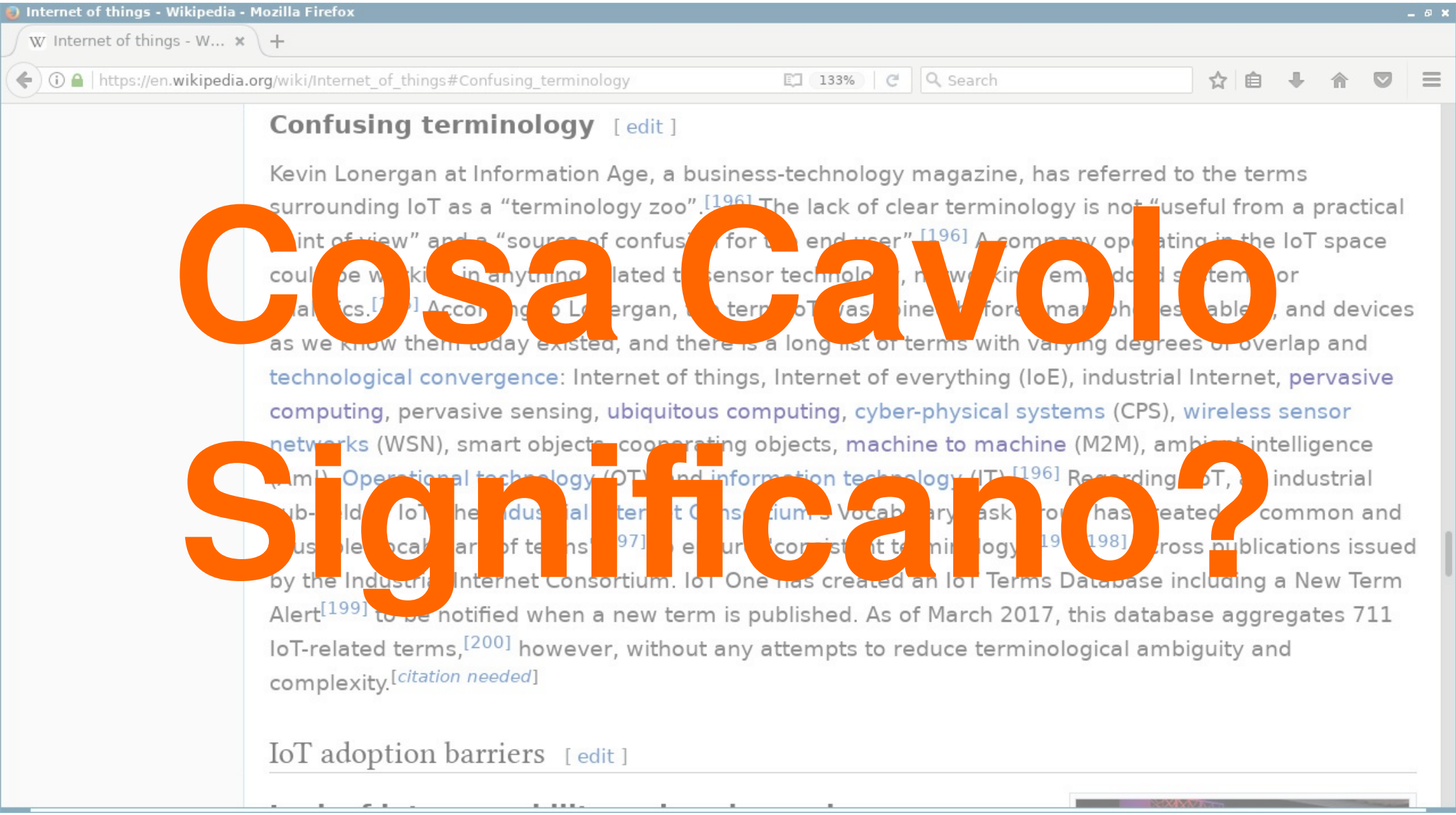
https://en.wikipedia.org/wiki/Internet_of_things#Confusing_terminology 133% Search

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 (AmI), 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, ..



Cosa Cavolo Significano?

CCS?

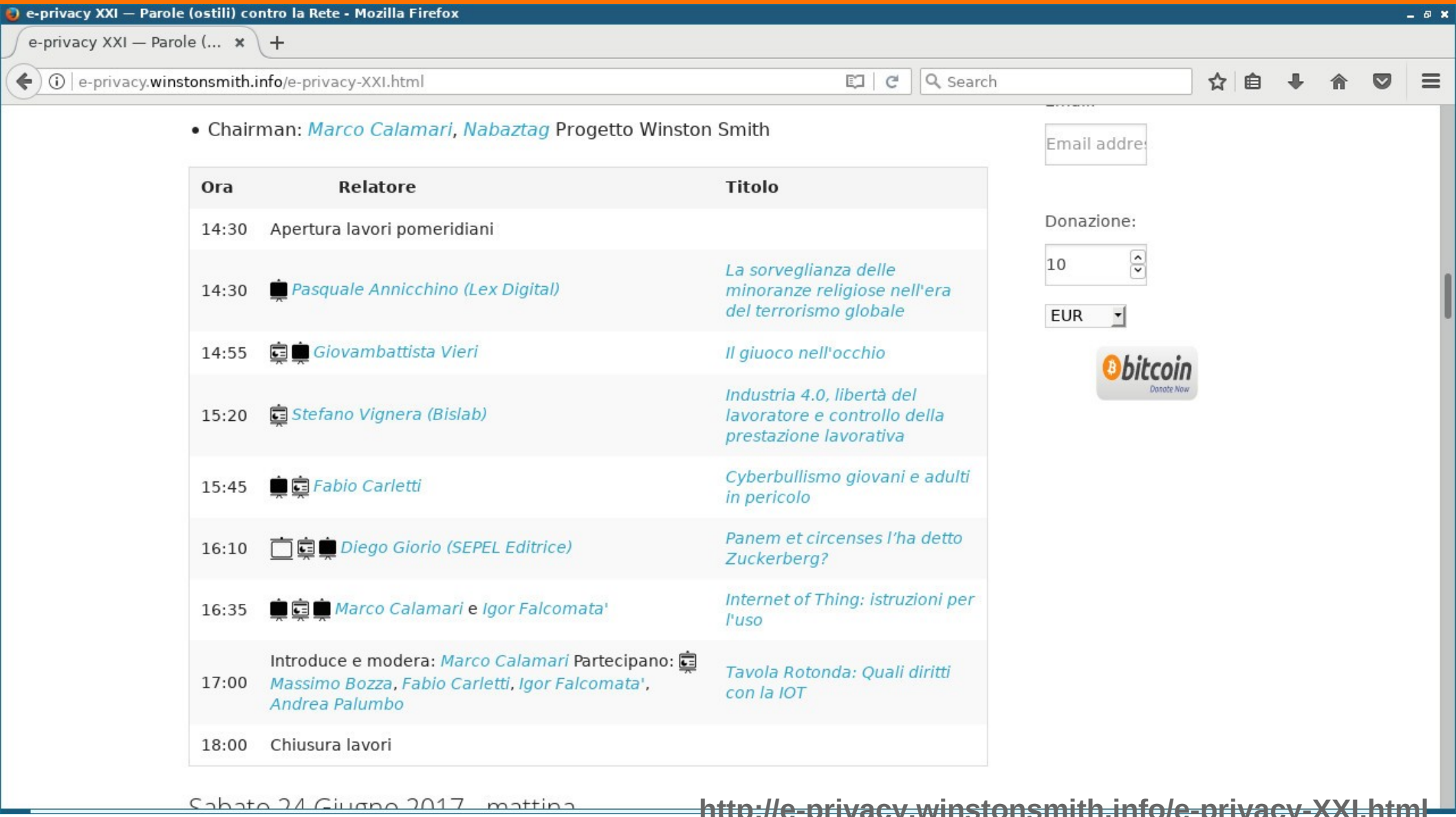
IoT: Dispositivi, computer, software ....

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 funzionalita' 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)

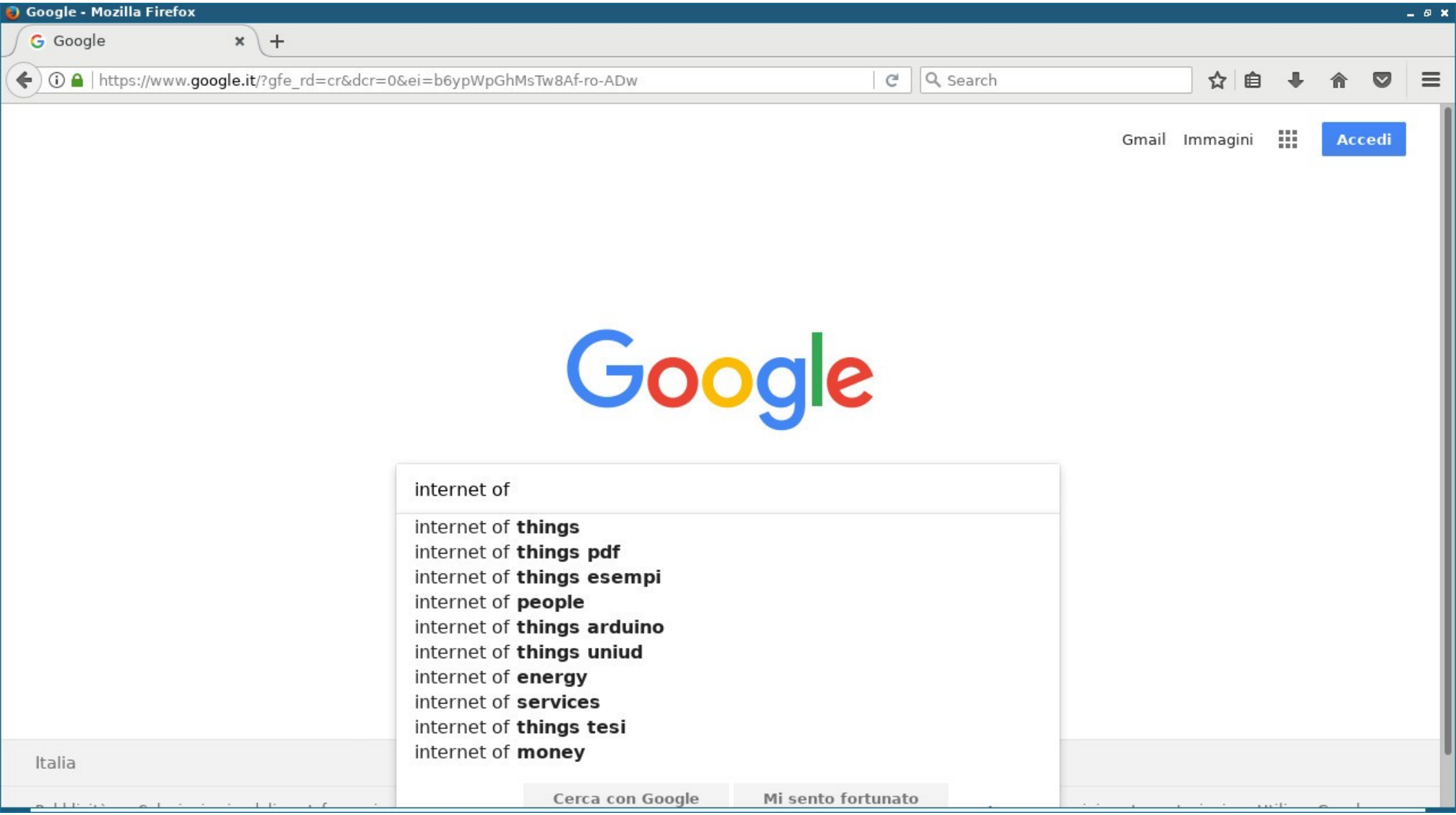


http://e-privacy.winstonsmith.info/e-privacy-XXI.html

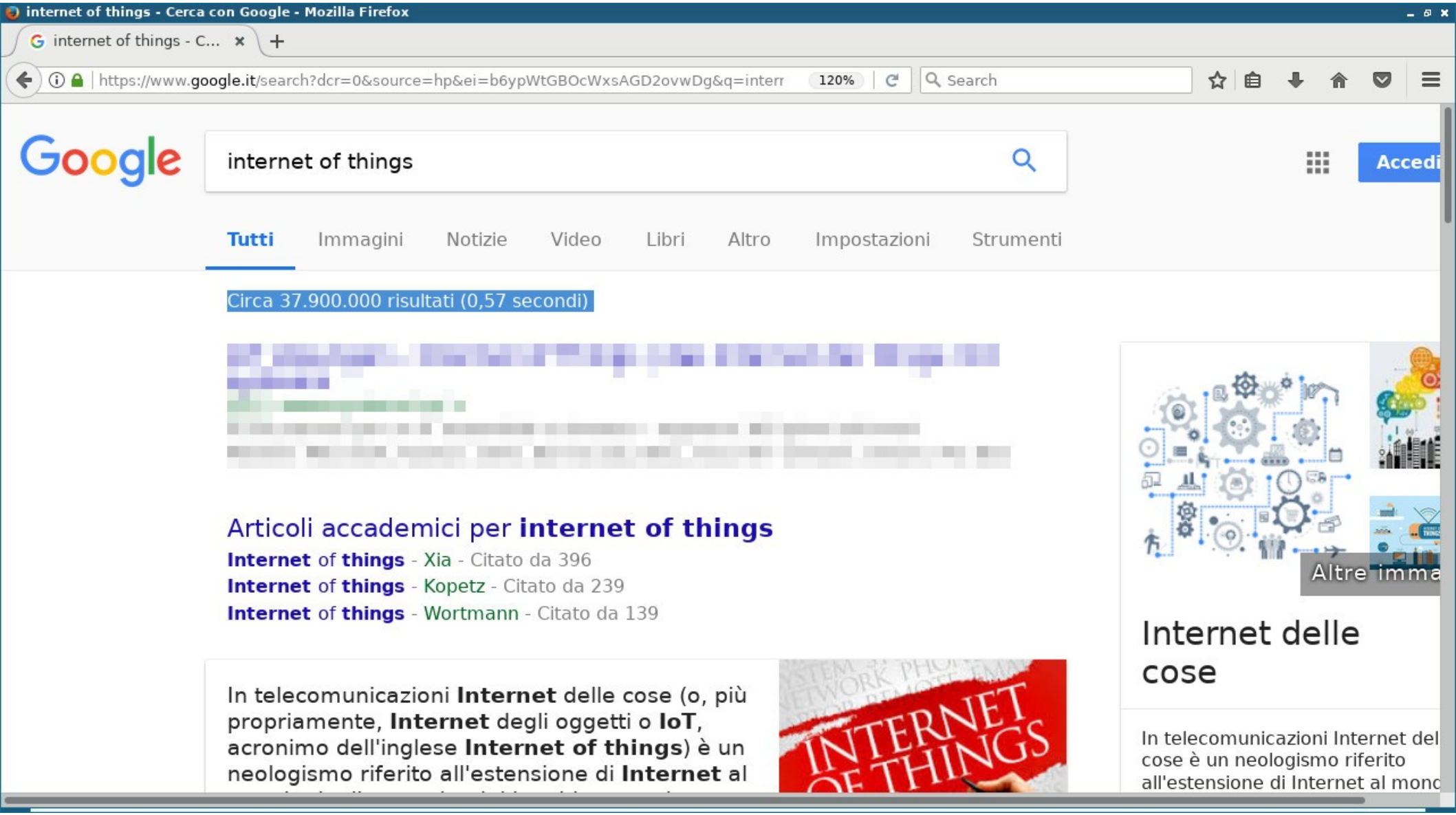
Agenda

- 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



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?!**

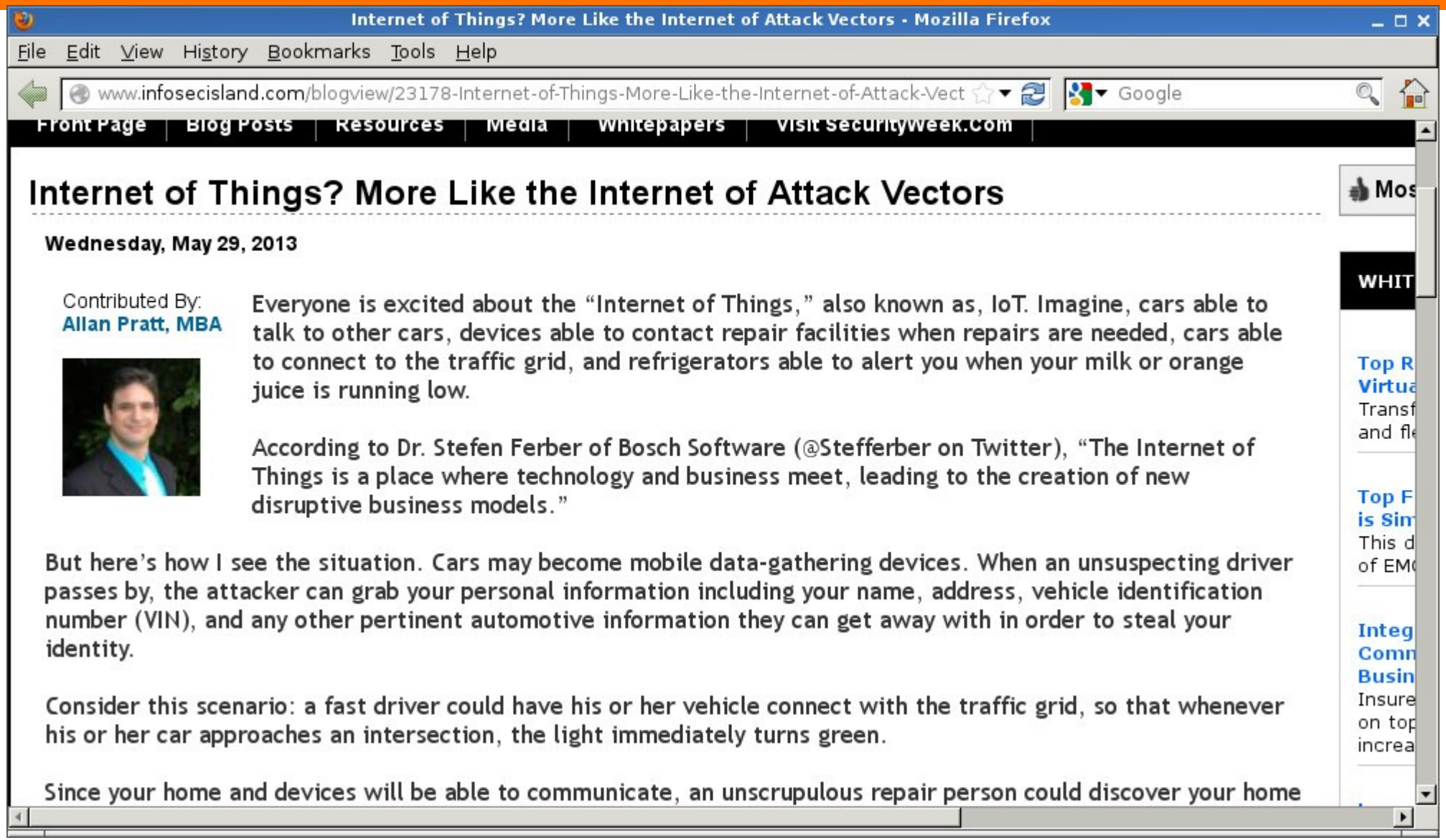
“internettizzazione” e miniaturizzazione degli apparati di tracciamento, spionaggio, law enforcement, remote access, ..

Agenda

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

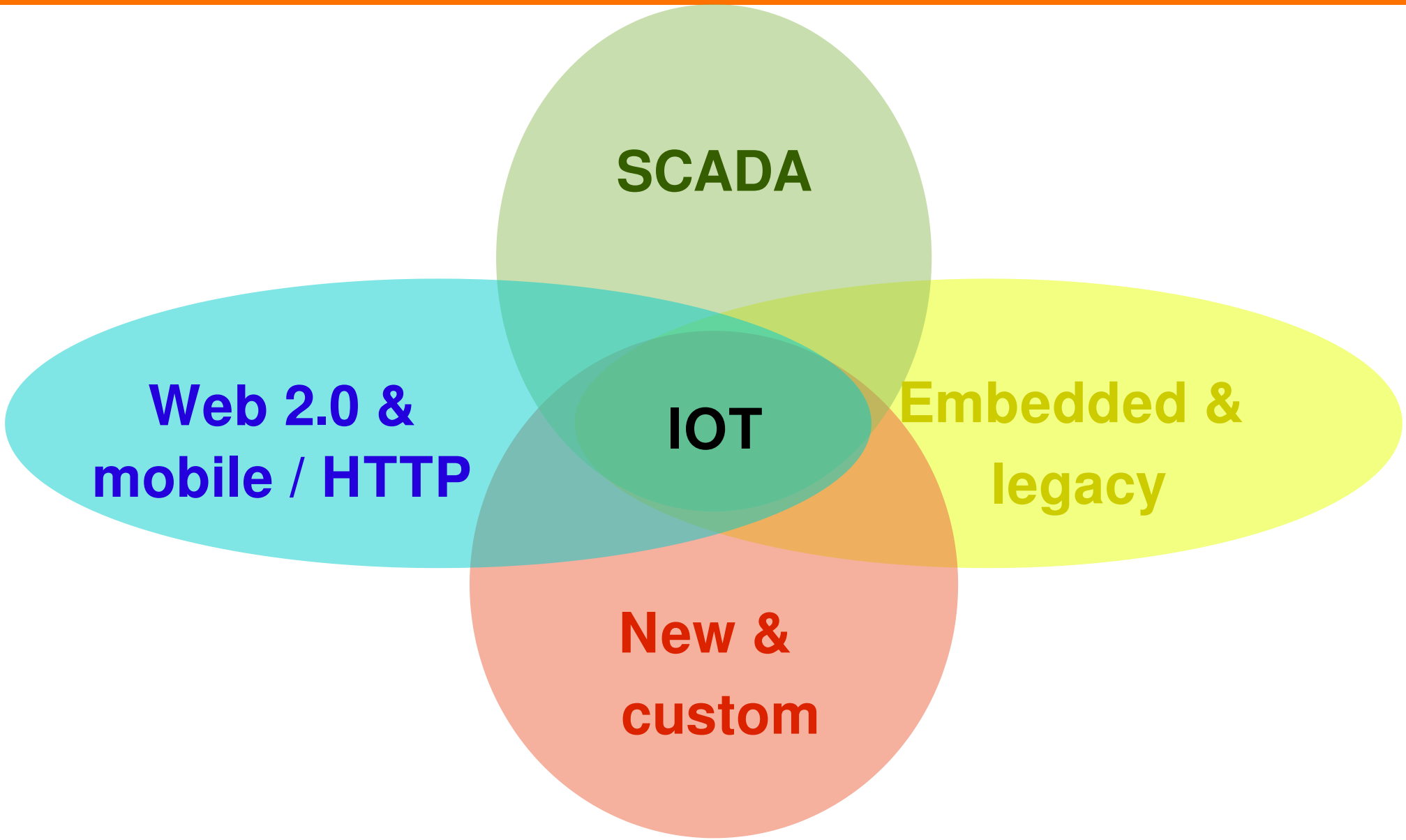
The S in IOT stands for Security

Internet of Threats?



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

Tecnologia



SCADA?!

ma non sono quei grossi "cosi" 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, ..)

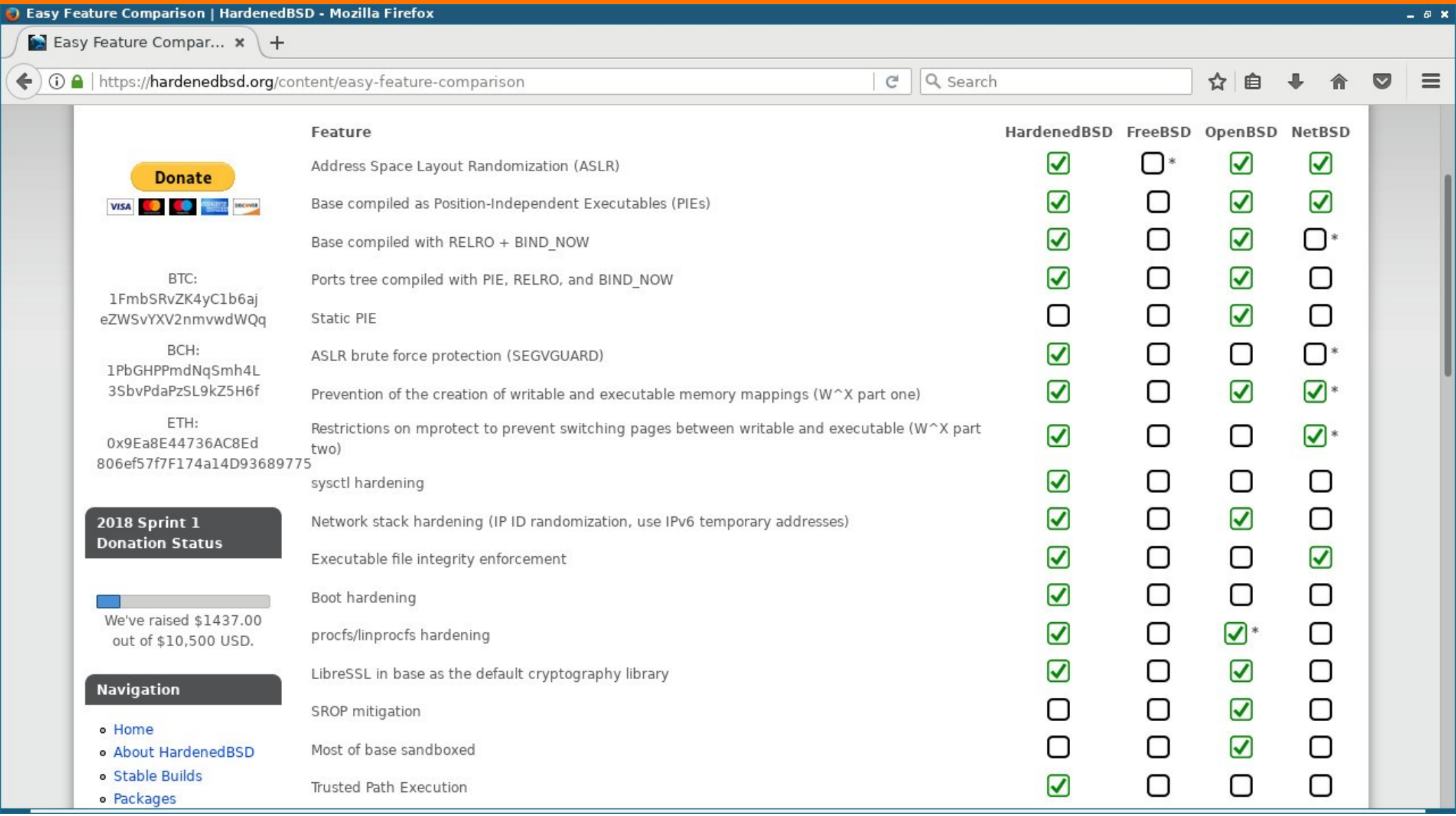
che cosa mai potrà andare storto?

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 ..

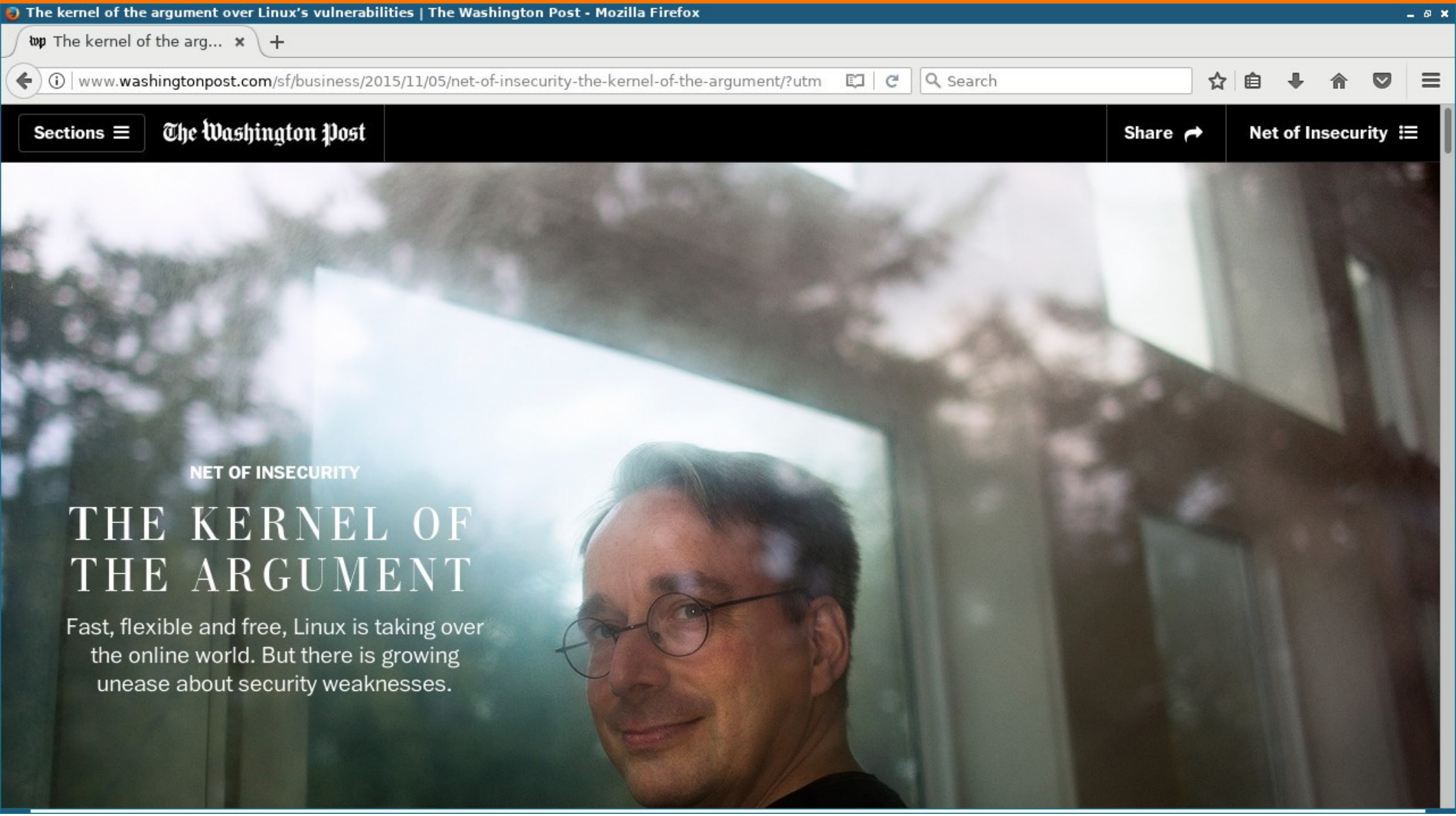
Tecniche anti-exploiting?



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

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

OS IoT più diffuso?



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

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: Կարեւոր Փաստեր - 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, legggervi 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.

XMPP

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) + OpenJabNab

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

All client/server communications use the XMPP (aka 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 or the radio is sent to the server that rasterize it in a MP3 file, then transferred during the XMPP session using plain HTTP.

XMPP

TLS sì,

ma soggetto a MITM

(non verifica cert)

(tempo: ~30 min)

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 ARPspoof 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.

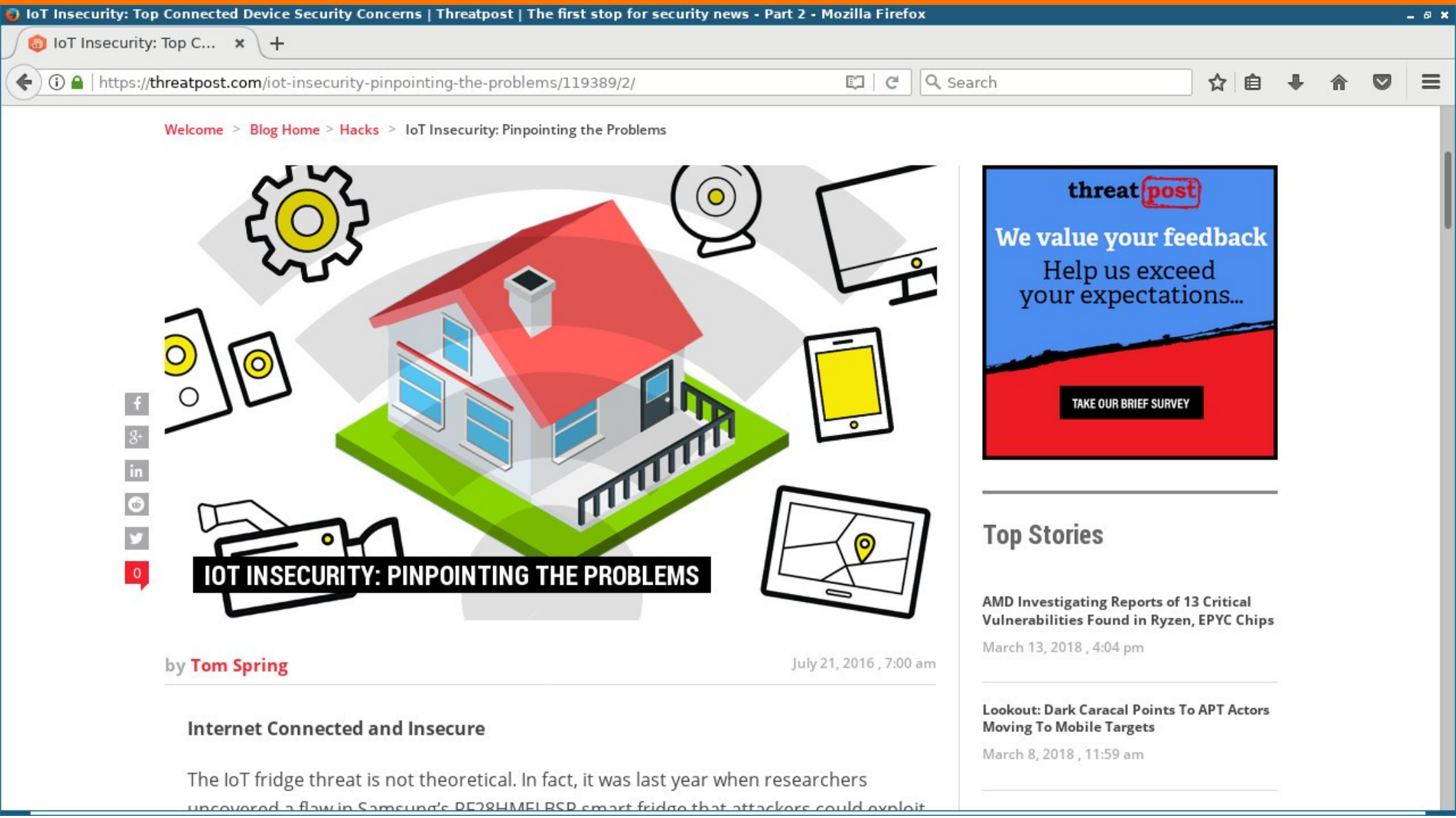
Case study: nabaztag

- 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..

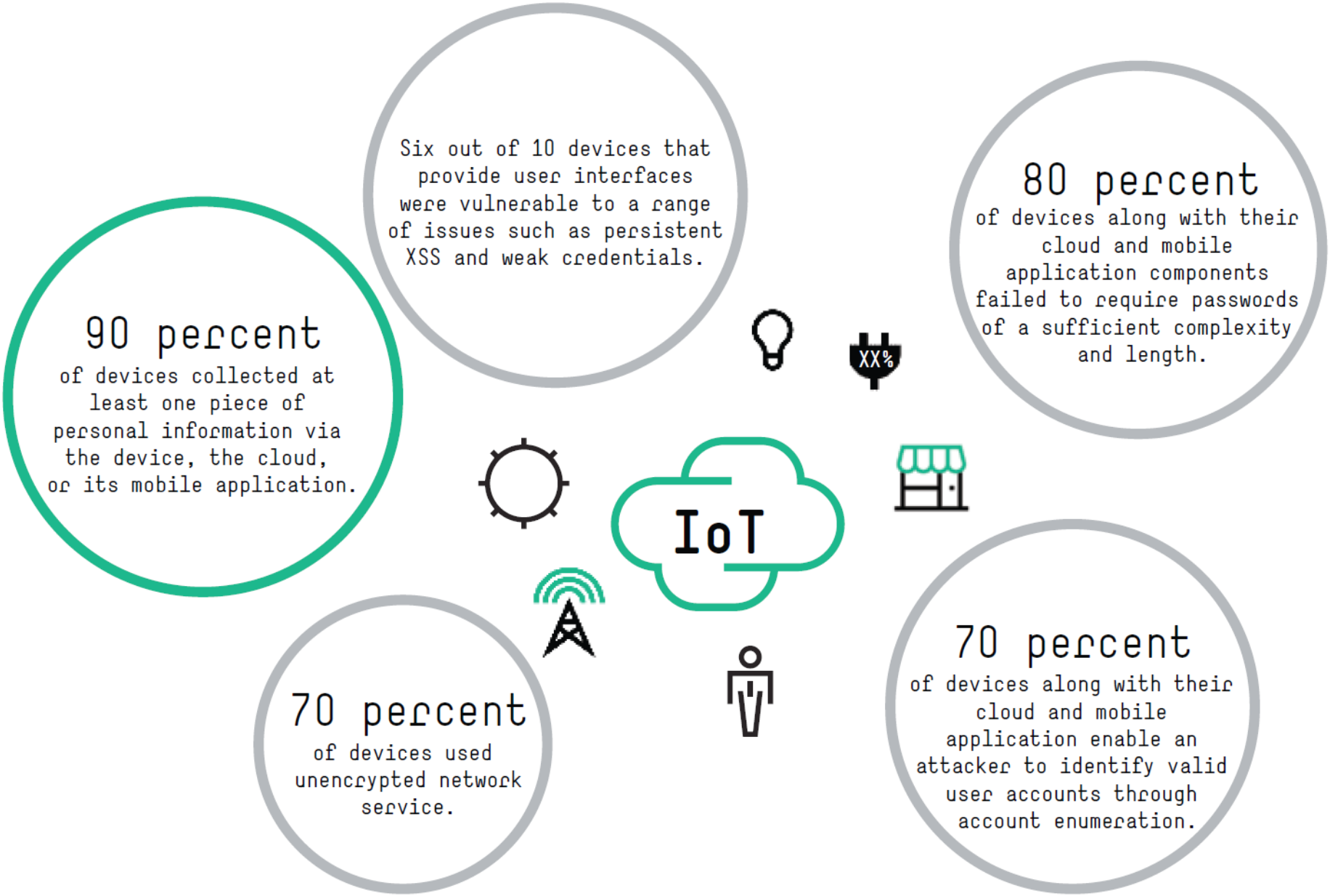
..siamo nel 2020..

..come siamo messi?



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 ...

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

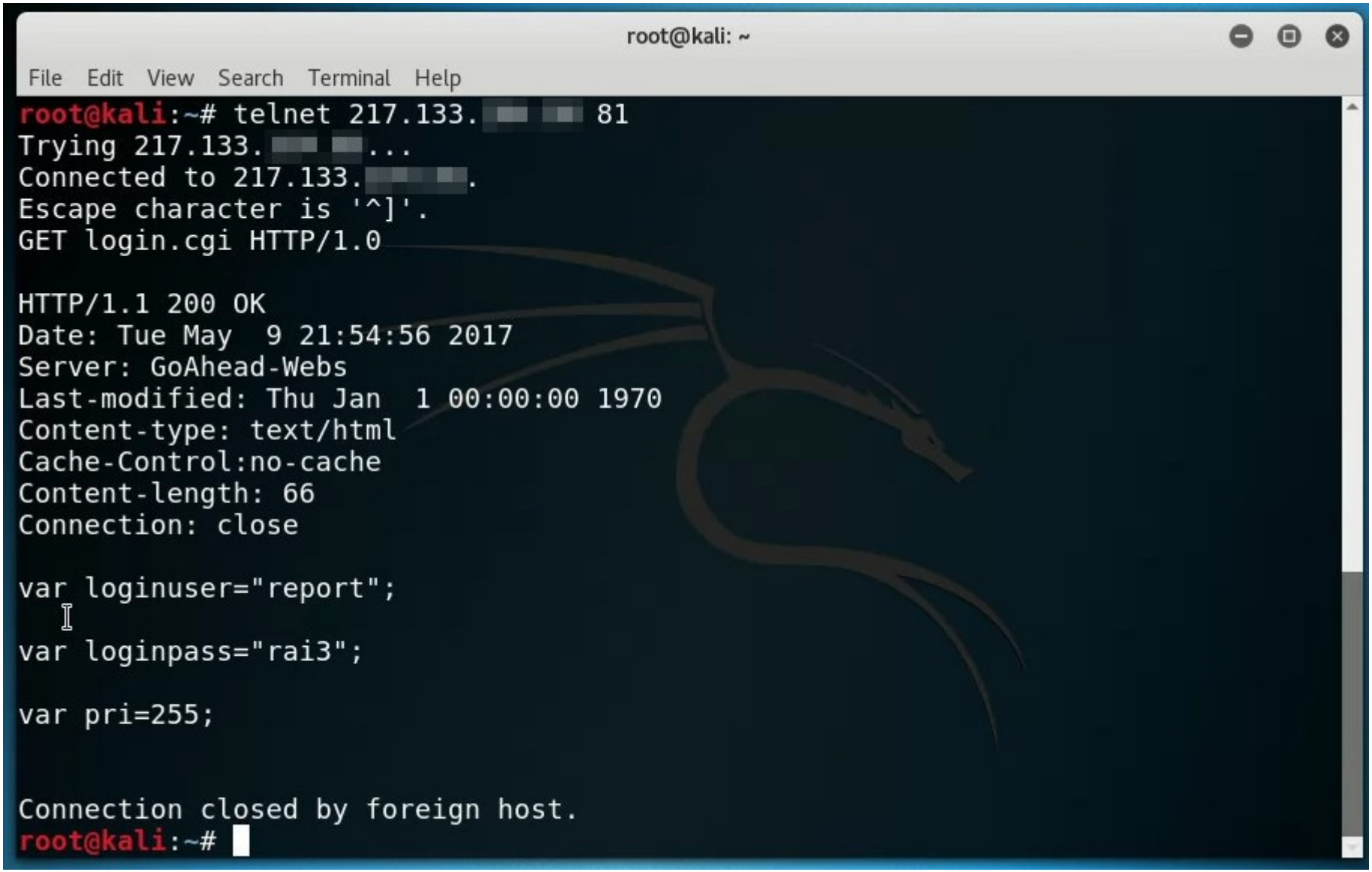
In the webroot of the host vibratissimo.com a .DS_STORE file was found. Those files are always a

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

Case study: IP Cam

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

Case study: IP Cam



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...

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

Search

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 automaticaly 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) [**]

Shodan: The IoT search engine for watching sleeping kids and bedroom antics | ZDNet - Mozilla Firefox

Shodan: The IoT sear...

www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-

Search

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

to the Internet while they enjoy a cheeky pint.

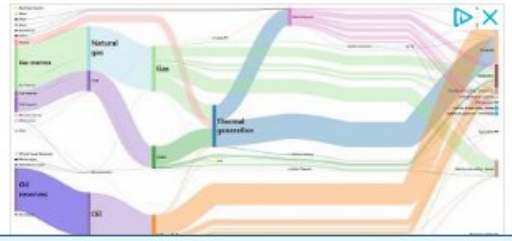
As the gallery of snapshots shows below, every facet of our lives can be recorded for the viewing of the Internet at large. (*Faces and identifiable markers have been blurred by ZDNet to protect identities.*)

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.



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

Ecosystem Access Control	Device Memory	Device Physical Interfaces
Device Web Interface	Device Firmware	Device Network Services
Administrative Interface	Local Data Storage	Cloud Web Interface
Ecosystem Communication	Vendor Backend APIs	Third-party Backend APIs
Update Mechanism	Mobile Application	Vendor Backend APIs
Network Traffic		

Image credits: Dan Miesseler

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?

- Awarness: 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?

HACK THE TOWER

Domande?

(grazie dell'attenzione)

Relatore:

easynet group | enforcer SECURITY

Igor Falcomatà, CEO
ifalcomata@enforcer.it