Internet of Things

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Internet of Things

- Internet of Things

..

Internet of Things

IoT (Internet of Things)
Internet delle cose e dei sensori, tutto ciò che è connesso è attaccabile (o è già stato attaccato).

“The S in IoT stands for security.”

IoDROSTtVWNBtP
“Internet of Devices Running Outdated Software That the Vendor Will Never Bother to Patch”

Quando la sicurezza informatica diventa un problema del mondo reale.
Ritorno al passato, sistemi pervasivi, quindi a basso costo, quindi manca potenza e sicurezza.
(la “s” c’è ma è in fondo)
Dispositivi IOT hanno marginalità del 1-2% come faccio ad aggiungere sicurezza?
Aziende non informatiche che fanno informatica e non hanno la cultura della sicurezza (e nemmeno la struttura per gestire il ciclo delle vulnerabilità, Esempio lavastoviglie Miele directory traversal https://www.theregister.co.uk/2017/03/26/miele_joins_internetofst_hall_of_shame/).
Dispositivi del mondo reale → problemi di real time → la sicurezza/crittografia rallenta (es. air-bag).

Internet of Things

Diverse priorità

Mondo IT → 1) Confidentiality
2) Integrity
3) Availability

Produzione → 1) Availability
2) Integrity
3) Confidentiality

Corporate IT Security is about Data protection

Industrial Security is about Process protection

Process should be continuous and only then secure

CPS = Cyber Phisical Systems
Tutte le volte che il mondo fisico e quello digitale sono integrati

Stuxnet attack

http://en.wikipedia.org/wiki/Stuxnet

Giugno 2010: “The computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran’s nuclear centrifuges by disrupting industrial PLCs”

Israele+USA lo hanno scritto

https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Distribuito tramite chiavette USB infette.

Potenziale compromissione di un impianto nucleare (con quello che ne consegue).

Richiede altissimo livello di competenze e di conoscenza del target (sistemi SCADA Supervisory Control and Data Acquisition).

C’è ancora qualche chiavetta in giro?

Hanno fatto un film

https://www.imdb.com/title/tt5446858/

Internet of Things

Far esplodere un generatore da 27 tonnellate

Aurora: Homeland Security's secret project to change how we think about cybersecurity

The "Aurora Generator Test" proved that hackers could exploit cybersecurity vulnerabilities in infrastructure with explosive results

Written by Curtis Waltman Edited by JPat Brown

In 2014 MuckRock user Scott Ainslie received an unexpected response from the Department of Homeland Security. Despite requesting DHS files related to a series of foreign cyberattacks codenamed "Operation Aurora," they responded with a video clip and 840 pages of documents relating to a *different* Operation Aurora that DHS conducted in 2007.

Articolo:
https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/
https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/

Video:
https://www.youtube.com/watch?v=LM8kLaJ2NDU

Internet of Things

Qui entra in gioco la vita delle persone

These Hackers Made an App That Kills to Prove a Point

Medtronic and the FDA left an insulin pump with a potentially deadly vulnerability on the market—until researchers who found the flaw showed how bad it could be.

Pompa di insulina, attivabile o bloccabile via wifi, vulnerabile. Posso uccidere con una app.

https://www.wired.com/story/medtronic-insulin-pump-hack-app/

Internet of Things

E magari gli oleodotti
"The scary reality of hacking infrastructure"

Oppure i pacemaker
Researchers hack a pacemaker, kill a man(nequin)

Feb 19, 2019

Impiantato il primo cuore artificiale wireless

Senza cavi né batterie, è stato impiantato in Kazakistan da un'équipe cui ha

Magari vogliamo solo farci i fatti altrui
World online live cameras directory
Nel dubbio possiamo cercare
Search engine for Internet-connected devices.

 8

http://money.cnn.com/video/technology/2013/09/05/t-cyber-warfare-hacking-infrastructure-syria.cnnmoney/index.html

http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html

http://www.insecam.org/en/bycity/Bologna/

https://www.shodan.io/

https://censys.io/

IOT Hall of Shame
https://codecurmudgeon.com/wp/iot-hall-shame/

IOS Internet of shit
https://twitter.com/internetofshit

Internet of Things

Fare ricerche con Shodan mette preoccupazione.
https://voidsec.com/state-of-industrial-control-systems-ics-in-italy/

https://www.shodan.io/search?query=port%3A47808+country%3AIT

(Bacnet, building automation)

Search interessanti su Shodan
https://github.com/jakejarvis/awesome-shodan-queries

Internet of Things

Recupero componenti standard per risparmiare

Per risparmiare si recuperano parti di software standard, ad esempio stack TCP/IP.

https://treck.com/ produce stack TCP/IP leggeri e adatti per dispositivi IOT, trovate le vulnerabilità = tutti i dispositivi a rischio indipendentemente dal vendor e dal tipo di dispositivo (e non facilmente patchabili).

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-treck-tcpip-stack-could-allow-for-remote-code-execution_2020-083/

Internet of Things

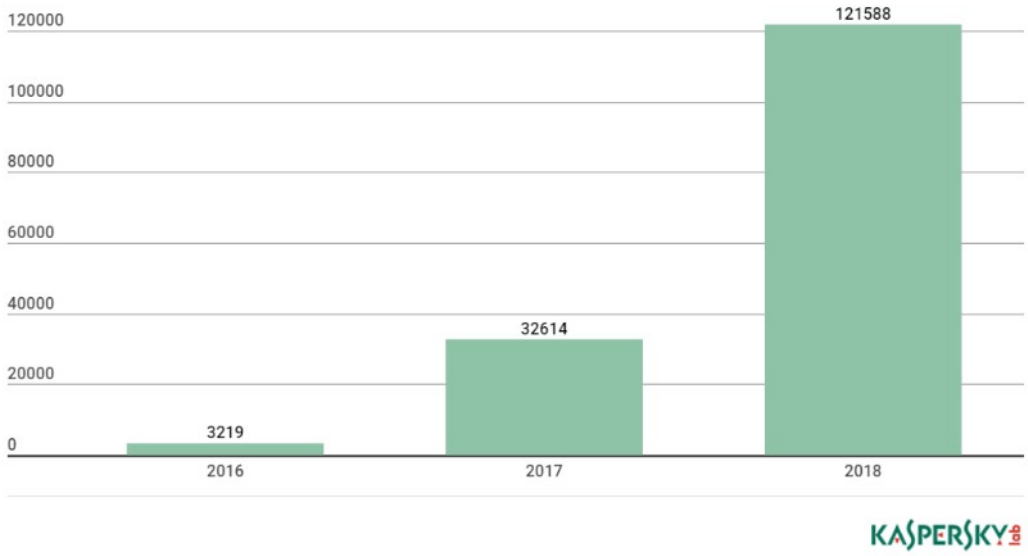
How a fish tank helped hack a casino

By **Alex Schiffer**
July 21, 2017

Webcam per vedere i pesci, sensori in rete per temperatura e pulizia dell'acqua ecc.

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Internet of Things



Number of malware samples for IoT devices in Kaspersky Lab's collection, 2016-2018. (download)

Report Kaspersky estate 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

Internet of Things

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	–
winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	–
RDP	3389	0.12%	Bruteforce	–
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–

Report Kaspersky estate 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

Internet of Things

Attacchi DDOS sfruttando i dispositivi IOT: milioni di termostati contro di noi!


NETWORKWORLD
FROM IDG

Home > Security

Largest DDoS attack ever delivered by botnet of hijacked IoT devices

http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

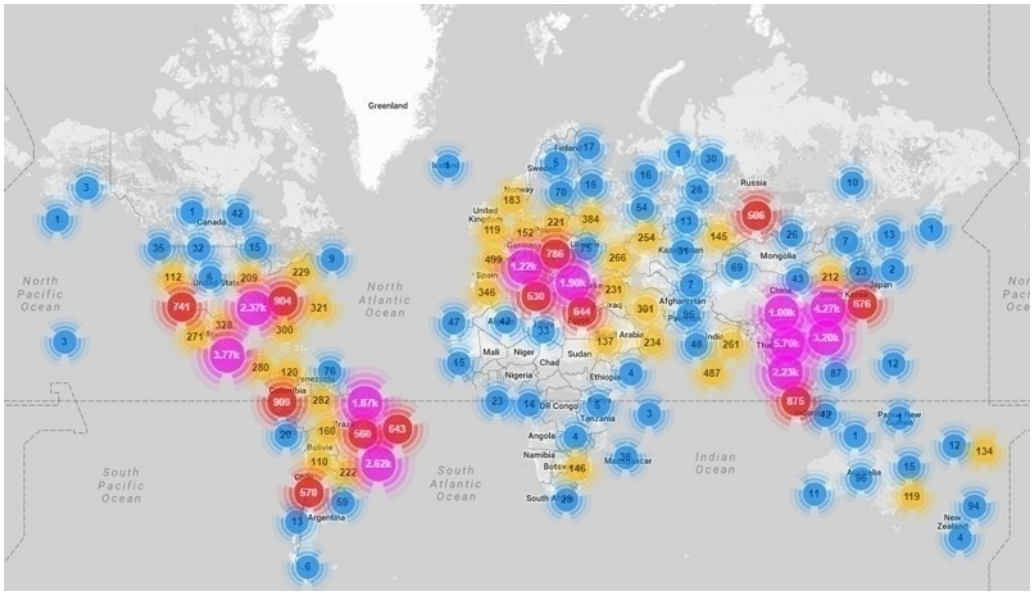
Utilizza Malware Mirai, disponibile come servizio in rete.
https://it.wikipedia.org/wiki/Mirai_(malware)

Nato (probabilmente) come un sistema per fregare i giochi online (DDOS contro i miei “nemici”).

https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet

Internet of Things

Attacco globale:



Analisi dell'attacco:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Internet of Things

19 Mirai Botnet Authors Avoid Jail Time

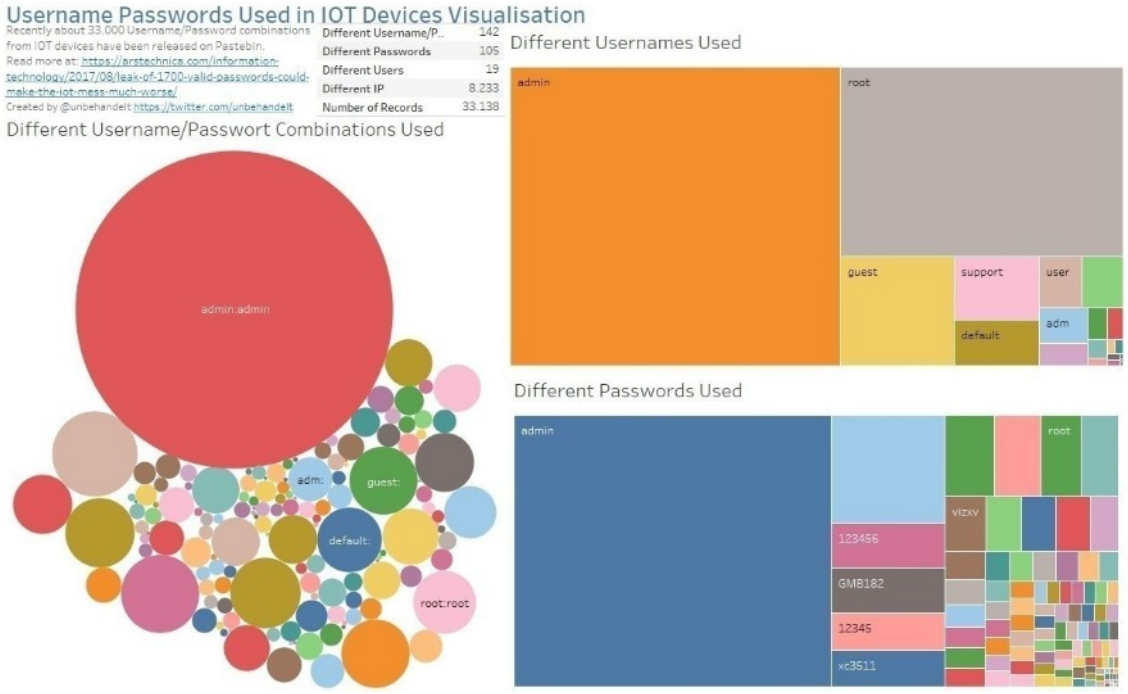
SEP 18

Citing "extraordinary cooperation" with the government, a court in Alaska on Tuesday sentenced three men to probation, community service and fines for their admitted roles in authoring and using "**Mirai**," a potent malware strain used in countless attacks designed to knock Web sites offline — including an enormously powerful attack in 2016 that sidelined this Web site for nearly four days.

The men — 22-year-old **Paras Jha** Fanwood, New Jersey, **Josiah White,** 21 of Washington, Pa., and **Dalton Norman** from Metairie, La. — were each sentenced to five years probation, 2,500 hours of community service, and ordered to pay $127,000 in restitution for the damage caused by their malware.

Se la sono cavata con poco
https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/

Internet of Things



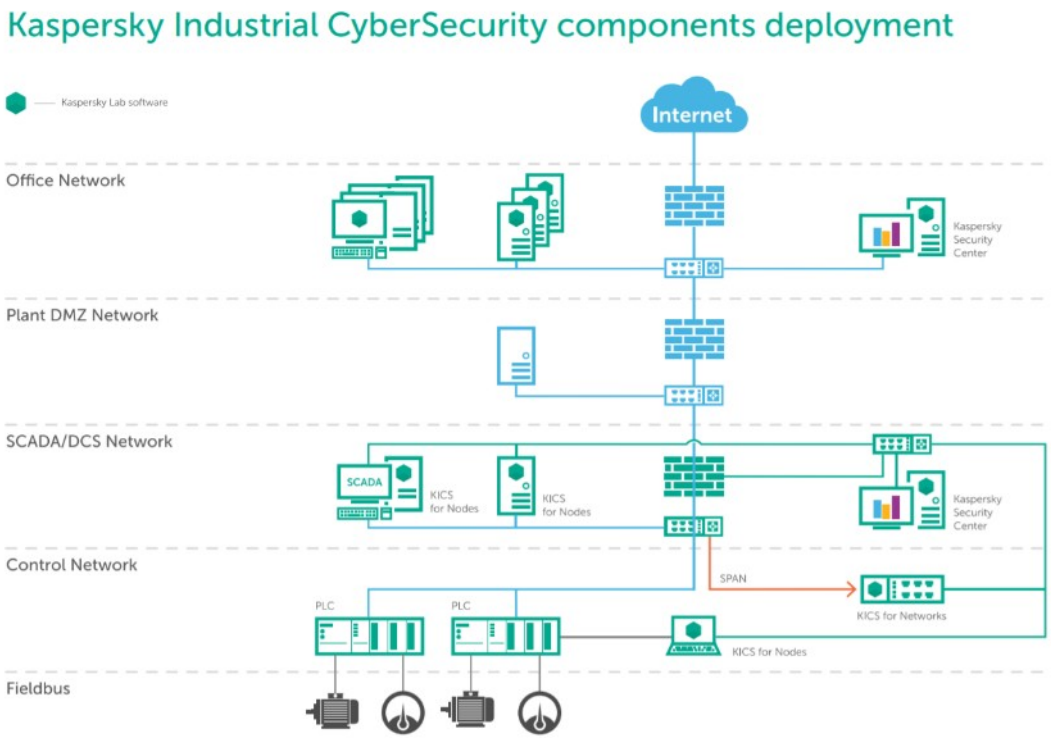
 17

Il problema delle password dei dispositivi IOT, maggior parte admin:admin (ci era cascata anche Vodafone) oppure root, 123456 ecc.

Comunque spesso password di default che non vengono cambiate.

https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/

Internet of Things



Stanno nascendo soluzioni/prodotti ad hoc, integrati con la sicurezza “tradizionale” ma che scendono fino al livello SCADA o PLC.

Whitelisting dei comportamenti, tanto mediamente sono oggetti piuttosto stabili nel tempo.

Nel frattempo la California ha fatto una legge per vietare la vendita dei dispositivi che non rispettano i livelli minimi (password di default, aggiornamenti sw ecc.)

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

ISA/IEC 62443

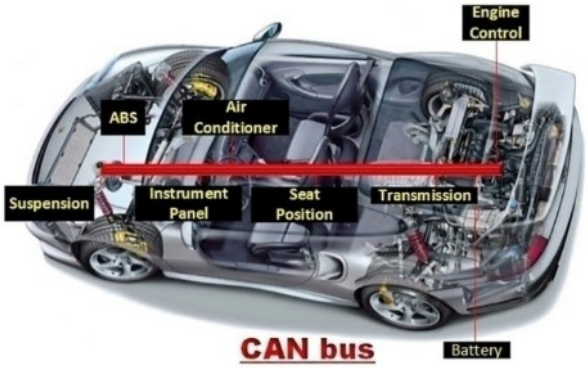
ISA/IEC 62443 standard specifies security capabilities for control system components

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

https://www.isa.org/intech/201810standards/

Internet of Things

Ma il grande business sono le auto!



Dal 2020 tutte le auto EU in rete

Autovettura è un insieme di processori (fino a un centinaio) collegati da uno o più CAN bus con un meccanismo di trust. Architettura molto semplice, basso costo, traffico non crittografato (prestazioni, air-bag). Ultimamente collegato ad Internet (VPN) per ricevere aggiornamenti software, per assicurazioni ecc. Da 11/2020 tutte le auto in UE con connettività internet per segnalazione incidente.
https://en.wikipedia.org/wiki/ECall
In alcuni casi anche wifi e bluetooth (chiavi, accensione da remoto).
Già disponibile un POC di un attacco ad una Jeep Cheroke
http://illmatics.com/Remote%20Car%20Hacking.pdf

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Internet of Things

- **V2V** (fra veicoli)
- **V2I** (segnali, infrastrutture, semafori)
- **V2P** (pedoni)
- **V2N** (rete di servizi)

V2X (vehicle to everything)
(802.11p o ITS-G5)

Servono nuove regole

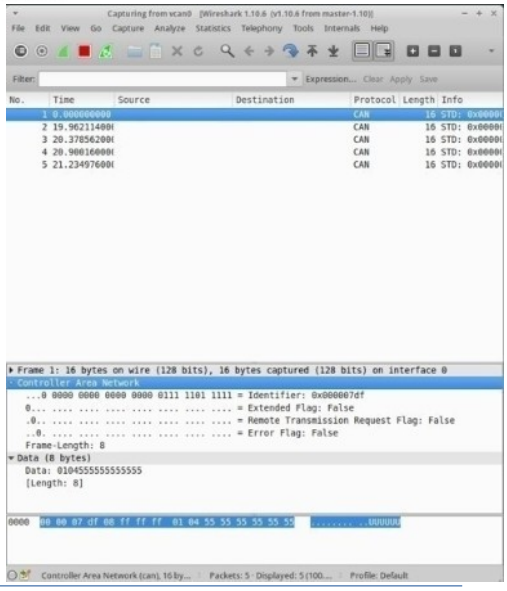
G5 DIVERSO DA 5G
5G fondamentale per erogare questi servizi, anche per la bassa latenza rispetto ai protocolli precedenti, comunicazione a corto raggio in banda 5.9 Ghz (forse, discutibile, probabilmente si può fare anche con 4G)

Necessaria normativa mondiale:
the United Nations Economic Commission for Europe (UNECE) has been developing a vehicle regulation(WP.29) with regards to cybersecurity in connected and autonomous vehicles. UNECE vehicle regulations are law in 54 nations
https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations

Internet of Things

Canale di attacco tramite porte diagnostiche

CANtact v1.0 Open Source Controller Area Network (CAN) to USB Converter

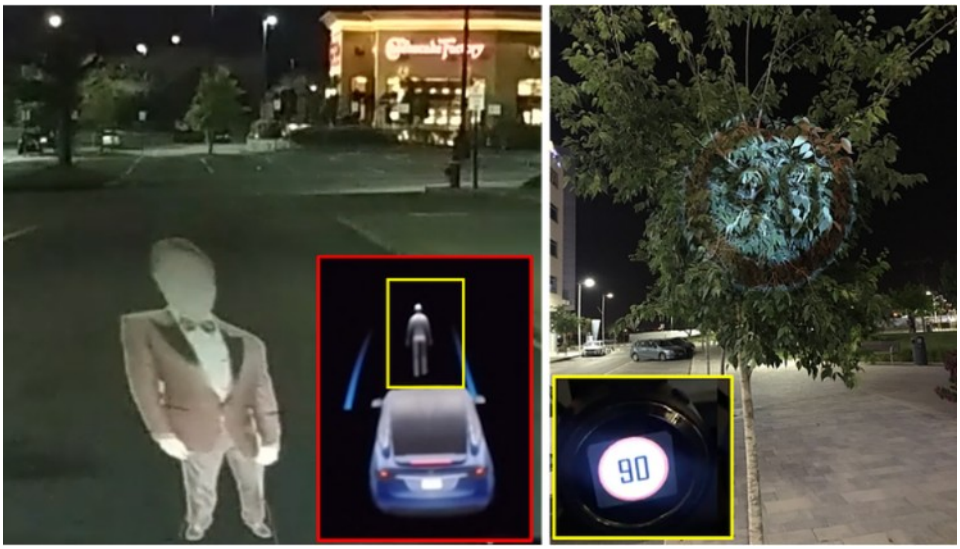


Posso utilizzare le porte diagnostiche per accedere al BUS (in alternativa wifi, bluetooth o internet).
Controller + software + wireshark e vedo tutto.
L'hardware si compera con 60$.

https://store.linklayer.com/products/cantact-v1-0

Internet of Things

Attacchi alle auto a guida (semi)automatica

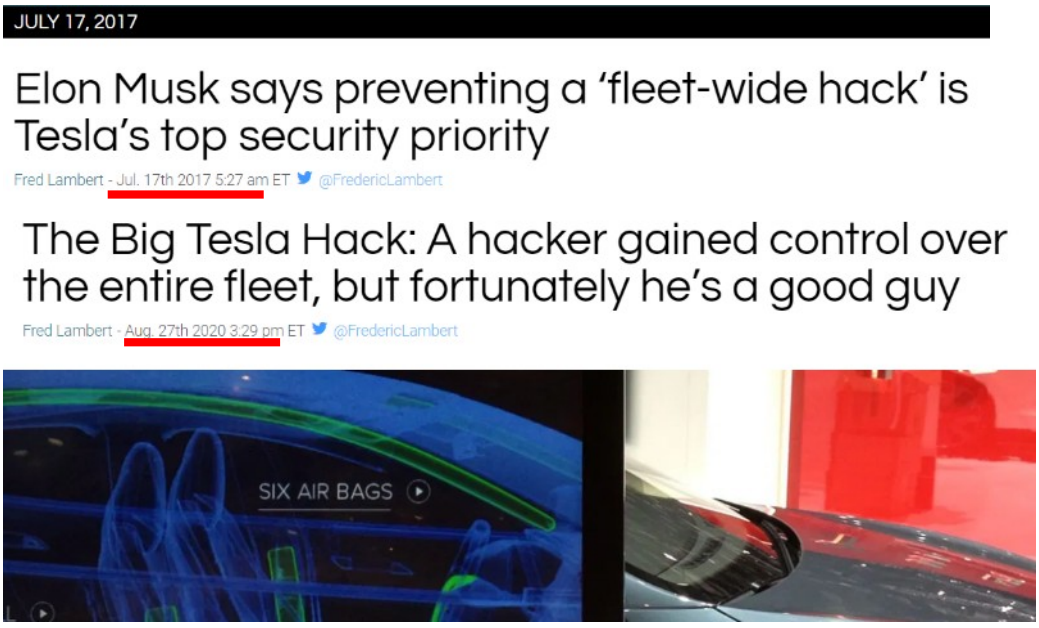


Dall’esterno posso attaccare la auto (o i sistemi) a guida autonoma o semi autonoma ad esempio proiettando immagini “fantasma” sulla strada o a lato della strada. Potrei farlo con un drone.

https://www.nassiben.com/phantoms

Internet of Things

Attacco ad una flotta intera di vetture



Se attacco i server (ad esempio di Tesla) posso prendere il controllo di un'intera flotta di vetture (tipo "Zombie car scene" di Fast&Furious 8 https://www.youtube.com/watch?v=gGXNvQ1xhPU)

Poteva succedere nel 2017 https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/ erano preparati https://electrek.co/2017/07/17/tesla-fleet-hack-elon-musk/

Lo abbiamo scoperto nel 2020

