Internet de la Cosas: Ciberseguridad

Marco Antonio Arenas Porcel

Sucre – Bolivia

2016

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- About Me:
  - Marco Antonio Arenas Porcel
  - CCNA
  - CCNA Security
  - ESR1 & ESR2
  - Docente Investigador
  - Blog: http://telecomusfx.blogspot.com/

CISCO

Introducción

OWASP
The Open Web Application Security Project

- Internet of Things – IoT
- Internet of Everything - IoE

Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

Antecedentes del IoT

OWASP
The Open Web Application Security Project

- 1990 Jhon Romkey y Simon Hacket desarrollaron el primer objeto con conexión a Internet, su tostadora inteligente.

Antecedentes del IoT

OWASP
The Open Web Application Security Project

- 1999, el ingeniero Bill Joy, fue quien profundizo el concepto de Internet de las cosas. Comunicaciones entre dispositivos.

Java

Antecedentes del IoT

OWASP
The Open Web Application Security Project

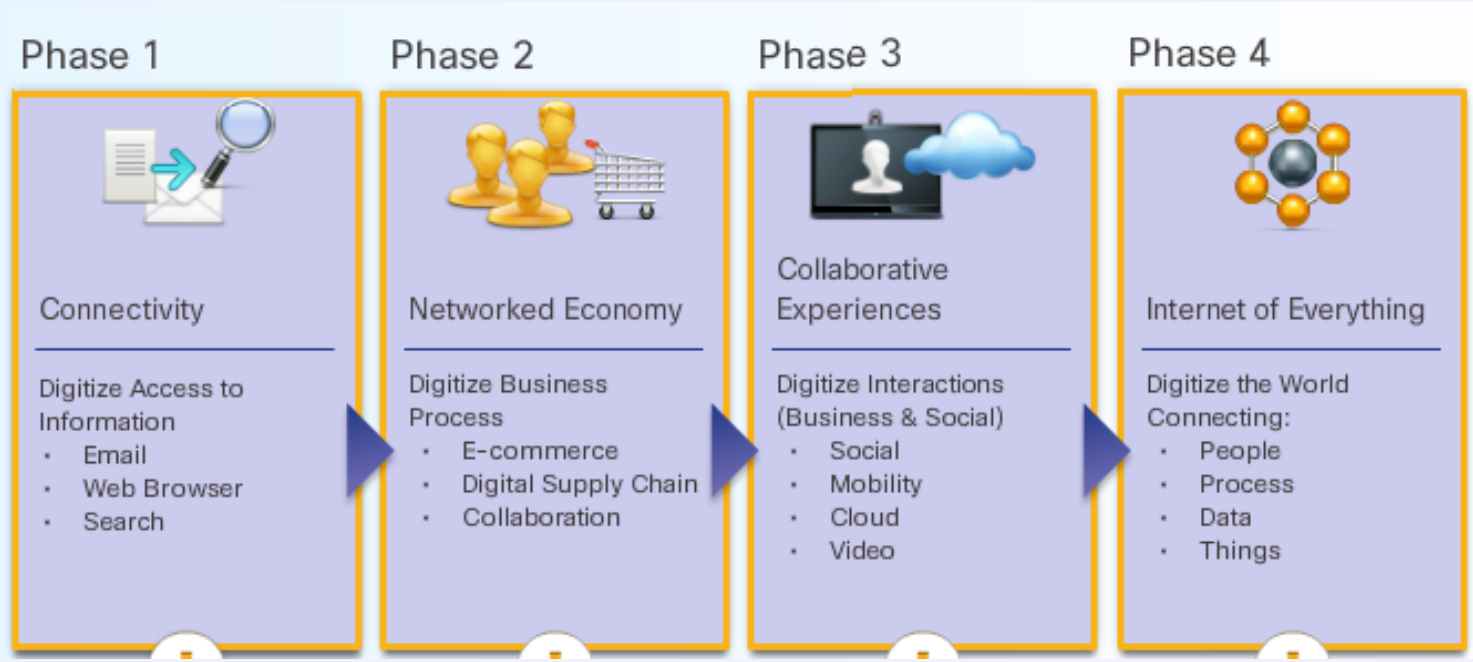
- 2009, el británico Kevin Ashton acuñó por primera vez el nombre de internet de las cosas gracias al artículo publicado en el RFID Journal.

Evolución de Internet

OWASP
The Open Web Application Security Project

- *IoE ha logrado que el internet sea sensorial, (temperatura, presion, vibracion, luz, humedad, estres) lo que nos permite ser mas proactivos y menos reactivos*

Primera Evolución Real

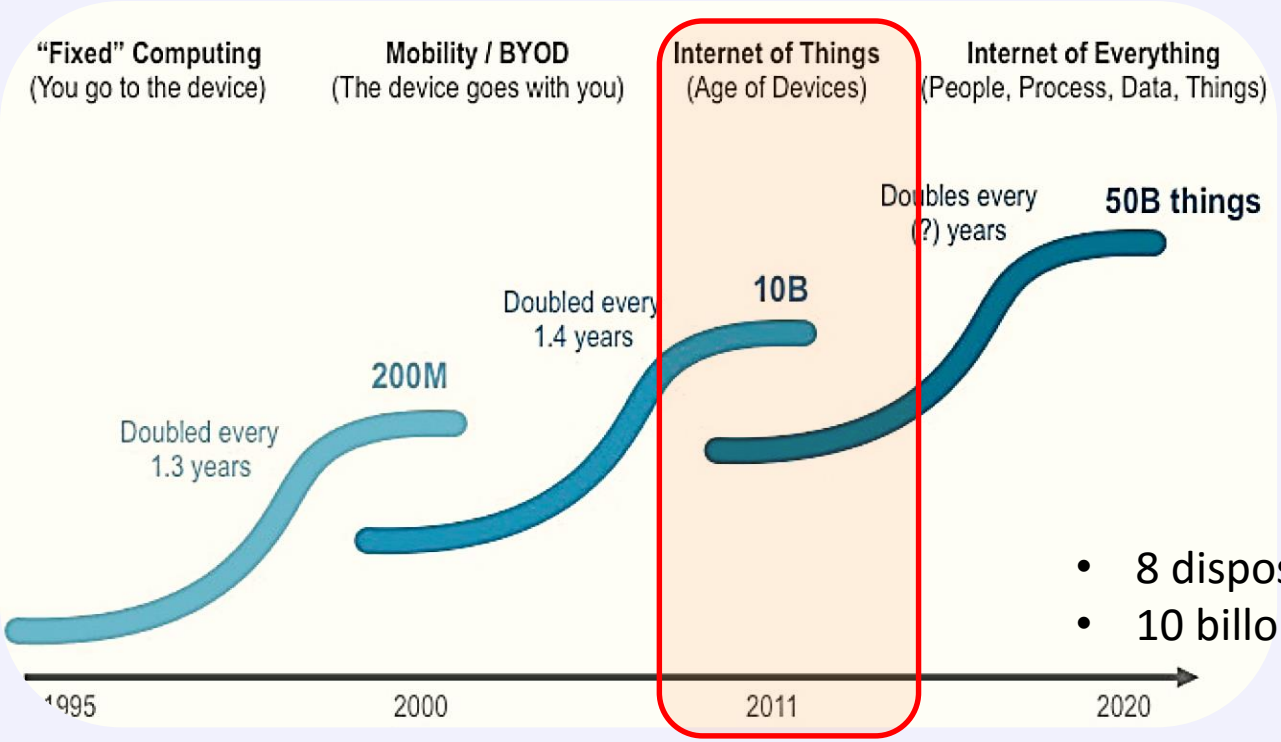


Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

Evolución de Internet

OWASP
The Open Web Application Security Project

- El futuro de Internet



- 8 dispositivos/persona
- 10 billones de dólares

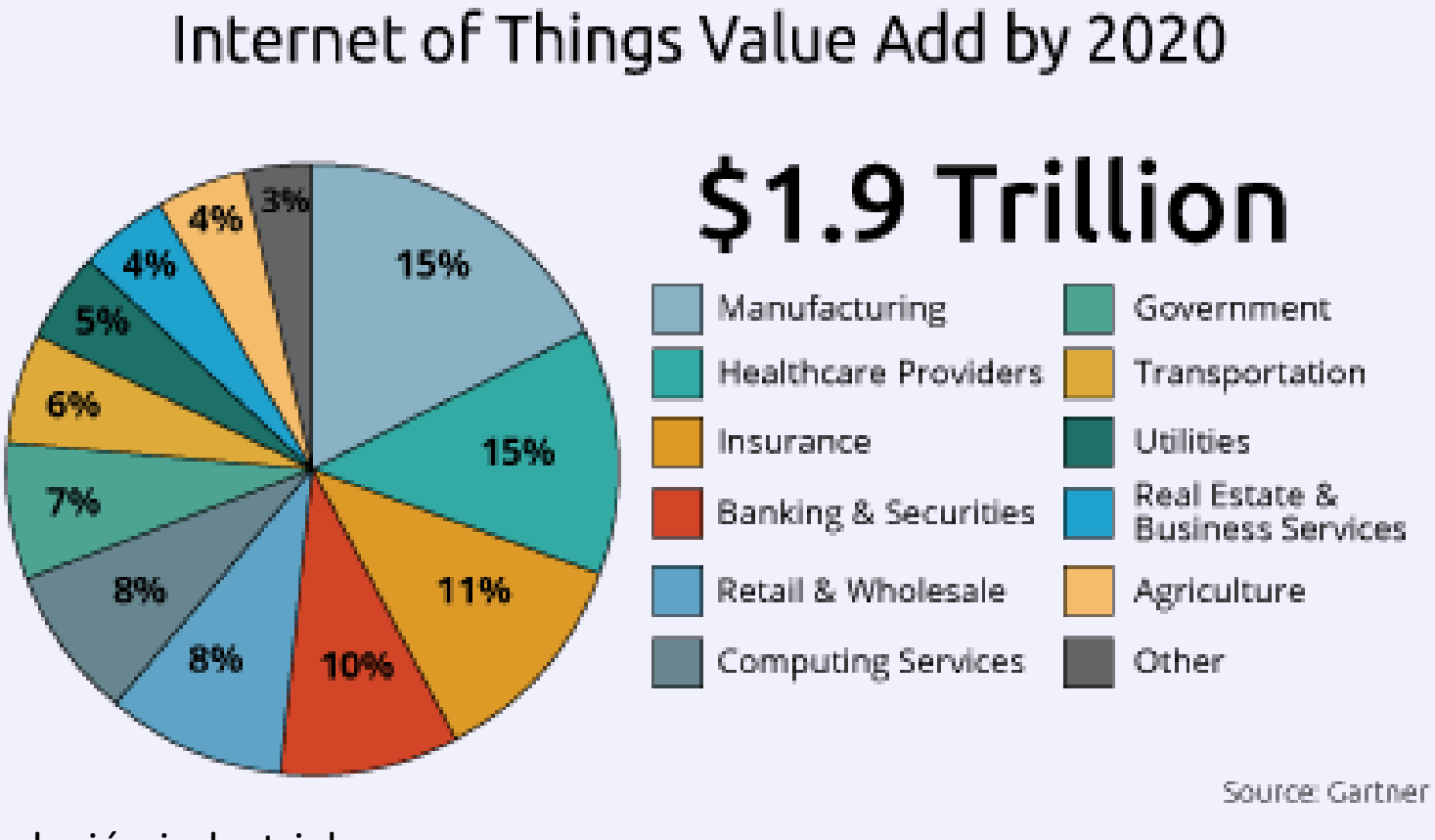
2008-2009 nace el Internet de la cosas

Fuente: *Cisco IBSG, 2012 http://www.cisco.com/go/ibsg*

IoE es economía

OWASP
The Open Web Application Security Project

- Proyecciones de Gartner

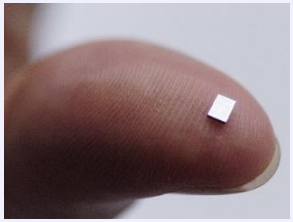


Otra revolución industrial…

IoE tecnologías asociadas

OWASP
The Open Web Application Security Project

- IoT, trae nuevas tecnologías y así mismo realza otras ya antiguas:
  - Conectividad móvil IEEE 802.15
  - RFID
  - Big Data (Minería de Datos)
  - Analystics (BI)
  - Cloud computing/fog computing
  - Smart Cities



Bluetooth®

ZigBee®

NFC

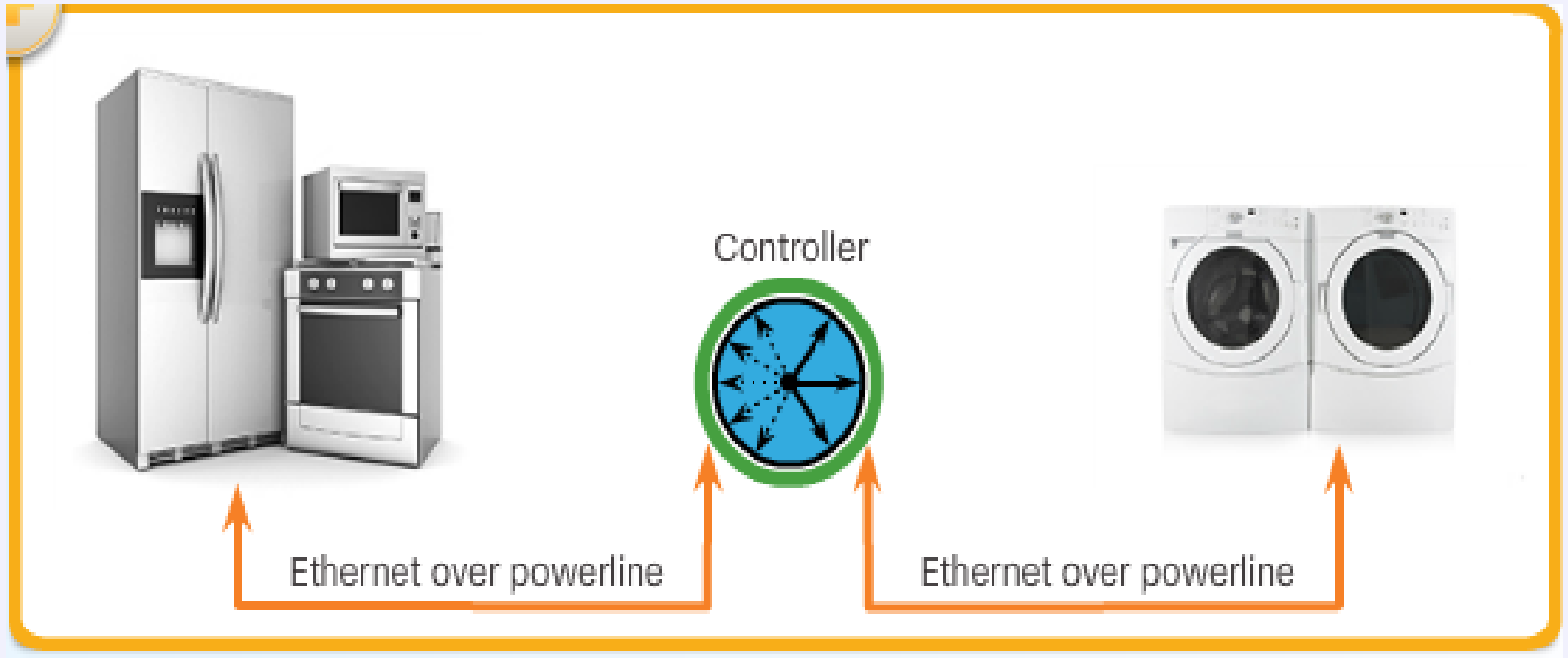
6LoWPAN
IPv6-based Low-power Wireless Personal Area Networks

Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

Redes mixtas

OWASP
The Open Web Application Security Project

- Además de los medios guiados clásicos

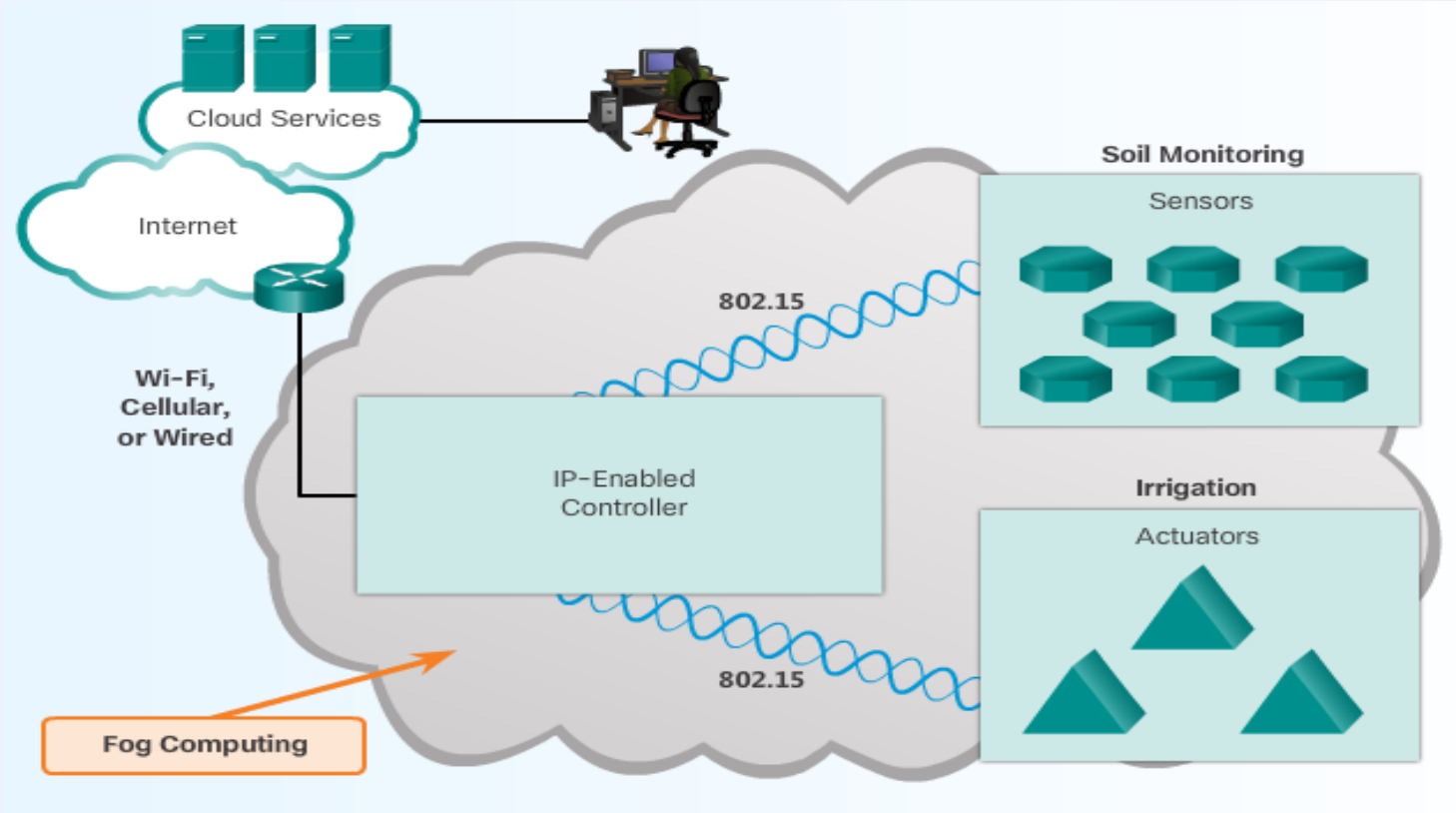


Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

Redes Mixtas

OWASP
The Open Web Application Security Project

- Evolución de los controladores de red



Comunicaciones:
P2P
M2P
M2M
Ej: Sensores envían señales al controlador, lo procesa, envía señal al actuador y realizar ajustes (Semáforos Inteligentes)

Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

Redes mixtas

Actuador: solenoide eléctrico utilizado para controlar el sistema hidráulico

Fuente: https://www.netacad.com/courses/intro-internet-of-everything/

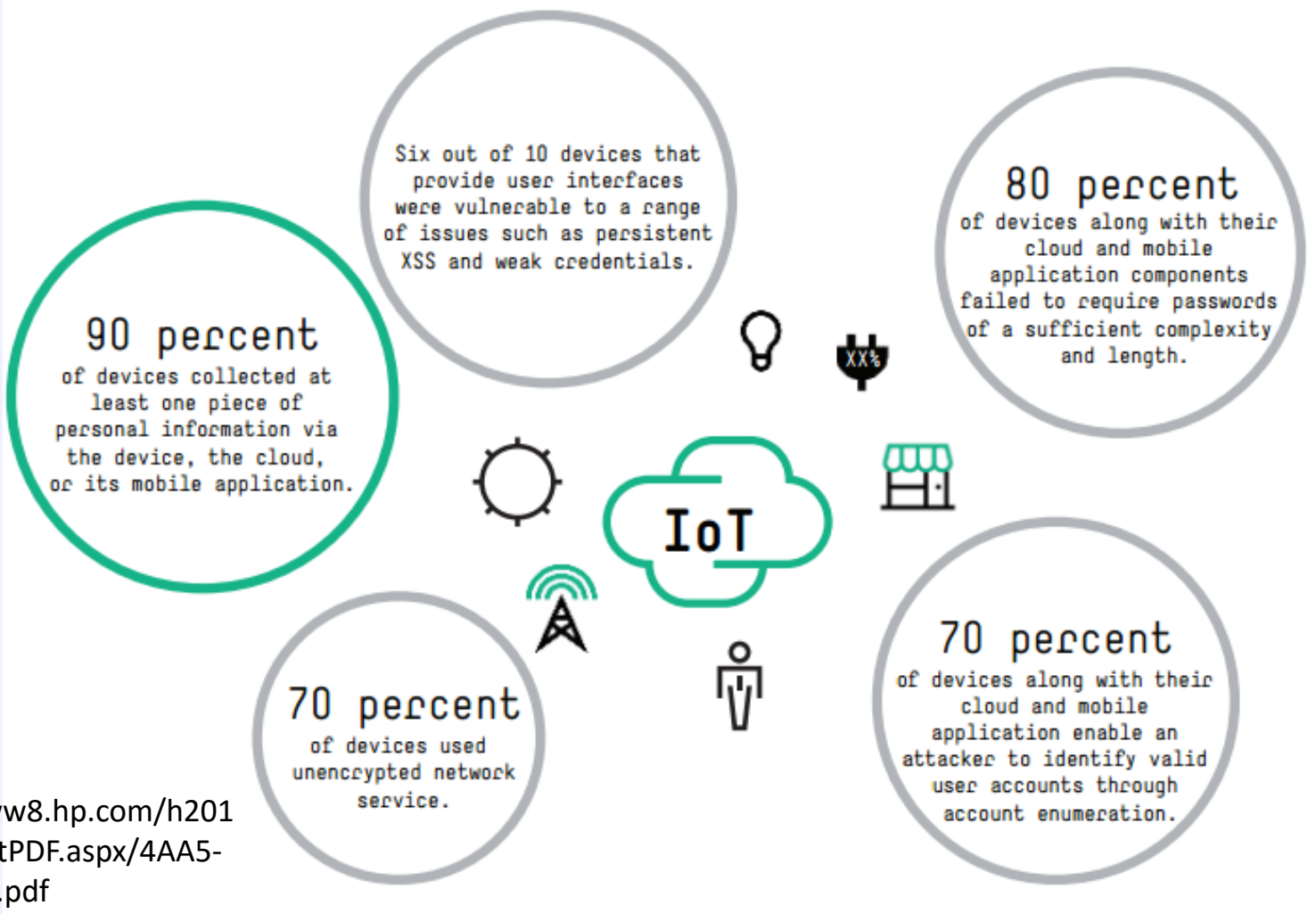
El alcance de la seguridad

OWASP
The Open Web Application Security Project

- Cada vez hay más dispositivos conectados a Internet (masas de información compartida)
- La seguridad informática esta dependiendo de Internet (ciberespacio)
- Los dispositivos de IoT no parecen críticos, pero podrían llegar a serlo (depende como los usamos).
- Según el informe de Julio de 2014 de HP FORTIFY el 80% de los dispositivos tienen fallos en la autenticación y 6 de cada 10 dispositivos con interfaz de usuario son vulnerables.

IoE=Reto de seguridad

El problema

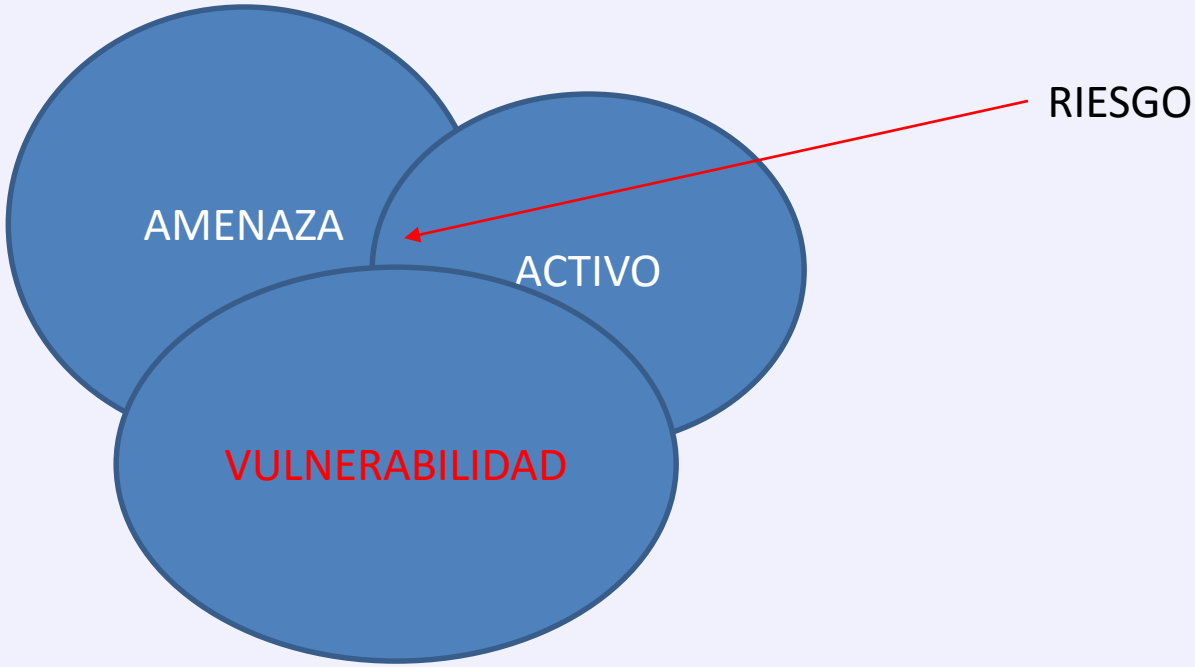


Fuente: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Riesgos

- Más vectores de Ataques
  - Físicos, Entorno, Criptoanálisis, software, red, etc.
  - Side channel attacks (Análisis electrománetico, POWER)



Cultura de seguridad de los usuarios ???

The Internet of Things and wearables: Driving the next phase of personal computing

Riesgos de IoT

OWASP
The Open Web Application Security Project

- Se pone en riesgo la integridad, confidencialidad, disponibilidad, pero ojo la identidad de las personas.
  - Posicionamiento GPS de las personas, mediante los dispositivos *wearables* (Nike+)

Fuente: http://www.dscuento.com.mx/nike-and-ipod/

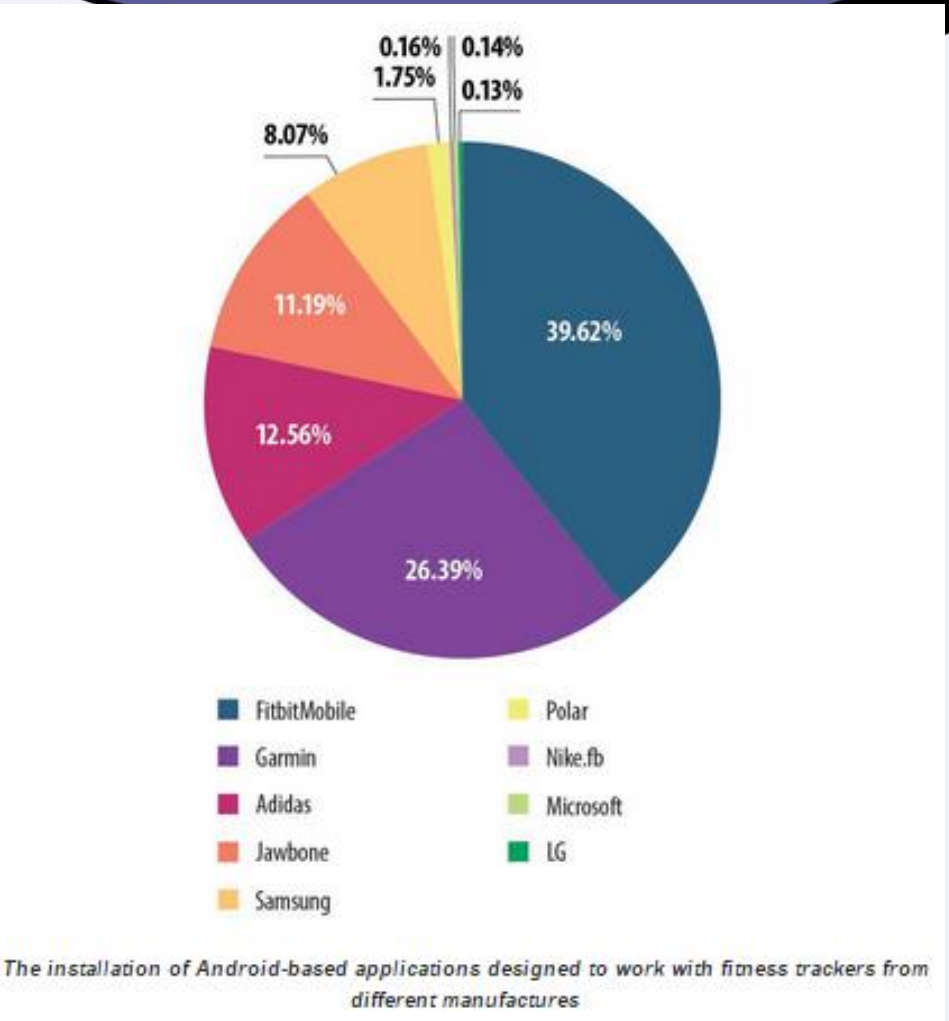
Riesgos de IoT

OWASP
The Open Web Application Security Project

Riesgos- IoT

OWASP
The Open Web Application Security Project

- Dispositivos wearables - Bluetooth LE technology

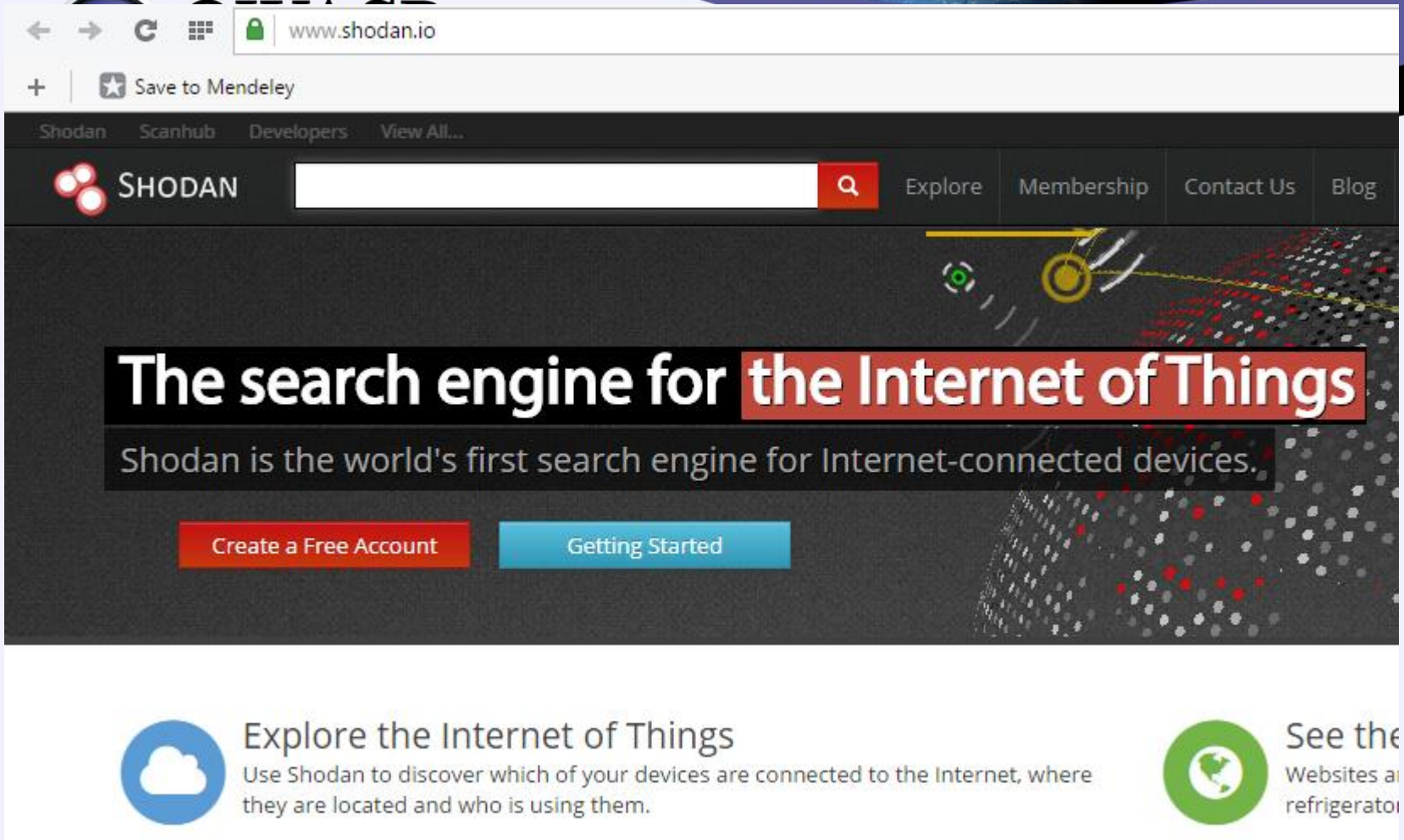


The installation of Android-based applications designed to work with fitness trackers from different manufactures

Kaspersky Security Network (KSN)

http://securelist.com/blog/research/69369/how-i-hacked-my-smart-bracelet/

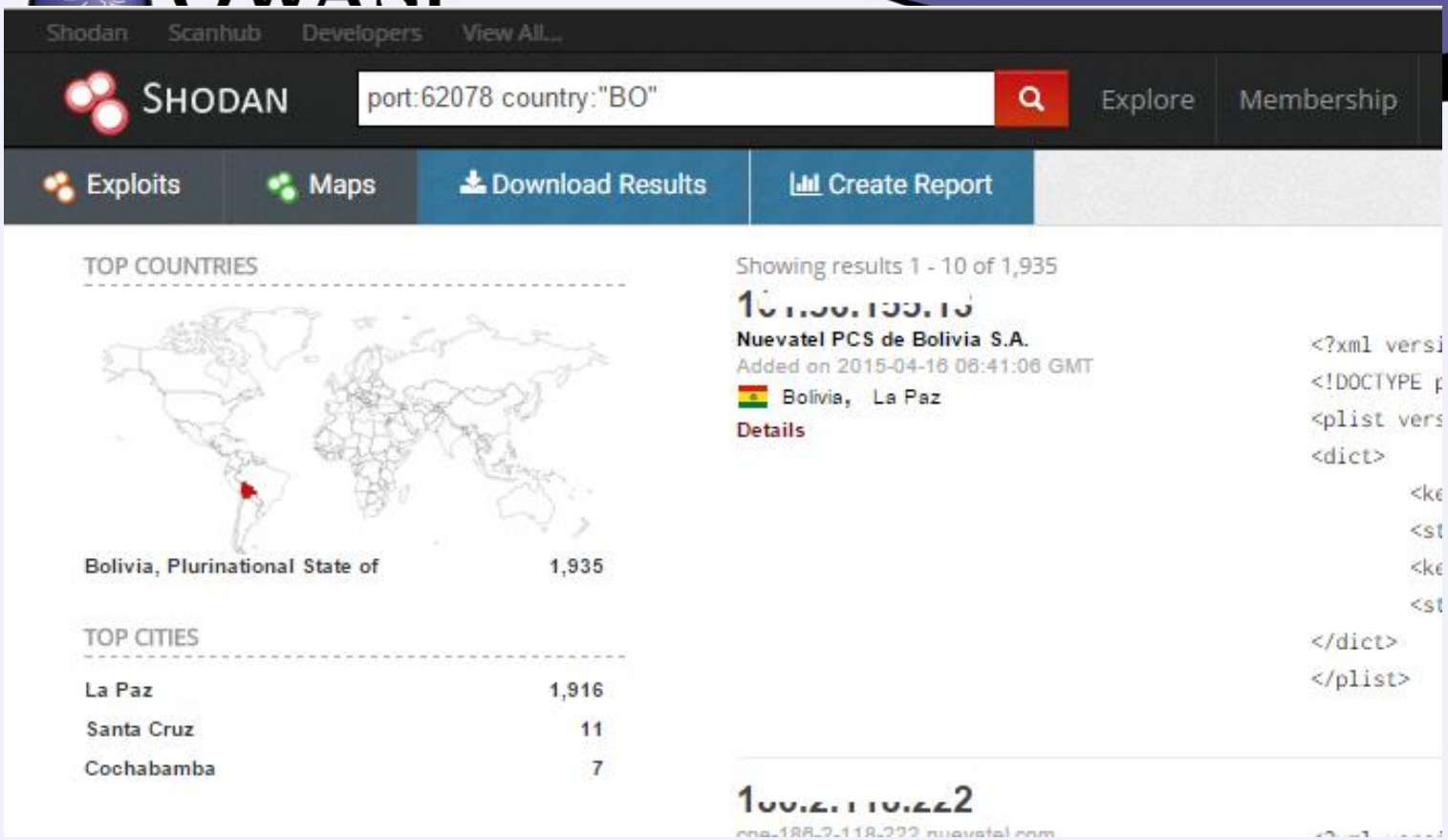
Riesgos de IoT



https://www.shodan.io

Riesgos de IoT

OWASP



Riesgos de IoT

OWASP
The Open Web Application Security Project

Average Internet of Things device has 25 security flaws

In a study of ten devices including home thermostats, remote power outlets and door locks, HP found 250 potentially dangerous security vulnerabilities

Ikea's vision of the connected home is one that should be adopted by businesses Photo: IKEA

La casa inteligente

http://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html

Riesgos de IoT

OWASP
The Open Web Application Security Project

- Robo de Información (disponible en la nube).
- Control y uso malintencionado de los dispositivos.
  - A nivel personal:
    - Tu coche

www.**tesla**motors.com/

Riesgos de IoT

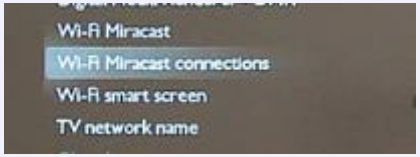
OWASP
The Open Web Application Security Project

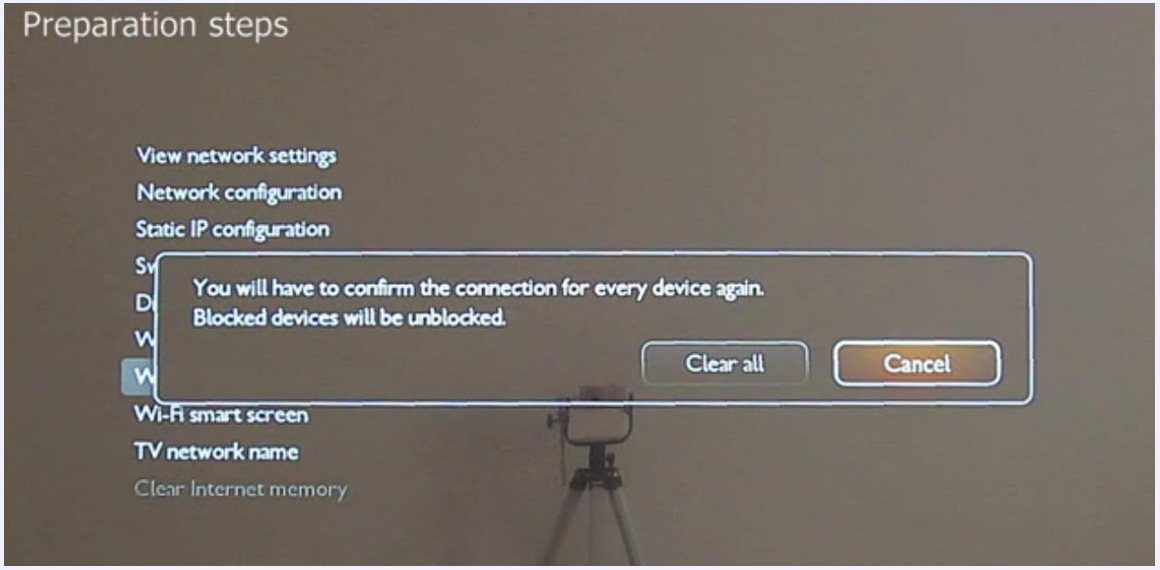
- SmartTV
  - La vulnerabilidad es la simplicidad misma: la función WiFi Miracast está activada por defecto, tiene una contraseña fija ("Miracast"), sin PIN, y no pedir permiso para nuevas conexiones WiFi .

Riesgos de IoT

OWASP
The Open Web Application Security Project

- SmartTV
  - SmartTV, dumb vuln: **Philips** hard-codes Miracast passwords

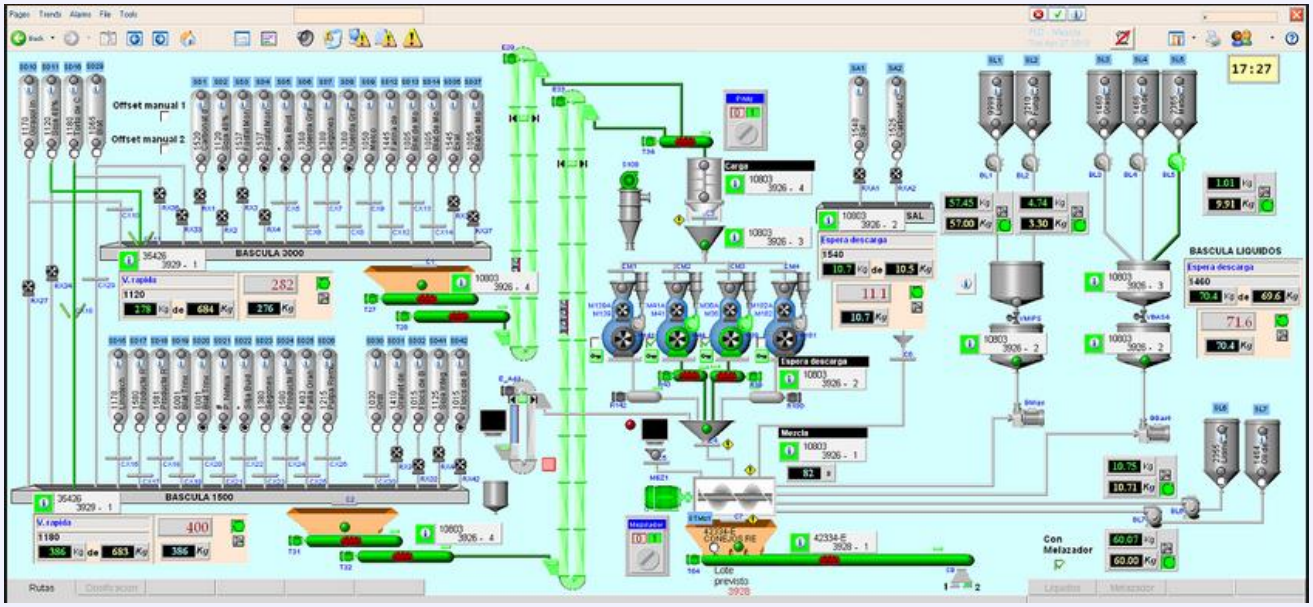




http://www.theregister.co.uk/2014/04/02/smarttv_dumb_vuln_philips_hardcodes_miracast_passwords/

Riesgos de IoT

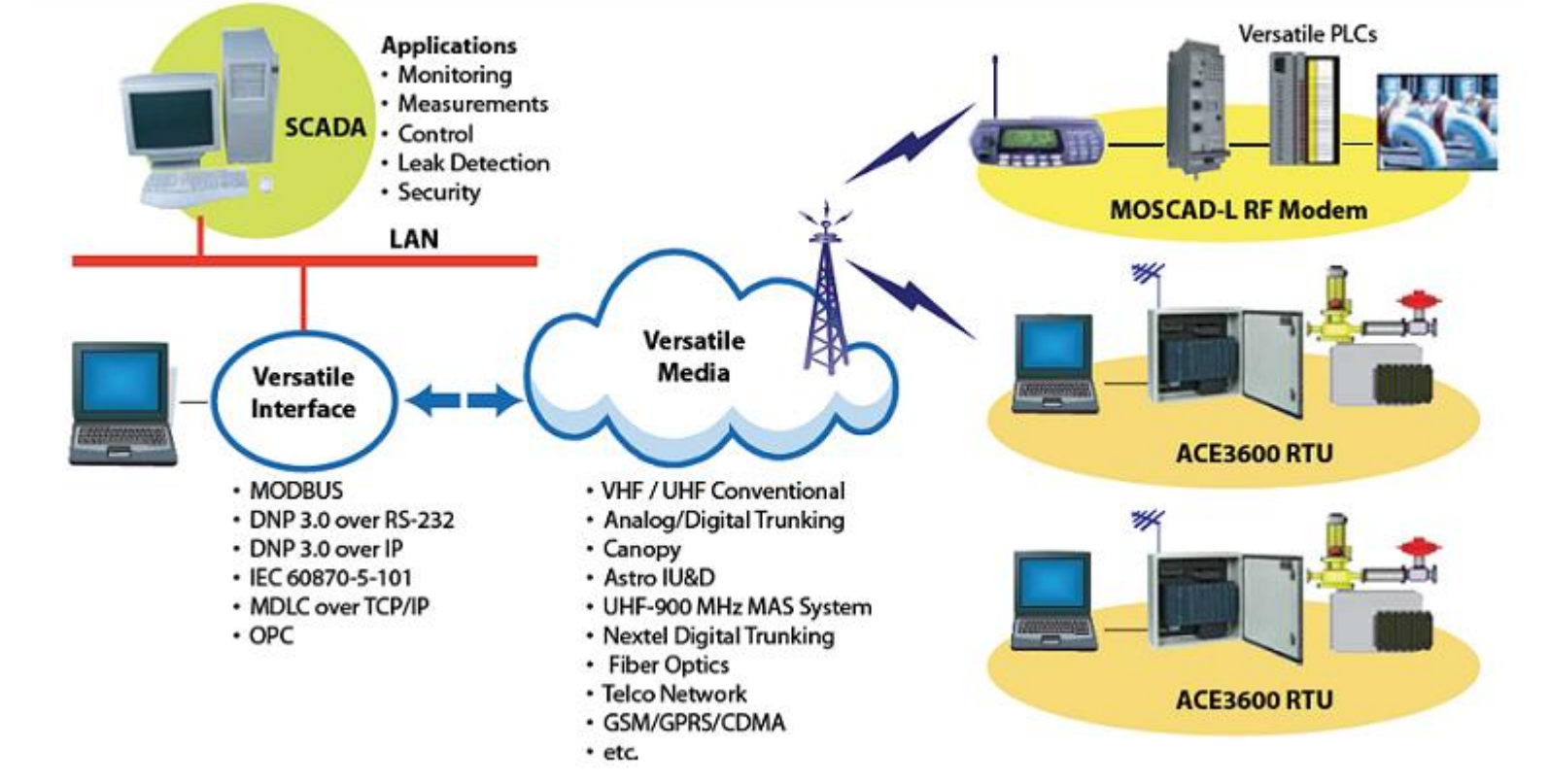
- IoT en la Industria
  - Infraestructuras Críticas monitorizadas en tiempo real por sistemas complejos, llamados sistemas **SCADA** (*Supervisory Control And Data Acquisition; Supervisión, Control y* Adquisición de Datos) ampliamente utilizados.



Riesgos de IoT

OWASP
The Open Web Application Security Project

- SCADA
  - La incorporación de Sensores
  - Sus sistemas empotrados.



Riesgos de IoT

OWASP
The Open Web Application Security Project

- **State-sponsored cyber operations**

Estados Unidos contra China, un conflicto no declarado pero evidente. Guerra cibernética contra estados enemigos como Irán y Correa del Norte.

WorldTribune.com | WINDOW ON THE REAL WORLD

HOME | AFRICA / EUROPE | COLUMNISTS | RECENT HITS | INTEL BRIEF | MIDEAST | NE ASIA

China's top prioity

Obama's inner circle

World Tribune TV

Find it at Localpages.com
localpages.com
Looking for colon cleansing foods and drinks? Find it at Localpages.com

Find it at Localpages.com

Tuesday, August 13th, 2013 | Posted by WorldTribune.com

Chinese military attempted to hack Missouri water plant

Special to WorldTribune.com

East-Asia-Intel.com

The fear of U.S. infrastructure being vulnerable to Chinese military hacking attacks was further intensified after a tech publication revealed that the Chinese military attempted to hack a water plant in Missouri.

Of all the cyber attacks tracked by a U.S. security company, half originated in China.

The report from the online tech journal Quartz concluded that "new research confirms one of the scarier possibilities: that the Chinese army is going after critical U.S. infrastructure."

In a feature story, Quartz asked "If the Chinese army is trying to hack a Missouri water plant, what else is it infiltrating?"

The article cited the research conducted by a security company called Trend Micro, which uses an elaborate system of tricks to track sophisticated electronic "honeypots" set up in a dozen foreign countries.

Fuente: http://www.worldtribune.com

Ciber Guerras nos afectaran

OWASP
The Open Web Application Security Project

- Los tipos de armas utilizadas son las mismas herramientas y tipos de ataques utilizados en la ciberseguridad en general, pero enfocados a un estado o nación. Se tienen:
- Herramientas usadas en ataques:
  - Botnet’s (ataques programados desde redes internas)
  - Gusanos y Troyanos
- Tipos de ataques
  - Ataques de denegación de servicios – DoS
  - Envenenamiento DNS
  - Ingeniería Social
  - Data Gathering (apuntado a la obtención de la información de un blanco)
  - Espionaje informático, capturando o remplazando paquetes: Sniffers y Spyware.
- Herramientas usadas en defensa
  - Honey Pot´s y Honey Net´s (señuelos)
  - Monitores y filtros de tráfico: IDS, IPS y Firewalls

Ciber Guerras

OWASP
The Open Web Application Security Project

Blancos en la ciberguerra

Los blancos de una ciberguerra son:

- Sistemas de comunicación
- Sistemas Bancarios.
- Sistemas gubernamentales o diplomáticos
- Sistemas de SCADA.
- Sistemas de Servicios Básicos.
- Sistemas Militares.
- Personal militar, gubernamental o diplomático, usuarios en general involucrados con los anteriores sistemas.

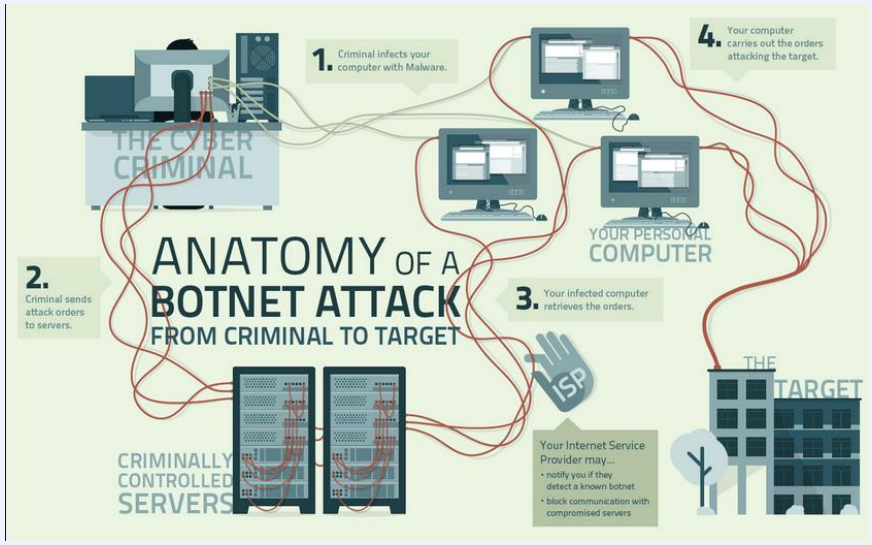
Cuantas cosas …

OWASP
The Open Web Application Security Project

- *Thingbotnet (Botnet* de las Cosas).

Proofpoint discovered more Than 750,000 Phishing and SPAM Emails Launched From "Thingbots" Including Televisions, Fridge

Recently security researchers from *Proofpoint* uncovered a cyber attack against the Internet of Things (IoT), more than 100,000 Refrigerators, Smart TVs and other smart household appliances have been hacked to send out 750,000 malicious spam emails.



http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

- **Ideological and political extremism (hacktivism)**

Grupo activistas:
LulzSec y Anonymous

U.S. SOPA legislation

Stop Online Piracy Act

Cyber Adversaries

Fuente:http://www.cso.com.au/article/564611/2015-social-engineering-survival-guide/

A diferencia de los verdaderos criminales, a los hackers les encanta el anonimato que Internet les da por lo que pueden esconderse detrás de cualquier cosa

Ellos pueden esconderse detrás de un nombre; usan **seudónimos**.

Donde están?

OWASP
The Open Web Application Security Project

Facebook sets up 'dark web' link to access network via Tor

By Dave Lee
Technology reporter, BBC News

3 November 2014 | Technology

Facebook's Tor support means users' traffic remains in the anonymising network

Como muestra un botón

OWASP
The Open Web Application Security Project

Ataques a celebridades: Las personas en general están en riesgo, como en el caso de la ***Miss Teen USA Cassidy Wolf***, que hackeron su cámara web, para tomar imágenes de su privacidad.

NEWS. CONTROVERSY. OPINION.
OPPOSING VIEWS

September 5, 2013 LOGIN | SIGN UP FOLLOW

Enterprise Collaboration:
The How-To Guide to Unified Communicati
Download the eBook

HOME POLITICS ENTERTAINMENT SPORTS HEALTH RELIGION SOCIETY TE

Home » Society » Crime » Miss Teen USA Cassidy Wolf's Webcam Hacked, Nude Pictures Taken (Video)

SOCIETY

Miss Teen USA Cassidy Wolf's Webcam Hacked, Nude Pictures Taken (Video)

Share this with a friend 1 Recommend 2 Tweet Follow us and never miss a story! 78k Like

By Michael Allen, Thu, August 29, 2013

Cassidy Wolf, who was crowned Miss Teen USA earlier this month, says that the webcam on her computer was hacked and someone took nude pictures of her without her knowledge.

The hacker then allegedly tried to extort sexual favors from the 19 year old in exchange for not leaking the photos.

"I was terrified. I started screaming, bawling my eyes out. I was on the phone with my mom, and I felt helpless because I wasn't sure what to do, so it was a very terrifying moment," Wolf told the "Today" show (video below).

"You would never think somebody would be watching you in your room and this guy had been. The thought of that just gave me nightmares."

The alleged incident happened four months before Wolf won Miss Teen USA.

"It happened to me when I was a normal girl and it can happen to anybody. The message is to tell somebody. The longer it goes on, the worse it will get, so if you can get the word out. Talk to the authorities.'" said the Temecula, California teen.

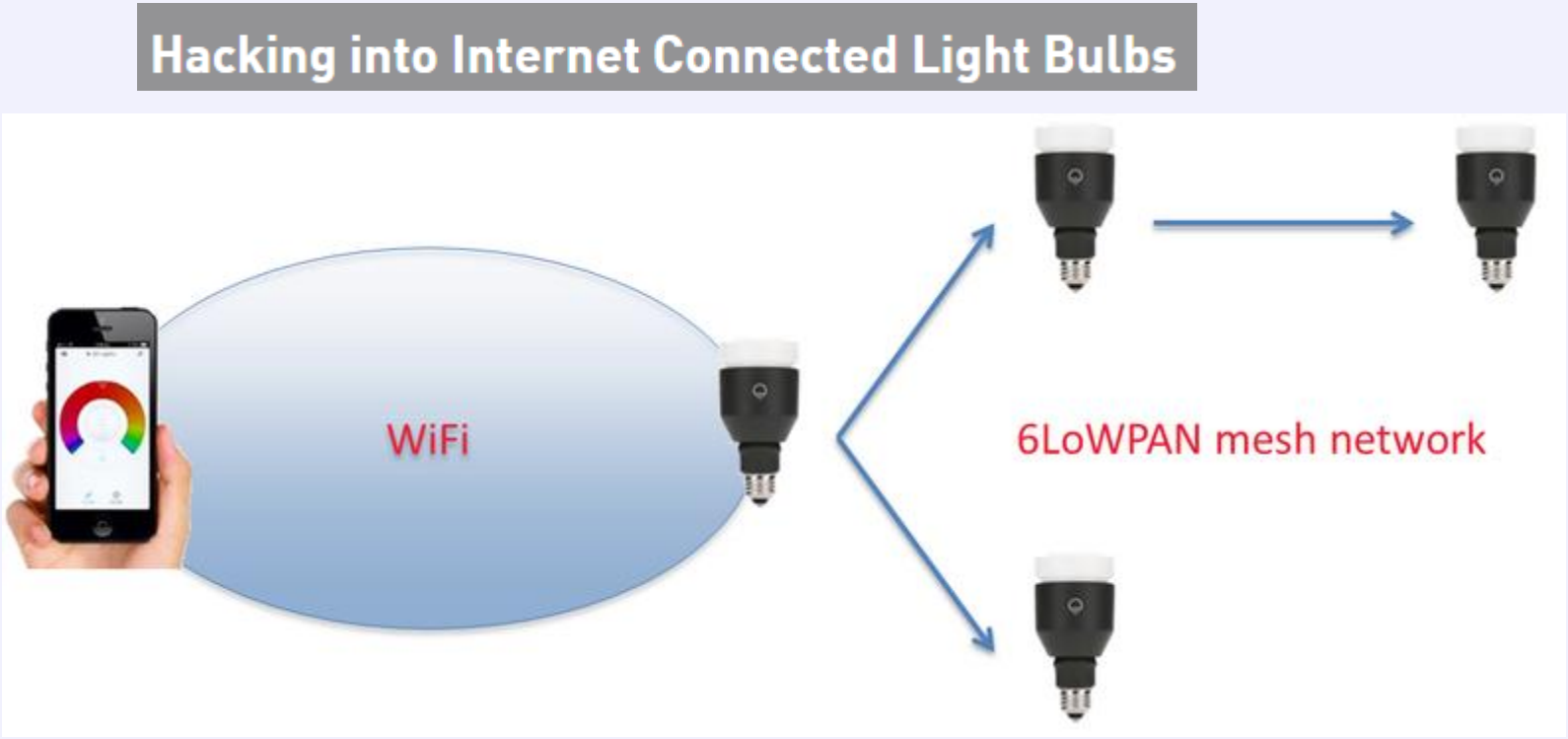
Casos

OWASP
The Open Web Application Security Project

Casos

OWASP
The Open Web Application Security Project

- En la domótica



http://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/

Casos

OWASP
The Open Web Application Security Project

- ***Karotz,*** *"smart rabbit".*

El 2013 se descubrieron vulnerabilidades, *Black Hat 2013 en Estados Unidos*

https://media.blackhat.com/us-13/US-13-Crowley-Home-Invasion-2-0-WP.pdf

Casos

OWASP
The Open Web Application Security Project

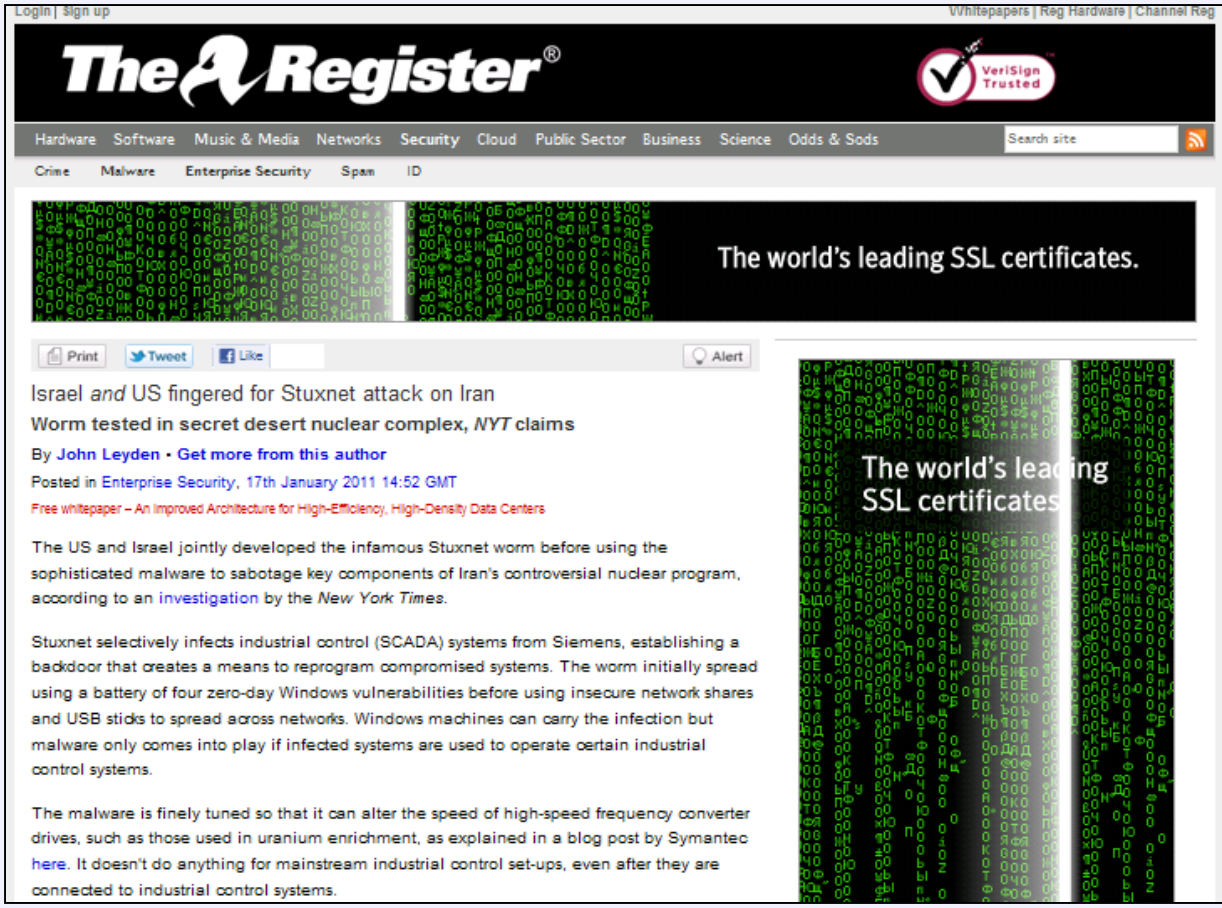
- **reloj *Pebble***

- El reloj *Pebble es un smartwacth* que se puede enlazar a un *smartphone, mostrando* por su pantalla las notificaciones recibidas. La vulnerabilidad podía provocar **condiciones de denegación de servicio, así como en algunos casos borrar la memoria del dispositivo** (aplicaciones, configuraciones, notas, mensajes, etc.). El ataque únicamente consistía en enviar 1500 mensajes de Whatsapp al dispositivo en un periodo de 5 segundos.

http://thehackernews.com/2014/08/remote-attack-could-damage-your-pebble.html

Los sistema SCADA

- El 2010 en Irán, **Stuxnet** invade las centrifugadoras del programa de enriquecimiento de uranio, se culpa a España del ataque.



Login | Sign up

Whitepapers | Reg Hardware | Channel Reg

The Register®

VeriSign Trusted

Hardware Software Music & Media Networks Security Cloud Public Sector Business Science Odds & Sods

Search site

Crime Malware Enterprise Security Spam ID

The world's leading SSL certificates.

Print Tweet Like Alert

Israel *and* US fingered for Stuxnet attack on Iran

Worm tested in secret desert nuclear complex, *NYT* claims

By John Leyden • Get more from this author

Posted in Enterprise Security, 17th January 2011 14:52 GMT

Free whitepaper – An Improved Architecture for High-Efficiency, High-Density Data Centers

The US and Israel jointly developed the infamous Stuxnet worm before using the sophisticated malware to sabotage key components of Iran's controversial nuclear program, according to an investigation by the *New York Times*.

Stuxnet selectively infects industrial control (SCADA) systems from Siemens, establishing a backdoor that creates a means to reprogram compromised systems. The worm initially spread using a battery of four zero-day Windows vulnerabilities before using insecure network shares and USB sticks to spread across networks. Windows machines can carry the infection but malware only comes into play if infected systems are used to operate certain industrial control systems.

The malware is finely tuned so that it can alter the speed of high-speed frequency converter drives, such as those used in uranium enrichment, as explained in a blog post by Symantec here. It doesn't do anything for mainstream industrial control set-ups, even after they are connected to industrial control systems.

The world's leading SSL certificates

Casos

OWASP
The Open Web Application Security Project

Drones del pentágono.

www.ikerjimenez.com/noticias/piratean-aviones-espias-no-tripulados/

'PIRATEAN' AVIONES ESPÍAS EE.UU.

ikerjimenez.com
Periodismo de lo desconocido

Noticias en ikerjimenez.com

Inicio | Titulares RSS | Escríbenos

«Piratean aviones no tripulados de EE.UU.»

Los insurgentes iraquíes han usado de manera frecuente un software de bajo coste y fácil de encontrar en el mercado para 'piratear' los datos transmitidos por los aviones no tripulados de Estados Unidos, según ha informado el Wall Street Journal.

Escucha esta noticia

18 diciembre 2009.- Citando a funcionarios de defensa e inteligencia, el diario desvela que los insurgentes apoyados por Irán han empleado programas como SkyGrabber - disponible en Internet por menos de 26 dólares - para interceptar estos aviones que EE.UU. utiliza de manera frecuente en la zona para atacar objetivos insurgentes y talibanes.

Esta práctica fue descubierta en julio de 2009 cuando los militares de EE.UU. hallaron en el ordenador portátil de un insurgente archivos de vídeo de los vehículos aéreos no tripulados. Encontraron "días y horas y horas de pruebas", según ha desvelado la fuente al periódico, que ha advertido que esta práctica "se ha convertido en parte de sus herramientas".

Gary McKinnon, el 'hacker del Pentágono'

Gary McKinnon se describe a si mismo como un inofensivo programador de computación, obsesionado

Exceso de Confianza

Fuente: http://shukanshah26.blogspot.com/2014/03/cyber-security.html

Think Like a Hacker, Defend Like a Ninja

Proactivo

Capacitación

OWASP
The Open Web Application S

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firware
10. Poor Physical Security

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

Capacitación

OWASP
The Open Web Application Security Project

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29

Top 10 IoT Vulnerabilities (2014) Project

The OWASP Top 10 IoT Vulnerabilties 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

What is the Top 10 IoT Vulnerabiltiies Project?

The Top 10 IoT Vulnerabilities Project provides:

- A list of the top 10 internet of things vulnerabilities

Project Leaders

- Daniel Miessler
- Craig Smith

Related Projects

- OWASP Mobile Security
- OWASP Web Top 10

Email List

Mailing List

Capacitación

OWASP
The Open Web Application Security Project

Top 10 2014-I5 Privacy Concerns

Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not being properly protected or is being collected unnecessarily. Attack could come from external or internal users.	Privacy concerns generated by the collection of personal data in addition to the lack of proper protection of that data is prevalent. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.		Collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?

Capacitación

OWASP
The Open Web Application Security Project

Does My Device Present Privacy Concerns?

Checking for Privacy Concerns includes:

- Identifying all data types that are being collected by the device, its mobile application and any cloud interfaces
- The device and it's various components should only collect what is necessary to perform its function
- Personally identifiable information can be exposed when not properly encrypted while at rest on storage mediums and during transit over networks
- Reviewing who has access to personal information that is collected
- Determining if data collected can be de-identified or anonymized
- Determining if data collected is beyond what is needed for proper operation of the device (Does the end-user have a choice for this data collection?)
- Determining if a data retention policy is in place

How Do I Prevent Privacy Concerns?

Minimizing privacy concerns requires:

1. Ensuring only data critical to the functionality of the device is collected
2. Ensuring that any data collected is of a less sensitive nature (i.e., try not to collect sensitive data)
3. Ensuring that any data collected is de-identified or anonymized
4. Ensuring any data collected is properly protected with encryption
5. Ensuring the device and all of its components properly protect personal information
6. Ensuring only authorized individuals have access to collected personal information
7. Ensuring that retention limits are set for collected data
8. Ensuring that end-users are provided with "Notice and Choice" if data collected is more than what would be expected from the product
9. Ensuring the role based access control/authorization to the collected data/analyzed data is applied
10. Ensuring that the analyzed data is de-identified

Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer

Example Attack Scenarios

Scenario #1: Collection of personal data.

```
Date of birth, home address, phone number, etc.
```

Scenario #2: Collection of financial and/or health information.

```
Credit card data and bank account information.
```

In the cases above, exposure of any of the data examples could lead to identity theft or compromise of accounts.

References

OWASP

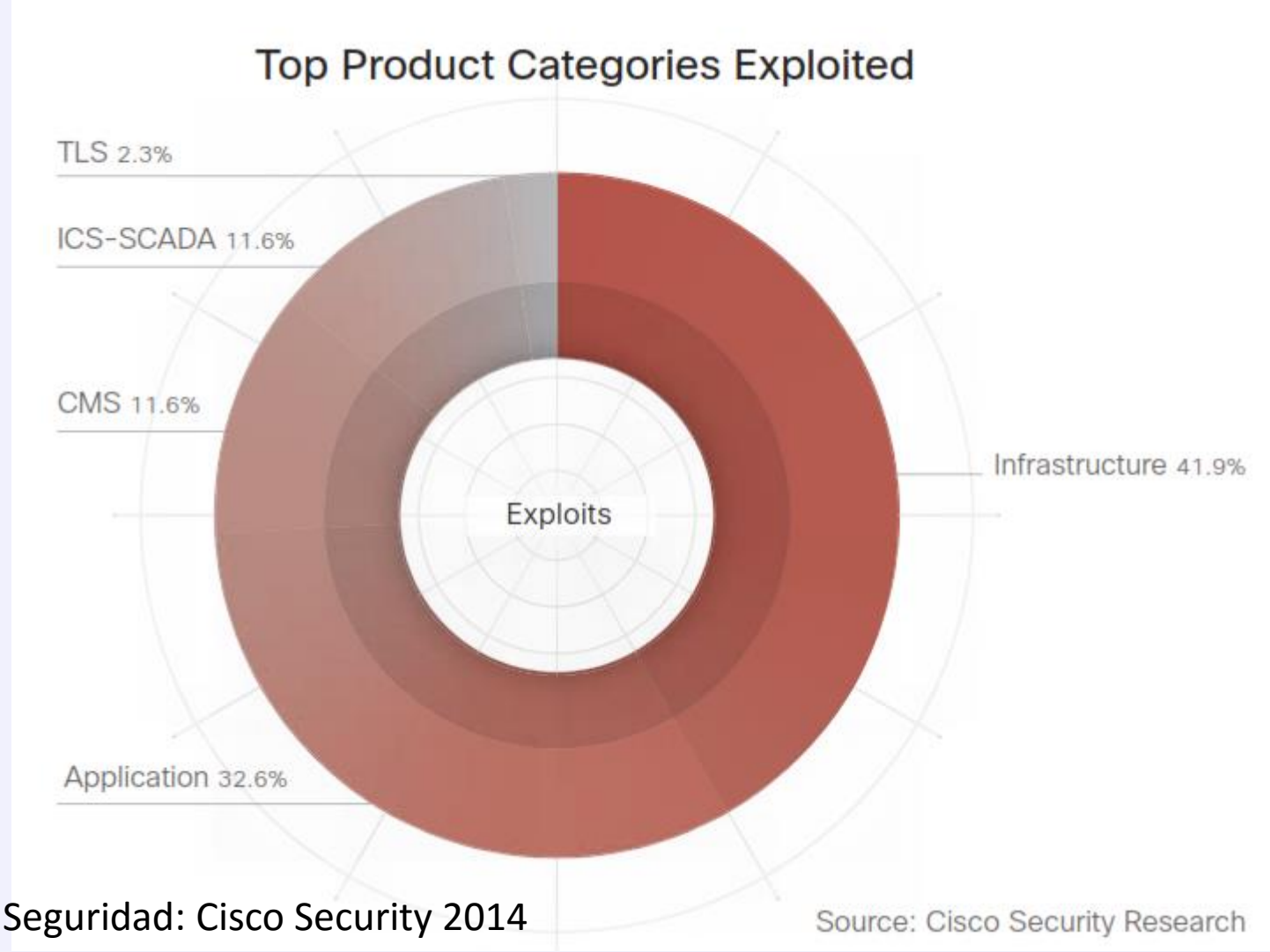
Top 10 2013-A6-Sensitive Data Exposure

External

FTC: Careful Connections: Building Security in the Internet of Things

FTC: Internet of Things, Privacy & Security in a Connected World

Conclusión



Reporte de Seguridad: Cisco Security 2014

Conclusión

OWASP
The Open Web Application Security Project

- IoT cabio en panorama de la seguridad
- Java sigue siendo el lenguaje más explotado
- Los hackers se centran en las vulnerabilidades más recientes.
- Mucha publicidad, más malware
- El malvertising prevalece.

Conclusión

OWASP

Fuente: https://blog.kaspersky.es/internet-de-las-cosas-problemas-de-seguridad/1045/

Recomendaciones

OWASP
The Open Web Application Security Project

- Identificación y control del uso de servicios en la nube o cloud services.
- Uso de aplicaciones móviles para dispositivos IoT
  - Apps confiables
  - Limitar accesos a otras aplicaciones
- Buenas prácticas y cultura de seguridad
  - Cuidado con la ingeniería social (phising)
  - Uso de diferentes credenciales, para diferentes servicios (email, redes sociales, etc.)
  - Tratar de usar más de un método de autenticación (SMS móvil)

Recomendaciones

OWASP
The Open Web Application Security Project

- Además de la precaución, la **formación y la concienciación son la principal** salvaguarda en estos casos, ya que otorgan al usuario la capacidad de identificar las estafas y reaccionar adecuadamente contra ellas.
  - Mantener campañas de concienciación y cursos para facilitar cultura de seguridad de los usuarios.

http://www.csirtcv.gva.es/es/paginas/descargas-informes-csirt-cv.html

Las Ciberseguridad es responsabilidad de quién?

OWASP
The Open Web Application Security Project

- Generamos cultura de seguridad de los usuarios.

Feria preventiva de la seguridad ciudadana

OWASP
The Open Web Application Security Project

Sucre – 29/08/2015

Feria preventiva de la seguridad ciudadana

OWASP
The Open Web Application Security Project

Sucre – 29/08/2015

OWASP
The Open Web Application Security Project

Sucre – 29/08/2015

Feria preventiva de la seguridad ciudadana

OWASP
The Open Web Application Security Project

Sucre – 29/08/2015

Referencias

- Informe: “Internet of Things Research Study”. Fuente: HP FORTIFY - http://fortifyprotect.com/HP_IoT_Research_Study.pdf

- Web: “OWASP Internet of Things Top Ten Project”. Fuente: OWASP - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

- Informe: “Internet de las cosas. Como la próxima evolución de Internet lo cambia todo” Fuente: Cisco - http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

- Artículo: “’Hackers’ chinos logran vulnerar la seguridad del coche Tesla” Fuente: elconfidencial.com - http://www.elconfidencial.com/tecnologia/2014-07-21/hackers-chinos-logran-vulnerar-la-seguridad-del-coche-tesla_165313/

- Artículo: “Hacking into Internet Connected Light Bulbs” Fuente: Context - http://contextis.co.uk/resources/blog/hacking-internet-connected-light-bulbs/

Referencias

OWASP
The Open Web Application Security Project

- Security for the 'Internet of Things' - http://www.epanorama.net/newepa/2014/03/31/security-for-the-internet-of-things/comment-page-1/
- Estudio annual de coches conectados - http://www.iabspain.net/wp-content/uploads/downloads/2014/07/Informe-coches-conectados-2014.pdf
- Artículo: "IoT: How I hacked my home." Fuente: Securelist - http://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/
- Artículo: "Remote Attack Coud Format Your Pebble Smartwatch Easily" Fuente: The Hacker News - http://thehackernews.com/2014/08/remote-attack-could-damage-your-pebble.html
- Ponencia "Home Invasion 2.0: Attacking Network-Connected Embedded Devices" Fuente: BlackHat - https://media.blackhat.com/us-13/US-13-Crowley-Home-Invasion-2-0-WP.pdf

OWASP
The Open Web Application Security Project

Ing. Marco Antonio. Arenas Porcel

Email:marcoap@usfx.edu.bo
:markituxfor@gmail.com

Fuente:
http://programacion.net/articulo/consecuencias_de_privacidad_en_el_internet_de_las_cosas_998

PREGUNTAS???

Email:marcoap@usfx.edu.bo
:markituxfor@gmail.com