Ciberseguridad en el Internet de las Cosas

Administración de Sistemas y Seguridad

Pablo Valenzuela Álvarez (pvalenzuela@correo.ugr.es)

Índice de Contenidos

- Introducción
- Desafíos de seguridad en IoT
- Problemas de seguridad en empresas
- Conclusión

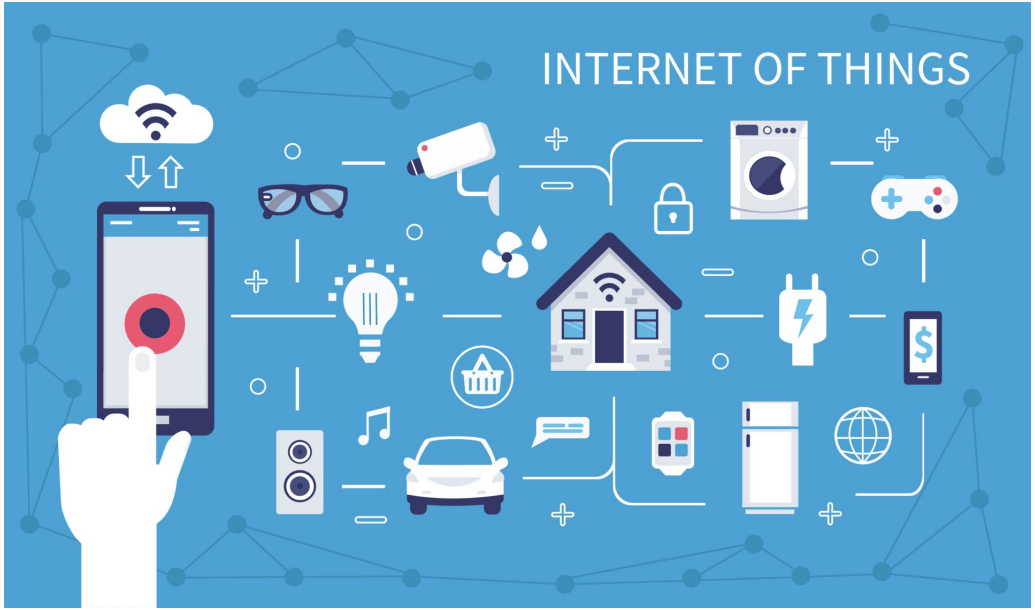
INTRODUCCIÓN

IoT y su importancia en el mundo actual

El término **IoT** (Internet de las Cosas) se refiere a objetos físicos equipados con sensores, capacidad de procesamiento, software, etc, y que tienen la capacidad de recibir o transmitir información a través de redes inalámbricas y con una mínima intervención humana.

INTRODUCCIÓN

IoT y su importancia en el mundo actual



En el mercado actual, la tecnología IoT se asocia principalmente con productos relacionados con el concepto de “**hogar inteligente**”.

Introducción

IoT y su importancia en el mundo actual

La proliferación de este tipo de productos ha levantado preocupaciones, especialmente en lo que respecta a la privacidad y la seguridad.

La industria y los gobiernos han comenzado a tomar medidas para hacer frente a estas preocupaciones, desarrollando **normas** y **marcos regulatorios**.

INTRODUCCIÓN

Por qué es importante la seguridad en IoT?

El IoT abarca un gran conjunto diversificado de elementos que generan una ingente cantidad de información sobre **datos** de usuarios, equipos, maquinaria, etc. Estos datos quedan expuestos y son propensos a ser robados.

Si a esto le sumamos el crecimiento exponencial previsto en el uso de los dispositivos IoT, la necesidad de proteger los dispositivos y las conexiones, resulta vital.

Desafíos de Seguridad en IoT

Los ataques de ciberseguridad en el entorno IoT pueden amenazar los procesos, la comunicación, el flujo de datos y su almacenamiento.

En general, podemos clasificar los ataques en distintas categorías:

- La **suplantación de identidad**.
- La **revelación de información**.
- La **provocación de alteraciones**.
- La **denegación de servicio**.
- La **elevación de privilegios**.

Desafíos de Seguridad en IoT

Vulnerabilidad en el software

Una de las principales vulnerabilidades tiene que ver con las **credenciales** de administración. Algunos dispositivos no permiten modificar las credenciales que por defecto, lo que supone un grave riesgo ya que generalmente estas son de dominio público. Las credenciales de acceso embebidas o la existencia de cuentas con privilegios utilizadas por el fabricante y no documentadas suponen el mismo riesgo.

Además, los dispositivos IoT no están exentos de sufrir otro tipo de vulnerabilidades como el **desbordamiento de buffer**, **condiciones de carrera**, **denegaciones de servicio**, etc.

Desafíos de Seguridad en IoT

Ataques sobre contraseñas y credenciales

Muchos dispositivos IoT vienen configurados con contraseñas por defecto muy inseguras, muchos usuarios no la cambian.

Este tipo de contraseñas exponen al dispositivo a los ataques por **fuerza bruta**, es decir. En este tipo de ataques se suelen usar diccionarios o las llamadas **tablas arcoiris**.

Desafíos de Seguridad en IoT

Acceso físico al dispositvo

Ya sea en **interior** o en **exterior**, los dispositivos IoT siempre son susceptibles a recibir ataque mediante el acceso físico.

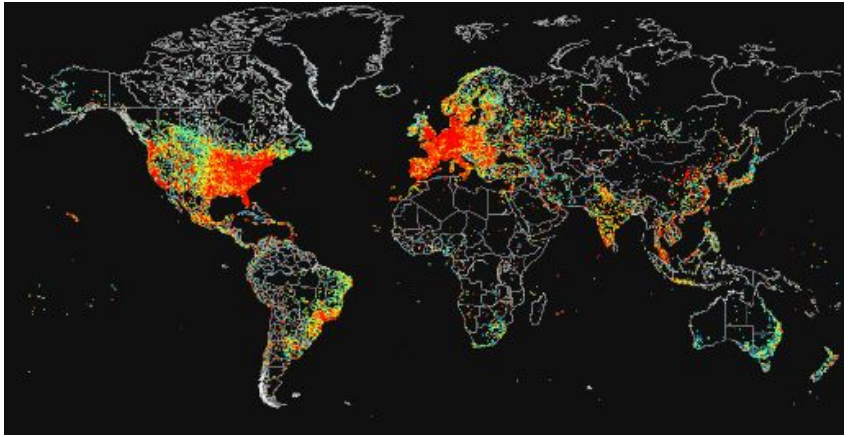
Desafíos de Seguridad en IoT

Conexión a internet

Existen buscadores como **Shodan**, con el que puedes encontrar dispositivos y servicios accesibles vía internet.

Cuando un ciberdelincuente accede a múltiples dispositivos, esta red se denomina **botnet**, donde cada dispositivo es un bot o zombi.

Con este tipo de redes se pueden efectuar acciones maliciosas como robar información, difundir **spam**, **malware** o realizar ataques **DDoS**.



Mapa de dispositivos IoT (enlace)

Desafíos de Seguridad en IoT

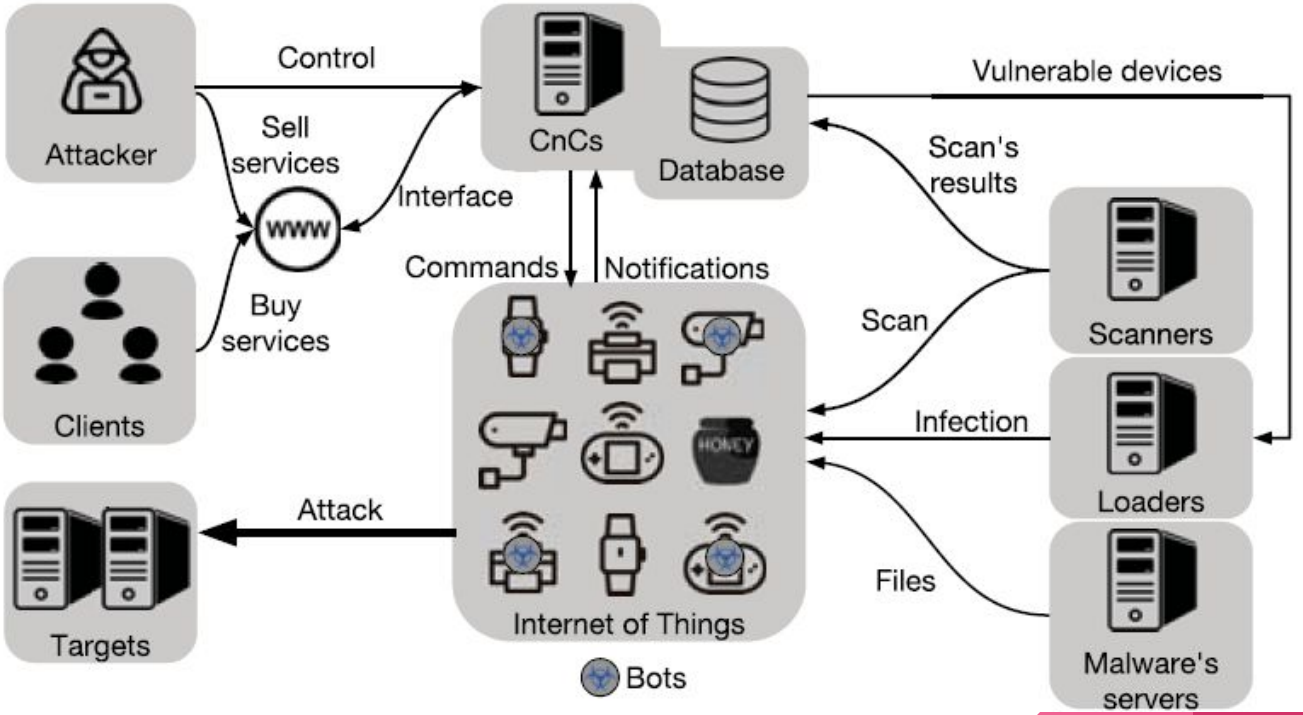
Ataques DDoS

Los dispositivos secuestrados se utilizan como base de ataque para infectar más “cosas” o esconder una actividad maliciosa. Estos ciberataques consisten en saturar un servicio enviando **peticiones masivas** de conexión al mismo tiempo.

Aunque este tipo de amenaza suele dirigirse hacia las organizaciones, también pueden afectar a hogares inteligentes.

Desafíos de Seguridad en IoT

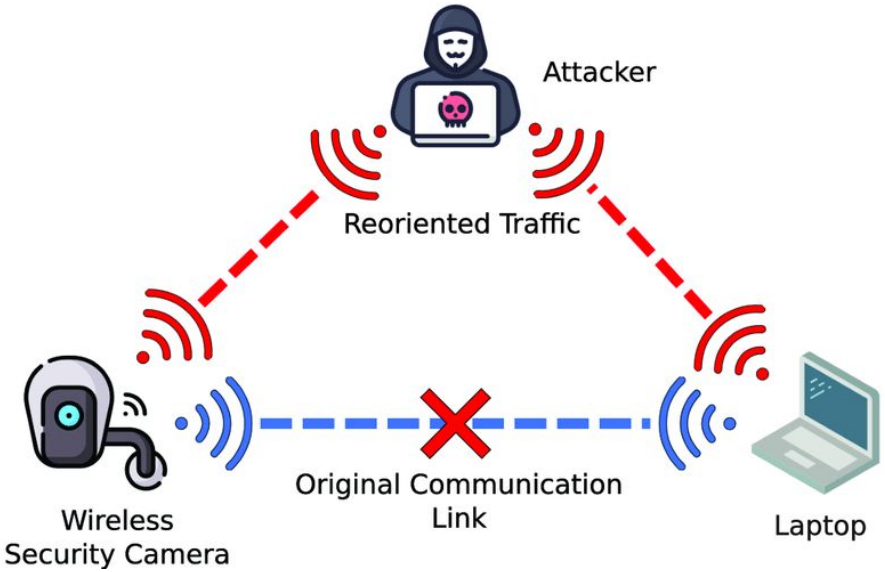
Malware y ransomware



Procedimiento de ataque botnet IoT (enlace)

Desafíos de Seguridad en IoT

Interceptación de datos de tránsito



Ejemplo de MitM en una cámara de seguridad (enlace)

Si un ciberdelincuente consigue acceso a la red local o LAN donde se encuentra el dispositivo o el receptor de información, podría acceder a esta o modificarla. A este tipo de ciberataques se les conoce como Hombre en el medio (**MitM**).

- **MitM pasivo**
- **MitM activo**

Desafíos de Seguridad en IoT

Ataque basados en hardware

Muchos dispositivos IoT no aplican los principios de **mínimo privilegio**. Aplicándolos, el dispositivo proporcionaría una funcionalidad básica, haciendo que cualquier uso inseguro sea una decisión consciente del usuario.

Sin embargo, incorporar este tipo de seguridad por defecto puede ser un incordio para usuario, que encontrará maneras de saltarsela.

Algunos fabricantes pueden dejar habilitados servicios o herramientas que el aparato o el usuario no necesite para un uso normal. Cuantos más servicios estén instalados y habilitados, mayor será la probabilidad de que alguno de ellos sufra alguna vulnerabilidad.

Desafíos de Seguridad en IoT

Ataques a la plataforma de administración

Debido a su tamaño, muchos dispositivos no cuentan con elementos que permitan interactuar directamente con ellos. En su lugar, suelen utilizar **interfaces web** o **aplicaciones móviles**.

Si una de estas opciones cuenta con alguna vulnerabilidad o carece de las medidas de seguridad necesarias para evitar accesos no autorizados, los ciberdelincuentes podrían acceder a ella y controlar el dispositivo.

Desafíos de Seguridad en IoT

Ataques sobre la privacidad de los datos

La obtención de datos personales, historial médico, claves de cerraduras y cuentas bancarias, etc, puede ser utilizada por ciberdelincuentes para su propio beneficio o para venderla, comprometiendo así la privacidad y seguridad de los afectados.

Problemas de Seguridad en Empresas

Stuxnet (2010)

Stuxnet fue considerado el primer gusano en atacar sistemas de control industrial.

Su objetivo era el de sabotear los procesos de enriquecimiento de uranio del programa nuclear iraní.

Se estima que destruyó hasta **mil** máquinas centrifugadoras de la planta antes de ser descubierto.

Problemas de Seguridad en Empresas

Robo de información en la empresa Calpine (2013)

Los datos incluían planos detallados de la red y de 71 estaciones eléctricas, la ubicación precisa de dispositivos, diagramas de red y contraseñas de dispositivos.

Este robo de información permitió ataques posteriores como la infiltración en el sistema de una presa a través de un **módem**.

Problemas de Seguridad en Empresas

Botnet Mirai (2016)

Se cree que las interrupciones de funcionamiento en servicios como Twitter, Amazon, Spotify, Netflix, etc, en octubre de 2016 fueron debido al uso de esta botnet.

Mirai funcionaba escaneando Internet en busca de dispositivos IoT que se ejecutan con el procesador ARC (versión reducida de Linux), y **aprovechando la configuración por defecto** que permitirá acceso al dispositivo e infectarlo.

Problemas de Seguridad en Empresas

Botnet Persirai (2017)

Dirigía sus ataques hacia modelos de **cámaras IP** de distintos fabricantes. Se descubrió que había infectado a aproximadamente **120000** dispositivos a través de **Shodan**.

Explotando una vulnerabilidad hardware (protocolos Universal Plug & Play) los ciberdelincuentes accedían a las cámaras.

Problemas de Seguridad en Empresas

Malware VPNFilter (2018)

Se estima que este malware infectó a más de **medio millón** de enrutadores en cincuenta países.

Dicho malware actuaba como **MitM,** recopilando información, bloqueando tráfico de red y robando contraseñas.

Sus principales objetivos son ASUS, D-Link, Huawei, Ubiquiti, UPVEL y ZTE, así como los nuevos modelos de Linksys, MicroTik, Netgear y TP-Link.

Problemas de Seguridad en Empresas

Pirateo del Tesla Model X (2020)

Un experto en ciberseguridad aprovechó una vulnerabilidad del Bluetooth para clonar la llave y acceder al vehículo en apenas **90 segundos**.

Utilizando los últimos cinco dígitos del bastidor (visibles en el parabrisas) y un equipo de alrededor de 300$, el experto creó un algoritmo capaz de clonar la llave electrónica, pudiendo acceder y conducir el coche.

Problemas de Seguridad en Empresas

Pirateo de las cámaras de Verkada (2021)

Sufrió un ataque que expuso alrededor de **150,000** transmisiones en directo de sus cámaras.

Además del metraje en la cámara, el grupo de hackers afirma que consiguió también acceder a la lista completa de clientes de la empresa Verkada y su información financiera.

Conclusión

La seguridad en IoT no es una meta inalcanzable, sino más bien un proceso continuo que requiere atención constante.

- Mantener actualizado el dispositivo y el software que lo respalda.
- Educar, concienciar a usuario en temas de ciberseguridad.
- Segmentación de redes y uso de VPN.
- Cortafuegos, monitoreo constante.
- Involucrar a fabricantes, proveedores, usuarios y organismos reguladores.

Referencias

- “Internet de las cosas.” *Wikipedia*, enlace.
- “¿Qué es IoT y cómo está transformando nuestras vidas?” *Linkedin*, enlace.
- “Seguridad en IoT, riesgos y desafíos de la Internet de las Cosas.” *Redes & Telecom*, enlace.
- “Search Engine for the Internet of Everything.” *Shodan Search Engine*, enlace.
- “Ciberataque a metalúrgica en Alemania y la seguridad física en empresas.” *Seguridad digital*, enlace.
- “Iranian hackers infiltrated U.S. power grid, dam computers.” *CBC*, enlace.

Referencias

- “¿Qué es la botnet Mirai?” *Cloudflare*, enlace.
- “Botnet Mirai: ¿nuestros electrodomésticos pueden atacarnos?” *WeLiveSecurity*, enlace.
- “Persirai: nueva red botnet de IoT que infecta las cámaras IP | Redes&Telecom.” *Redes & Telecom*, enlace.
- “200.000 routers más podrían estár infectados por VPNFilter.” *RedesTelecom*, enlace.
- “Tesla Model X Has Flaw Allowing It to Be Hacked and Stolen.” *Car and Driver*, enlace.
- “Security startup Verkada hack exposes 150000 security cameras in Tesla factories, jails, and more.” *The Verge*, enlace.