
IMAX
BIG DRUG
GODZILLA ROAD
海賊とよばれた男
12.10
ROADSHOW
MARUHAN
TOHO CINEMAS
きんくら酒場
カラオケ
IDOL STAGE
Don Quijote

HACKING IoT

¿Quién soy?

MARTA BELTRÁN

- Profesora Titular de Universidad.
- Líneas de investigación principales: sistemas distribuidos, ciberseguridad y privacidad.
- Investigadora o directora en más de 15 proyectos de investigación. Más de 60 trabajos de investigación publicados.
- No suelo trabajar con sudadera con capucha negra (ni con bata blanca).
- Sólo me pongo gorro de lana cuando nieva.
- Nunca he penetrado en los sistemas del Pentágono.
- No tengo ninguna certificación de hacking ético.
- No desarrollo malware por la noche en un sótano.

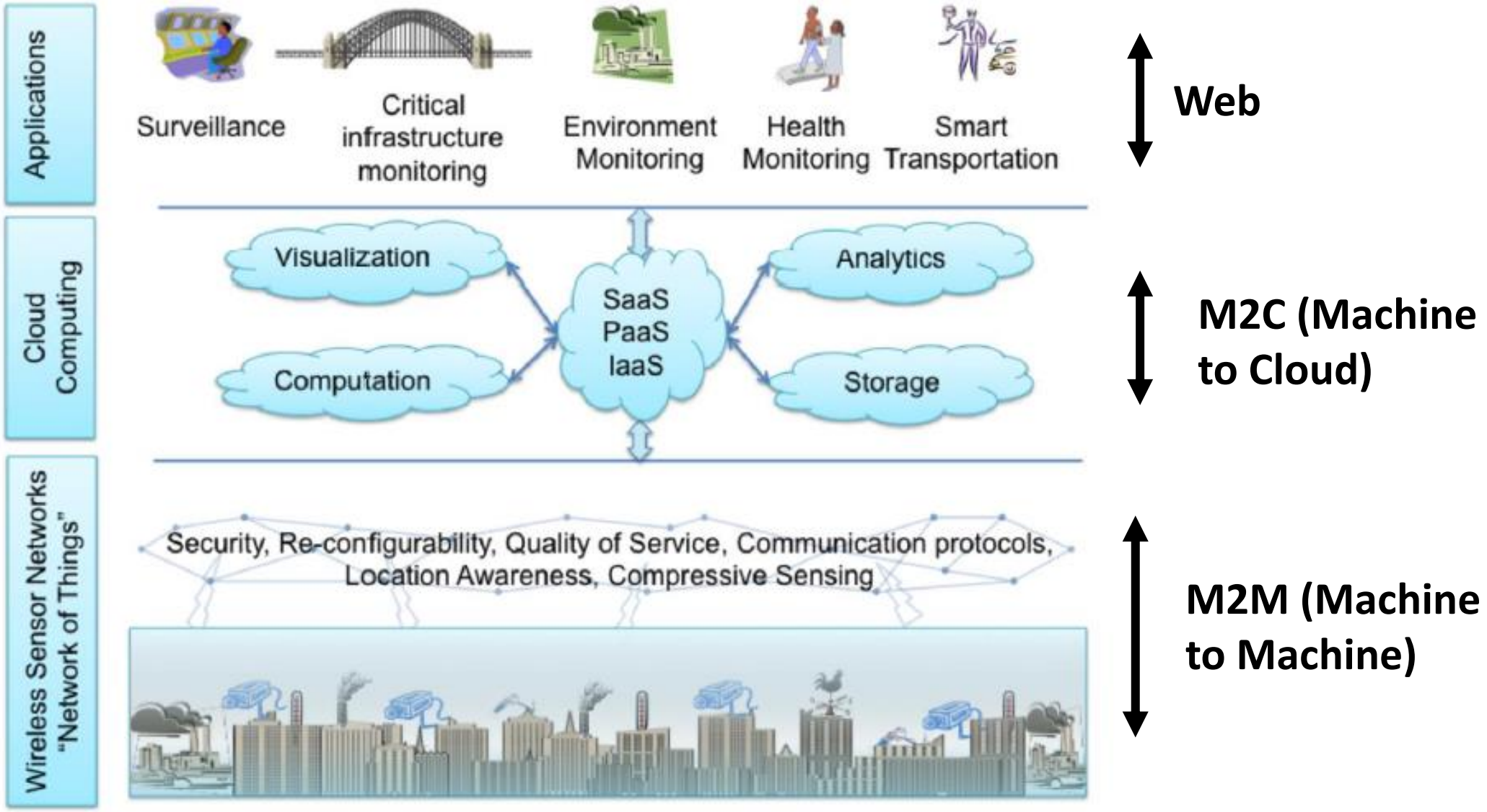
marta.beltran@urjc.es

@experiencia_T

¿De qué vamos a hablar con la próxima cerveza?

1. Introducción a IoT.
2. Superficie de ataque en IoT.
3. Trucos para hacer hacking en IoT.

The Internet of Things schematic representation (fuente: Gubbi, Buyya, Marusic,& Palaniswami, 2013)



The Internet of Things schematic representation (fuente: Gubbi, Buyya, Marusic,& Palaniswami, 2013)

1. Introducción a IoT

- Arquitecturas estándar (algunas, por lo que muy “estándar” no son…):
  - AIOTI High Level Architecture functional model.
  - FP7-ICT – IoT-A Architectural reference model.
  - NIST Network of Things (NoT).
  - ITU-T IoT reference model.
  - ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA).
  - ISACA Conceptual IoT Architecture.
  - oneM2M Architecture Model.
  - IEEE P2413 Standard for an Architectural Framework.

APIs

Aplicaciones

Integración

Almacenamiento, visualización y analítica

Persistencia e inteligencia

Protocolos

Comunicaciones y gestion de eventos

Dispositivos

Pasarelas

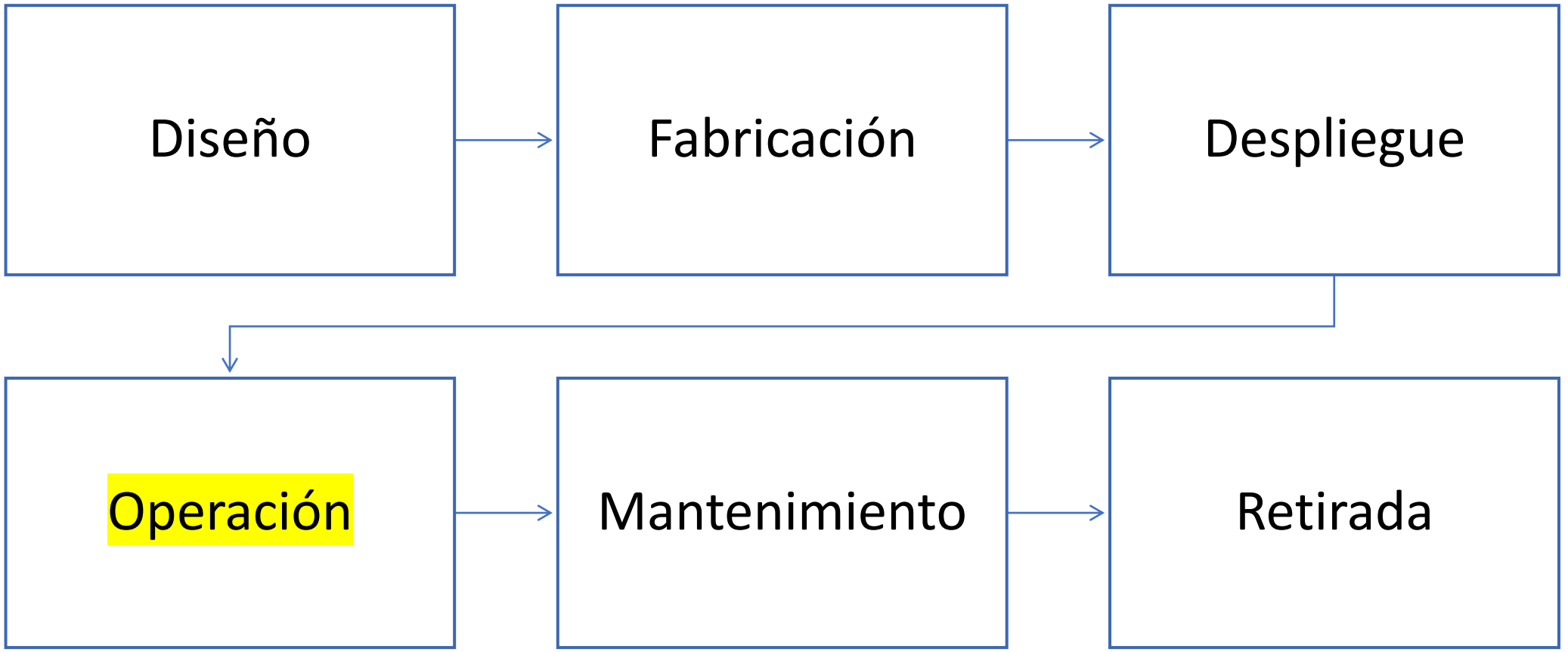
Interacción con la realidad

Sensores y WSN

Actuadores

Procesadores y controladores

1. Introducción a IoT



1. Introducción a IoT

Falta de concienciación y conocimientos

Fragmentación de estándares y regulación

Escasez de recursos y de energía

Black Hat USA 2015: The full story of how that Jeep was hacked

August 6, 2015

Recently we wrote about the now-famous hack of a Jeep Cherokee. At Black Hat USA 2015, a large security conference, researchers Charlie Miller and Chris Valasek finally explained in detail, how exactly that hack happened.

https://finitestate.io/blog/top-12-iot-exploits-of-2021-p1

TE STATE

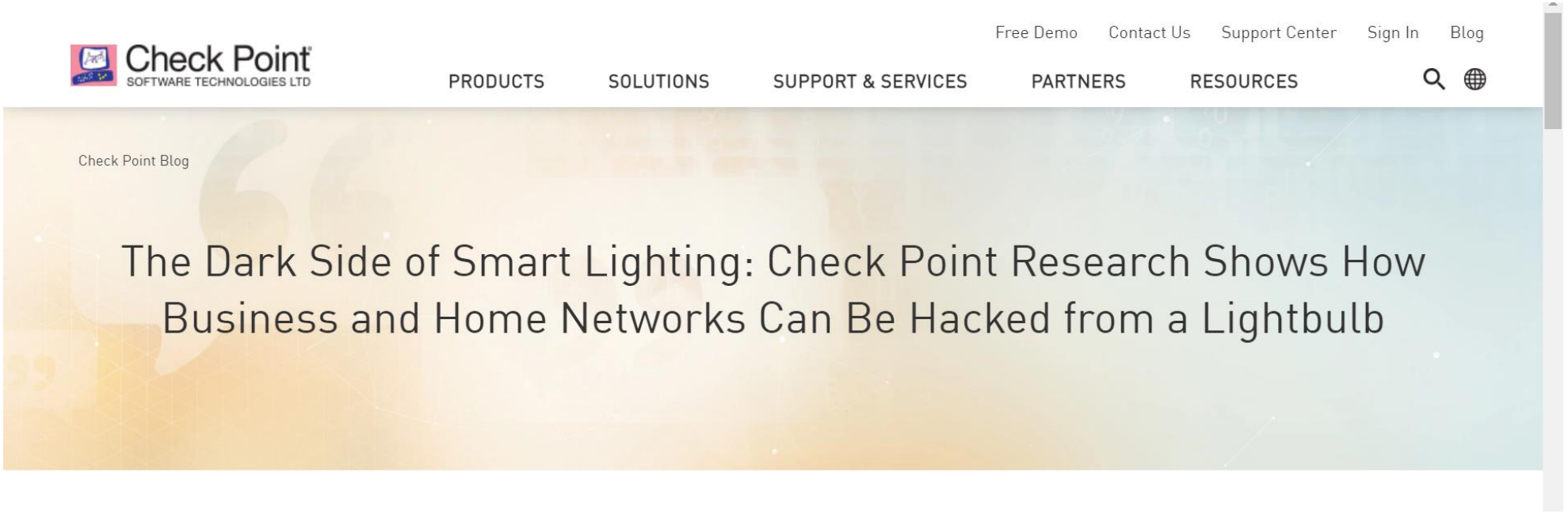
Product Solutions Resources Partners Company

this

Hotel Room Hacks: Vulnerabilities in Smart Rooms

The stakes are a bit lower on this one, although in the wrong hands these vulnerabilities could have been more disruptive. This story came out of one of the Black Hat sessions where Kya Supa, a security consultant at LEXFO, told everyone about the time he hacked his capsule hotel. Show of hands: Who has ever wanted to teach a noisy neighbor a lesson? Supa used the iPod touch given at check-in, meant to control his room, to start messing with the noisy neighbor that wouldn't pipe down.

In a presentation deck, Supa outlined exactly how he did it. He used six vulnerabilities and exploited them to take advantage of controls in other capsules. Via the iPod touch, guests could control the light, change the position of the adjustable bed, and control the ventilation fan. Supa's goal


Free Demo
Contact Us
Support Center
Sign In
Blog
Check Point
SOFTWARE TECHNOLOGIES LTD
PRODUCTS
SOLUTIONS
SUPPORT & SERVICES
PARTNERS
RESOURCES
Check Point Blog
The Dark Side of Smart Lighting: Check Point Research Shows How Business and Home Networks Can Be Hacked from a Lightbulb


US
JP
LIGHT COMMANDS
Laser-Based Audio Injection on Voice-Controllable Systems

FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson @selenalarson

January 9, 2017: 3:53 PM ET

Recommend 1.6K

Social Surge - What's Trending

Starbucks' Howard Schultz: Our

https://www.hipaajournal.com/vulnerabilities-philips-intellibridge-patient-information-center-efficia/

HIPAA JOURNAL

HIPAA Journal is th
and indepe

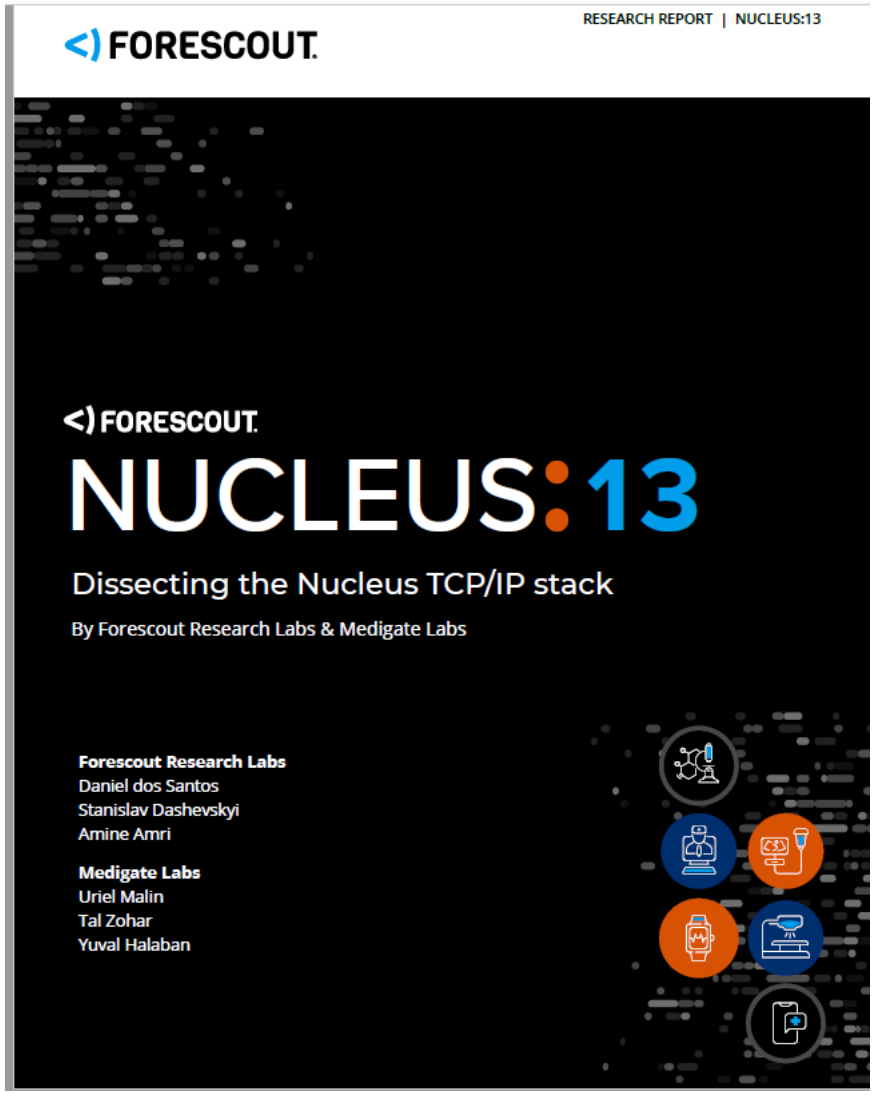
HIPAA Compliance News | Practical HIPAA Advice » | HIPAA Compliance Checklist | HIPAA Rules & Regulations » | About HIPAA Journal

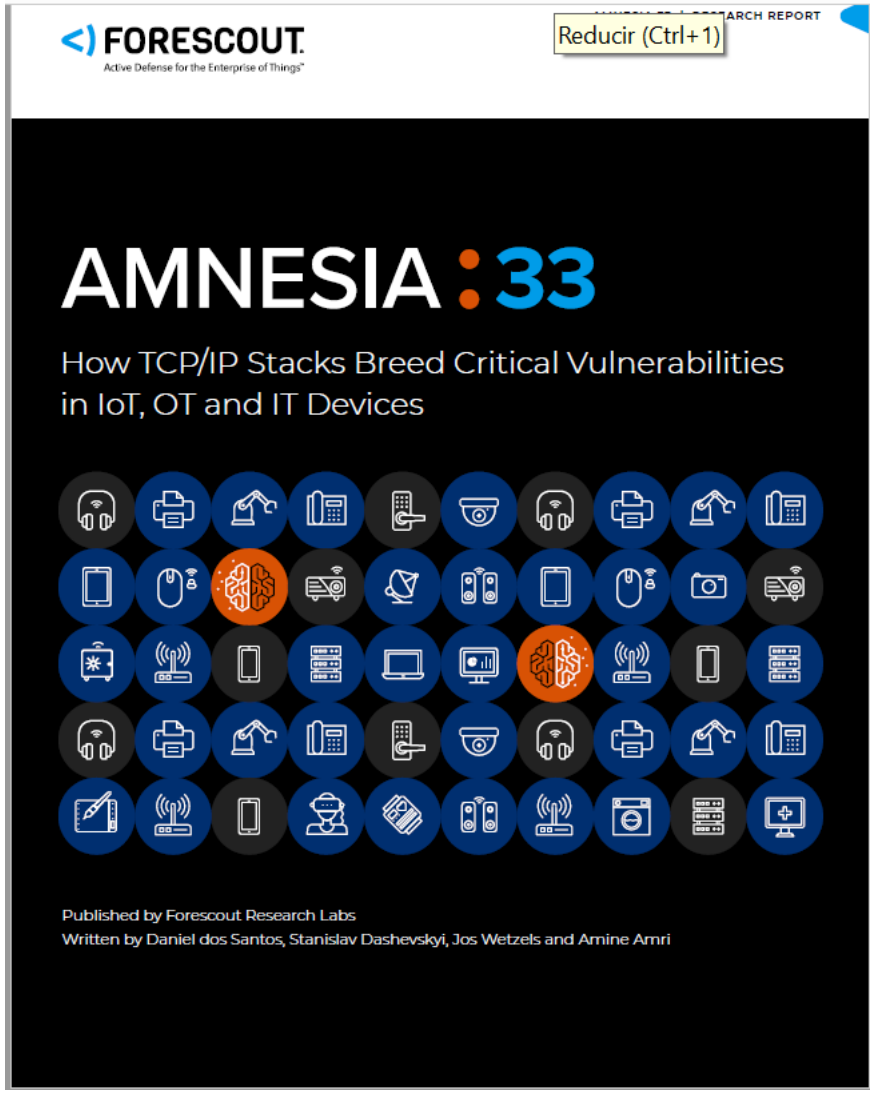
Vulnerabilities Identified in Philips IntelliBridge, Patient Information Center and Efficia Patient Monitors

Posted By HIPAA Journal on Nov 19, 2021

Five vulnerabilities have been identified that affect the IntelliBridge EC 40 and EC 80 Hub, Philips Patient Information Center iX, and Efficia CM series patient monitors.

IntelliBride EC 40 and EC 80 Hub


FORESCOUT
RESEARCH REPORT | NUCLEUS:13
FORESCOUT
NUCLEUS:13
Dissecting the Nucleus TCP/IP stack
By Forescout Research Labs & Medigate Labs
Forescout Research Labs
Daniel dos Santos
Stanislav Dashevskyi
Amine Amri
Medigate Labs
Uriel Malin
Tal Zohar
Yuval Halaban


FORESCOUT
Active Defense for the Enterprise of Things™
Reducir (Ctrl+1)
AMNESIA:33
How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices
Published by Forescout Research Labs
Written by Daniel dos Santos, Stanislav Dashevskyi, Jos Wetzels and Amine Amri

https://www.lunasec.io/docs/blog/log4j-zero-day/ 80%

Subscribe to our mailing list to get the latest security news and product updates.

LunaDefend Blog Contact Us

lnerability in Java library
ons Text (CVE-2022-42889,

or Startups: How to think
while moving quickly

ly Silence False Positives with
change

e Overhaul of the JavaScript

n and PHP dependencies, ctx
came malware that stole
dentials

n Vulnerability Scanning: Why
an Do Better

llation Guide For Developers

curity Analysis of the latest
' vulnerabilities in Spring

ow node-ipc turned into

bility in Log4j 2.17.0 more

Log4Shell: RCE 0-day exploit found in log4j, a popular Java logging package

December 9, 2021 · 11 min read

Free Wortley
CEO at LunaSec

Chris Thompson
Developer at LunaSec

Forrest Allison
Developer at LunaSec

Beltrán, 2022

https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

Apache Log4j Vulnerability Guidance

Summary

Note: *CISA will continue to update this webpage as well as our community-sourced GitHub repository as we have further guidance to impart and additional vendor information to provide.*

CISA and its partners, through the Joint Cyber Defense Collaborative, are responding to active, widespread exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) in Apache's Log4j software library, versions 2.0-beta9 to 2.14.1, known as "Log4Shell." Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system.

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Hacking

This article is more than **6 years old**

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

- **Major cyber attack disrupts internet service across Europe and US**

Nicky Woolf *in San Francisco*

@nickywoolf

Wed 26 Oct 2016 21.42 BST

423

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The cyber-attack that brought down much of America's internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its kind in history, experts said.

The victim was the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. It was hit on 21 October

Meet Hajime, the IoT Botnet Built to Vaccinate Your Devices Against Mirai

By Jessica Hall on April 24, 2017 at 11:23 am | Comments

https://github.com/jgamblin/Mirai-Source-Code

Product | Solutions | Open Source | Pricing | Search

jgamblin / Mirai-Source-Code Public

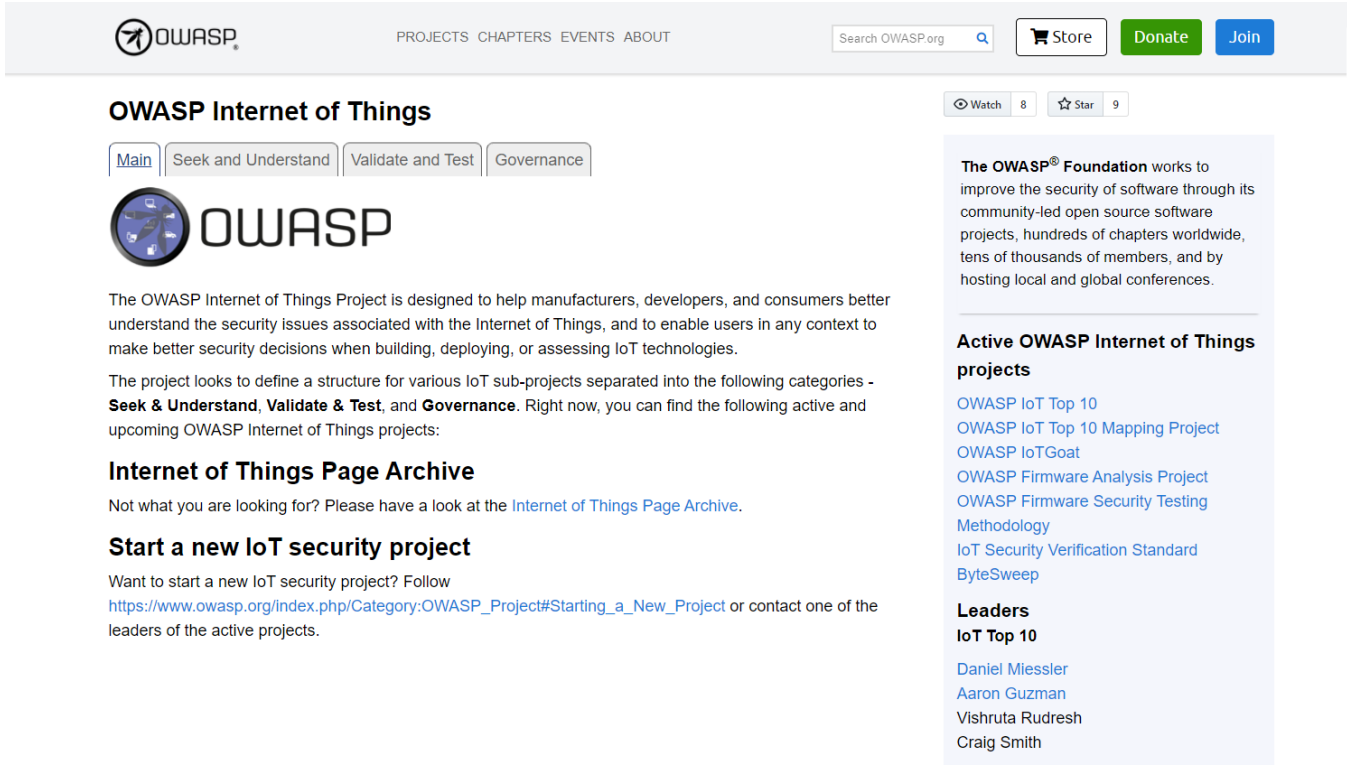
Code | Pull requests 1 | Actions | Projects | Security | Insights

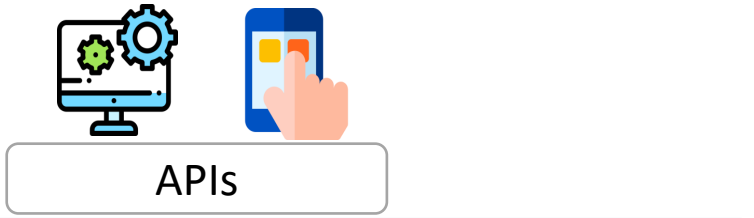
master | 1 branch | 0 tags | Go to file | Code

jgamblin Merge pull request #38 from Red54/patch-1 ... 3273043 on 15 Jul 2017 | 8 commits

dlr	Trying to Shrink Size	6 years ago
loader	Trying to Shrink Size	6 years ago
mirai	Trying to Shrink Size	6 years ago
scripts	Transcribe post to markdown while preserving	6 years ago
ForumPost.md	Transcribe post to markdown while preserving	6 years ago
ForumPost.txt	Update ForumPost.txt	6 years ago
LICENSE.md	Trying to Shrink Size	6 years ago

Beltrán, 2022





https://owasp.org/www-project-internet-of-things/

2. Superficie de ataque en IoT

Superficie de ataque - Dispositivos

Interfaces físicas	Memoria	Firmware
Servicios	Sistema operativo	Interfaces web

Interfaces físicos	• Destrucción o tampering. • Manipulación de sensores. • Extracción de firmware. • Acceso a consola de comandos. • Reseteo a estado de fábrica. • Retirada de medios de almacenamiento externo. • Acceso a puertos de diagnóstico o debug. • Exposición de IDs, números de serie.
Memoria	• Exposición de información sensible: nombres de usuario, contraseñas y credenciales, claves de cifrado, código.

Firmware	• Exposición de información sensible: nombres de usuario, contraseñas y credenciales, claves de cifrado, puertas traseras, URLs sensibles • Versión de firmware instalada y fecha de la última actualización. • Servicios vulnerables como http(s), ssh, ftp. • Alternativas para el downgrade.

Servicios	• UDP como protocolo de transporte.
	• Criptografía inexistente o mal implementada.
	• Ataques de replay.
	• Falta de mecanismos de integridad.
	• Servicios de actualización que no funcionan sobre TLS, protocolos OTA inseguros.
	• Corrupciones de memoria y overflows.
	• Denegaciones de servicio.
	• Inyecciones.
	• Mala gestión de identidades y accesos:
	  • Enumeración de usuarios.
	  • Contraseñas por defecto o débiles.
	  • Mala gestión de sesiones, de logout.
	  • Recuperación de contraseñas insegura.

Sistema operativo	• Vulnerabilidades estándar. • Vulnerabilidades específicas de sistemas empotrados o tiempo real, de módulos TPM, etc.

Interfaces web	• Vulnerabilidades estándar.
	• Mala gestión de identidades y accesos:
	  • Enumeración de usuarios.
	  • Contraseñas por defecto o débiles.
	  • Mala gestión de sesiones, de logout.
	  • Recuperación de contraseñas insegura..

2. Superficie de ataque en IoT

Superficie de ataque - Protocolos

Mecanismos de actualización	Tráfico de datos	IAM (Identity and Access Management)

Mecanismos de actualización	• Falta de mecanismos de actualización manuales y automáticos. • Cifrado inexistente o débil. • Actualizaciones sin firma, origen no autenticado. • Zona de memoria para las actualizaciones sin protección. • Actualizaciones por “push”.
Tráfico de datos (M2M, M2C)	• Vulnerabilidades estándar. • Vulnerabilidades específicas de los protocolos IoT (CoAP, MQTT, etc.). • Mal uso de health checks, heartbeats, etc.

IAM (device to device, device to service, user to service, etc.)	• Falta de protocolos IAM. • Revelación de datos sensibles relacionados con los protocolos IAM (IDs, contraseñas, claves, credenciales). • Reutilización de secretos criptográficos. • Problemas con el enrollment. • Falta de logs y de capacidad de auditoria.

2. Superficie de ataque en IoT

Superficie de ataque– Aplicaciones, plataformas y datos

Interfaces administrativos	Interfaces cloud	APIs	Aplicaciones web
Aplicaciones móviles	Almacenamiento local	Almacenamiento en la nube	

3. Trucos

1) Intenta manipular los dispositivos, sus interfaces y su memoria.
    1) Busca datos sensibles.
2) Busca canales encubiertos, hay muchas posibilidades.
3) Recupera el firmware de los dispositivos y juega con él (con herramientas como **binwalk**, **firmwalker** o **bytesweep**).
4) Identifica los sistemas operativos que se usan y sus versiones/estado de actualización.
5) Utiliza **nmap** para ver qué servicios se ofrecen en la red, qué puertos están abiertos en los dispositivos, etc.

3. Trucos

5) Intercepta el tráfico con un **sniffer** y analízalo. ¿Qué protocolos se usan? ¿Cifran, autentican?
6) Busca funcionalidades de auto-update. Si existen, intenta hacer un Man in The Middle, por ejemplo, intenta actualizar un firmware o sistema operativo en un dispositivo sin que vaya convenientemente firmado, suplantando al servidor de actualizaciones legítimo. ¿Funciona?
7) ¿Cómo se controlan los accesos a los dispositivos? ¿Y los interfaces y APIs a diferentes niveles? ¿Has encontrado cuentas y contraseñas por defecto? ¿Es posible aplicar fuerza bruta?
8) Busca tecnologías web en los dispositivos (servidores de acceso remoto, configuración, paneles de control) e intenta acceder a ellos explotando las vulnerabilidades tradicionales.

No hay nada demasiado simple o antiguo… ¿buffer overflow? Haz la prueba!

¡GRACIAS!

MARTA BELTRÁN

marta.beltran@urjc.es

@experiencia_T

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/
- Proyecto OWASP Internet of Things
  - https://owasp.org/www-project-internet-of-things/