MINISTERIO DE DEFENSA

JSTCIS/DCD

DIRECCIÓN DE CIBERDEFENSA
JEFATURA DE SERVICIOS TÉCNICOS Y CIS
EJÉRCITO DEL AIRE

LUCHANDO CONTRA LA OBSOLESCENCIA, Y LA DEPENDENCIA TECNOLÓGICA, CON SOFTWARE LIBRE

OpenExpo 20 de Junio de 2019

AGENDA:

- ESCENARIO
- ESTRATEGIA DE SEG. AEROESPACIAL
- LA SOLUCIÓN: SOFTWARE LIBRE

El caos de Huawei tiene solución: Trump sorprende y abre la puerta a un acuerdo para acabar con la guerra comercial

La UE quiere competir con Intel y AMD fabricando sus propios procesadores

Escrito por **Javier (Javisoft) López** 6 de junio de 2019 a las 16:00

procesadores 32

El mercado va unido en cierta manera a la política de cada país y actualmente éste está controlado por dos grandes superpotencias: **China y EE. UU.** La guerra comercial en la que están inmersos será aprovechada por la **Unión Europea** para lanzar una iniciativa con la que pretende ser menos dependiente de tecnología extranjera a la que han llamado **EPI (European Processor Initiative)** la cual construirá procesadores de alto rendimiento.

La UE reacciona a tiempo, EPI será apoyado por 23 empresas líderes europeas

Los ejércitos de China y Rusia no se fían de Windows y preparan el reemplazo

por J.Pomeyrol 3 de junio, 2019

Twittear

APÚNTATE A NUESTRAS NEWSLETTER

LO ÚLTIMO

Mark Shuttleworth «Ibamos

POPULAR MECHANICS TECHNOLOGY CARS TOOLS DEFENSE CAMPING GUIDE SUBSCRIBE NEWSLETTER

Britain's Doomsday Nuke Subs Still Run Windows XP

The fate of the country's nukes is in the hands of an obsolete operating system.

By Kyle Mizokami Jan 21, 2016

ESCENARIO III

- DESEQUILIBRIO ENTRE SECURITY & SAFETY
- NECESIDAD DE CIBERSEGURIDAD POR DISEÑO Y POR DEFECTO
- NECESIDAD DE SOLUCIONES Y ESTÁNDARES CIBER
- ENSAMBLAJE FRENTE A LA FABRICACIÓN (PARTNERS) COMPLICA EL CONTROL DE LA CADENA DE SUMINISTRO Y GENERA DEPENDENCIA TECNOLÓGICA
- SHADOW IT (INGENIERÍA INVERSA)
- OBSOLESCENCIA (CICLO DE VIDA CIS/TIC):
  - PROBLEMA MUY COMPLEJO (MEJOR EVITARLA QUE GESTIONARLA)
  - EFECTO DE ARRASTRE CON RESULTADOS CATASTRÓFICOS
  - SOFTWARE, HARDWARE, FIRMWARE, ALGORITMOS, PROTOCOLOS E INTERFACES
  - MANTENIMIENTO PREVENTIVO, CORRECTIVO, PERFECTIVO, EVOLUTIVO ADAPTATIVO Y PREDICTIVO

ELEMENTOS BÁSICOS DE LA CIBERSEGURIDAD:

A) ACTUALIZACIÓN.

B) BASTIONADO (CONFIGURACIÓN DE SEGURIDAD).

C) CONCIENCIACIÓN Y CIBERINTELIGENCIA.

D) DEFENSA ACTIVA.

E) EXTENSIÓN DE LAS MEDIDAS DE SEGURIDAD A TODA LA ORGANIZACIÓN.

Las Ciberamenazas del siglo XXI

PREFIJO **CIBER** → DIVERSIFICANDO FINES

COMPARTIENDO TECNOLOGÍAS DE ATAQUE

EL MUNDO

Berlín atribuye a espías extranjeros un 'ciberataque' a su centro aeroespacial

Noticias Relacionadas

Más leídas

La seguridad aérea amenazada por nuevos riesgos como drones o ciberataques

lainformacion.com

jueves, 04/12/14 - 18:47

comentar

Los "exitosos" resultados de la gestión de la seguridad aérea seguirán poniéndose a prueba en el futuro por nuevos casos de riesgo posibles provocados por ciberataques o drones de uso comercial, según un informe de la aseguradora Allianz Global Corporate and Specialty (AGCS), que presta su servicio al sector de la aviación.

Temas Accidentes aéreos y espaciales | América | Asia | Estados Unidos | Europa | Tecnología (general) | Transporte aéreo | África

Twittear 0 | 0

Recomendar 0 | 0

Madrid, 4 dic.- Los "exitosos" resultados de la gestión de la seguridad aérea seguirán poniéndose a prueba en el futuro por nuevos casos de riesgo posibles provocados por ciberataques o drones de uso comercial, según un informe de la aseguradora Allianz Global Corporate and Specialty (AGCS), que presta su servicio al sector de la aviación.

El estudio señala que la probabilidad de ciberataques va a ser cada vez mayor, porque los aviones de nueva generación están muy expuestos al cibercrimen por el uso generalizado de redes de datos, sistemas informáticos incorporados y sistemas de navegación.

Asimismo, se prevé un aumento de los drones (vehículos aéreos no tripulados o UAV) de uso comercial, la reducción en un futuro de mano de obra cualificada, como son los pilotos, y un incremento de las turbulencias que genera el cambio climático.

La FAA reconoce que fue víctima de un ciberataque a principios de año

Publicado: 7 abr 2015 19:44 GMT

Control aéreo de EEUU es vulnerable a ciberataques

WASHINGTON.- Una de las áreas débiles es la capacidad de prevenir y detectar acceso sin autorización a la amplia red de sistemas de cómputo y comunicación que utiliza la FAA para procesar y rastrear vuelos alrededor del mundo, señala el informe

ALTO PELIGRO | 03 de Marzo de 2015

El sistema para guiar aviones y otras aeronaves en Estados Unidos corre un "riesgo incrementado e innecesario" de sufrir ataques cibernéticos, indica un informe. (AP)

WASHINGTON.- **AP**

AGENDA:

- ESCENARIO
- ESTRATEGIA DE SEG. AEROESPACIAL
- LA SOLUCIÓN: SOFTWARE LIBRE

BOLETÍN OFICIAL DEL ESTADO

Núm. 103 Martes 30 de abril de 2019 Sec. I. Pág. 43482

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

6349 *Orden PCI/489/2019, de 26 de abril, por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional.*

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia de Seguridad Aeroespacial Nacional.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

Madrid, 26 de abril de 2019.–La Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, Carmen Calvo Poyato.

ANEXO

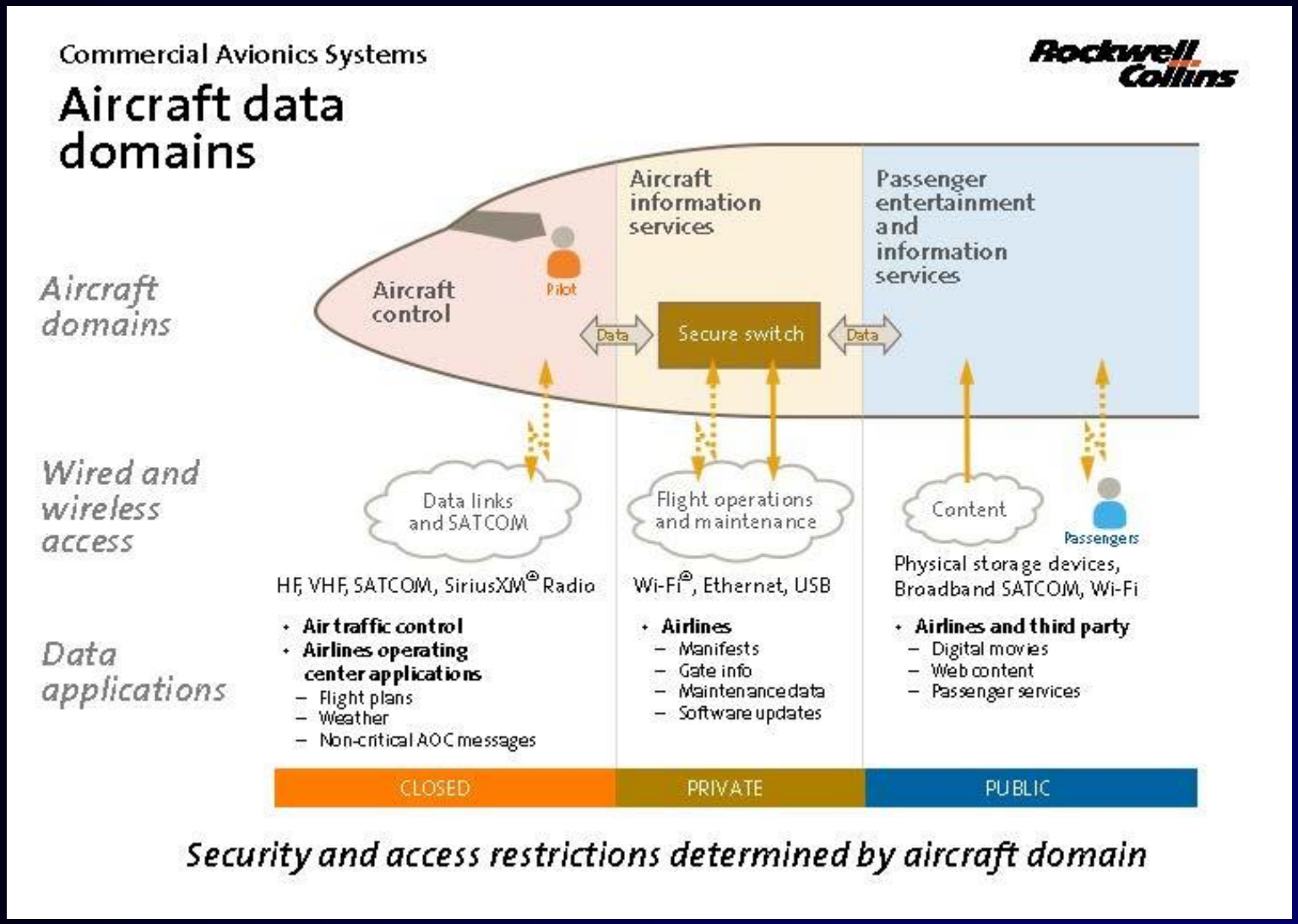
Estrategia de Seguridad Aeroespacial Nacional

Sumario

Resumen ejecutivo

LÍNEAS DE ACCIÓN:

- FORTALECER PREVENCIÓN, DETECCIÓN, VIGILANCIA Y RESPUESTA
- ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD
- **FOMENTAR EL EMPLEO DE PRODUCTOS CERTIFICADOS Y ACREDITADOS**
- CONCIENCIAR EN CIBERSEGURIDAD AL SECTOR
- MECANISMOS DE INTELIGENCIA Y CONTRAINTELIGENCIA
- COOPERACIÓN CON OTROS ESTADOS Y DESARROLLO DE LEGISLACIÓN
- IMPLANTAR UNA POLÍTICA DE SEGURIDAD INTEGRAL QUE:
  - **PROMUEVA REDUNDANCIA, RESILIENCIA, RESISTENCIA**
  - **GESTIONE DE LA OBSOLESCENCIA**
  - AUDITE LA SEGURIDAD DE SISTEMAS CRÍTICOS
  - DETERMINE LA FORMACIÓN CIBER DEL PERSONAL QUE OPERA Y SOSTIENE SISTEMAS AEROESPACIALES.
  - ORGANICE EJERCICIOS DE CIBER PARA EVALUAR SISTEMAS Y PERSONAL


Commercial Avionics Systems
Rockwell Collins
Aircraft data domains
Aircraft domains
Wired and wireless access
Data applications
Aircraft control
Pilot
Aircraft information services
Passenger entertainment and information services
Data
Secure switch
Data
Data links and SATCOM
Flight operations and maintenance
Content
Passengers
HF, VHF, SATCOM, SiriusXM® Radio
Wi-Fi®, Ethernet, USB
Physical storage devices, Broadband SATCOM, Wi-Fi
• Air traffic control
• Airlines operating center applications
– Flight plans
– Weather
– Non-critical AOC messages
• Airlines
– Manifests
– Gate info
– Maintenance data
– Software updates
• Airlines and third party
– Digital movies
– Web content
– Passenger services
CLOSED
PRIVATE
PUBLIC
Security and access restrictions determined by aircraft domain

AGENDA:

- ESCENARIO
- ESTRATEGIA DE SEG. AEROESPACIAL
- LA SOLUCIÓN: SOFTWARE LIBRE

LA SOLUCIÓN: SOFTWARE LIBRE I

OTAN:

LAS CAPACIDADES DEL NÚCLEO LINUX DICTAN LAS FRONTERAS DE LO QUE SE PUEDE LOGRAR. EN LA ACTUALIDAD, PERMITE LA EJECUCIÓN EN TIEMPO REAL Y LOS SISTEMAS EMBEBIDOS, SIENDO ÓPTIMO PARA APLICACIONES CRÍTICAS, SEGURAS Y DE SEGURIDAD. ADEMÁS, ES FÁCILMENTE ESCALABLE Y PUEDE SER USADO EN VARIAS PLATAFORMAS DIFERENTES.

Emerging Techonologies. NATOC3TA 2004.

CALIDAD DEL CÓDIGO LIBRE:

INICIO EN 2006 POR HOMELAND SECURITY (1,2 MILL).

COVERITY Y UNIVERSIDAD DE STANFORD.

ERRORES POR CADA 1.000 LÍNEAS DE CÓDIGO 0,54. (PYTHON 0,005).

CALIDAD LIGERAMENTE SUPERIOR AL PRIVATIVO, Y POR ENCIMA DEL ESTÁNDAR INDUSTRIAL.

INVERSIÓN EN MEJORA DE LA SEGURIDAD (“Core Infrastructure Initiative”).

AUDITORÍAS (GPG/TRUECRYPT).

Homeland Security

CORE INFRASTRUCTURE INITIATIVE

LA SOLUCIÓN: SOFTWARE LIBRE III

INFORME DE LATENCIA:

EVANS DATA CORPORATION (EDC) PUBLICA EN SU INFORME ANUAL QUE PARA EL SOFTWARE LIBRE, EL TIEMPO MEDIO ENTRE QUE SE DESCUBRE UN FALLO CRÍTICO Y SE RESUELVE ES INFERIOR A LAS 8 HORAS EN EL 36% DE LOS CASOS.

SEGÚN UNA ENCUESTA REALIZADA POR FORRESTER, PARA EL SOFTWARE PRIVATIVO EL TIEMPO MEDIO PARA RESOLVER UN FALLO CRÍTICO ES DE 6,9 DÍAS PARA LOS DESARROLLADORES EMPRESARIALES Y 6,7 DÍAS PARA LOS VENDEDORES DE SOFTWARE.

LA SOLUCIÓN: SOFTWARE LIBRE IV

Android Artwork Cine/TV GNU/Linux Hacktivismo Internet Juegos Leer

Los drones de la Navy migrarán de Solaris a Linux

LPS, la distro Linux ultrasegura de la USAF

Como señalan nuestros compañeros de MuyComputer, esta distribución ha sido desarrollada en los laboratorios de la fuerza aérea y departamento de defensa estadounidense. LPS es una **pequeña distribución Linux diseñada para usos seguros y arrancable desde unidades ópticas CD o pendrives USB** en cualquier ordenador con plataforma x86.

LO ÚLTIMO

MUYTV

El servidor proxy está

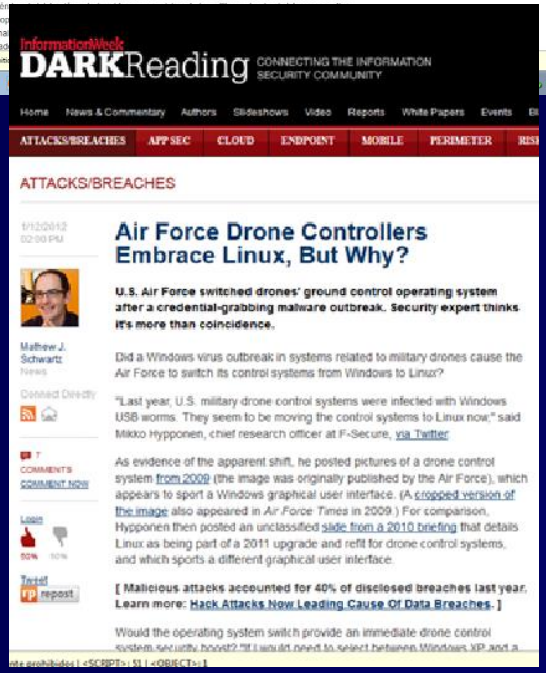
Más allá de la cuota de mercado de Linux en el escritorio, monopolizado por el Windows de Microsoft, **la relación gubernamental con Linux es amplia**, desde el Red Flag chino, el Pardus turco o los rusos en camino de mover toda su infraestructura a Linux y software libre.

R-Gator, el robot militar Linux

OFF-TOPIC
etiquetas: off-topic

0 FLARES

El prototipo tiene un kernel Linux 2.6La empresa iRobot ha desarrollado un vehiculo militar autonomo UGV orientado al uso militar y de exploracion, que es operado por una version propietaria embebida de Linux, llamada BlueCat Linux.
El R-Gator esta basado en el prototipo de John Dere, de 658 centimetros cubicos y alimentado a combustible diesel.
El vehiculo es un UGV inteligente que puede realizar misiones militares de manera autonoma, incluyendo el actuar como un explorador, apuntador o guardian, ademas de poder llevar equipaje militar para alivianar el trabajo de los soldados.
Puede cambiar rapidamente los modos de automatico a manual o a operacion remota, lo que le permite adaptarse a los mas diversos escenarios.
En modo autonomo, el vehiculo puede seguir a los soldados como un simple robot. O navegar a traves de



InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home News & Commentary Authors Slideshows Video Reports White Papers Events

ATTACKS/BREACHES APP SEC CLOUD ENDPOINT MOBILE PERIMETER

ATTACKS/BREACHES

Air Force Drone Controllers Embrace Linux, But Why?

U.S. Air Force switched drones' ground control operating system after a credential-grabbing malware outbreak. Security expert thinks it's more than coincidence.

Matthew J. Schwartz

Did a Windows virus outbreak in systems related to military drones cause the Air Force to switch its control systems from Windows to Linux?

"Last year, U.S. military drone control systems were infected with Windows USB worms. They seem to be moving the control systems to Linux now," said Mikko Hypponen, chief research officer at F-Secure, via Twitter.

As evidence of the apparent shift, he posted pictures of a drone control system from 2009 (the image was originally published by the Air Force), which appears to sport a Windows graphical user interface. (A cropped version of the image also appeared in *Air Force Times* in 2009.) For comparison, Hypponen then posted an unclassified slide from a 2010 briefing that details Linux as being part of a 2011 upgrade and refit for drone control systems, and which sports a different graphical user interface.

[Malicious attacks accounted for 40% of disclosed breaches last year. Learn more: Hack Attacks Now Leading Cause Of Data Breaches.]

Would the operating system switch provide an immediate drone control

NUESTRA EXPERIENCIA CON SLES 12:

- AHORRO QUE PERMITE INVERTIR EN CIBERSEGURIDAD.
- POSIBILIDAD DE OBTENER SOPORTE LOCAL.
- ACCESO A TODA LA TECNOLOGÍA E INDEPENDENCIA TECNOLÓGICA.
- CERTIFICACIÓN DE SEGURIDAD EAL 4 + (SLES 12) Y EAL 2 (UBUNTU).
- PLANTILLAS DE SEGURIDAD PARA ENS Y SISTEMAS CLASIFICADOS (SLES 12).
- CICLO DE VIDA EXTENDIDO (13 + 2) Y 5 PARA UN SERVICE PACK.
- OPTIMIZACIÓN ACTUALIZACIONES SATÉLITE.
- REDUCCIÓN DE LA SUPERFICIE DE EXPOSICIÓN (SUSE STUDIO).
- ACTUALIZACIÓN CON PLANTILLA DE SEGURIDAD MÁS FIABLE.
- MEJOR SOPORTE DEL HARDWARE LEGACY.
- SIMPLIFICACIÓN DE LAS LICENCIAS.

LA SOLUCIÓN: SOFTWARE LIBRE VI

POSIBLES VÍAS A FUTURO:

- ADECUAR EL CICLO DE VIDA DE LOS SISTEMAS CIS/TIC AEROESPACIALES
- DISPONER DE UN FRAMEWORK TECNOLÓGICO COMÚN, CERTIFICADO Y ACREDITADO, CON CICLO DE VIDA ADECUADO (BASADO EN SOFTWARE LIBRE).
- CONTEMPLAR TODOS LOS TIPOS DE MANTENIMIENTO EN LOS CIS/TIC
- CONTROLAR LA CIBERSEGURIDAD DE LA CADENA DE SUMINISTRO Y LIMITAR LA DEPENDENCIA TECNOLÓGICA (BASADO EN SOFTWARE LIBRE).
- APLICAR PROGRAMACIÓN SEGURA Y DEFENSIVA

MUCHAS GRACIAS POR SU ATENCIÓN

¿PREGUNTAS?