Introducción a la Ciberseguridad

Teoría: Javier Díaz
jdiaz@unlp.edu.ar
Práctica: Soledad Gomez
Ulises Cabrera

Hardening en Sistemas Operativos

- Servicios y procesos
  - Desactivar servicios no utilizados.
  - Revisar procesos en ejecución y puertos abiertos.

- Gestión de cuentas y accesos
  - Deshabilitar cuentas innecesarias.
  - Uso de contraseñas robustas y MFA.
  - Principio de mínimo privilegio (PoLP) (principio de least privilege)

- Aplicar parches y actualizaciones de seguridad.

Hardening en Sistemas Operativos…

- **Configurar firewalls locales (iptables, Windows Defender Firewall).**
- **Activar logs y auditoría, backups seguros.**
- **EDR (Endpoint Detection and Response) y cifrado de discos**
  - **OpenEDR: plataforma EDR de código abierto que ofrece telemetría avanzada, detección en tiempo real y visibilidad MITRE**

ATT&CKMITRE ATT&CK es una base de conocimiento de acceso global sobre tácticas y técnicas adversarias basadas en observaciones del mundo.

Hardening en Redes

- **Segmentación de red** con VLANs y firewalls internos.
  - Sniffing:Al
  - Barrido de Puertos (Port Scanning):.
  - Ataques a Protocolos:
- **Autenticación fuerte**
  - **MFA**
  - control de accesos basado en roles (RBAC)
- **Deshabilitar servicios/protocolos inseguros** (Telnet, SNMPv1/v2).
- **Monitoreo constante** con IDS/IPS y SIEM.
  - Patrones de trafico
- **Gestión de parches y firmware** actualizados.
- **Backups y pruebas periódicas de vulnerabilidades**.

Hardening en Redes

- **Segmentación de red** con VLANs y firewalls internos.
  - Sniffing:Al
  - Barrido de Puertos (Port Scanning):.
  - Ataques a Protocolos:
- **Autenticación fuerte**
  - **MFA**
  - control de accesos basado en roles (**RBAC**)
- **Deshabilitar servicios/protocolos inseguros** (Telnet, SNMPv1/v2).
  - Autenticación: **SNMPv3 r**equiere autenticación de paquetes para garantizar fuente legítima. Esto se Con hash (como MD5 o SHA).
  - Privacidad (Cifrado): **SNMPv3** cifrado de datos en tránsito con DES o AES.
  - Control de acceso: **SNMPv3** permite la creación de usuarios y grupos con diferentes niveles de acceso. P.ej solo GE) y no SET.

VPN tradicional vs Zero Trust

- **Modelo de confianza:**

• VPN: perímetro fuerte, interior débil; se confía al conectarse

• Zero Trust: nunca confiar, siempre verificar cada acceso

- **Acceso a recursos:**

• VPN: acceso amplio a la red interna

• Zero Trust: acceso granular solo al recurso autorizado (menor superficie de ataque)

VPN tradicional vs Zero Trust…

- **Autenticación:**
- VPN: usuario + contraseña al inicio
- Zero Trust: autenticación continua, MFA y validación contextual
- **Segmentación:**
- VPN: VLANs y firewalls internos
- Zero Trust: microsegmentación dinámica basada en identidades y políticas
- **Protección ante ataques internos:**
- VPN: mayor riesgo de movimiento lateral
- Zero Trust: control granular que reduce el impacto

VPN tradicional vs Zero Trust…

- **Escalabilidad:**

• VPN: compleja y rígida al crecer la red

• Zero Trust: flexible; políticas centralizadas en entornos híbridos/cloud

- **Visibilidad y monitoreo:**

• VPN: limitado; depende de registros en VPN/firewall

• Zero Trust: monitoreo continuo del comportamiento y anomalías

- **Entornos modernos (cloud, SaaS, BYOD):**

• VPN: difícil de adaptar

• Zero Trust: diseñado para entornos distribuidos y heterogéneos

Siguiente paso: definir identidades, MFA, políticas por aplicación y telemetría.

Arquitectura simplificada Zero Trust

- **Proxy de identidad (ZTNA por aplicación)**
  - **Un proxy de identidad no confía en la ubicación de un usuario (como una VPN tradicional). verifica la identidad de cada usuario y su dispositivo antes de darle acceso a una aplicación específica, y solo a esa aplicación.**
- **Microservicios/Kubernetes (mTLS + SPIFFE/SPIRE)**
  - **seguridad "servicio a servicio". Con microservicios, las aplicaciones se comunican constantemente entre sí. Utilizar mTLS (Mutual TLS) asegura que cada servicio autentica. SPIFFE/SPIRE automatiza la creación de estas identidades par cada microservicio, simplificando la gestión de certificados y claves a gran escala.**

Arquitectura simplificada Zero Trust...

- **Acceso remoto/ZTNA de red (overlay por identidad)**
  - **se centra en el acceso a la red completa o a una subred. Un "overlay por identidad" crea una red superpuesta (o "overlay") que solo permite el acceso a recursos específicos a los usuarios y dispositivos que han sido autenticados y autorizados. Es una forma de aplicar los principios de Zero Trust a nivel de red, lo que es crucial para empleados que acceden a recursos de la empresa desde ubicaciones remotas.**

Zero Trust vs Segmentación clásica con VPN

Aspecto	Segmentación clásica con VPN	Zero Trust
Modelo de confianza	Confianza en lo interno (perímetro fuerte, interior débil)	Nunca confiar, siempre verificar cada acceso
Acceso a recursos	Acceso amplio a la red al conectarse	Acceso granular solo al recurso autorizado
Autenticación	Usuario + contraseña al iniciar sesión	Autenticación continua, MFA, validación contextual
Segmentación	VLANs y firewalls internos	Microsegmentación dinámica basada en identidades y políticas
Escalabilidad	Complejo y rígido al crecer la red	Flexible: políticas centralizadas en entornos híbridos/cloud
Visibilidad y monitoreo	Limitado, depende de registros en VPN/firewall	Monitoreo continuo del comportamiento y anomalías
Protección ante ataques internos	Débil: movimiento lateral posible dentro de la VPN	Fuerte: control granular reduce superficie de ataque
Entornos modernos (cloud, SaaS, BYOD)	Difícil de adaptar	Diseñado para entornos distribuidos y heterogéneos

Hardening en Aplicaciones y Servicios

- Deshabilitar módulos no usados (ej. en Apache, IIS, MySQL).
- Revisar y limitar permisos de archivos y directorios.
- Configurar contraseñas seguras y autenticación multifactor (MFA).
- Proteger bases de datos (encriptación, revisar y limitar permisos de archivos y directorios).
- Uso de parámetros seguros en aplicaciones web.
  - TLS (Transport Layer Security)
  - Cabeceras HTTP p.ej. HTTP Strict Transport Security (HSTS)
  - Cookies Seguras p.ej. Atributo Secure y Atributo HttpOnly:

Ejemplo: Configurar Apache para no mostrar versión del servidor → evita dar pistas al atacante.

Vulnerabilidades de hardware

Zenbleed (CVE-2023-20593): vulnerabilidad de ejecución especulativa, afecta a los procesadores AMD Zen 2, incluyendo EPYC, Ryzen 3000/4000/5000 y algunos 7000. Permite el filtrado de datos sensibles como claves de cifrado o credenciales desde registros internos del CPU, incluso a través de código JavaScript malicioso en un navegador.
https://www.kaspersky.com/blog/zenbleed-vulnerability/48836/

►AMD lanzó actualizaciones de microcódigo para múltiples líneas afectadas. Se recomienda estar al día con las actualizacione de BIOS/OS que incluyen estos parches.

Vulnerabilidades en Infraestructura Critica IC

- Ámbito: energía, agua, transporte, telecomunicaciones, salud.
- Impacto típico:
  - Interrupción de servicios esenciales para la sociedad.
  - Riesgo de seguridad física para personas.
  - Consecuencias políticas y económicas a gran escala.
- Ejemplos:
  - Stuxnet (2010): sabotaje en sistemas industriales.
  - Ataques a la red eléctrica de Ucrania (2015, 2016).

Ciberseguridad OT en IC

- La **ciberseguridad OT (Operational Technology) en Infraestructuras Críticas (IC)** se refiere al conjunto de **estrategias, procesos, tecnologías y prácticas de seguridad informática aplicadas a los sistemas de control industrial**

ICS, Sistemas de Control Industrial,
SCADA, Sistemas de Supervisión, Control y Adquisición de Datos
DCS, Sistemas de Control Distribuido
PLCs, Controladores Lógicos Programables
y otros componentes de la tecnología operativa que gestionan servicios esenciales como energía, transporte, agua, telecomunicaciones y salud.

Ciberseguridad OT en IC

OBJETIVO: garantizar la disponibilidad, integridad y confiabilidad de los procesos físicos y digitales, protegiéndolos frente a amenazas cibernéticas que podrían tener consecuencias no solo económicas, sino también **sociales, ambientales y de seguridad física para la población**.

Estándares de seguridad en IC

- **Objetivos principales:**
- **Protección de sistemas de control industrial.**
- **Separación de redes IT y OT (defensa en profundidad).**
- **Monitoreo continuo y detección temprana de anomalías.**
- **Planes de respuesta ante incidentes de alto impacto.**

Defensa en profundidad OT/IC

- **Gobernanza:** políticas, capacitación, gestión de proveedores.
- **Seguridad Física:** control de accesos, vigilancia, segregación de áreas.
- **Redes:** segmentación IT/OT, firewalls, IDS/IPS industriales.
- **Dispositivos:** acceso seguro a PLC/RTU/HMI, gestión de parches.
- **Aplicaciones:** endurecimiento de SCADA, listas blancas, backups.
- **Datos:** cifrado, monitoreo de logs, integridad de procesos.
- **Resiliencia:** SOC/CSIRT OT, redundancia, planes de recuperación.

Riesgos PLC y SCADA en entornos industriales

- **PLC (Controladores Lógicos Programables):**
  - Alteración de lógica de control → interrupción de procesos críticos.
  - Accesos no autorizados → manipulación remota.
  - Malware específico (ej. Stuxnet) que explota vulnerabilidades en firmware.
  - Ausencia de autenticación robusta en muchos dispositivos legacy.
- **SCADA (Supervisory Control and Data Acquisition):**
  - Intercepción de comunicaciones → alteración de datos en tránsito.
  - Secuestro de HMI → visualización falsa de parámetros.
  - Denegación de servicio (DoS) → pérdida de monitoreo y control.
  - Uso de protocolos inseguros (ej. Modbus, DNP3 sin cifrado).

Recomendaciones

- Implementar autenticación y control de acceso a PLC y SCADA.
- Monitorear continuamente tráfico OT con IDS/IPS especializados.
- Segregar entornos IT/OT mediante firewalls y DMZ industriales.
- Aplicar gestión de parches y pruebas en entornos controlados.
- Desarrollar planes de respuesta a incidentes con foco OT.
- Capacitar al personal en ciberseguridad industrial.

Ejemplos de Incidentes Reales en OT/ICS

- **Stuxnet (2010):** malware que alteró el funcionamiento de PLC Siemens en instalaciones nucleares iraníes.
  https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
- **BlackEnergy (2015):** ciberataque a la red eléctrica de Ucrania que provocó apagones masivos. https://www.incibe.es/incibe-cert/blog/estudio-del-analisis-de-malware-en-sci-blackenergy
- **Triton/Trisis (2017):** malware que comprometió sistemas de seguridad industrial (SIS) en plantas petroquímicas. En 2022 Schneider Electric Triconex.
  https://www.ic3.gov/CSA/2022/220325.pdf
- **Colonial Pipeline (2021):** ataque de ransomware que afectó la infraestructura energética de EE.UU., mostrando la interdependencia IT/OT.
  https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Ciberseguridad OT en IC

- **Enfoque en disponibilidad: a diferencia de la ciberseguridad TI, donde prima la confidencialidad, en OT/IC la prioridad es mantener la operación continua.**
- **Superficie de ataque híbrida: combina riesgos cibernéticos (malware, ransomware, intrusiones) con riesgos físicos (fallas de sistemas de control).**
- **Otro desafio es integrar la seguridad OT/IC con los sistemas informáticos (IT) como por ejemplo SAP**
- **P.ej. Multiples sistemas SCADA cada uno corriendo una version distinta según el operador o prestador y según cuando entre en operacion**

Estándares de seguridad en IC/OT

Normativas y marcos relevantes

- **NIST Cybersecurity Framework (CSF) → Gestión de riesgos de ciberseguridad.**

https://www.nist.gov/cyberframework

- **NERC CIP (Critical Infrastructure Protection) → Estándares para sector eléctrico.**

https://claroty.com/complying-with-the-nerc-cip-standards

- **IEC 62443 → Seguridad para sistemas de automatización industrial y control.**

https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

- **ISO/IEC 27019 → Seguridad de la información en sistemas de energía.**

https://www.iso.org/standard/85056.html

- **CIS Controls → Buenas prácticas aplicables a ICS/SCADA.**

https://www.cisecurity.org/controls

Vulnerabilidades en IoT

- **Ámbito: dispositivos inteligentes: cámaras IP, wearables, domótica, autos conectados, sensores médicos.**

- **Impacto típico:**
  - **Invasión de la privacidad (ej. cámaras hackeadas).**
  - **Uso de dispositivos como botnets para ataques DDoS.**
  - **Riesgos en seguridad física (ej. autos conectados, dispositivos médicos).**
- **Ejemplos:**
  - **Botnet Mirai (2016): millones de dispositivos IoT usados en ataques masivos.**
  - **Vulnerabilidades en marcapasos y bombas de insulina reportadas por la FDA.**

Seguridad en IoT

- **Objetivos principales:**
  - **Autenticación segura y gestión de credenciales.**
  - **Cifrado de datos en tránsito y en reposo.**
  - **Actualizaciones seguras de firmware/software.**
  - **Resiliencia frente a ataques de botnets y DD**

IoT LoRaWAN

Seguridad en Dispositivos

- Secure Elements (AppKey/NwkKey): Microchip ATECC608A-TNG(LORA), STSAFE-A110, NXP SE050.

- Firmware seguro: MCUboot (boot firmado), mbedTLS/TinyCrypt, TrustedFirmware-M (ARMv8-M).

- Prácticas: OTAA, LoRaWAN 1.1, claves únicas, rejoin para rotación, FUOTA con firma.

IoT LoRaWAN

Seguridad en Gateways (edge)

- Semtech LoRa Basics Station (TLS/WebSocket) + CUPS para provisión y rotación de certificados.
- Modelos: Kerlink, Tektelic, MultiTech, Laird, MikroTik (ver compatibilidad con Basics Station).
- Hardening: SO actualizado, SSH con claves, iptables/ufw mínimo, postura con Wazuh u osquery/Fleet.

Referencias:

- Semtech LoRa Basics™ Station & CUPS
- LoRa Alliance – LoRaWAN 1.1 Especificación
- MCUboot / mbedTLS / TrustedFirmware-M

Core LoRaWAN y Gestión de Claves

Network/Join/Application Server:

- OSS: ChirpStack (NS/AS + Prometheus), The Things Stack (OSS/Cloud, JS integrado).

- Comerciales: Actility ThingPark, Loriot.

Gestión de claves/certificados:

- PKI: Smallstep step-ca, HashiCorp Vault (PKI + secretos).

- HSM/KMS: YubiHSM 2, Cloud KMS (AWS/Azure/GCP).

Core LoRaWAN y Gestión de Claves

Buenas prácticas de clave:

- Separar AppSKey (en App Server) de claves de red (FNwkSIntKey/SNwkSIntKey/NwkSEncKey).
- Forzar TLS/mTLS entre gateway ↔ LNS/JS ↔ App; vigilar counters y DevNonce.

Referencias:

- ChirpStack docs
- The Things Stack docs
- HashiCorp Vault / Smallstep step-ca

Arquitectura On-Premises IoT LoRaWAN

Componentes principales:

- End-nodes: Secure Element (ATECC608A/STSAFE/SE050), firmware firmado (MCUboot), OTAA y LoRaWAN 1.1.
- Gateways: LoRa Basics Station (WebSocket TLS) + CUPS para provisión/rotación de certificados.
- Core: ChirpStack (NS/AS) + Join Server propio; gestión de secretos con Vault y PKI con step-ca.

Seguridad de comunicaciones:

- mTLS en GW ↔ LNS/JS y AS ↔ apps; AppSKey solo en Application Server; separación de claves (1.1).
- Rejoin para rotación de claves; alertas por reuse de nonce y reseteo de frame counters.

Arquitectura On-Premises IoT LoRaWAN…

Diseño de red y hardening:

- Segmentación: VLAN/VRF para mgmt de gateways y red del core; firewall solo a puertos LNS/CUPS.
- Gateways endurecidos: SSH con llaves, mínimos servicios, postura con Wazuh u osquery/Fleet.

Observabilidad y respuesta:

- Prometheus + Grafana (métricas), Loki/Elastic (logs); paneles para join rate, MIC fails, gateways mudos.
- SIEM con Wazuh; correlación (nonce reuse + múltiples joins) y alertas.

Operación (playbook):

- Alta de dispositivo → provisión de claves/SE → alta en JS/NS → pruebas de join/uplink.
- FUOTA firmado; backup/DR de JS/DB y rotación periódica de certificados.

Arquitectura On-Premises IoT LoRaWAN…

Escalabilidad:

- Balanceo de NS/AS con HAProxy/NGINX; métricas/logs en TSDB/objeto; particionar decoders.

Referencias:

- LoRa Alliance — Especificación LoRaWAN 1.1
- Semtech — LoRa Basics™ Station & CUPS
- ChirpStack — Documentación (NS/AS/Join Server + métricas)
- HashiCorp Vault / Smallstep step-ca — PKI/secretos
- Prometheus/Grafana/Loki — Observabilidad
- Wazuh — SIEM/IDS
- FUOTA — Paquetes LoRa Alliance

Seguridad en IoT

- **Normativas y estándares clave**
  - **ISO/IEC 30141 → Arquitectura de referencia IoT.2018**
    https://www.iso.org/standard/88800.html
  - **ISO/IEC 27400 → Seguridad y privacidad en IoT.2022**
    https://www.iso.org/standard/44373.html
  - **NISTIR 8259 → Ciberseguridad para dispositivos IoT. 2020**
    https://csrc.nist.gov/pubs/ir/8259/final
  - **ETSI EN 303 645 → Estándar europeo de ciberseguridad en IoT. 2020**
    https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
  - **OWASP IoT Top 10 → Principales riesgos en IoT. 2021**
    https://owasp.org/www-project-internet-of-things/