Introducción a la Ciberseguridad

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

X.509: La infraestructura invisible de la confianza digital

- Estándar ITU-T X.509 (1988), parte de la familia X.500.
- Base de la Infraestructura de Clave Pública (PKI).
- X.509 v3 (1997) Introdujo las extensiones de certificado
- Usado en HTTPS, VPN, S/MIME, Code Signing, IoT.
- Objetivo: vigencia técnica y arquitectónica.

Arquitectura y fundamentos técnicos

- odelo jerárquico: CA raíz → Sub-CA → RA → Usuario final.
- ASN.1: codificación **DER**/BER.
- Certificados vinculan identidad ↔ clave pública.
- Extensiones X.509v3 para compatibilidad y personalización.

Diseño modular y longevidad

- “Relevance, scale and longevity reside in GOOD DESIGN.”
- Modularidad y extensibilidad.
- Evolución sin ruptura (desde 1988 hasta TLS 1.3 de 2018).
- Documentación formal y estandarización continua.

RPKI (Resource Public Key Infrastructure)

- BGP (Border Gateway Protocol) rutea sistemas autónomos (AS). BGP no tiene autenticación incorporada → (ataque de route hijacking o prefix hijacking).
- RPKI asocia criptográficamente los bloques de direcciones IP (IPv4/IPv6) y los números de sistema autónomo (ASN) a certificados X.509 emitidos por los RIR: LACNIC, ARIN, RIPE.
- Cada certificado genera un ROA (Route Origin Authorization), tal AS está autorizado a anunciar este prefijo IP. Routers validan criptográficamente

SG11 (ITU-T): señalización y autenticación

- SG11 del ITU-T: desarrolla normas de interoperabilidad entre operadores: señalización/autenticación dispositivos y redes
- X.509 se utiliza en estos estándares como mecanismo de autenticación mutua entre nodos de red: Equipos de telecomunicaciones intercambian certificados X.509 para probar su identidad.
- garantiza integridad y autenticidad en las sesiones de señalización (por ejemplo, SIP, H.323, 5G Core, etc.).

TLS/SSL: validación en tiempo real

- protocolos que aseguran la comunicación en la web (HTTPS)
- Cada servidor HTTPS presenta un certificado X.509 emitido por una CA. El cliente (navegador) valida la firma y la cadena de confianza.
- Validación en tiempo realEl cliente necesita confirmar que el certificado no esté revocado ni manipulado:
    - CRL (Certificate Revocation List): lista publicada por la CA.
    - OCSP (Online Certificate Status Protocol): permite consultar en línea
    - CT Logs (Certificate Transparency Logs): registros públicos inmutables

Nuevos contextos tecnológicos

- **DPKI (Decentralized Public Key Infrastructure) evolución del modelo PKI tradicional elimina las Autoridades Certificadoras (CA) centrales**

De jerarquía a confianza distribuida: **blockchain** o **ledger distribuido (DLT)**.

- Cada entidad (persona, organización, dispositivo) **genera y publica su propia clave pública** en un registro distribuido.
- No hay una CA que firme los certificados: la **verificación se basa en consenso** o en “anclajes de confianza” descentralizados.
- Se integran conceptos como **Identidad Autosoberana (SSI)** y **Verifiable Credentials (W3C)**.

Un dispositivo IoT podría tener su identidad registrada en una **red blockchain**; cualquier otro nodo podría verificar su autenticidad sin consultar una CA central.

Nuevos contextos tecnológicos

- Post-Quantum Cryptography (PQC): transición híbrida.
- “Transición híbrida”:durante el proceso de migración se usarán dos tipos de claves simultáneamente: una clásica (RSA/ECC) y una post-cuántica (por ejemplo, CRYSTALS-Kyber, Dilithium, etc.).
- Los certificados X.509 se ampliarán para incluir ambos tipos de claves y firmas. ◇ Objetivo:Garantizar compatibilidad con sistemas actuales sin romper TLS, VPNs, ni PKI existentes.

Nuevos contextos tecnológicos

- Agentic AI: identidad verificable entre agentes autónomos.
- Los agentes autónomos (IA que actúa o toma decisiones por sí misma) requerirán identidad digital verificable para interactuar de forma segura con otros agentes o humanos.
- Rol de X.509:El modelo PKI (y sus extensiones futuras) podría permitir que cada agente tenga un certificado digital o un token criptográfico que acredite su identidad, reputación y permisos. Habilitando que las comunicaciones entre agentes estén firmadas y autenticadas.

Ejemplo:Un asistente de IA que realiza transacciones podría firmarlas digitalmente con un certificado emitido bajo un marco de confianza (por ejemplo, un DPKI o una PKI federada).

Nuevos contextos tecnológicos

EU Cyber Resilience Act (CRA): refuerza la dependencia PK.

- El Cyber Resilience Act (CRA) es una regulación de la Unión Europea (2024) para productos digitales y software: Obliga a los fabricantes y desarrolladores a garantizar autenticidad, integridad y actualizaciones seguras.
- Impulsa el uso de firmas digitales basadas en X.509 para:Firmar firmware y software; Autenticar dispositivos conectados; Validar actualizaciones y comunicaciones seguras.
- Fortalece la dependencia de la infraestructura PKI y X.509, ya que muchos productos deberán implementar certificados digitales y mecanismos de validación automática.

Riesgos y desafíos operativos

- Escalabilidad de validaciones (OCSP Stapling, CRL, SCTs).
    - Problemas: Latencia, carga, disponibilidad
- Sostenibilidad de CAs y RAs.
    - Problemas: Concentración, fallas sistémicas
- Falta de nuevos especialistas en PKI y ASN.1.
- Complejidad de migración post-cuántica.
    - Problemas: Incompatibilidad y vulnerabilidad futura

Lecciones de ingeniería

- • Diseños duraderos comparten:
- - Modularidad y abstracción adecuada.
- - Estandarización formal y documentación abierta.
- - Evolución incremental sin ruptura.
- • X.509 = arquitectura resiliente y sostenible.

Conclusiones y referencias

- • “El secreto de la vigencia tecnológica está en el buen diseño.”
- • X.509 sostiene la confianza digital en Internet.

- Referencias:
- - ITU-T X.509 (11/2019)
- - RFC 5280
- - NIST SP 800-208
- - EU CRA (2024)
- - Erik Andersen – ITU-T Q1 DPKI Design Talk

Frameworks y Regulaciones en Ciberseguridad…

5. GDPR (General Data Protection Regulation – UE)

Descripción: Reglamento europeo sobre protección de datos personales y privacidad, aplicable a todas las organizaciones que procesen datos de residentes en la UE.
Referencia: Regulation (EU) 2016/679 of the European Parliament and of the Council.
https://gdpr-info.eu/

6. ISO/IEC 27032 (Cybersecurity Guidelines)

Descripción: Norma internacional que proporciona directrices específicas en ciberseguridad (distinguida de la seguridad de la información de ISO/IEC 27001).
Referencia: ISO/IEC 27032:2012. Guidelines for Cybersecurity.
https://www.iso.org/standard/76070.html

GDPR: Protección de Datos y Privacidad en la Era Digital

- Aplica a todas las organizaciones que procesen datos de residentes en la UE.
- Principios:
  - licitud,
  - transparencia,
  - finalidad,
  - minimización,
  - exactitud,
  - limitación del almacenamiento,
  - integridad
  - responsabilidad.

La Seguridad de la Información como Pilar del GDPR

- Exige medidas técnicas y organizativas para proteger los datos
- Vincula directamente la ciberseguridad con la protección legal de datos.
- Ejemplos de medidas:
  - Cifrado y seudonimización.
  - Control de acceso y autenticación.
  - Gestión de vulnerabilidades y resiliencia.
  - Protocolos de notificación de incidentes (72 h).
- • Se complementa con ISO 27001, NIST CSF y COBIT 2019.

Derechos y Responsabilidades en el GDPR

- El responsable del tratamiento debe demostrar cumplimiento (accountability).
- Derechos del usuario:
  - Acceso, rectificación y supresión (derecho al olvido).
  - Portabilidad, limitación y oposición.
- Requiere 'Privacy by Design' y 'Privacy by Default'.
- Sanciones: hasta el 4 % del volumen global de negocios anual.

Privacy by Design

Protección de datos desde el diseño y por defecto” (Privacy by Design & by Default).

- Los principios son:
  - **Proactivo,** no reactivo; **preventivo**, no correctivo.
  - Privacidad como configuración por defecto.
  - Privacidad incrustada en el diseño.
  - Funcionalidad total — ganar/ganar, no suma cero.
  - Seguridad de extremo a extremo — protección completa del ciclo de vida.
  - Visibilidad y transparencia.
  - Respeto por la privacidad del usuario — centrado en el individuo.

Privacy by Design…

Estrategias técnicas complementarias:

- **Minimizar:** recolectar solo los datos estrictamente necesarios.
- **Ocultar:** proteger y enmascarar la información sensible (p. ej. cifrado)
- **Separar:** distribuir datos para evitar correlaciones innecesarias.
- **Agregar:** anonimizar o generalizar información.
- **Informar:** garantizar transparencia al usuario.
- **Controlar:** dar al usuario mecanismos para gestionar su información.
- **Cumplir:** adoptar políticas de cumplimiento verificable.
- **Demostrar: documentar y auditar decisiones de privacidad.**

Tipos de Datos Personales en el GDPR

- Datos identificativos directos: nombre, DNI, email, imagen, voz.
- Datos indirectos: IP, geolocalización, ID de dispositivo, hábitos de uso.
- Datos sensibles (Art. 9): salud, biometría, ideología, religión, orientación sexual, origen étnico.
- Datos financieros y de menores: sujetos a consentimientos y controles específicos.

Implicancias técnicas:

- Requieren medidas de ciberseguridad proporcionales al riesgo.
- Los datos sensibles exigen cifrado fuerte, segmentación de acceso y monitoreo activo.

Ciberseguridad y Técnicas de Cifrado en el GDPR

- Cifrado de datos:
  - En tránsito: TLS 1.3, HTTPS, VPN, SSH.
  - En reposo: AES-256, ChaCha20, BitLocker, LUKS.
  - Cifrado homomórfico o seudonimización para análisis.
- Control de acceso y autenticación multifactor (MFA).
- Políticas de mínimo privilegio (Least Privilege) y registros de acceso.
- Resiliencia: backups cifrados, redundancia y planes de continuidad.
- Gestión de incidentes y comunicación a autoridades en 72 h.