UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Nombre:

Felipe De Jesús González Reyes

Profesor:

Mtro. Servando López Contreras

Tema:

ITU-T X.800 / RFC 4949

martes, 27 de enero de 2026

Introducción

Los estándares X.800 y RFC 4949 son fundamentales en la arquitectura y terminología de seguridad en redes y sistemas informáticos. X.800 define un marco conceptual para la seguridad en sistemas de comunicación, incluyendo tipos de ataques, servicios de seguridad y mecanismos.

Por otro lado, RFC 4949, proporciona una definición detallada de términos y conceptos relacionados con la seguridad de la información, sirviendo como una guía para la comprensión y aplicación de principios de seguridad en entornos digitales. RFC 4949 es más amplio y actualizado en su enfoque sobre los conceptos de seguridad en la era digital.

Ambos documentos son esenciales, aunque provienen de diferentes organizaciones y tienen enfoques complementarios.

X.800 clasifica los servicios de seguridad en cinco categorías con catorce servicios específicos:

- **Autenticación:** Verificación de la identidad de entidades pares o del origen de los datos.
- **Control de Acceso:** Limitación del acceso a recursos del sistema solo a entidades autorizadas.
- **Confidencialidad:** Protección de datos contra acceso no autorizado, incluyendo la confidencialidad del flujo de tráfico.
- **Integridad:** Garantía de que los datos no han sido alterados, ya sea en flujos de mensajes o en unidades individuales.
- **No Repudio:** Prevención de que el emisor o receptor niegue la transmisión de un mensaje, con pruebas de origen o entrega.

El RFC 4949, es un documento informativo del Grupo de Trabajo de Ingeniería de Internet (IETF). Proporciona definiciones estandarizadas de términos de seguridad en la red, con el objetivo de promover la claridad y consistencia en la documentación técnica.

A diferencia de X.800, que es un marco arquitectónico, sus definiciones son ampliamente citadas y utilizadas como referencia en estándares de seguridad. Por ejemplo:

- Define confidencialidad como la propiedad de que la información no esté disponible para entidades no autorizadas.
- Distingue entre privacidad (un concepto más amplio relacionado con los derechos individuales) y confidencialidad (un servicio técnico de seguridad).
- Define servicios como autenticación de entidad par, integridad del flujo de mensajes, y no repudio con prueba de origen.

Escenario 01 Grupo LockBit

Servicios X.800 comprometidos:

- Confidencialidad: La exfiltración de información sensible
- Integridad: El cifrado masivo de los servidores compromete la integridad de los datos almacenados
- Disponibilidad: El cifrado de los servidores y la amenaza de publicación de datos hacen que los sistemas sean inaccesibles (indisponibles) para los usuarios legítimos.

Definición(es) aplicable(s) RFC 4949:

- Multi-stage attack: RFC 4949 define este tipo de ataque como una secuencia de eventos maliciosos.
- Data Breach: término definido en RFC 4949 como la exposición no autorizada de información sensible.

Tipo de amenaza:

- Ransomware: El uso de software malicioso para cifrar los datos y exigir un rescate es la característica definitoria del ataque.
- Data Leakage / Extortion: La amenaza de publicar la información robada añade una dimensión de extorsión al ataque.

Vector de ataque:

- Acceso inicial no autorizado: Esto implica que los atacantes explotaron una vulnerabilidad en la seguridad, ya sea a través de phishing, ingeniería social, explotación de vulnerabilidades de software, o credenciales comprometidas.
- Exfiltración: La exfiltración se realiza después del acceso inicial, utilizando métodos como la copia de archivos a servidores controlados por los atacantes.

Impacto técnico / operativo:

- Técnico: Cifrado de servidores, pérdida de datos, corrupción de sistemas, necesidad de reconstruir sistemas desde cero.
- Operativo: Interrupción de servicios, pérdida de productividad, daño a la reputación, posibles multas por incumplimiento de normativas (GDPR, etc.), pérdida de confianza de los clientes, costos de recuperación.

Medida de control recomendada:

- Respaldos inmutables: Implementar respaldos que no puedan ser modificados o eliminados por los atacantes.
- Detección temprana: Implementar sistemas de detección de intrusiones (IDS/IPS), monitoreo de seguridad (SIEM), y análisis de comportamiento (UEBA) para identificar actividades sospechosas en tiempo real.
- Segmentación de red: Dividir la red en segmentos para limitar el impacto de un ataque.
- Autenticación multifactor (MFA): Implementar MFA para proteger el acceso a los sistemas y datos.

Escenario 02

Servicios X.800 comprometidos

- Confidencialidad: Los datos almacenados quedaron expuestos públicamente, permitiendo acceso no autorizado a información sensible.
- Control de Acceso: Fallo en la implementación de mecanismos que restringen quién puede acceder a los recursos.

Definición(es) aplicable(s) RFC 4949

- Data Breach: Incidente de seguridad que resulta en acceso no autorizado o divulgación de información protegida.
- Vulnerability: Debilidad en el sistema que puede ser explotada para violar la política de seguridad.

Tipo de amenaza

- Amenaza no intencional / Error humano: Configuración incorrecta de permisos de acceso.
- Amenaza pasiva: No requiere acción maliciosa activa, solo observación o acceso a datos expuestos.

Vector de ataque

- Acceso directo no autenticado: URLs o endpoints públicamente accesibles sin credenciales.
- Enumeración de buckets/contenedores: Descubrimiento de recursos mal configurados en servicios cloud (S3, Azure Blob, etc.).

Impacto técnico / operativo

- Pérdida de confidencialidad de datos sensibles (PII, credenciales, información corporativa).
- Impacto legal: Violación de regulaciones, leyes de protección de datos.
- Daño reputacional: Pérdida de confianza de clientes y stakeholders.
- Sanciones económicas: Multas regulatorias y costos de remediación.

Medida de control recomendada

- Principio de mínimo privilegio: Configurar acceso privado por defecto.
- Auditorías de configuración: Revisiones periódicas automatizadas de permisos.
- Herramientas de escaneo: Implementar soluciones CSPM (Cloud Security Posture Management).
- Autenticación y autorización robusta: IAM policies, MFA, y cifrado de datos.
- Monitoreo continuo: Alertas sobre cambios en configuraciones de seguridad.
- Capacitación: Entrenamiento del personal en buenas prácticas de configuración cloud.

Escenario 03

Servicios X.800 Comprometidos

- Integridad: El código malicioso alteró el software legítimo, violando la garantía de que los datos no fueron modificados.
- Confidencialidad: Accesos no autorizados posteriores permitieron la exposición de información sensible.
- Autenticación: Se comprometió la verificación de la legitimidad del software y su origen.

Definiciones Aplicables RFC 4949

- Supply Chain Attack: Ataque que compromete un sistema mediante la explotación de vulnerabilidades en la cadena de suministro de hardware o software.
- Troyano: Código malicioso oculto dentro de software aparentemente legítimo.
- Integridad: Propiedad que garantiza que los datos no han sido alterados de manera no autorizada.

Tipo de Amenaza
Amenaza activa de tipo modificación y fabricación.

Vector de Ataque

- Compromiso del proveedor de software
- Mecanismo de actualización automática como canal de distribución del malware
- Explotación

Impacto Técnico / Operativo

- Técnico: persistencia en sistemas, escalación de privilegios
- Operativo: Interrupción de servicios, pérdida de confianza en la cadena de suministro, costos de remediación masiva
- Reputacional: Daño severo a la credibilidad del proveedor comprometido

Medidas de Control Recomendadas

1. Preventivas:
    - Verificación de integridad mediante hashes criptográficos independientes
    - Auditorías de seguridad a proveedores críticos
    - Sandbox para pruebas de actualizaciones antes del despliegue
2. Monitoreo:
    - Monitoreo de comportamiento anómalo post-actualización
    - Análisis de firmas digitales y certificados
    - EDR/XDR para detección de amenazas avanzadas
3. Correctivas:
    - Capacidad de rollback rápido de actualizaciones
    - Segmentación de red para limitar propagación lateral

Escenario 04

Servicios X.800 comprometidos

- Autenticación: Comprometido por el uso de credenciales robadas
- Control de Acceso: Afectado directamente al permitir acceso no autorizado con credenciales válidas
- Confidencialidad: Potencialmente comprometida por el acceso no autorizado durante meses

Definiciones aplicables RFC 4949

- Divulgación o pérdida de control sobre credenciales de autenticación
- Fallo en verificar correctamente la identidad del usuario real vs. el atacante
- Phishing: Técnica de ingeniería social para obtener información sensible haciéndose pasar por entidad confiable
- Acceso a sistemas sin permiso legítimo del propietario

Tipo de amenaza

- Amenaza activa: Suplantación de identidad
- Ingeniería social: Manipulación de usuarios para obtener credenciales
- Amenaza persistente: Acceso prolongado sin detección

Vector de ataque

- Phishing (correos electrónicos maliciosos)
- Ingeniería social
- Reutilización de credenciales válidas robadas

Impacto técnico / operativo

Técnico:

- Compromiso de credenciales de autenticación
- Acceso no autorizado a sistemas corporativos
- Pérdida de integridad en logs de auditoría

Operativo:

- Exposición prolongada (meses) sin detección
- Pérdida de confianza en el sistema de autenticación
- Costos de respuesta a incidentes y remediación

Medida de control recomendada

Preventivas:

- Autenticación Multifactor (MFA): Implementación obligatoria para todos los usuarios
- Filtrado de correo avanzado: Detección de campañas de phishing

Detectivas:

- Análisis de logs: Correlación de eventos de autenticación
- Alertas de acceso desde ubicaciones/dispositivos inusuales

Correctivas:

- Políticas de rotación de credenciales
- Gestión de identidades y accesos (IAM) robusta

Escenario 05

Servicios X.800 comprometidos:

- Confidencialidad: el cifrado de los sistemas productivos podría considerarse una violación de la confidencialidad.
- Integridad: La modificación o cifrado de los datos, compromete directamente la integridad de la información.
- Disponibilidad: La imposibilidad de acceder a los sistemas y datos debido al ransomware y la eliminación/cifrado de los respaldos resulta en una interrupción de la disponibilidad.

Definición(es) aplicable(s) RFC 4949:

- Destrucción de Datos: La eliminación o cifrado de datos, especialmente de los respaldos, se alinea directamente con la definición de "Data Destruction" en RFC 4949.
- Ataque Malicioso: la acción intencional realizada por un atacante con el propósito de causar daño, lo que se enmarca en la definición de un "Malicious Attack".

Tipo de amenaza:

- Ransomware: es un tipo de malware que cifra los datos y exige un rescate para su descifrado.

Vector de ataque:

- Compromiso de sistemas productivos y respaldos: El vector de ataque es la combinación de la infección inicial de los sistemas productivos con ransomware y la posterior eliminación o cifrado de los respaldos. Esto demuestra una sofisticación en la táctica del atacante.
- Posible explotación de vulnerabilidades: La infección inicial del ransomware probablemente se aprovechó de una vulnerabilidad en los sistemas o en la configuración de seguridad.

Impacto técnico / operativo:

- Técnico: Pérdida de datos, cifrado de sistemas, inoperancia de aplicaciones y servicios, corrupción de la infraestructura.
- Operativo: Interrupción de las operaciones comerciales, pérdida de productividad, daño a la reputación, posibles sanciones regulatorias, costos de recuperación, pérdida de ingresos. La ausencia de respaldos agrava significativamente el impacto.

Medida de control recomendada:

- Almacenamiento fuera de sitio: Guardar copias de seguridad en un lugar físico diferente a la ubicación principal.
- Almacenamiento en la nube: Utilizar servicios de almacenamiento en la nube

con características de inmutabilidad.
- Segmentación de red: Aislar los sistemas críticos y los sistemas de respaldo en segmentos de red separados para limitar el alcance de un ataque.
- Autenticación multifactor (MFA): Implementar MFA en todos los sistemas y aplicaciones para dificultar el acceso no autorizado.
- Actualizaciones y parches: Mantener los sistemas y el software actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

Escenario 05

Servicios X.800 comprometidos:
- Confidencialidad: Este es el servicio afectado, ya que las bases de datos fueron extraídas y vendidas, exponiendo información sensible.
- Integridad: la venta de las bases de datos podría afectar la integridad de la información si los terceros las modifican o utilizan de manera indebida.

Definición(es) aplicable(s) RFC 4949:
- Exceso de Privilegio: El escenario menciona fallas en el control de acceso por exceso de privilegios, lo que se alinea con el concepto de "privilege creep" o acumulación de privilegios que no son necesarios para el rol del empleado.

Tipo de amenaza:
- Amenaza Interna: La amenaza proviene de un empleado con acceso legítimo, lo que la convierte en una amenaza interna.

Vector de ataque:
- Abuso de Acceso Legítimo: El empleado utilizó su acceso autorizado para extraer las bases de datos. No se explotaron vulnerabilidades técnicas, lo que significa que el vector de ataque fue la acción maliciosa del empleado.

Impacto técnico / operativo:
- Técnico: Pérdida de confidencialidad de los datos.
- Operativo: Daño a la reputación de la organización, posibles consecuencias legales por la filtración de datos, pérdida de confianza de los clientes, y posibles sanciones regulatorias.

Medida de control recomendada:
- Implementación de Principio de Mínimo Privilegio: Asegurarse de que los empleados solo tengan acceso a los recursos y datos estrictamente necesarios para realizar sus funciones laborales.
- Monitoreo de Actividad de Usuarios: Implementar sistemas de monitoreo de la actividad de los usuarios para detectar comportamientos anómalos o sospechosos.
- Políticas de Seguridad Robustas: Establecer políticas claras sobre el manejo de datos sensibles, el uso de sistemas y la confidencialidad de la información.
- Auditorías de Acceso: Realizar auditorías periódicas de los derechos de acceso de los empleados para identificar y corregir cualquier exceso de privilegios.

Fuentes

Benitez, C. (2018, 3 octubre). *GoConqr - Modelo de seguridad X.800*. GoConqr. https://www.goconqr.com/es/mindmap/15401358/modelo-de-seguridad-x-800