Arquitectura de Seguridad OSI

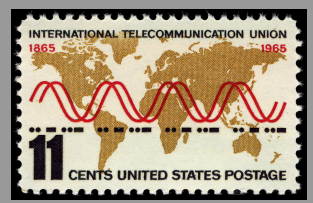
Miguel Angel Astor Romero

10 de mayo de 2019

Agenda

Unión Internacional de Telecomunicaciones

- Agencia Especial de la ONU.
- Fundada en 1865.
- Cuartel general en Ginebra, Suiza.
- Cuatro Sectores:
  - Radio (ITU-R)
  - Telecomunicaciones (ITU-T)
  - Desarrollo (ITU-D)
  - ITU Telecom



Sectores de ITU

ITU-T

Ente de estandarización para telefonía y telecomunicaciones, excepto la radio.

ITU-R

Ente de gestión del espectro radioeléctrico y comunicaciones satelitales.

ITU-D

Ente de planificación, regulación y entrenamiento en telecomunicaciones para paises en desarrollo.

Telecom

Ente de gestión de eventos en materia de telecomunicaciones.

Recomendaciones ITU-T

ITU-T produce estándares voluntarios para gran variedad de campos relacionados a la computación y telecomunicaciones.

Recomendaciones ITU-T

T.80 y T.800	JPEG y JPEG2000
X.509	PKI
H.323	Sesiones VoIP
X.200	Modelo OSI
T.30	Fax

Organización Internacional de Estandarización

- Fundada en 1947.
- Cuartel general en Ginebra, Suiza.
- Organización con estado consultivo en la ONU.
- Produce estándares en muchas áreas.

Modelo de Referencia Open Systems Interconnection

Estándares ISO 7498 e ITU-T X.200.

	Capa	PDU	Función
7	Aplicación	Datos	API's de alto nivel.
6	Presentación	Datos	Traducción de datos entre los servicios y la aplicación.
5	Sesión	Datos	Manejo de sesiones de comunicación.
4	Transporte	Segmentos Datagramas	Transmisión confiable, segmentación, multiplexado, control de flujo, etc.
3	Red	Paquetes	Esructuración de la red, enrutamiento, direccionamiento.
2	Enlace	Tramas	Transmisión confiable entre dos puntos conectados fisicamente.
1	Física	Símbolos	Transmisión y recepción de flujos de bits.

Conceptos

La recomendación ITU-T X.800 define un marco conceptual estándar para representar la seguridad de un sistema informático.

Amenaza

Posibilidad de violación de la seguridad de un sistema.

Ataque

Acción que vulnera la seguridad de un sistema.

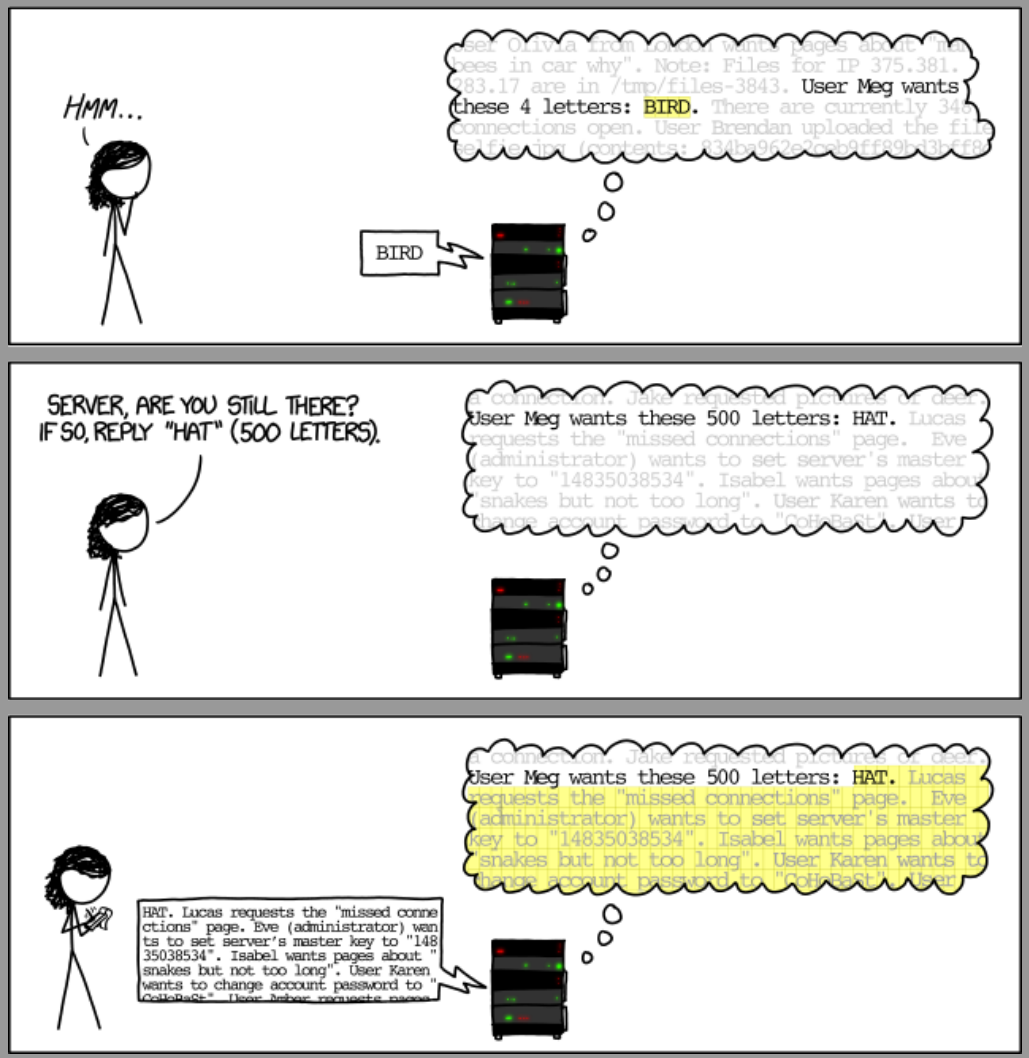
Servicio de Seguridad

Combinación de mecanismos y políticas para mejorar la seguridad de un sistema u organización.

Mecanismo de Seguridad

Herramientas, técnicas y/o algoritmos para detectar, prevenir y recuperarse de ataques.

Amenazas



Ejemplos:

- Heartbleed
- Goto Fail
- Shellshock
- SQL Injection
- Stegosploit
- XSS

Ataques

Ataques Pasivos

- Obtención del contenido de un mensaje
- Análisis de tráfico

Ataques activos

- Suplantación de identidad
- Repetición
- Modificación de mensajes
- Negación de servicio

Servicios de Seguridad

RFC 2828 Servicio de procesamiento o de comunicación proporcionado por un sistema para dar un tipo especial de protección a los recursos del mismo.

Los servicios definen políticas y son implementados por mecanismos de seguridad.

Categorías de servicios de seguridad X.800

- Autenticación
- Control de Acceso
- Confidencialidad de Datos
- Integridad de Datos
- No Repudio
- Servicio de Disponibilidad

Servicios por Categoría X.800

Autenticación

- De entidades origen/destino
- De origen de datos

Confidencialidad

- De la conexión
- No orientada a conexión
- De campos seleccionados
- De flujo de tráfico

Integridad de datos

- De conexión con recuperación
- De conexión sin recuperación
- De campos, orientada a conexión
- No orientada a conexión
- De campos, no orientada a conexión

No repudio

- De origen
- De destino

Relación entre servicios y ataques

Servicio	Obtención de mensaje	Análisis de tráfico	Suplantación de identidad	Repetición de mensaje	Modificación de mensaje	Negación de servicio
Autenticación de entidades			Y			
Autenticación de datos			Y			
Control de acceso			Y			
Confidencialidad	Y					
Confidencialidad de tráfico		Y				
Integridad de datos				Y	Y	
No repudio						
Disponibilidad						Y

Mecanismos de Seguridad

Mecanismos Específicos

- Criptografía
- Firmas digitales
- Control de acceso
- Integridad de datos
- Intercambio de autenticación
- Relleno de tráfico
- Control de enrutamiento
- Notarización

Mecanismos Generales

- Funcionalidad Confiable
- Etiquetado de seguridad
- Detección de acciones
- Informe para auditorías
- Recuperación

Modelo de Seguridad en Redes

Servicio	Cifrado	Firmas Digitales	Integridad de datos	Intercambio de autenticación	Relleno de tráfico	Control de rutas	Notarización
Autenticación de entidades	Y	Y		Y			
Autenticación de datos	Y	Y					
Control de acceso			Y				
Confidencialidad	Y					Y	
Confidencialidad de tráfico	Y				Y	Y	
Integridad de datos	Y	Y	Y				
No repudio		Y	Y				Y
Disponibilidad			Y	Y			

Internet Engineering Task Force

Internet se define como una gran red mundial de redes interconectadas mediante los llamados Protocolos de Internet, fundamentados en la pila de protocolos TCP/IP.

Nos preguntamos entonces:

- ¿Cómo se desarrollan esos protocolos que hacen funcionar al Internet?
- ¿Quienes son los encargados de desarrollar esos protocolos?
- ¿Como se logra que todos los usuarios, fabricantes y proveedores de servicio acepten utilizar los Protocolos de Internet?

¿Qué es la IETF?

La IETF es un grupo internacional de personas que contribuyen a la ingeniería y evolución de las tecnologías de Internet.

Como organización, la IETF es bastante inusual

- No posee miembros formales, ni junta directiva.
- Todos sus participantes son voluntarios.
- No posee sede y se da como una serie de sucesos.

Entonces, ¿como se puede participar en la IETF?

- La IETF se divide en múltiples *Working Groups* (WG).
- Los voluntarios se unen a los WG de su interés.
- Los sucesos de la IETF se llevan a cabo en las listas de correo de los WG y en las 3 reuniones anuales.

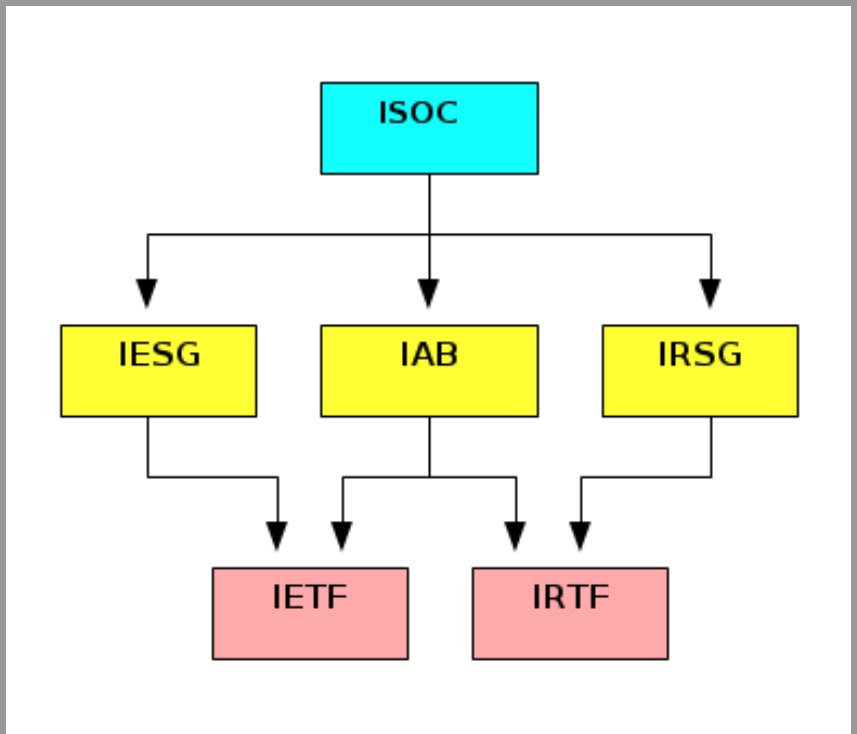
Organigrama de la IETF y grupos relacionados

Las actividades de la IETF son supervisadas por la Internet Society (ISOC).

La ISOC gestiona las siguientes organizaciones:

- Internet Engineering Steering Group (IESG)
- Internet Architecture Board (IAB)
- Internet Research Steering Group (IRSG)

Organigrama



Objetivos de la IETF

La IETF se fundamenta en un objetivo y una misión establecidos en el RFC 3935:

Objetivo principal

"Hacer que el Internet funcione mejor."

Misión de la IETF

Producir documentos técnicos de alta calidad para influenciar el diseño, uso y administración de Internet.

Principios de la IETF

Los grupos de trabajo cumplen la misión de la IETF guiados por los siguientes principios:

- Proceso abierto.
- Competencia técnica.
- Nucleo voluntario.
- Consenso approximado y código corriendo.
- Propiedad de protocolos.

Principios de la IETF

RFC 3935:

Proceso abierto

Cualquier persona interesada puede participar del trabajo, conocer que decisiones se están tomando, y dar a conocer su voz sobre los temas tratados.

Competencia técnica

Los temas sobre los cuales la IETF produce sus documentos son temas sobre los cuales la IETF posee la competencia necesaria para hablar al respecto, y en los cuales la IETF esta dispuesta a escuchar opiniones competentes provenientes de cualquier fuente.

Principios de la IETF

Núcleo voluntario

Los participantes y líderes son personas que se acercan a la IETF porque quieren trabajar para fomentar la misión de la IETF.

Propiedad de protocolos

Cuando la IETF toma propiedad de un protocolo acepta la responsabilidad de mantener todos los aspectos de dicho protocolo. De igual forma, la IETF nunca tratará de ejercer control sobre protocolos o funciones sobre las cuales no es responsable.

Principios de la IETF

Uno de los principios fundacionales de la IETF:

Consenso aproximado y código corriendo.

Hacemos estándares basados en el juicio conjunto de nuestros participantes y nuestra experiencia en la implementación y despliegue de nuestras especificaciones.

David Clark - MIT

"*We reject kings, presidents and voting. We believe in rough consensus and running code*"

Documentos producidos por la IETF

Para cumplir la misión de la IETF sus voluntarios producen una serie de documentos técnicos conocidos como *Request for Comments* (RFC). Estos documentos se agrupan en las siguientes categorías:

- *Standards Track* (STD):
  - Propuesta.
  - Borrador.
  - Estándar de Internet.
- Mejores prácticas (BCP).
- Informativos.
- Experimentales.
- Históricos.

El Internet *Standards Track*

Cuadno un borrador está lo suficientemente pulido, este es presentado a la IESG por medio del correspondiente director de área. Luego dicho borrador seguirá este ciclo de vida:

Propuesta de estándar

- No necesitan implementación, aunque esto es recomendable.
- Cualquier propuesta puede ser retractada por la IESG.

Borrador de estándar

- Poseer dos (2) implementaciones completas, interoperables y documentadas producidas de manera independiente.

Estándar de Internet

- Poseer despliegues y experiencia operativa existosa y documentada.

Non-Standards Track

Existen 3 niveles del ciclo de vida de un borrador que aplican a investigaciones y documentos de interés documental en lugar de técnico:

Experimental

El borrador en cuestión es producto de un trabajo de investigación en curso.

Informativos

Documentos de interés general para la comunidad de Internet.

Históricos

Protocolos obsoletos y otros documentos de valor histórico.

Conclusiones

- Como todo en materia de redes de computadoras, la seguridad también está estandarizada.
- Tanto la ITU-T como la IETF producen estándares en materia de seguridad informática.
- La base de estos estándares es la recomendación ITU-T X.200.

Próxima clase - 17/05/2019

- Introducción a la criptografía simétrica
- Historia de la criptografía
- Tecnicas clásicas de criptografía
- Introducción al criptoanálisis

¿Preguntas?