Temas de Interés en el ITU-T SG-17

Plan 2020

Lic. Hugo Miguel
Subsecretario de Planeamiento

Ministerio de Modernización
Presidencia de la Nación

DLT Tecnología de asientos distribuidos

- ¿Cómo deberían identificarse y definirse los aspectos de seguridad (por ejemplo, arquitectura y subsistemas de seguridad) en un entorno DLT?
- ¿Cómo deberían manejarse las amenazas y vulnerabilidades en aplicaciones y servicios basados en DLT?
- ¿Cuáles son los requisitos de seguridad para mitigar las amenazas en un entorno DLT?
- ¿Qué son las tecnologías de seguridad para admitir aplicaciones y servicios basados en DLT?
- ¿Cómo se debe mantener y mantener la interconexión segura entre entidades en un entorno DLT?
- ¿Qué técnicas de seguridad, mecanismos y protocolos se necesitan para las aplicaciones y servicios basados en DLT?
- ¿Cuáles son las soluciones de seguridad aceptables a nivel mundial para aplicaciones y servicios basados en DLT, que se basan en redes de telecomunicaciones / TIC?
- ¿Cuáles son las mejores prácticas o directrices de seguridad para aplicaciones y servicios basados en DLT?
- ¿Qué protección PII (información de identificación personal) y gestión de la seguridad de la información se necesitan para las aplicaciones y servicios basados en DLT?
- ¿Con qué partes interesadas debería colaborar SG17?

DLT Tecnología de Asientos Distribuidos

- Realizar un análisis de brechas en el trabajo actual de seguridad relevante en otras organizaciones para las tecnologías de contabilidad distribuida.
- Produzca un conjunto de Recomendaciones que brinden soluciones de seguridad integrales para aplicaciones y servicios basados en DLT.
- Estudiar los aspectos de seguridad de las aplicaciones y servicios basados en DLT, que se basan en redes de telecomunicaciones / TIC.
- Estudiar e identificar problemas de seguridad y amenazas en aplicaciones y servicios basados en DLT.
- Estudiar y desarrollar mecanismos de seguridad, protocolos y tecnologías para aplicaciones y servicios basados en DLT.
- Estudiar y desarrollar mecanismos seguros de interconectividad para aplicaciones y servicios basados en DLT.
- Estudiar e identificar problemas y amenazas de protección PII en aplicaciones y servicios basados en DLT.
- Estudiar y desarrollar un sistema de gestión de la información para las entidades que proporcionan aplicaciones y servicios basados en DLT.

Aspectos de seguridad de los servicios de telecomunicaciones, redes e Internet de las cosas

-) ¿Cómo deben identificarse y definirse los aspectos de seguridad de los servicios y redes de telecomunicaciones en las telecomunicaciones móviles?
  b) ¿Cómo deben identificarse y manejarse las amenazas detrás de los servicios y redes de telecomunicaciones?
  c) ¿Cuáles son las tecnologías de seguridad para apoyar los servicios y redes de telecomunicaciones?
  d) ¿Cómo se debe mantener y mantener la interconectividad segura entre los servicios de telecomunicaciones y las redes?
  e) ¿Qué técnicas, mecanismos y protocolos de seguridad se necesitan para los servicios y redes emergentes de telecomunicaciones, especialmente para los servicios emergentes de protección de contenidos digitales?
  f) ¿Cuáles son las soluciones de seguridad global para los servicios y redes de telecomunicaciones (por ejemplo, incluidos los servicios para redes inteligentes que se basan en redes de telecomunicaciones / TIC)?
  g) ¿Cuáles son las mejores prácticas o directrices para servicios y redes de telecomunicaciones seguros?
  h) ¿Qué mejoras a las Recomendaciones actualmente bajo revisión o nuevas Recomendaciones en desarrollo deberían adoptarse para reducir el impacto en los cambios climáticos (por ejemplo, ahorro de energía, reducción de emisiones de gases de efecto invernadero, implementación de sistemas de monitoreo) directa o indirectamente en telecomunicaciones / TIC o en otras industrias?
  i) ¿Qué mecanismos de protección y gestión PII (información de identificación personal) se necesitan para servicios y redes de telecomunicaciones seguros?

Aspectos de seguridad de los servicios de telecomunicaciones, redes e Internet de las cosas

-) En colaboración con otros grupos de estudio del UIT-T y organizaciones de desarrollo de normas, especialmente con IETF, ISO / CEI JTC 1 / SC 6, 25, 27 y 31, producir un conjunto de Recomendaciones para proporcionar soluciones de seguridad completas para servicios y redes de telecomunicaciones seguros.
  b) Revisar las Recomendaciones / Estándares existentes de ITU-T, ISO / IEC y otros organismos de normalización en el área de red doméstica, red inteligente, red móvil (incluida la seguridad de teléfonos inteligentes), servicio de IoT móvil y red de sensores ubicua para identificar servicios de telecomunicaciones seguros y redes.
  c) Estudie más a fondo para definir los aspectos de seguridad de los servicios y redes de telecomunicaciones para un entorno de telecomunicaciones internacionales de múltiples proveedores y para los nuevos servicios emergentes. (por ejemplo, para aquellos para redes inteligentes que se basan en redes de telecomunicaciones / TIC).
  d) Estudiar e identificar problemas de seguridad y amenazas en servicios y redes de telecomunicaciones seguros.
  e) Estudiar y desarrollar mecanismos de seguridad para servicios y redes de telecomunicaciones seguros.
  f) Estudie y desarrolle mecanismos de interconectividad para servicios y redes de telecomunicaciones seguros en un entorno de telecomunicación de proveedor único o de múltiples proveedores.
  g) Estudiar e identificar los problemas y amenazas de protección PII en servicios y redes de telecomunicaciones seguros.
  h) Estudiar y desarrollar mecanismos de protección y gestión de PII para servicios y redes de telecomunicaciones seguros.

Seguridad informática en la nube

- a) Qué nuevas Recomendaciones u otro tipo de documentos deben desarrollarse para actores principales como proveedores de servicios, usuarios de servicios y socios de servicios, y otras partes interesadas clave de la industria para avanzar la seguridad de la computación en la nube ?
  b) ¿Qué nuevas Recomendaciones deberían desarrollarse para la arquitectura de seguridad y la organización de funcionalidades de seguridad en línea con la arquitectura de referencia?
  c) ¿Qué nuevas Recomendaciones deberían desarrollarse para los mecanismos de aseguramiento, las tecnologías de auditoría y la evaluación de los riesgos asociados para establecer la confianza entre los diferentes actores?
  d) ¿Qué colaboración es necesaria para minimizar la duplicación de esfuerzos con otras Preguntas, grupos de estudio y ODS?
  e) ¿Cómo debería desarrollarse la seguridad como servicio para proteger los sistemas de telecomunicaciones / TIC?

Seguridad informática en la nube

- a) Desarrollar Recomendaciones u otro tipo de documentos para avanzar en la seguridad de la computación en la nube.
  b) Desarrollar Recomendaciones para identificar requisitos de seguridad y amenazas para proteger servicios de computación en la nube basados en los requisitos generales de computación en la nube especificados por la Comisión de Estudio 13 del UIT-T.
  c) Desarrollar Recomendaciones para definir la arquitectura de seguridad y organizar funciones de seguridad basadas en la arquitectura de referencia especificado por la Comisión de Estudio 13 del UIT-T.
  d) Elaboración de Recomendaciones para definir una arquitectura de seguridad fuerte, flexible y elástica y la implementación de sistemas de computación en la nube.
  e) Desarrollar Recomendaciones para identificar mecanismos de aseguramiento, tecnologías de auditoría, evaluación de riesgos con el objetivo de lograr relaciones confiables dentro del ecosistema de computación en la nube.
  f) Encargarse de todas las actividades de la Comisión de Estudio 17 sobre seguridad informática en la nube.
  g) Representación del trabajo de la Comisión de Estudio 17 relacionado con la seguridad de la computación en la nube en la Actividad de Coordinación Conjunta sobre computación en la nube.
-

Lenguajes formales para software de telecomunicación y pruebas

- Las **cuestiones de** estudio que se considerarán incluyen, entre otras:
  a) ¿Qué mantenimiento de las definiciones de los lenguajes de diseño de sistemas de la UIT (excepto ASN.1) se adapta a los requisitos actuales de los usuarios y se necesitan nuevas arquitecturas y marcos emergentes?
  b) ¿Qué nuevos idiomas se necesitan para otros requisitos contemporáneos de los usuarios y nuevas arquitecturas y marcos emergentes (como la Internet de las cosas) teniendo en cuenta la Recomendación UIT-T Z.110?

Lenguajes formales para software de telecomunicación y pruebas

- a) Mantener recomendaciones bajo la responsabilidad de esta Cuestión;
  b) Proporcionar asesoramiento general a los usuarios de los idiomas, metodología (y / ies), marco (s) para el (los) idioma (s) cubierto (s) por el estudio de la Cuestión;
  c) Promover el uso de las metodologías, los marcos y los idiomas cubiertos por el estudio de la Cuestión dentro de otros grupos de estudio y SDO externos.

Arquitectura de gestión de identidad y mecanismos

- a) ¿Cuáles son los conceptos funcionales para una infraestructura de gestión de identidad común (IdM)?
  b) ¿Qué es un modelo IdM apropiado que es independiente de las tecnologías de red, admite la participación centrada en el usuario, representa información IdM y admite el intercambio seguro de información IdM entre las entidades involucradas (por ejemplo, usuarios, partes confiantes y proveedores de identidad)?
  c) ¿Cuáles son los componentes necesarios para unificar IdM social, móvil y empresarial de una manera que promueva transacciones digitales más seguras?
  d) ¿Cuáles son los aspectos funcionales de los modelos IdM?
  e) ¿Cuáles son los requisitos específicos de IdM de los proveedores de servicios y consumidores de servicios?
  f) ¿Cuáles son los atributos de las identidades que pueden compartir los proveedores de identidades dentro de los marcos de confianza?
  g) ¿Cuáles son los requisitos, las capacidades y las posibles estrategias para lograr la interoperabilidad entre diferentes sistemas de IdM (por ejemplo, aseguramiento de identidad, inter-trabajo)?

Arquitectura de gestión de identidad y mecanismos

- h) ¿Cuáles son los mecanismos candidatos para la interoperabilidad de IdM para incluir la identificación y definición de perfiles aplicables para minimizar los problemas de interoperabilidad?
  i) ¿Cuáles son los requisitos y mecanismos para proteger y prevenir la divulgación de información de identificación personal (PII)?
  j) ¿Cuáles son los requisitos para proteger los sistemas IdM de los ciberataques?
  k) ¿Qué capacidades de IdM se pueden usar contra los ciberataques?
  l) ¿Cómo se debería integrar IdM con las tecnologías de seguridad avanzadas?
  m) ¿Qué requisitos únicos de IdM están asociados con la computación en la nube?
  n) ¿Qué requisitos únicos de IdM están asociados con la informática móvil?
  o) ¿Qué requisitos únicos de IdM están asociados con diversos entornos distribuidos, como IoT y la nube?
  p) ¿Cómo se puede integrar la prueba de identidad en los sistemas IdM?
  q) ¿Cómo se puede integrar la administración segura de credenciales en los sistemas IdM?
  r) ¿Cómo se pueden integrar las tecnologías de autenticación en los sistemas IdM?

Ciberseguridad

- a) ¿Cómo deben los proveedores de telecomunicaciones / TIC asegurar su infraestructura, mantener operaciones seguras y utilizar mecanismos de garantía de seguridad en las redes de telecomunicaciones / TIC?
  b) ¿Cuáles son los requisitos de seguridad que el software, los protocolos de telecomunicaciones, los diseñadores de sistemas de comunicaciones y los fabricantes deben tener en cuenta en el diseño, desarrollo e intercambio de las mejores prácticas en el entorno cibernético?
  c) ¿Cómo debería compartirse la información de vulnerabilidad de manera eficiente para ayudar en los procesos del ciclo de vida de la vulnerabilidad?
  d) ¿Qué requisitos y soluciones se necesitan para asegurar las telecomunicaciones / TIC de la resiliencia, seguridad e integridad de los sistemas?
  e) ¿Qué requisitos y soluciones se necesitan para la rendición de cuentas de telecomunicaciones / TIC, la respuesta a incidentes y el monitoreo de amenazas y la comunicación de riesgos?

Ciberseguridad

- f) ¿Qué mecanismos se necesitan para compartir la seguridad y la información relacionada con la seguridad de los sistemas habilitados para ciber, incluidos los sistemas basados en la nube?
  g) ¿Cómo se pueden usar las redes para proporcionar servicios críticos, como el uso de un protocolo de alerta común, de manera segura durante las emergencias nacionales?
  h) ¿Cuáles son las pautas de seguridad necesarias y las mejores prácticas para identificar, mitigar y reducir el impacto de las amenazas cibernéticas, incluido el malware, la denegación de servicio distribuida y la ingeniería social?
  i) Qué mejoras a las Recomendaciones actualmente en revisión o nuevas Recomendaciones en desarrollo deberían adoptarse para reducir el impacto en los cambios climáticos (por ejemplo, ahorro de energía, reducción de emisiones de gases de efecto invernadero, implementación de sistemas de monitoreo) directa o indirectamente en telecomunicaciones / TIC o en otras industrias?

Muchas Gracias

Ministerio de Modernización
Presidencia de la Nación