ENCUENTRO PRE IETF 113 – Lac

Miércoles 9 de marzo, 2022. 16:00h – 17:30h (UTC-3)

Hora	Presentación	Descripción
16:00	**Bienvenida**	Coordinación del grupo IETF-Lac
16:10	**Control de congestión para optimización de latencia y reparto justo de capacidad** Alejandro Popovsky	Proyecto ganador de la convocatoria Frida de LACNIC 2020, busca aliviar la congestión en Internet provocada por los mismos mecanismos que buscan maximizar la velocidad de transferencia, pero que generan retardos significativos a las personas usuarias. Considerando que el comportamiento individual de los dispositivos conectados a Internet provoca congestión y disminución de la calidad de la experiencia de navegación, busca compatibilizar el tráfico de contenido multimedia con el de servicios transaccionales. Una primera fase de esta investigación fue presentada en el *Congestion Control Research Group* de la IRTF 2016. Más info aquí.
16:25	**Gestão de vulnerabilidades para redes de IOT** Sávyo Morais	Este draft propõe a Intra-Network eXposure Utility (INXU) como uma solução de gestão de vulnerabilidades para redes IoT. O objectivo da INXU é alargar as funções do RFC 8520 para a protecção de múltiplas redes heterogéneas de IoT. A INXU identifica e analisa a capacidade de um dispositivo IoT que está a ser explorado por uma actividade maliciosa bem conhecida. É também proposto um modelo de dados para descrever o tráfego relacionado com actividades maliciosas. Mais info aquí.
16:40	**Deteccion unilateral de DNS Cifrado** Joey Salazar	DoH, Dot, y DoQ han normalizado opciones de cifrado del DNS en las comunicaciones entre cliente y servidor. Pero mucho queda por definirse para la proteccion de datos de DNS en las communicaciones entre servidores recursivos a servidores autoritativos. Este draft establece los pasos que dichos servidores DNS (recursivos y autoritativos) pueden tomar unilateralmente para defender la privacidad de las consultas DNS contra un monitoreo pasivo de la red. El objetivo es simplificar y acelerar el despliegue del transporte cifrado en el salto recursivo-autoritario del ecosistema DNS, para facilitar la futura especificación de metodos más fuertes, i.e uso de señalización para protejer contra ataques activos. Más info aquí.
16:55	**La red de servidores de llaves OpenPGP** Gunnar Wolf	Muchos proyectos utilizan el cifrado o las firmas OpenPGP para diversas tareas importantes, como la definición de los miembros, la autenticación de la participación, la afirmación de la identidad sobre una votación, etc. Pero su funcionamiento, basado en un modelo de malla de confianza transitiva (Web-of-Trust), que permite asignar de forma descentralizada la confianza en la identidad de una persona determinada, está en peligro debido a los ataques al protocolo de distribución de claves. Hace poco el Open Specification for Pretty Good Privacy-WG en IETF se reactivó para revisar y actualizar el RFC4880 que define el estándar OpenPGP, concentrándose en los mecanismos criptográficos. Este trabajo revisa el modelo distribuido de gestión de llaves en redes de servidores.
17:10	Preguntas y respuestas	
17:30	Cierre	