Relatoría LACIGF

Título de la sesión: Sesión 8 – Protección del cifrado y las implicancias a las comunicaciones seguras en Internet

Resumen de la sesión:

La sesión 8 trató del uso del cifrado, empezando con una introducción técnica y después con discusión de temas como regulación de su uso e inclusión de género en encriptación.

La primera panelista, **Nathalia Sautchuk (Internet Society Brasil, Brasil),** introdujo técnicamente el cifrado. Ella presentó, como motivación para su uso, los escenarios de aplicaciones de mensajería instantánea, *e-commerce* e *internet banking*; seguido de la definición de cifrado, basada en los conceptos de texto claro, texto cifrado, clave y algoritmo. Nathalia también dijo que no hay algoritmo de cifrado 100% seguro, pero es posible alcanzar uno que sea computacionalmente seguro, con base en métricas de tiempo y costo para romper el sistema criptográfico. Después de decir que seguridad por oscurantismo no es recomendado, por hacerlo imposible auditar el algoritmo, la panelista calificó algoritmos de cifrado basado en el número de claves (simétrico o clave pública); en el tipo de operación (reemplazo o transposición); modo de procesamiento (bloque o flujo). Por fin, Nathalia citó tres puntos que deben considerarse para la evaluación de seguridad de una aplicación: si su código es abierto; si el cifrado es de punta a punta; y si es usado forward secrecy, en que una clave es creada por cada nueva sesión.

La moderadora, **Adela Goberna (ALAI, Argentina)**, agradeció a Nathalia por sus palabras y propuso las preguntas: “¿Cuáles son los principios del uso técnico del cifrado?” y “¿Cómo es su costo beneficio?".

Dadas las tres propiedades de seguridad que proporciona el cifrado (es decir, confidencialidad, integridad y autenticidad), la segunda panelista, **Veridiana Alimonti (EFF, Brasil)** afirmó que el cifrado también se puede utilizar para garantizar otros derechos, como la libertad de expresión. Sin embargo, ella cuestionó cuál debería ser la regulación del cifrado, argumentando que una regulación incorrecta podría dar lugar a infracciones de los derechos.

Daniela Macías (Dirección Nacional de Registro de Datos Públicos, Ecuador) afirmó que un elemento esencial de la tecnología es la comunicación y, por lo tanto, es muy importante garantizar que este elemento sea seguro. Esto se puede hacer, por ejemplo, mediante el uso de cifrado. Ella también destacó la importancia y los intentos de crear normas sobre el uso de cifrado, agregando que las reglas deben ser amplias para no limitar los derechos; y dijo que el cifrado es esencial para garantizar la protección de los datos personales, pero aclarando que otras medidas deben usarse juntas, siendo el cifrado sólo una pequeña parte de esta protección.

María Cristina Capelo (Facebook, México) empezó diciendo que el cifrado de punta-a-punta es importante para la privacidad y seguridad, pero enfatizando que no es una tecnología perfecta, debiendo por eso, tener un equilibrio social. Maria afirmó que WhatsApp, uno de los productos de la compañía que representa, usa cifrado de punta-a-punta por defecto; y

Messenger, otro producto, puede tener este tipo de cifrado habilitado. Maria también afirma que el usuario debe tener el poder de elegir la plataforma que utilizará. Eso porque cualquier atacante explotará cualquier vulnerabilidad y el uso de alguna funcionalidad podría generar una vulnerabilidad (por ejemplo, hacer una copia de seguridad en la nube puede comprometer el cifrado).

Angélica Contreras (FemHackPartyLAC y Women SIG, México) tuvo su discurso más enfocado en cuestiones de inclusión de género en el uso del cifrado, afirmando que muchas mujeres son víctimas de violencia y vigilancia en el entorno digital, y que el uso del cifrado puede ayudar con esto, debido a sus propiedades de seguridad. La panelista, sin embargo, mencionó problemas de alfabetización digital e inclusión lingüística, ya que muchas documentaciones de tecnologías criptográficas no están escritas en muchos idiomas de los pueblos latinoamericanos. Esta falta de diversidad lingüística no promueve la inclusión digital.

Outputs y otros links relevantes:
Sesión completa en: https://youtu.be/8TJIzVp_yjE

Por: Gabriel Arquelau Pimenta Rodrigues (Universidade de Brasília, Brasil), Flavio Andre Garces Heredia (Colombia)

Revisado por: Pablo Jordan (Internet Society Bolivia, Bolivia)

Coordinación y edición: Nathalia Sautchuk Patrício (NIC.br, Brasil) y Guilherme Alves (Youth Observatory, Brasil)