26 de Marzo de 2021

Actividad 2.4.2

Seminario técnico en línea de INTERPOL: Cripto para las autoridades de justicia penal

7 – 16 Abril 2021

Proporcionado bajo el proyecto GLACY +

Contorno

Antecedentes y justificación

A medida que el uso y la dependencia de la tecnología de la información se generalizan cada vez más en la sociedad, la explotación y los ataques contra los sistemas informáticos también se han vuelto cada vez más común. Los delitos relacionados con las computadoras han aumentado rápidamente tanto en número como en sofisticación y las autoridades de justicia penal están llamadas a enfrentar un número cada vez mayor de desafíos a fin de garantizar una investigación eficiente y un enjuiciamiento exitoso de los delitos relacionados. Muchos países han realizado esfuerzos en los últimos años para establecer unidades especializadas en delitos cibernéticos a nivel de autoridades policiales, así como unidades responsables de la ciencia forense digital.

La criptografía es uno de los principales facilitadores tecnológicos de la tecnología tan ampliamente utilizada por el público. Sin esta herramienta, la poca confianza en Internet habría impedido que la red creciera tanto. Sin embargo, el conocimiento de la criptografía no se ha cubierto lo suficiente en el contexto de la capacitación policial. En el marco del proyecto GLACY+, este tema de formación se experimentó por primera vez en la formación de las unidades de primera respuesta organizada por el Grupo Europeo de Formación y Educación sobre Ciberdelincuencia (ECTEG) e INTERPOL en septiembre de 2020 como parte del módulo E-First.

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Resultado esperado

La capacitación tiene como objetivo proporcionar el conocimiento y la comprensión conceptual de la criptografía necesarios para los funcionarios de la autoridad de justicia penal, incluidos:

Parte I. Conceptos criptográficos

- Características y capacidades de una buena función hash criptográfica
- Cómo se almacenan y se roban las contraseñas
- Orientación conceptual de algoritmos en el contexto de la criptografía antigua
- Criptografía simétrica moderna con bloques y las capacidades que proporciona
- Cómo dos partes pueden compartir la clave secreta en presencia de un espía/interceptor (Internet)
- Por qué las claves públicas reutilizables son útiles para redes con grandes participantes
- Cómo se realizó el concepto de clave pública (ejemplo de RSA)
- Capacidades de no repudio del cifrado de la clave pública

Parte II. Criptografía aplicada

- Cómo se aplicó el cifrado de clave pública para convertirse en el icono de candado (https) en la barra de direcciones del navegador web.
- ¿Cuánta confianza podemos dar a los certificados y por qué (HTTP: quién verifica la entidad y cómo?)
- Cómo se aplica el hash y el cifrado de clave pública en las transacciones de Blockchain y criptomonedas en Bitcoin.

Los participantes

Se prevé la participación de los organismos encargados de hacer cumplir la ley y otras entidades públicas desempeñando funciones en el área, en base a las competencias y responsabilidades requeridas en la agenda.

Por lo tanto, los participantes recomendados incluirán:

- Agentes encargados de hacer cumplir la ley cuyo trabajo diario implica delitos cibernéticos y pruebas electrónicas
- Fiscales y jueces que quieran aprender y participar en este tema
- Instructores de instituciones gubernamentales responsables de la capacitación sobre el tema

Programa preliminar (borrador)

Fecha y hora	Temática
Mie. 7 de Abril 20:00 UTC 14:00 EST	**Seminario web 1. Conceptos básicos de hash y criptografía** – Función hash criptográfica, contraseñas. – Algoritmos de criptografía antigua
Vie. 9 de Abril 20:00 UTC 14:00 EST	**Seminario web 2. Criptografía simétrica** – Criptografía simétrica moderna con bloques – Compartir la clave secreta en presencia de un espía/interceptor Internet
Lun. 12 de Abril 20:00 UTC 14:00 EST	**Seminario web 3. Criptografía asimétrica** – Por qué las claves públicas reutilizables son útiles para redes con grandes participantes – Cómo se realizó el concepto de clave pública (ejemplo de RSA). – Capacidades de no repudio del cifrado de clave pública
Mie. 14 de Abril 20:00 UTC 14:00 EST	**Seminario web 4. Confianza en Internet: certificados digitales** – Cómo se aplicó el cifrado de clave pública para convertirse en el icono de candado (https) en la barra de direcciones del navegador web. – ¿Cuánta confianza podemos dar a los certificados y por qué (HTTPs: quién verifica la entidad y cómo?)
Vie. 16 de Abril 20:00 UTC 14:00 EST	**Seminario web 5. Fundamentos de las criptomonedas** – Cómo el hash habilitó la verificación de la integridad de los datos (ejemplo de Blockchain) – Cómo el cifrado de clave pública habilitó las transacciones de Bitcoin

Contactos

En el Consejo de Europa:

Sra. Catalina STROE
Project Manager
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Email: catalina.stroe@coe.int

En INTERPOL:

Sr. Donguk KIM
Specialized Officer, GLACY+ Project
INTERPOL Cybercrime Directorate
Singapore
Tel: +65 9679 4719
Email: d.kim@interpol.int