Criptografía moderna para Aplicaciones Web

Protección de datos

Prefacio

- ¿Quien es el presentador?
- ¿Para quién es este taller?
- Requisitos
- Organización
- ¿Que no cubriremos?

Contacto

Página web

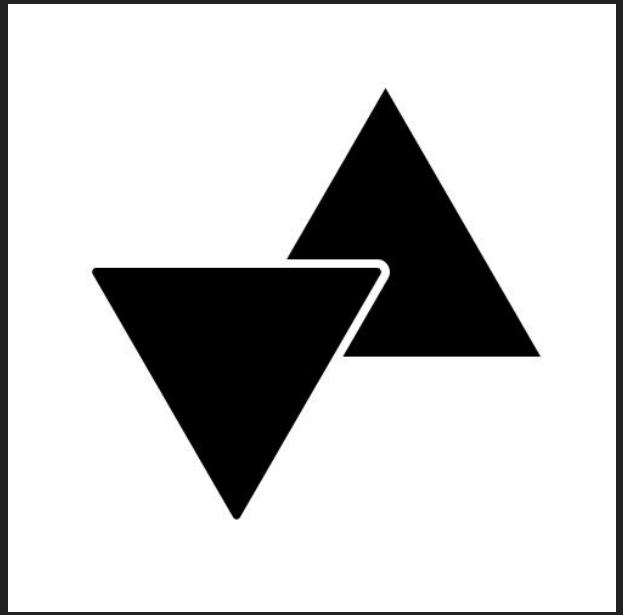
https://www.liesware.com/

Twitter

https://twitter.com/liesware

Mail

liesware@liesware.com



Dia 1

- Fugas de información
- Datos en movimiento, en descanso y en uso
- Protección de datos
- Algoritmos criptográficos
- OpenSSL

Día 2

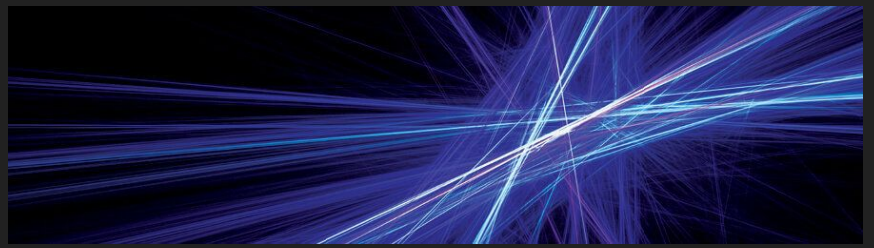
- Técnicas de protección de datos en movimiento
- Técnicas de protección de datos en descanso
- Técnicas de protección de datos en uso

Día 3

- Caso de estudio Telegram
- Implementación de propio protocolo criptográfico
- Sección de preguntas y respuestas
- Práctica

Highlights

- Cinco de las seis principales empresas del mundo por valoración de mercado son empresas de datos.
- El impacto de la violación de datos
- Los datos son lo más valioso



Las 100 empresas más grandes del mundo por valor de mercado en 2018.

- Apple
- Amazon.com
- Alphabet
- Microsoft
- Facebook
- Alibaba
- Berkshire Hathaway
- Tencent Holdings
- JPMorgan Chase
- ExxonMobil

Impacto de una fuga de información

Ashley Madison to Pay $11.2 Million to Data Breach Victims

Los datos son lo más valioso

- Basados en costos: el valor se determina en función del costo para producir los datos.
- Basados en el mercado: el valor se determina en función del precio de mercado de productos equivalentes o la disposición de los usuarios a pagar por los datos.
- Basados en los ingresos: el valor se define estimando los flujos de efectivo futuros que se pueden derivar de los datos.
- Monetización de beneficios: el valor se calcula definiendo los beneficios de productos de datos particulares, como un censo, y luego monetizando los beneficios.
- Bados en el impacto: el valor se determina evaluando el efecto causal de la disponibilidad de datos en los resultados económicos y sociales, o los costos en términos de ineficiencias o decisiones políticas deficientes debido a datos limitados o de mala calidad.

Top 2018

Aadhaar

- Cuentas de clientes afectadas: 1.1 mil millones (1 de cada 7 personas en el planeta!)
- Fecha de divulgación: 3 de enero de 2018.
- Aadhaar es un número de identidad único de 12 dígitos que pueden obtener los ciudadanos de la India

TOP 2018

Marriott Hotels

- Cuentas de clientes afectadas: 500 millones.
- Fecha de divulgación: 30 de noviembre de 2018.
- Marriott Hotels es una compañía que debido a una reciente adquisición ahora es propietaria de la cadena Starwood Hotels (Sheraton, St. Regis, Westin, W Hotels entre otros)

TOP 2018

Exactis

- Cuentas de clientes afectadas: 340 millones.
- Fecha de divulgación: 26 de junio de 2018.
- Exactis es un firma dedicada a la venta de datos

TOP 2018

Facebook

- Cuentas de clientes afectadas: un total de 257 millones en 3 incidentes separados.

- Cuentas de clientes afectadas: 87 millones.
- Fecha de divulgación: 17 de marzo de 2018.

- Cuentas de clientes afectadas: 120 millones.
- Fecha de divulgación: 27 de junio de 2018.

- Cuentas de clientes afectadas: 50 millones.
- Fecha de divulgación: 25 de septiembre de 2018.

Top 2018

- Under Armour - 150 millones
- Quora - 100 millones
- MyHeritage - 92 millones
- Cathay Pacific - 9.4 millones
- SingHealth - 1.5 millones
- British Airways - 380 mil

Resumen 2017 - 2018/2

Gemalto data breach report

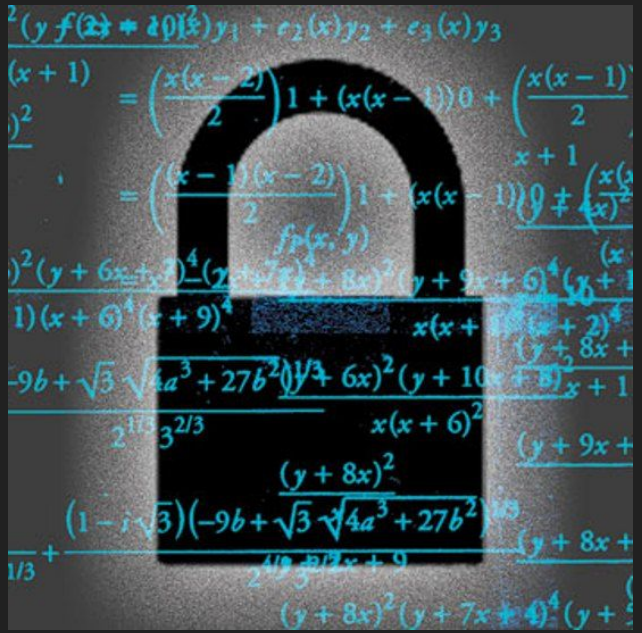
Aún más

- Collection #1
- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- https://breachlevelindex.com/

Criptografía

- Confidencialidad
- Integridad
- Autenticidad

- Funciones hash
- Criptografía Simétrica
- Criptografía Asimétrica
- Números aleatorios



Triada de la información

Enveil triad

Datos en movimiento

- TLS
- TOR
- VPN
- Wireguard
- SSH

Datos en descanso - Datos en uso

- Veracrypt
- Node.js - Javascript
- Coherence
- HSM
- Acra
- Enveil
- Vaultprotect
- SQLCipher

¿Por qué persiste?

1. Falta de conocimiento
2. Integración compleja
3. Falta de características