Un vistazo a la tokenización

Presentan

Daniel Ayala Zamorano

daz23ayala@gmail.com

Laura Natalia Borbolla Palacios

ln.borbolla.42@gmail.com

Ricardo Quezada Figueroa

qf7.ricardo@gmail.com

Sandra Díaz Santiago

sdiazs@gmail.com

Primera Reunión de Ciberseguridad para la Industria 4.0
Puebla, 14 de octubre de 2018

Escuela Superior de Cómputo
Instituto Politécnico Nacional

Contenido

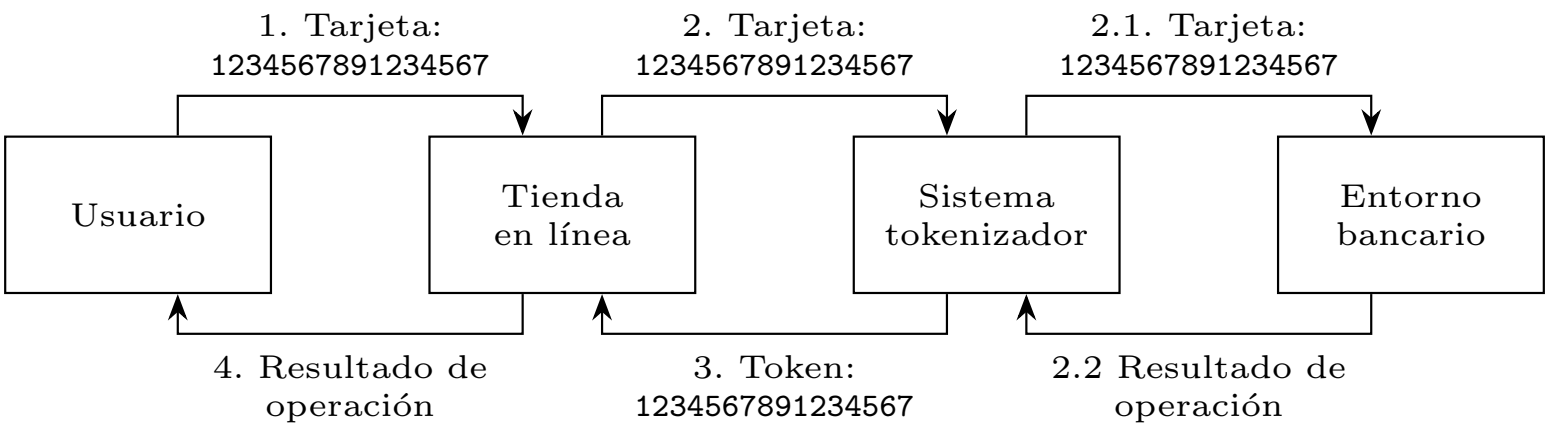
El problema de la protección de datos bancarios

- El crecimiento del comercio en línea aunado a sistemas débilmente protegidos propició un incremento en los robos de datos bancarios.
- En el 2004 se publicó el PCI DSS[1].
- Hasta este momento el enfoque es proteger la información en todo lugar en el que se encuentre.
- A pesar de la publicación del estándar, las filtraciones de datos no han terminado.

[1] *Payment Card Industry, Data Security Standard*

¿Qué es la tokenización?

- Es la sustitución de datos sensibles por valores representativos sin una relación directa.
- Existen muchas empresas que proveen el servicio de tokenización, pero lo hacen sin detallar la forma en la que se realiza.
- En 2011 el PCI publicó las guías para la tokenización.



Arquitectura típica de un sistema tokenizador.

Clasificación de los algoritmos tokenizadores

Clasificación del PCI:

- Reversibles
  - Criptográficos
  - No criptográficos
- Irreversibles
  - Autenticables
  - No autenticables

Clasificación propuesta:

- Criptográficos
  - Reversibles
  - Irreversibles
- No criptográficos

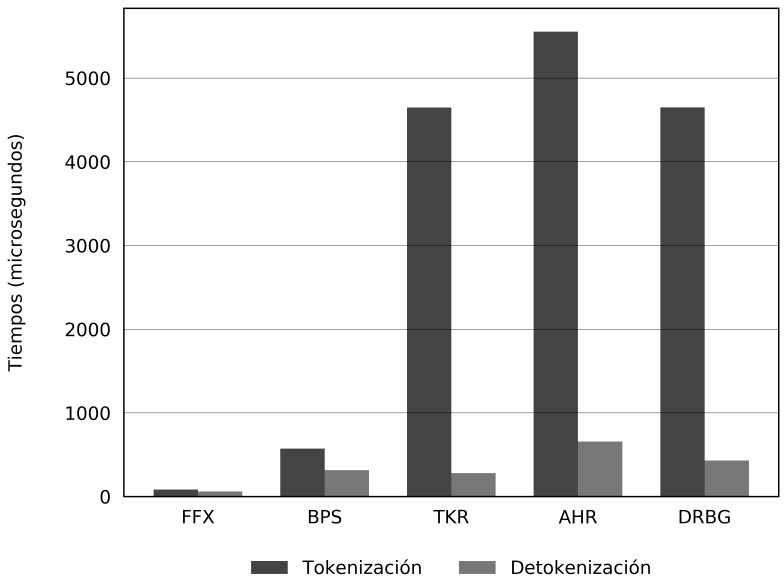
Métodos reversibles: FFX y BPS

- Métodos que utilizan cifrados que preservan el formato.
- Cifran la tarjeta y descifran el token.
- Se volvieron estándares en 2016 y fueron renombrados por el NIST a FF1 y FF3 respectivamente.
- Están basados en redes Feistel.

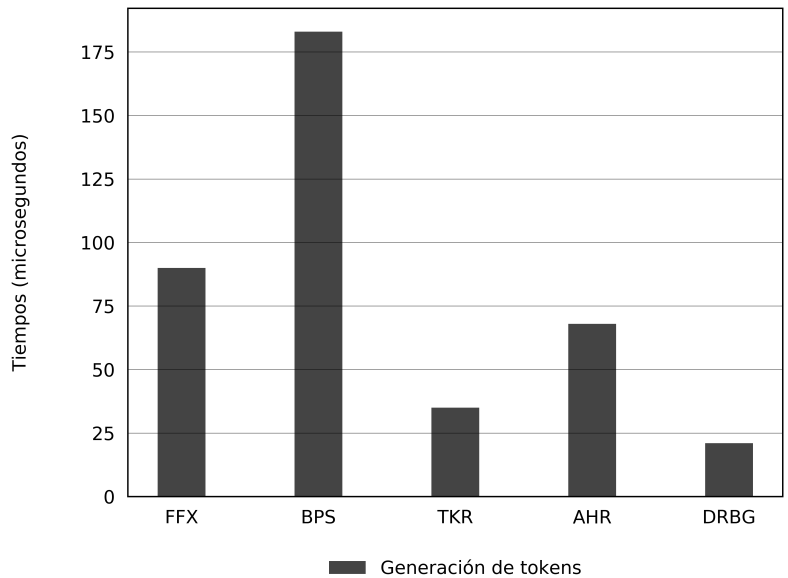
Métodos irreversibles: TKR, AHR y DRGB

- Utilizan varias primitivas criptográficas (cifrados por bloque, funciones HASH, generadores pseudoaleatorios).
- Requieren guardar la relación tarjeta-token.
- Su desempeño está ligado a la base de datos.

Resultados



(a) Tokenización y detokenización



(b) Generación de tokens

Conclusiones

- NO tenemos conclusiones, gracias.

Bibliografía I

Un vistazo a la tokenización

Presentan

Daniel Ayala Zamorano

daz23ayala@gmail.com

Laura Natalia Borbolla Palacios

ln.borbolla.42@gmail.com

Ricardo Quezada Figueroa

qf7.ricardo@gmail.com

Sandra Díaz Santiago

sdiazs@gmail.com

Primera Reunión de Ciberseguridad para la Industria 4.0
Puebla, 14 de octubre de 2018

Escuela Superior de Cómputo
Instituto Politécnico Nacional