Securosis

Presents

Tokenization Guidance

Adrian Lane

Outline

- PCI Tokenization Supplement: Highlights
- What's missing from the official story
- Overview of tokenization
- Tokenization Guidance

Objectivity Disclaimer

This webcast is sponsored by Prime Factors Inc, but all of the content is developed independently and represents Securosis objective research positions.

For more information about our Totally Transparent Research process, visit:

https://securosis.com/about/totally-transparent-research

Securosis

PCI Security Standards Council on Tokenization

Securosis

PCI Tokenization 'Information Supplement'

- August 2011 the PCI Council released a supplement on tokenization
- It described tokenization, how tokenization is used to **replace** credit card data, and discussed some deployment models
- It provides a security guide for token vaults
- It introduces new risks unique to tokens

Securosis

So what's the big deal about that?

Securosis

What was not said:

- It did not describe how security is improved
- It does address how tokenization augments the PCI standard
- It failed to or advise auditors on what to audit or how assessments will change
- In essence it talks about tokenization *without* providing guidance

Securosis

And that's a problem ...

- Tokenization removes credit cards and sensitive data
- Tokenization may replace encryption
- Tokenization alters audits and reports
- Location of the vault and how it's accessed is critical to security
- 'Maximizing PCI DSS Scope Reduction' says everything needs to be evaluated
- At the very least tokenization alters PCI DSS requirements if not replacing some

Securosis

- Audit checklists
- Updated self-assessments
- Transition & deployment
- Vendor lock-in concerns
- Definition of 'distinguishability'
- Token fraud
- Definitive endorsement

Merchant & Auditors left in the dark.

Securosis

"Any system component or process with access to the tokenization system or the tokenization/ de-tokenization process is considered in scope."

"Information provided here does not replace or supersede requirements in the PCI Data Security Standard"

"If tokens are used to replace PAN in the merchant environment, both the tokens, and the systems they reside on will need to be evaluated to determine whether they require protection and should be in scope of PCI DSS."

Securosis

If you follow the supplement to the letter, you can't reduce scope. But tokenization should reduce scope! They need to say how.

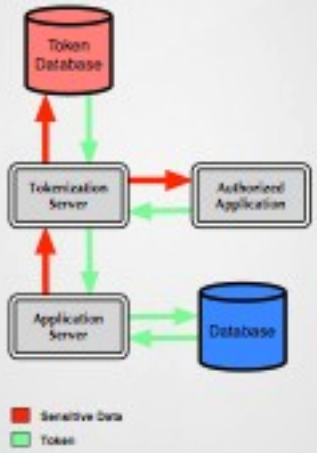
Securosis

Tokenization:

- Tokenization replaces the sensitive data with a (preferably) random value which can match the formatting of the original.
- Sensitive data is kept encrypted in a highly protected server or database.
- The token then replaces the sensitive data nearly everywhere and is used for internal systems.
- The real data is only exposed when absolutely necessary.
- Tokenization can be offered as a service.

Securosis

Basic Architecture



Securosis

What is Tokenization?

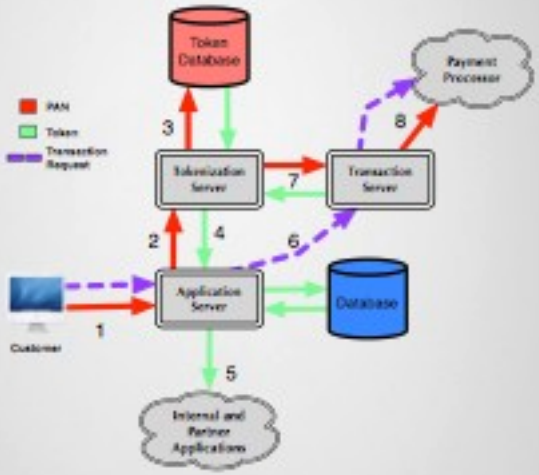
Securosis

The Tokens

- Should be random or semi-random.
- Same format as original value (e.g. 16 digits, passes LUHN check).
- Some characteristics may carry-over (e.g. last 4 digits of a credit card number).
- Single or multi-use.

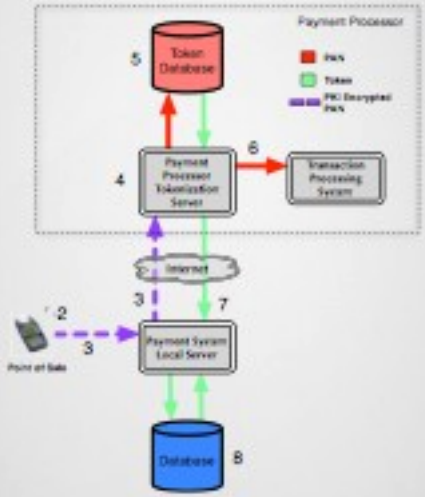
Securosis

Use Case: Internal Credit Cards



Securosis

Use Case: Credit Card SaaS



Securosis

You can't steal what's not there!

Securosis

But how do I reduce scope?

Securosis

- By removing confidential data
- Replace with low value token
- Not accessing token server
- Reducing system interdependence
- Fewer checks, controls and reports

Here's how:

Securosis

Token Server Functions

Token Creation

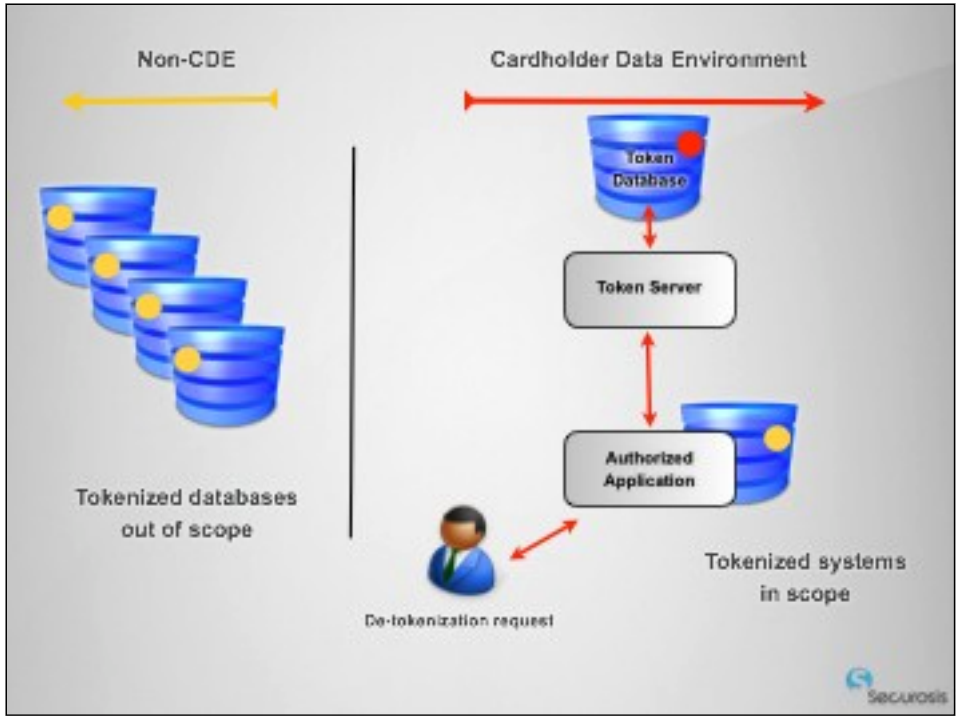
Token Storage

Key Management

Data Access

Administration/ Management

Securosis



Reduce Audit Costs

- Fewer systems
- Fewer controls
- Fewer reports
- Less complexity

Securosis

- Less work for the auditor
- Fewer reports to review
- Less complicated that cryptography review
- Less time spent on site

Auditors are Human too!

Securosis

Summary

- Reduces security risks
- Reduces complexity
- Minimal IT systems impact
- Should reduce compliance costs
- Get Securosis Whitepaper for more details

Securosis

Adrian Lane

Securosis, L.L.C.

alane@securosis.com

Twitter: AdrianLane