Protecting Credit Cards
10 years of security standards

Terence Spies
CTO
Voltage Security

Why This Talk is Boring

- No NSA, Snowden, Bitcoin, or ECC
- 1960s era technologies..
  - Magnetic stripe readers!
  - Mainframes!
- Mind-numbing array of acronyms
  - PAN, CVV, POS, BIN, IIN, etc, etc.
- Large scale brownfield engineering
  - Legacy everywhere

On the other hand…

- There are >14B credit cards in the world
- Which handle $3.6T in transactions a year
- With about $12B of fraud

  (most non-security related…)
- Breaches now prevalent enough that my mom knows what I do!

Meta-DJB comment

Tools need to be designed with use in mind.
Primitives, protocols, standards, applications..

Crypto Will be Misunderstood

- “Encrypted data has a mathematical relationship to plaintext”
- “Hashing is irreversible”
- Precise mathematical definitions can be abused in application contexts…

Payment Security

- Active standards groups and activities
- Tokenization and encryption
- Table-based tokenization

X9

- ANSI-chartered group for financial standards
- Standards cover:
  - MICR check printing, check imaging
  - PIN encryption for debit and ATM
  - Key exchange and management for ATM and POS
- Current standards projects:
  - Tokenization (X9.119 part 2)
  - Format Preserving Encryption (X9.124)
  - Wireless and network security

PCI SSC

- Payment Card Industry Security Standards Council
- Standards include:
  - PCI Data Security Standard
  - PCI Payment Application Security Standard
- Charters Qualified Security Assessors (QSAs)
  - QSAs audit merchants and processors

EMV

- Originally EuroPay-Mastercard-Visa, now includes Amex, Discover, JCB, CUP
- Relevant Standards:
  - EMV chipcard standards
  - EMV payment tokenization

US Federal Reserve

- Better Payments initiative aims to support standardization of security technologies
- Mobile Payments Industry Workgroup
  - Overall security of mobile platforms
  - Use of tokenization in mobile payments

PCI

- December 15, 2004 – PCI DSS 1.0 released
  - Sets standards for networking, IT management, and data protection
  - First standard to mandate encryption of credit card data
- PCI DSS is now on version 3.0
- The benchmark payment security standard
  - No compliance = potentially no CC processing!

Crypto in PCI

- PCI mandates data protection and encryption
  - "Compensating controls" can be used also
- Two main protection regimes
  - Point-to-Point Encryption (P2PE)
    - Encryption from point of swipe/dip to host
    - X9.119 part 1 provides guidance
  - Tokenization
    - Encryption for PAN data in storage/analytics
    - Creation of limited context PANs

P2PE

- A decade’s progress
  - All major POS manufacturers offer some P2PE
  - Many merchants have deployed
- Why isn’t this everywhere?
  - There are a LOT of POS devices
  - Requires support at the host/gateway/processor
  - Key management is a bear
    - Key injection
    - Device treatment

Tokenization

- Creating a replacement value for a PAN
- Tokenization is actually two technologies
  - Payment Tokenization
    - Creating a psuedo-PAN for a device or merchant
    - Apple Pay
    - Card on File
  - Security Tokenization
    - Creating a zero-value replacement for analytics
    - Internal applications

Payment Tokenization

- Replace the PAN with a limited context pseudo-PAN
- Apple Pay
  - User enrolls card, phone receives token
  - TSP associates the token with a specific phone
  - Transaction supplies token + cryptogram
  - Brand requests detokenization + auth
- Other application
  - Merchant specific token
  - Subscriptions and other recurrent payments

Security Tokenization

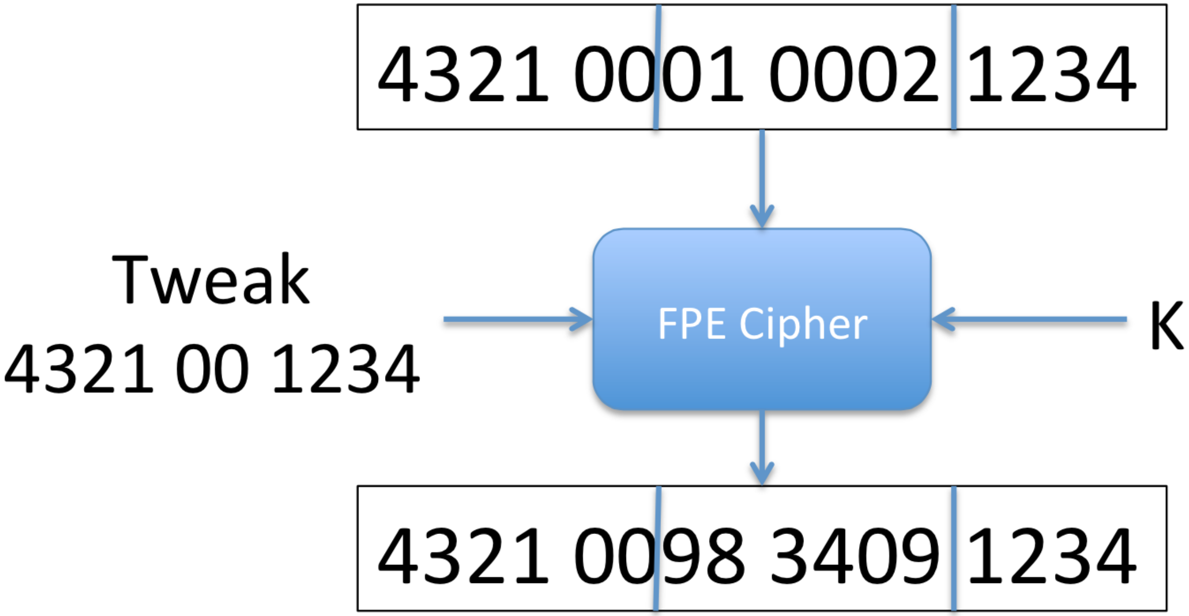
- Thousands of legacy apps depend on PAN
- Customer service, fraud detection, loyalty
- Want to remove the PAN from these apps
  - Minimizing application changes
    - Apps with no source code…
  - Minimizing performance overhead

“Classic” Tokenization

- Create a token to PAN mapping in a database
- Works in some circumstances
  - Multiple instances require replication
- Still requires mechanisms to protect the db

Crypto to the rescue?

- We now know how to create permutation factories (aka Format-Preserving Encryption)
- Now a draft NIST standard (SP800-38G)



“Mathematical Relationship”

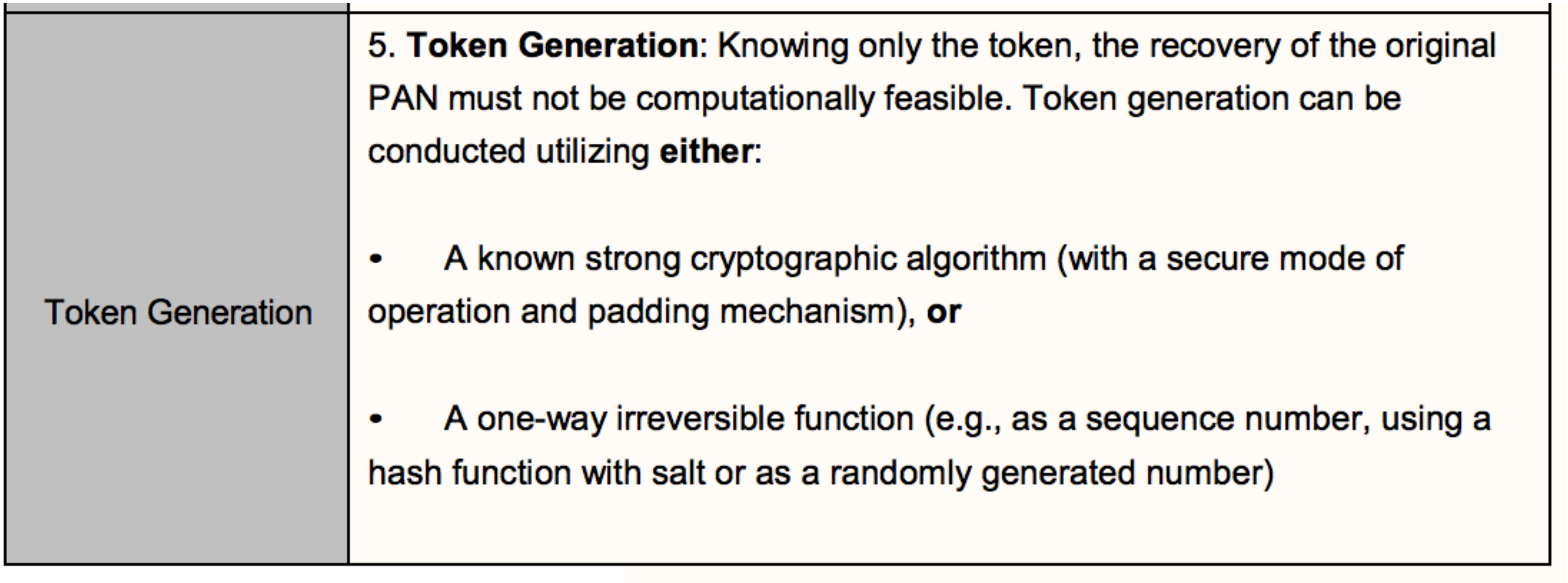
- The notion of “reversible” is problematic…

“where token generation is based on a reversible encryption method (where the token is mathematically derived from the original PAN through the use of an encryption algorithm and cryptographic key), the resultant token is an encrypted PAN, and may be subject to PCI DSS considerations”

- PCI DSS Tokenization Guidelines

Other Perspectives..

- Newer PCI documents
- Visa Tokenization Guidelines



Token Generation	5. **Token Generation**: Knowing only the token, the recovery of the original PAN must not be computationally feasible. Token generation can be conducted utilizing **either**: • A known strong cryptographic algorithm (with a secure mode of operation and padding mechanism), **or** • A one-way irreversible function (e.g., as a sequence number, using a hash function with salt or as a randomly generated number)

Static Table Tokenization

- One question around encryption is dependence on a single key
- Can we require that the attacker knows a large table to attack tokens?
- Informal security goal:
  - Create a tweakable PRP over an arbitrary set
  - Secrets used to map P_x->C_x and P_y->C_y (x != y) are highly likely to be distinct
  - Set is too large to create a complete table

Approaches to table tokenization

- Direct Tables with tweaking
- Fiestel constructions
- Sliding-window

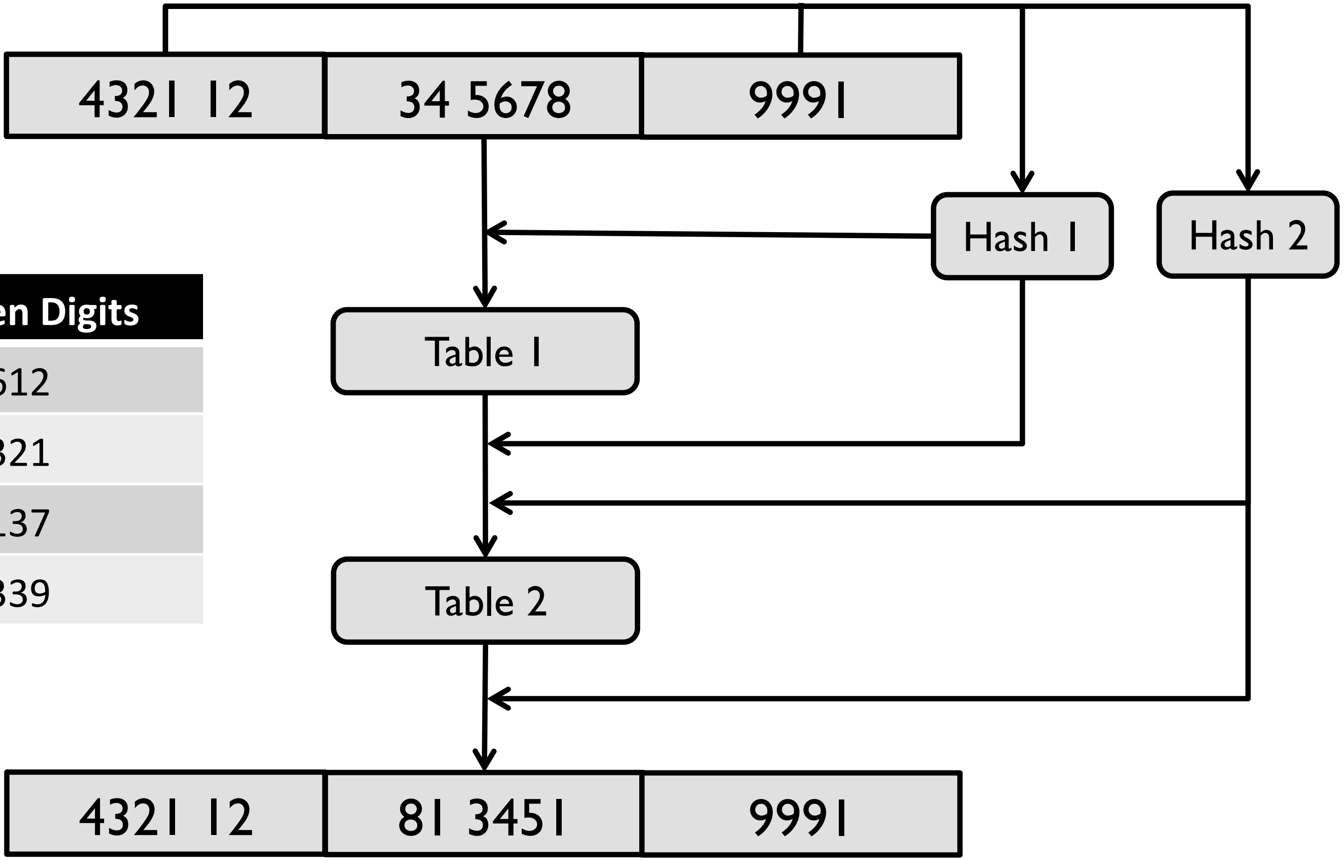
- There are probably more general solutions that allow for any table size…

Direct Tables

- In the credit card case, a format called 6-6-4 is popular
- First 6 (the BIN) and last 4 are in the clear
- Inner 6 are changed in the token
- 10^6 is a feasible table size, but we need a tweaking solution….
- Landecker-Shrimpton-Terashima show how to black box tweak beyond birthday bounds

Method 1 – Direct Table Lookup

Input Digits	Token Digits
000000	734612
000001	231321
000002	993137
000003	328339

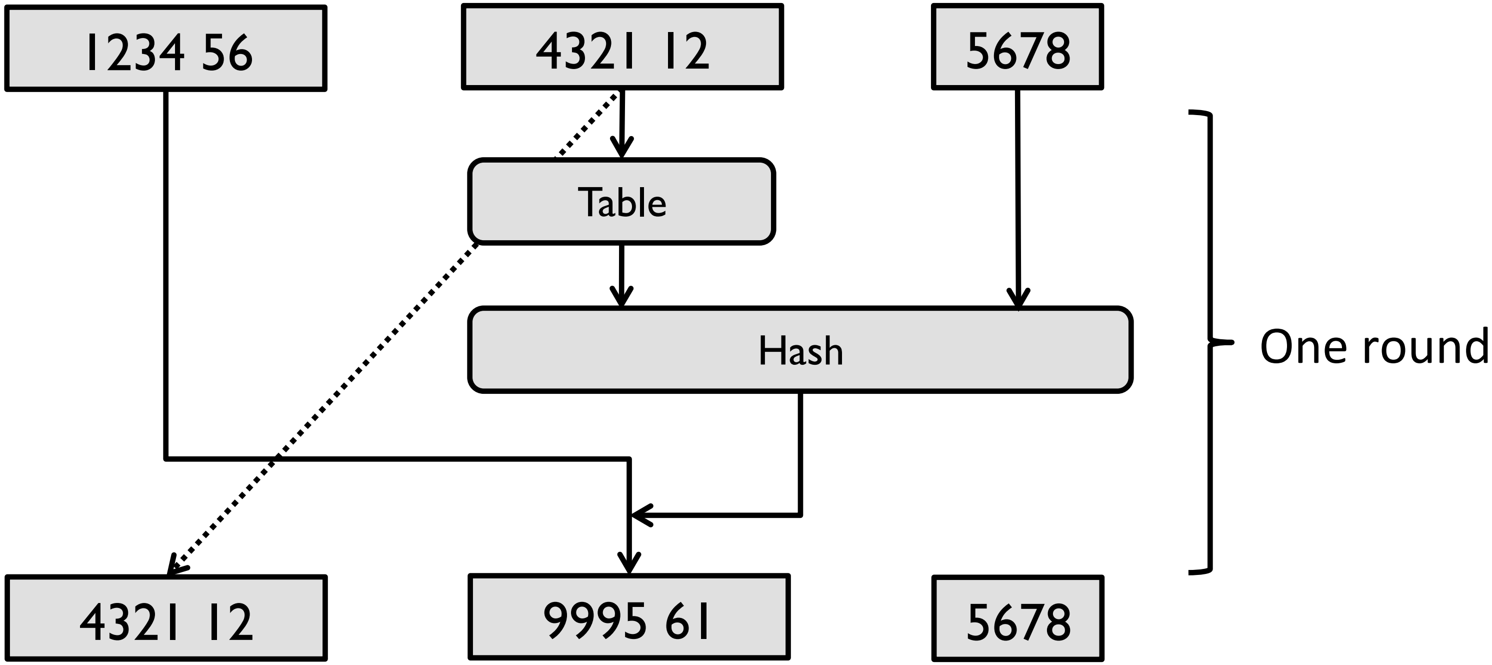


Copyright 2012 Voltage
Security

Feistel Constructions

- If set is > 10^7 or so, storage gets nasty
- As in FPE/FFX, we can use a Feistel network to turn a size n PRF into a size 2n PRP
- If we unbalance, we can go over 2n at the cost of more rounds

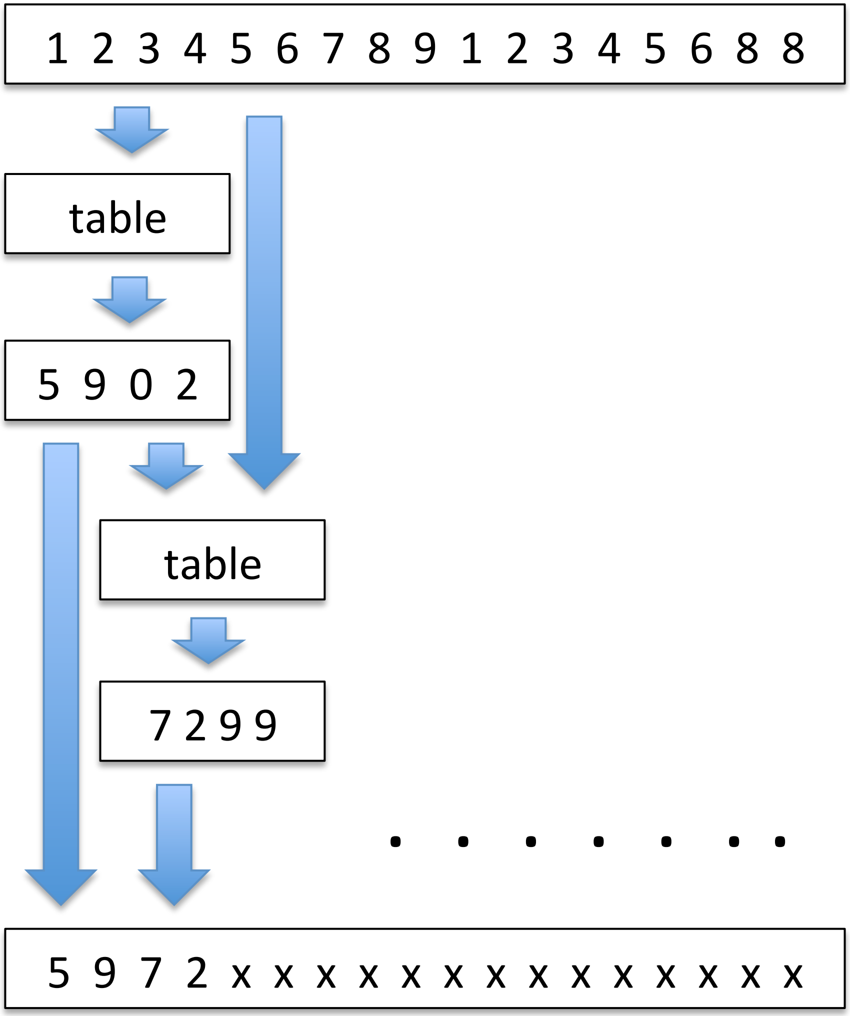
Method 2 – Feistel



Sliding Window

- “Slide” a table over the plaintext
- Approach not well documented
  - Smith and Brightwell
  - Mattsson patent application

Sliding Window



1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 8 8

table

5 9 0 2

table

7 2 9 9

. . . .

5 9 7 2 x x x x x x x x x x x x x x

Payment Security

- An enormous amount of value moves over a pre-crypto payment network
- Standards efforts are attempting to strengthen the system in-place
- Key management and trust in crypto in general present real issues
- Lots of space for protocol, primitive, and systems security efforts