Privacy Models in the Payments Industry*

Terence Spies
Voltage Security

* plus some editorializing

Why “Real-World Crypto”?

If we define the “Real World” as enterprises….

	Academic Crypto	Enterprise Crypto
Security Methodology	Define a model, show security in that model.	Does this reduce risk, regulatory or audit cost?
Credibility	Peer-reviewed publication	Standards (ie. NIST) acceptance
Success Criteria	Novelty, Publication	Cost-effective implementation

Real-world security models typically involve cost, legacy, and business process concerns that can be more complex than the underlying crypto model.

Why the disparity?

- Three factors:
  1. Parsing crypto papers is extremely difficult
  2. Crypto demos neglect the salient property
  3. Cryptographers keep changing their minds

A distributed system is a system where I can’t get my work done because a computer has failed that I’ve never even heard of.

Leslie Lamport

A real-world cryptographic system is a system where I can’t secure my data because a computer has succeeded that I’ve never even heard of.

Every security customer ever

A Real-World Example: Payments

What happens when a credit card is swiped at a retail terminal….surely that's encrypted, right?

- How payment systems work
- Cryptographic solutions in payments
- Future problems / models

Definitions

- **PIN** – Personal Identification Number, used to authenticate ATM and Debit transactions
- **PAN** – Primary Account Number. The number printed on the front of a credit or debit card.
- **Track Data** – Data read from the two magnetic stripes on the back of a credit card.
- **POS** – Point-of-Sale. The terminal reading a payment card.

PIN Security

- PIN Entry Devices (PEDs) are provisioned with individual keys.
  – Session or transaction keys are created (X9.24)
- The PIN is encrypted with the session key and PAN as randomizer
  – Multiple standards for DES and 3DES pinblock creation- (ISO 9564)
- Key management standards require PINs do not appear outside HSMs.

Payment Standards

- Payment standards evolve very slowly
  - 3DES is the default standard
  - Some PIN blocks are still DES encrypted
  - US and ISO AES pinblock standards in progress
- Why?
  - Cost of physical upgrade
  - No single party in charge
    - Millions of retailers
    - Hundreds of intermediaries
  - Extremely complex business processes
    - Recurrence, chargeback, preauth

Solving the PAN problem

- Payment systems were built with the assumption that PINs are private.
- But no assumption of PAN privacy
  - Receipt printing uses last 4 PAN digits
  - Card routing uses first 2-6 digits
  - Fuel cards use arbitrary digits
- PANs have value to attackers
  - Web transactions
  - Printing fraudulent cards
- Merchant PAN databases == breach risk
  - Storage at processors, lodging, etc.

Attempt #1: SET / STT

- The STT and SET protocols attempted to solve PAN privacy via public key encryption & signature.
- SET was cryptographically feature rich
- It was also extremely complex
  – Programmer's Guide: 619 pages
  – Protocol Specification: 250+ pages

Why SET Failed the Real-World Test

- SET had lots of interesting features (dual signature, etc.), but.....

	Academic Crypto	Enterprise Crypto
Security Methodology	Define a model, show security in that model.	Does this reduce risk, regulatory or audit cost? ?
Credibility	Peer-reviewed publication ☑	Standards (ie. NIST) acceptance
Success Criteria	Novelty, Publication ☑	Cost-effective implementation ☒

PCI

- In 2004, the major card brands join to form the Payment Card Industry Data Security Standard (PCIDSS)
- Imposes a set of requirements, and sets up a Qualified Security Assessor (QSA) audit framework.
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data

PAN Encryption

- Goal: Encrypt at POS
- Does TLS or other protocols solve this problem? No.
  - Existing payment system intermediaries
  - Security for stored PANs

The Simple Case: Small Merchant

Card swipe

↓

Processor / acquirer

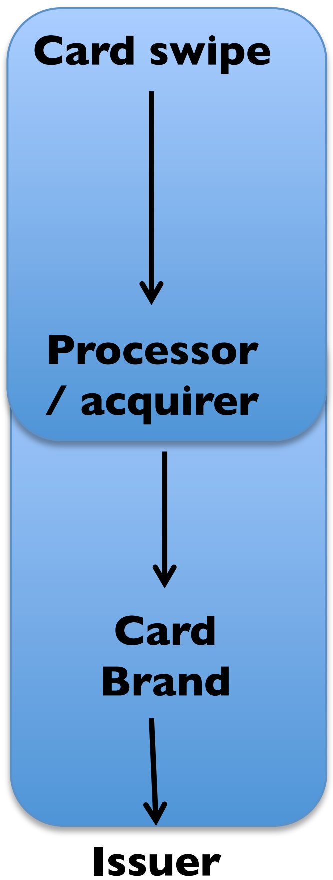
↓

Card Brand — ***Visa, MC, etc.***

↓

Issuer — ***Bank, Inc.***

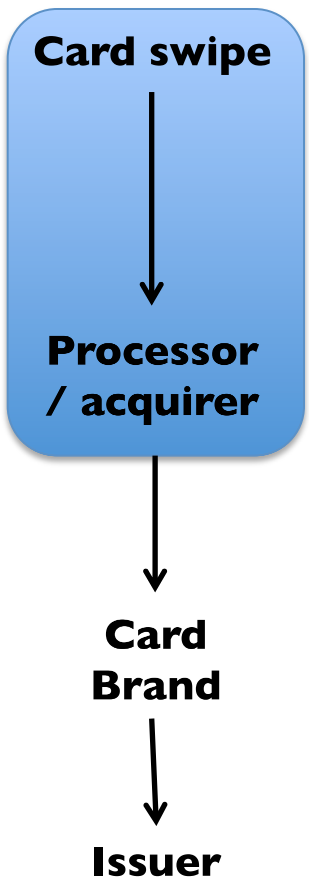
PIN Privacy Model



PIN is private from entry until it is checked at the issuer.

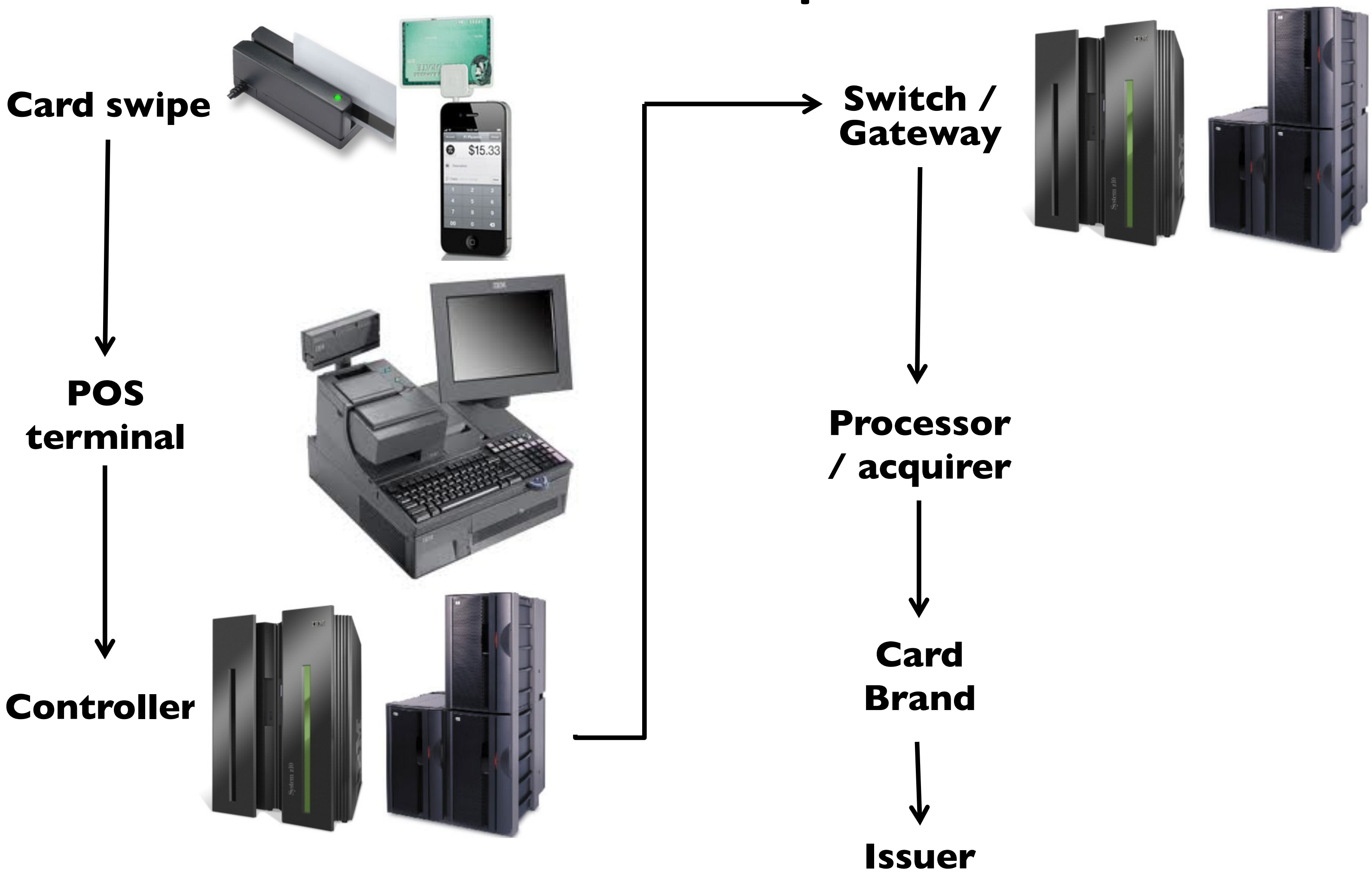
HSM based reencryption is done at the processor.

Simple PAN Privacy Model



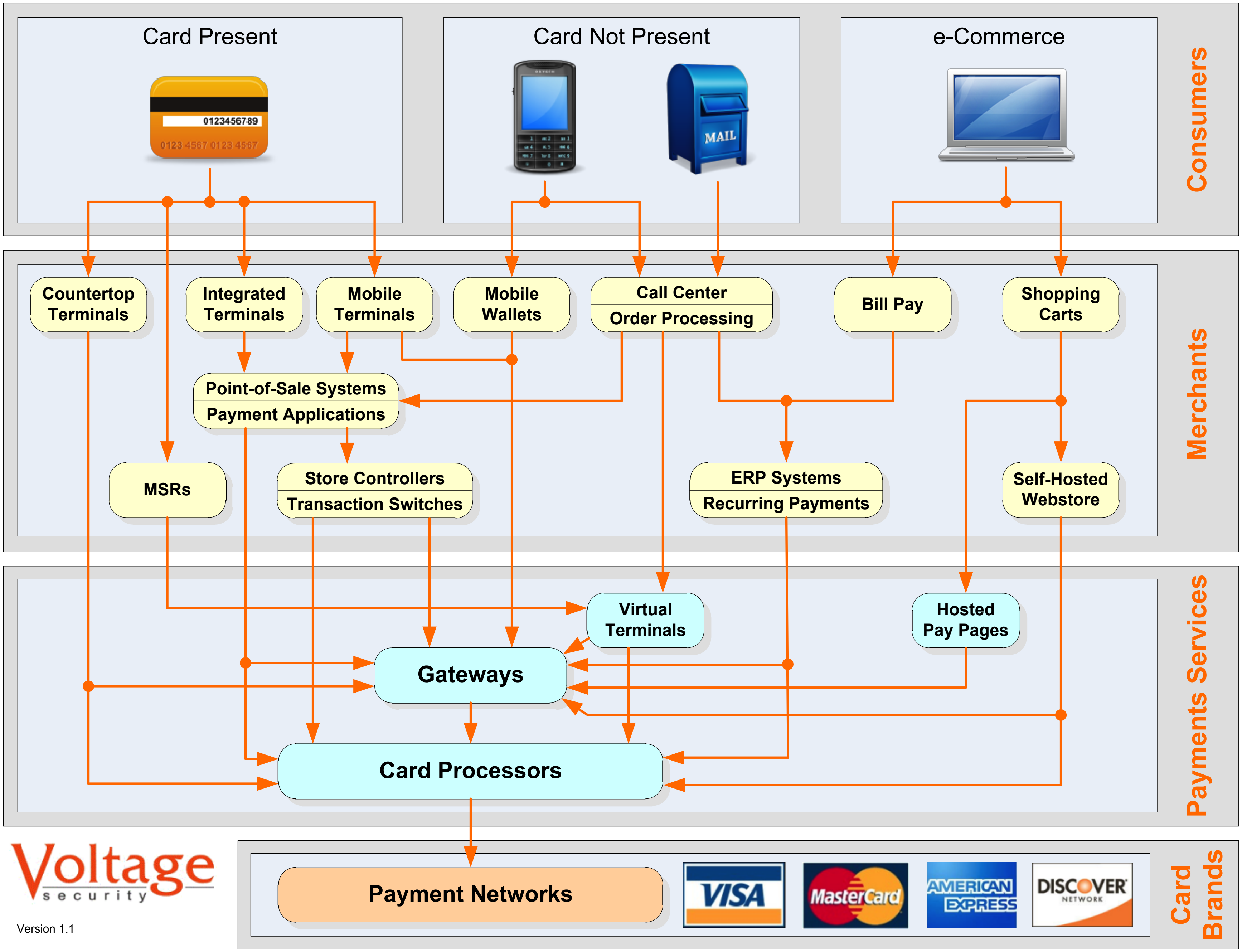
In this case, link encryption actually would seem to do the job.

More Complex Case



Payments Industry

Authorization Transaction Flow



Voltage security

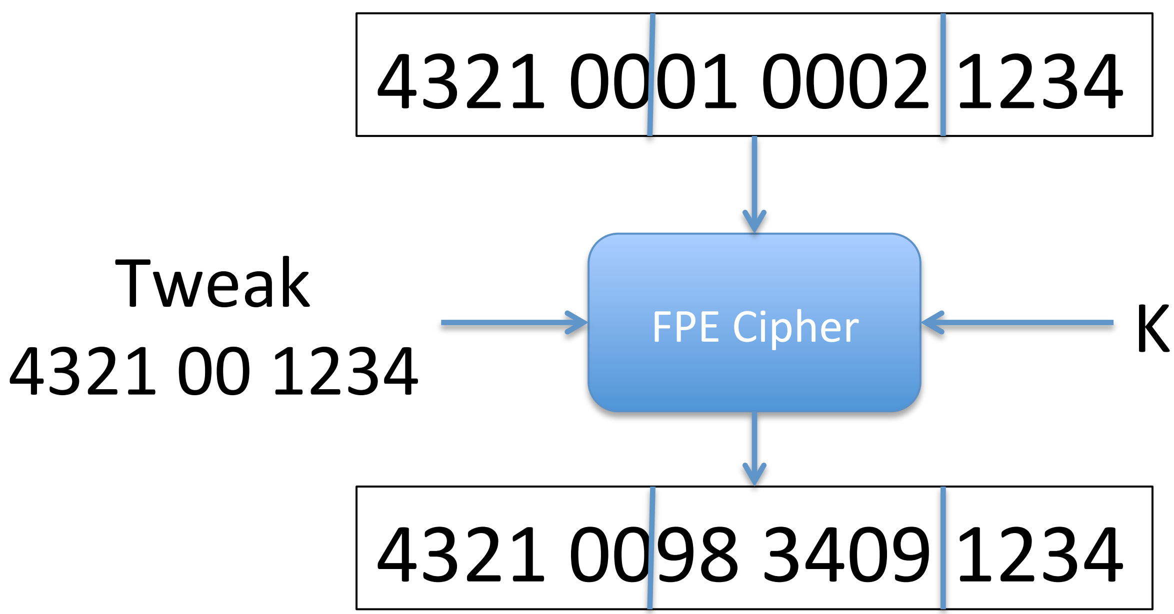
Version 1.1

Deployable PAN Encryption

- A realistic solution must:
  - Be secure
  - Not break every existing payment protocol
- Why not create a new protocol?
  - Every processor has it’s own message standard
  - ISO 8583 defines a framework, but all processors modify it
- Only baseline is the PAN and track data itself

Format Preserving Encryption

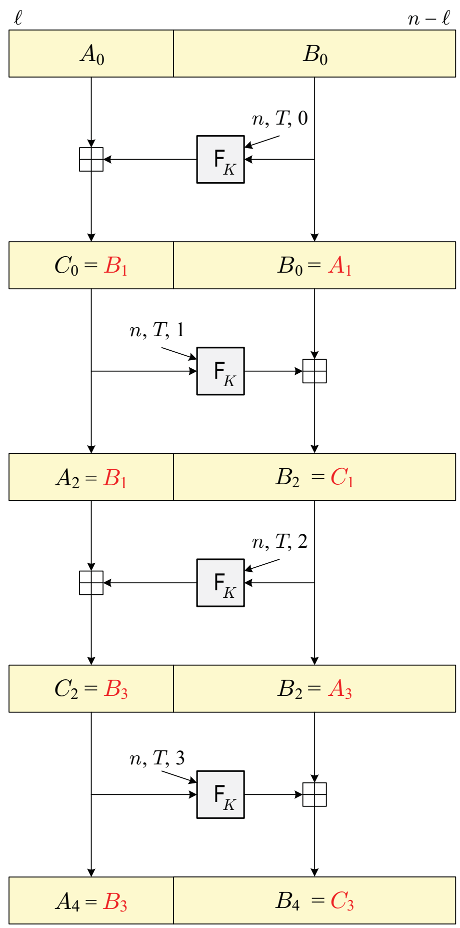
- Build a cipher so ciphertext looks like plain
  - Maintain length and alphabet
- Use a tweakable cipher to allow plain digits



History of FPE

- The first DES FIPS document (FIPS 74, in 1981) contains a section on character set preservation!
- An example of a user asking the crypto community for a primitive.
  - Smith and Brightwell, "Using datatype-preserving encryption to enhance data warehouse security", 1997 NIST conference
  - Defined the practical need and use, but proposed no secure solution
- Best alternative was storing plaintext in a database, returning a random index in the right format.

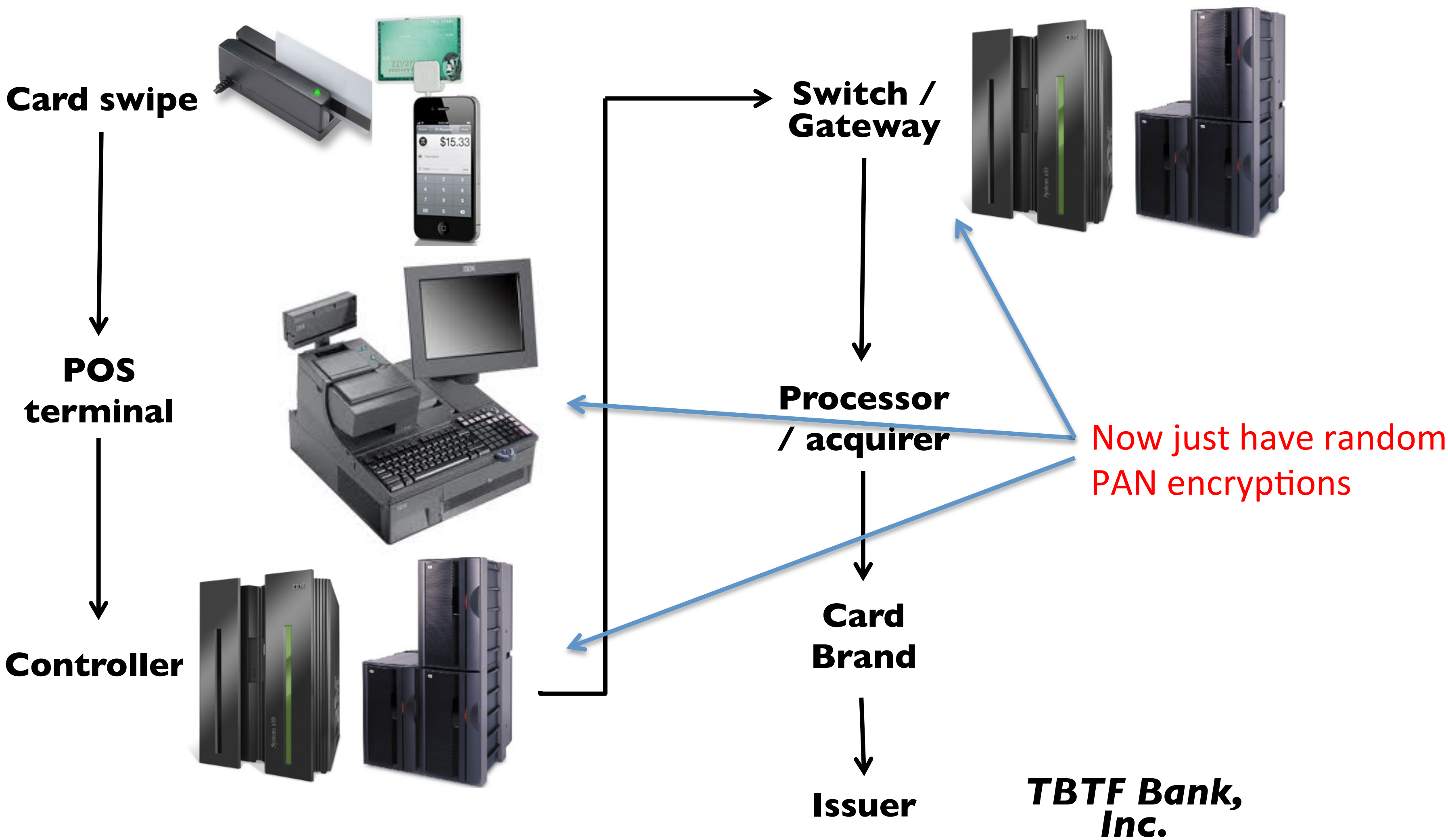
Format Preserving Encryption



Cryptographic challenge is to build a small domain cipher. Rogaway and Black in 2002 show the first provably secure techniques, using a PRP model.

Work by Bellare, Ristenpart, Rogaway, Stegers shows improved results for constructing FPE ciphers using Feistel networks.

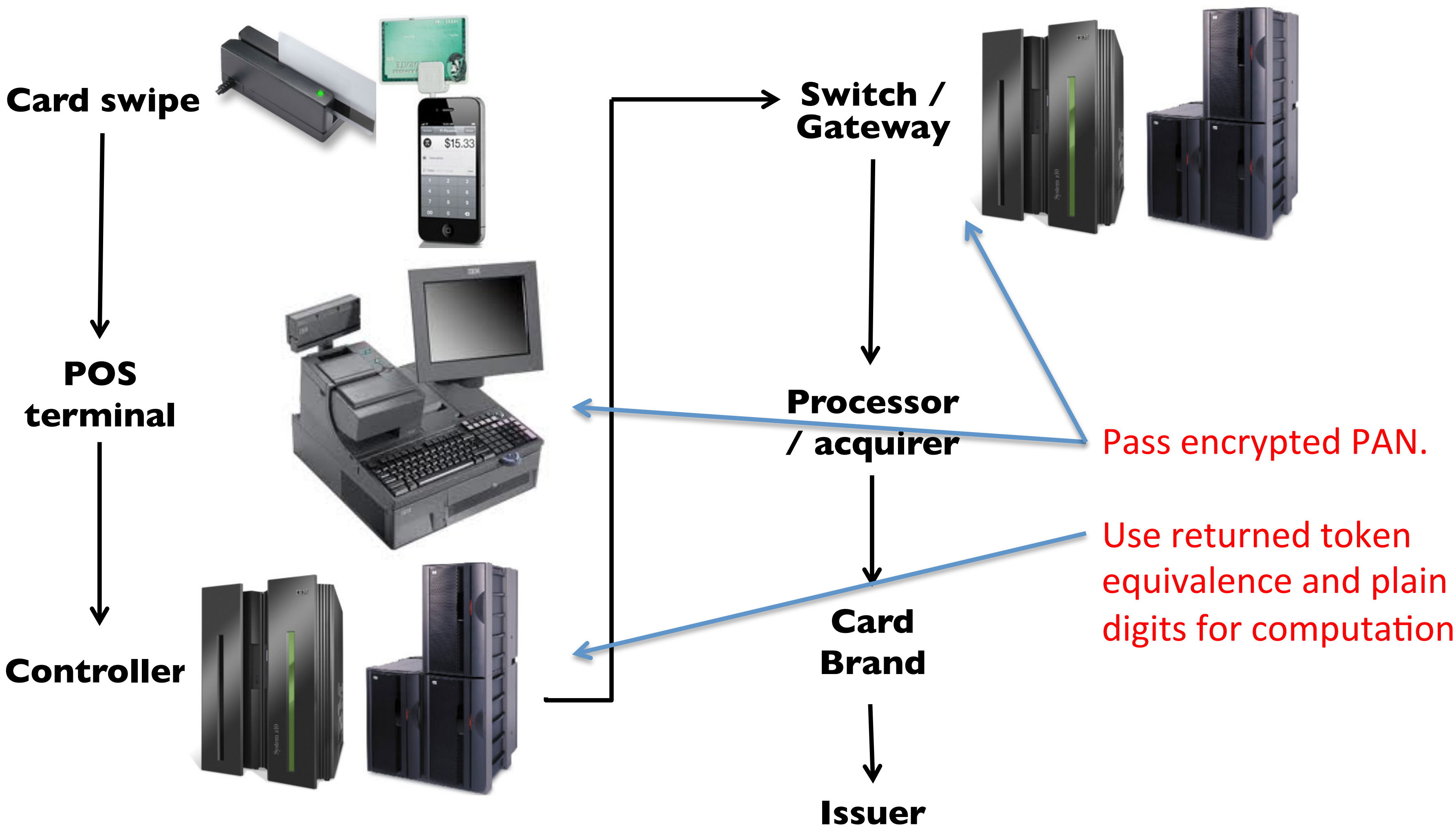
What about the intermediates?



Tokenization

- Generically, the replacement of a PAN with a random substitute.
- Tokenization creates a 1:1 replacement, enabling protection of permanently stored PAN data.
- Enables limited computation (identity)

Tokenized PAN Privacy



Future Work

- Multiple standardization efforts (PCI and X9) are now working on security definitions for tokenization and encryption of card data.
- Database vs encryption vs hashing
  - Are there real differences?
  - How do we explain and build requirements?
- Next generation PIN block and key management standards
  - AES pinblock
  - AES DUKPT