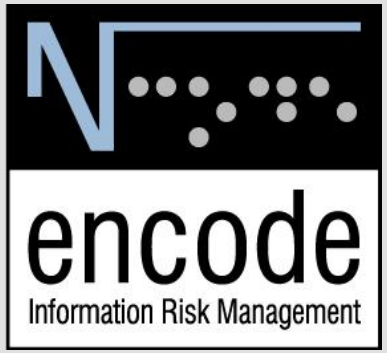
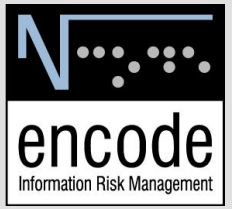


ATM Security
Having fun with ATMs & HSMs

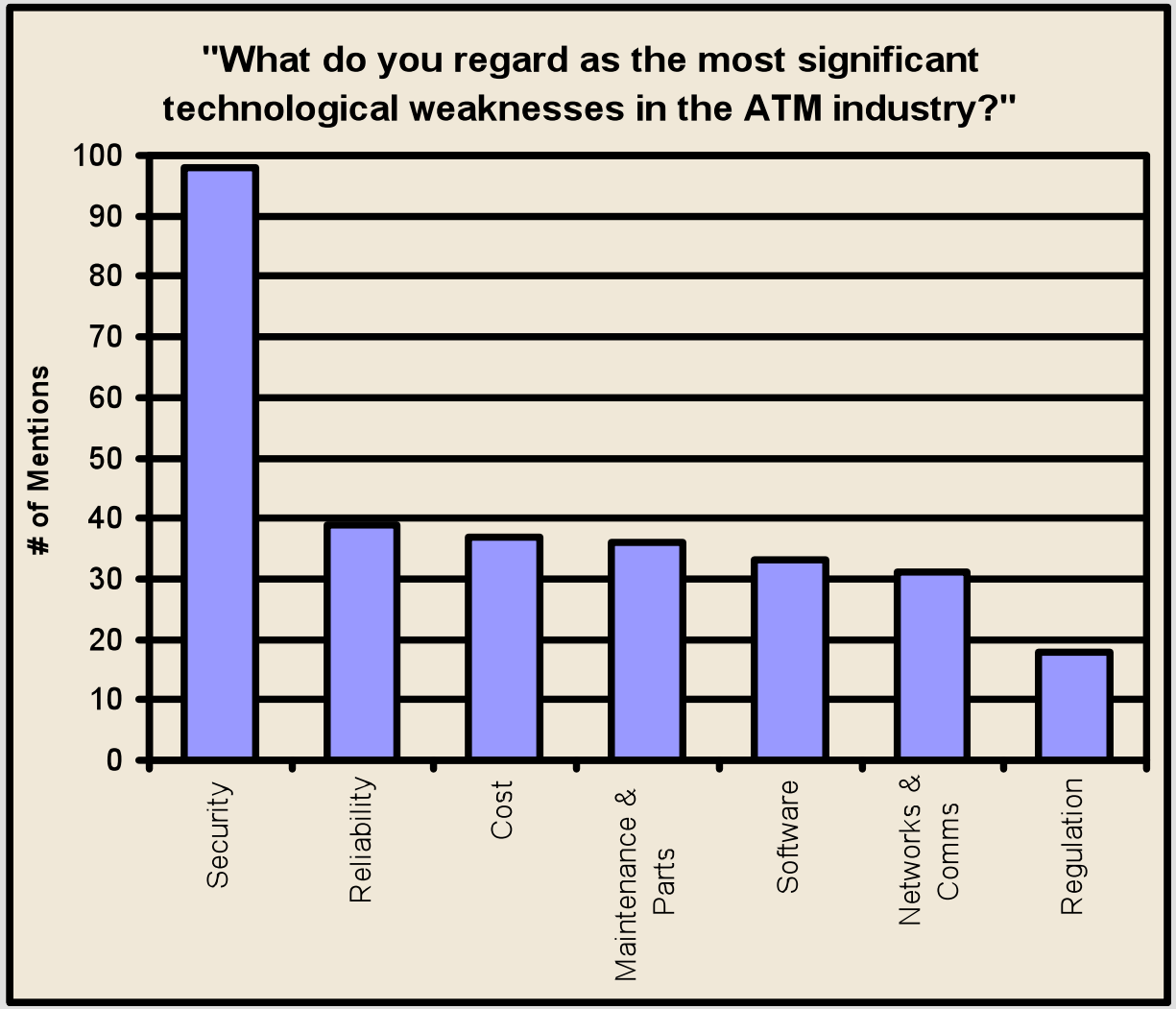
Dimitris Petropoulos
ENCODE Middle East
October2009

Agenda

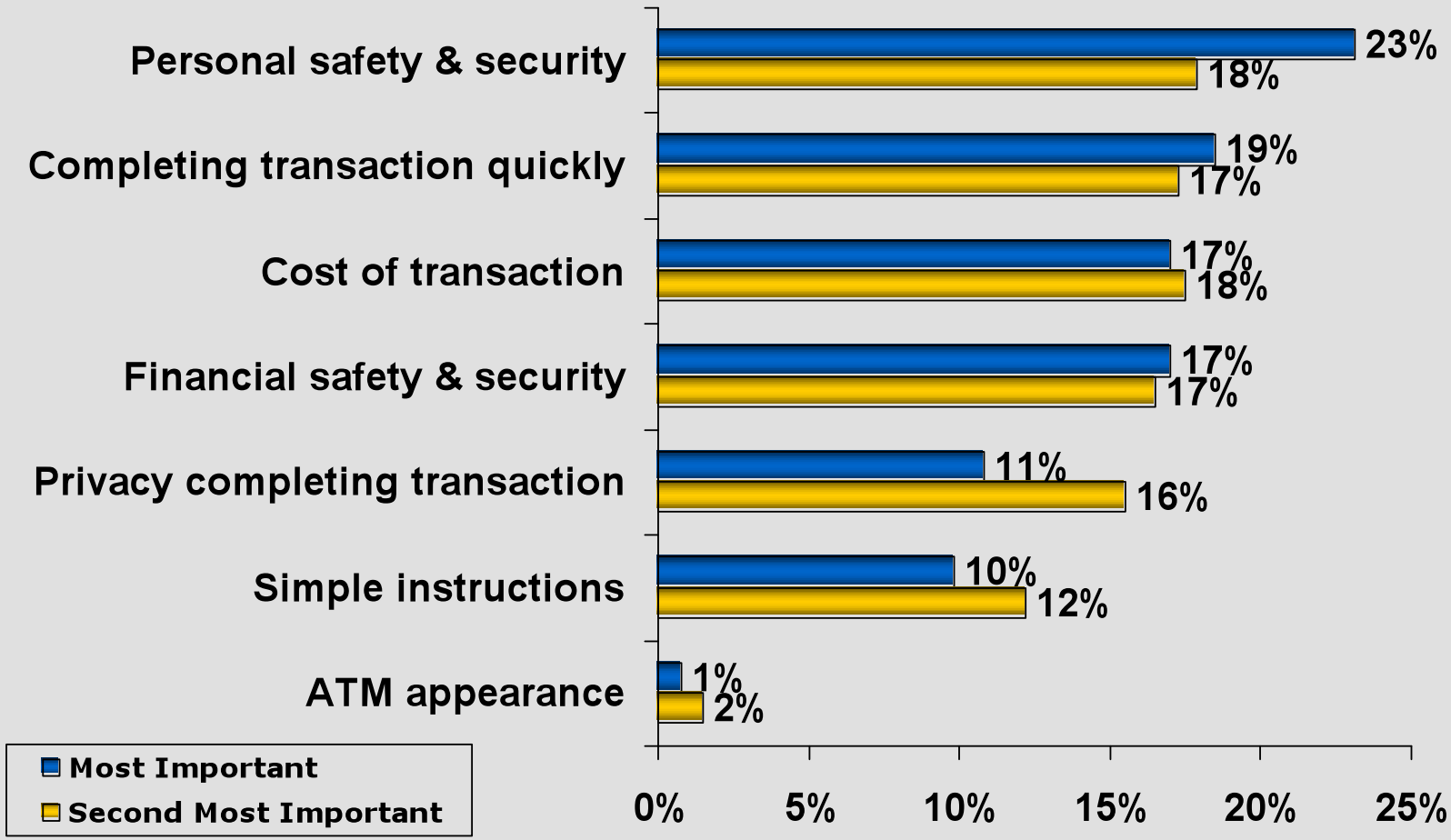


- Physical Attacks
  - Just an overview, for the sake of completeness
- IT attacks
  - PIN attacks
  - Network threats

ATMIA Member Survey

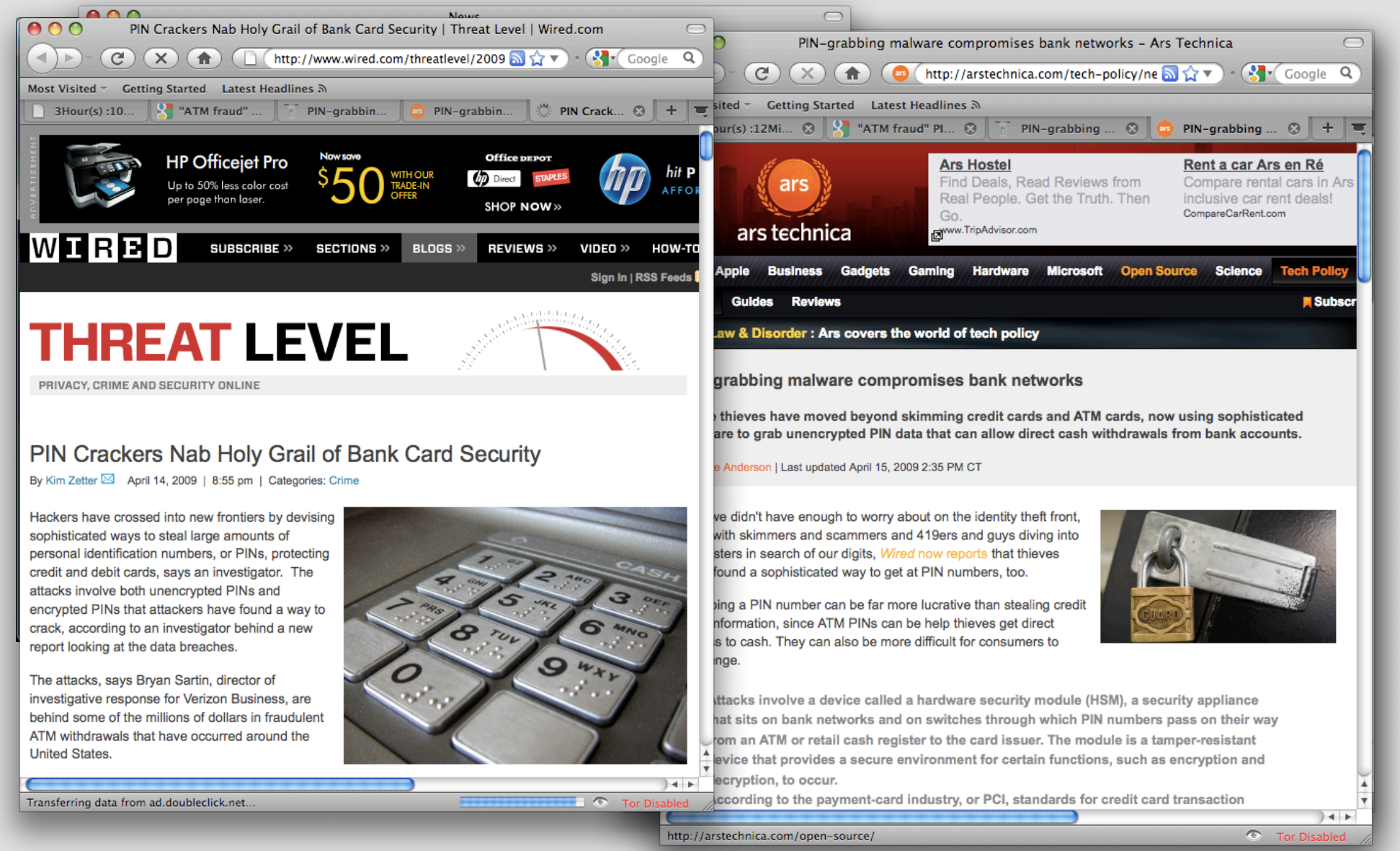


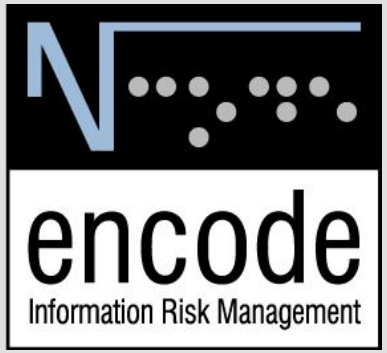
What does the client want?



*Decision Analyst, Inc

Seen those?


PIN Crackers Nab Holy Grail of Bank Card Security | Threat Level | Wired.com
http://www.wired.com/threatlevel/2009
HP Officejet Pro
Up to 50% less color cost per page than laser.
Now save $50 WITH OUR TRADE-IN OFFER
SHOP NOW»
WIRED
SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO »
THREAT LEVEL
PRIVACY, CRIME AND SECURITY ONLINE
PIN Crackers Nab Holy Grail of Bank Card Security
By Kim Zetter April 14, 2009 | 8:55 pm | Categories: Crime
Hackers have crossed into new frontiers by devising sophisticated ways to steal large amounts of personal identification numbers, or PINs, protecting credit and debit cards, says an investigator. The attacks involve both unencrypted PINs and encrypted PINs that attackers have found a way to crack, according to an investigator behind a new report looking at the data breaches.
The attacks, says Bryan Sartin, director of investigative response for Verizon Business, are behind some of the millions of dollars in fraudulent ATM withdrawals that have occurred around the United States.
Transferring data from ad.doubleclick.net...
Tor Disabled
PIN-grabbing malware compromises bank networks - Ars Technica
http://arstechnica.com/tech-policy/ne
ars technica
Ars Hostel
Find Deals, Read Reviews from Real People. Get the Truth. Then Go.
www.TripAdvisor.com
Rent a car Ars en Ré
Compare rental cars in Ars inclusive car rent deals!
CompareCarRent.com
Apple Business Gadgets Gaming Hardware Microsoft Open Source Science Tech Policy
Guides Reviews
Law & Disorder : Ars covers the world of tech policy
grabbing malware compromises bank networks
thieves have moved beyond skimming credit cards and ATM cards, now using sophisticated are to grab unencrypted PIN data that can allow direct cash withdrawals from bank accounts.
Anderson | Last updated April 15, 2009 2:35 PM CT
ve didn't have enough to worry about on the identity theft front, with skimmers and scammers and 419ers and guys diving into sters in search of our digits, Wired now reports that thieves found a sophisticated way to get at PIN numbers, too.
ing a PIN number can be far more lucrative than stealing credit nformation, since ATM PINs can be help thieves get direct s to cash. They can also be more difficult for consumers to nge.
ttacks involve a device called a hardware security module (HSM), a security appliance hat sits on bank networks and on switches through which PIN numbers pass on their way rom an ATM or retail cash register to the card issuer. The module is a tamper-resistant evice that provides a secure environment for certain functions, such as encryption and ecryption, to occur.
ccording to the payment-card industry, or PCI, standards for credit card transaction
http://arstechnica.com/open-source/
Tor Disabled



Physical Attacks

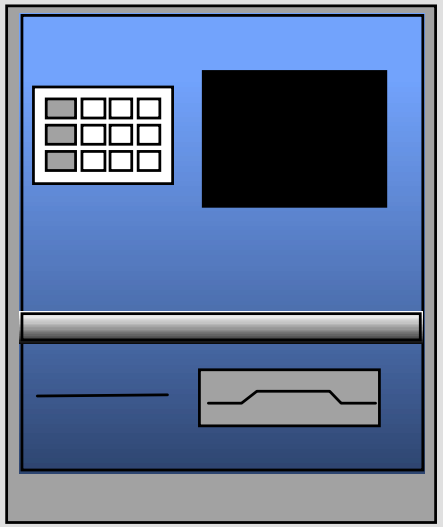
How ATMs Work (layman's view)

PIN: "1234"

XXX Bank Card

Keypad

Card Reader

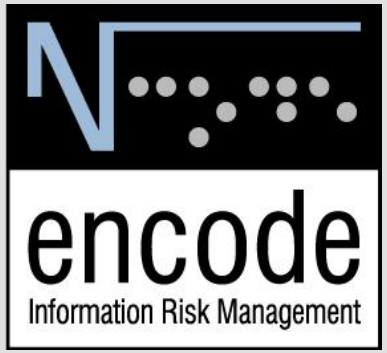


Display Screen

Cash Dispenser

ATM Physical Attacks

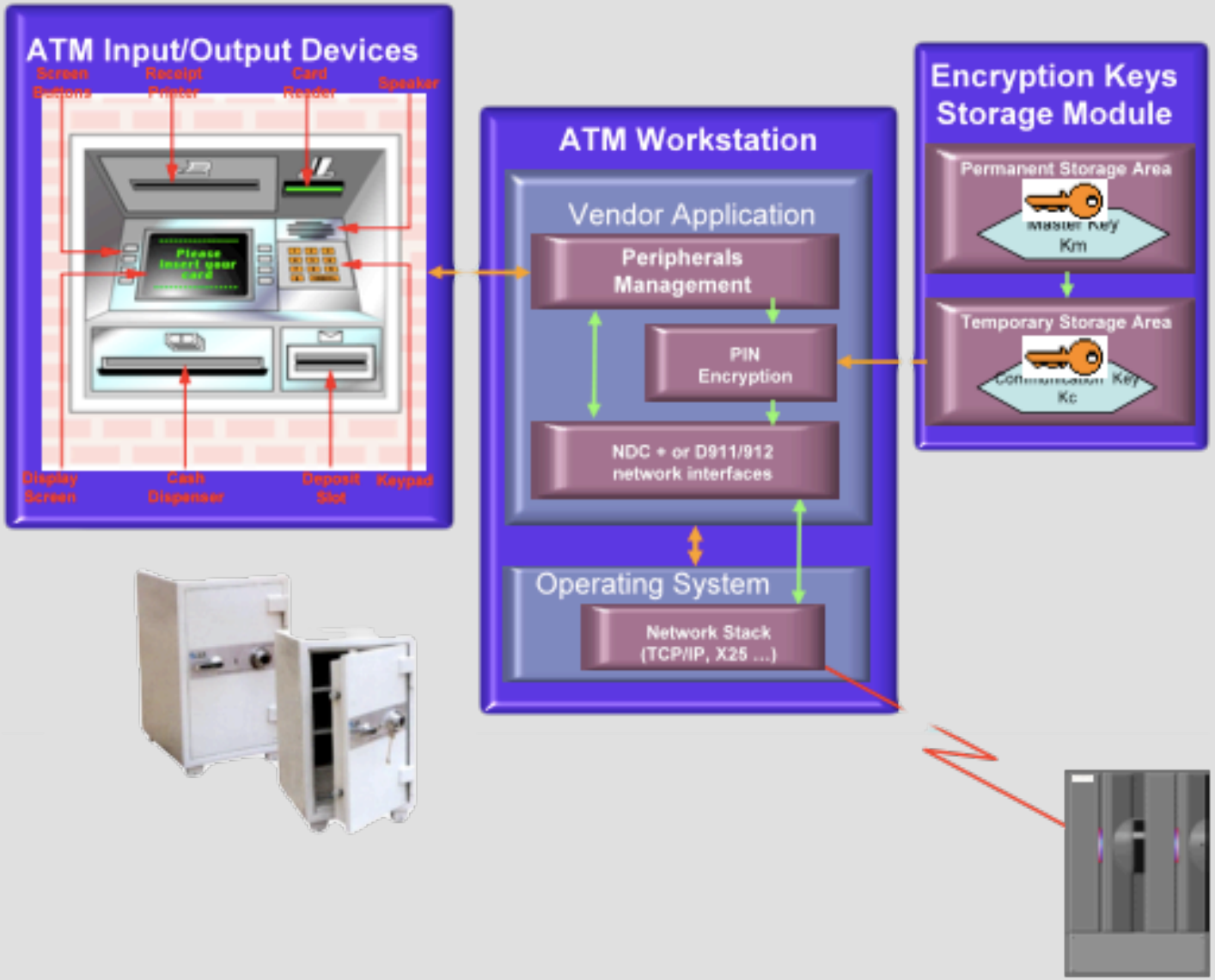
- Targeting the Client
  - Card Theft
    - Card Theft (Hooks)
    - Skimming Devices
    - Bogus ATM
  - PIN Theft
    - Shoulder Surfing
    - Fake PIN Pad Overlay
    - Micro-camera
  - Cash Theft
    - False ATM presenter
    - Robbery
  - Distraction Fraud
  - Fund Transfer Fraud
- Targeting the Bank
  - Cash Theft
    - Transaction Reversal
  - ATM Burglary Attacks
    - Door break-in
    - ATM removal


encode
Information Risk Management

PIN Attacks …

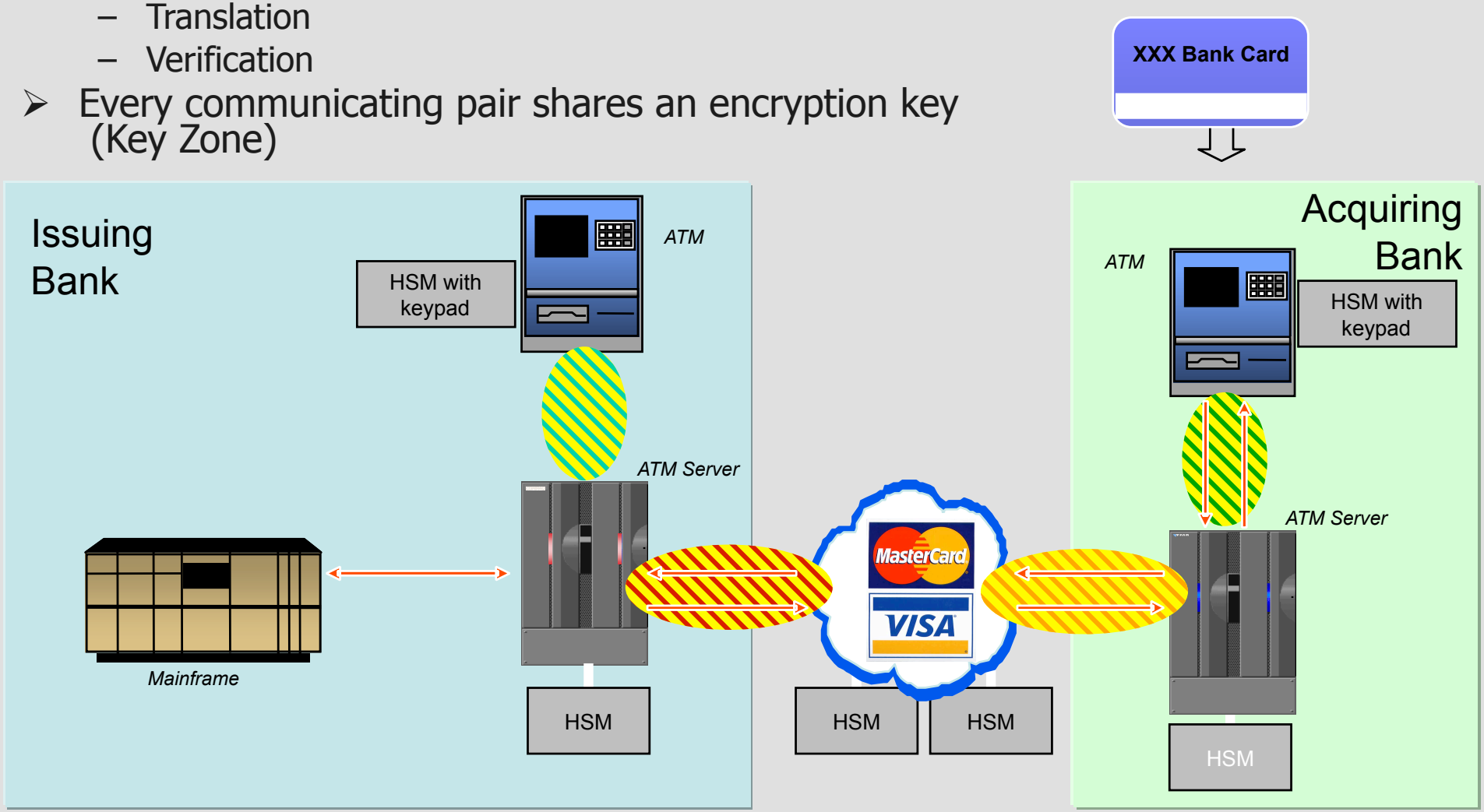

HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009

How ATMs Work



ATMs & Key Zones

- Three basic functions :
  - Encryption
  - Translation
  - Verification
- Every communicating pair shares an encryption key (Key Zone)



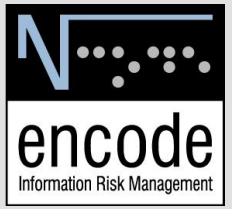
ATM PIN Encryption

PIN encryption is a trivial process:

- PIN is formatted into an 8 byte clear PIN block
- Encrypted using DES or 3DES

- There is a number of recognised formats for the clear PIN block

ATM PIN Block Formats



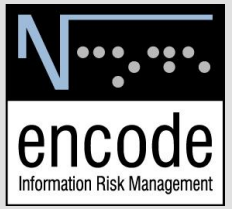
PIN block formats range from the simplest:

ISO-2 PIN Block = **`24PPPPXXXXXXXXXXX`**
where P is the 4-bit representation of a single PIN digit,
F is a 4-filler digit of value 0xF

…to slightly more complicated:

ISO-1 PIN Block = **`14PPPPRRRRRRRRRR`**
where P is the 4-bit representation of a single PIN digit,
R is a 4-filler random digit (permissible values are 0x0-0xF)

ATM PIN Block Formats [2]



…to even more complicated:

ISO-0 PIN Block:

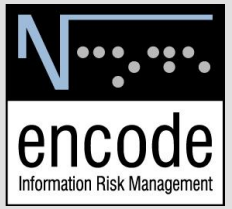
P1 = **04PPPPFFFFFFFFFF**

P2 = **ZZZZAAAAAAAAAAAA**

PB = P1 ⊕ P2

Where P is the 4-bit representation of a single PIN digit,
F is a filler digit of value 0xF,
Z is a 4-bit hexadecimal zero (0x0) and
A is a 4-bit representation of one digit of the user (PAN)

ATM PIN Block Formats [3]



…to the most complicated:

ISO-3 PIN Block:

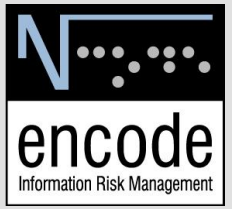
P1 = **34PPPPRRRRRRRRRR**

P2 = **ZZZZAAAAAAAAAAAA**

PB = P1 ⊕ P2

Where P is the 4-bit representation of a single PIN digit,
R is a filler digit (permissible values 0xA-0xF),
Z is a 4-bit hexadecimal zero (0x0) and
A is a 4-bit representation of one digit of the user (PAN)

ATM PIN Block Formats [3]



ISO-3 PIN Block Format is considered the most secure:

- Binds account number to PIN block
  - Protects against incorrect account number being used
- Diversifies encrypted PIN block according to account number
  - In cases where two distinct users use the same PIN the encrypted PIN blocks will be different
  - Prevents 'code book' attacks

Simple PIN Generation

Start with your Primary Account Number (PAN)

1234 5678 9012 3456

Encrypt with
PIN Master Key (PMK).

Result is **4FA2 910B 65F1 03C7**

Truncate

decimalise

4502

(F->5)
(A->2)

Decimalisation Tables

encode
Information Risk Management

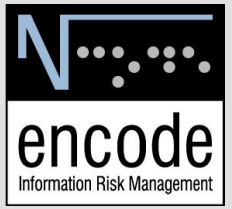
- Remember encrypted result was in hexadecimal?
- Encryption produces output that looks uniformly distributed, so 0-F are all equally likely
- Decimalisation Table used to map 0-F back to 0-9

```
digit in  0123456789ABCDEF
digit out 0123456789012345
```

- **Because some numbers (0-5) have several hexadecimal digits mapped to them, they are more likely to occur in issued PINs than others**

- e.g. 4FC2-> 4522

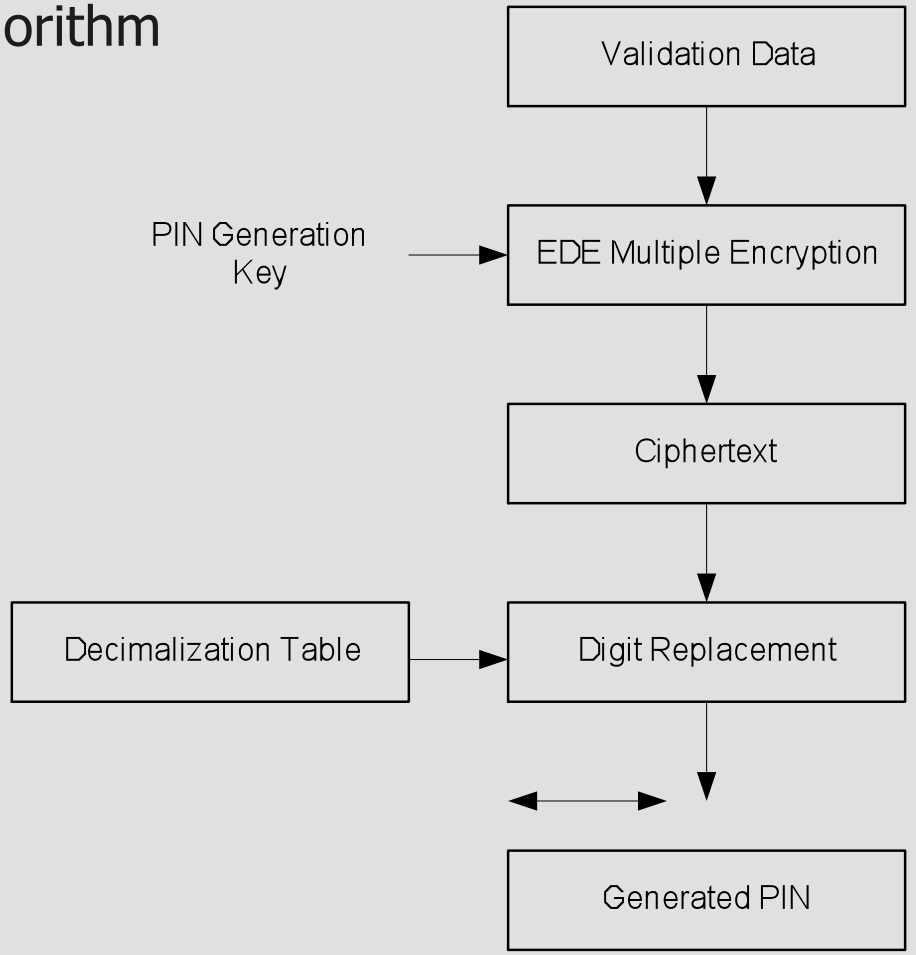
ATM PIN Verification



- Various alternative approaches:
  - Simple
  - PIN Verification Values (PVV)
  - Offsets

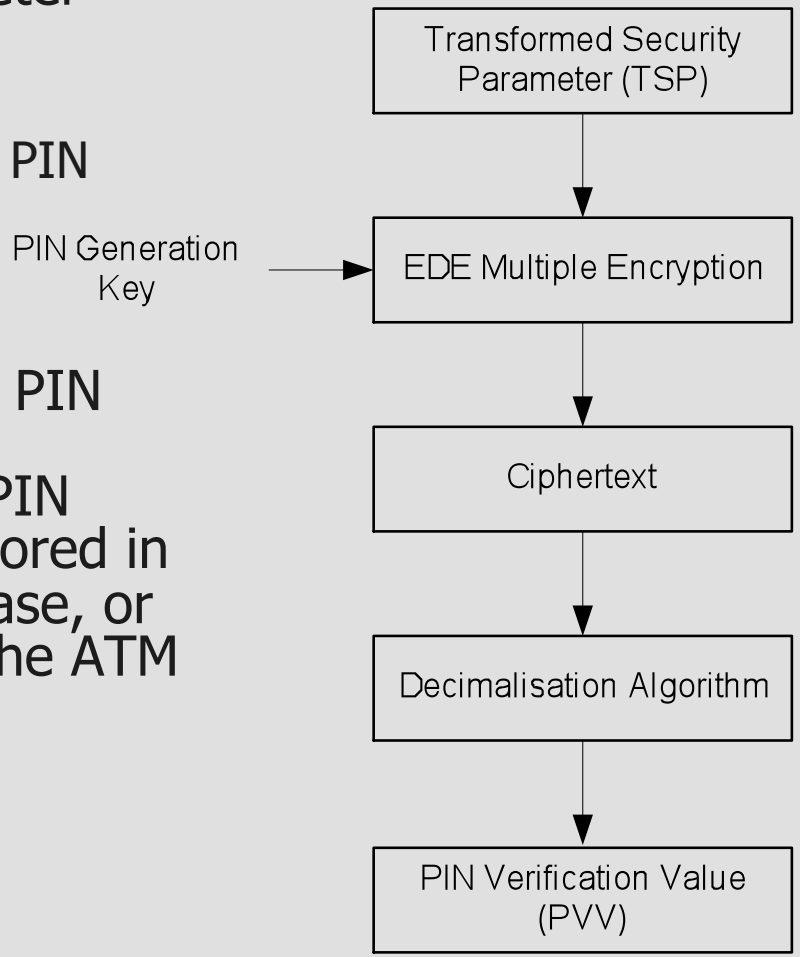
PIN Generation (simple)

- IBM 3624 PIN Generation Algorithm



PIN Verification Values

- Uses a Transaction Security Parameter (TSP), consisting of
  - the PAN,
  - an issue number referring to which PIN derivation key is to be used, and
  - the trial PIN itself.
- The TSP is then encrypted with the PIN master key, then truncated and decimalised, yielding a four digit "PIN Verification Value" which can be stored in the clear in the bank's main database, or written to the magnetic stripe on the ATM card.



PVV Clash Attack

- Due to the short length of the PVV, the birthday paradox ensures that multiple TSP values will produce the same PVV as a result.

- In practical terms, there will be several correct PINs for each account!
  - Approximately 60% of accounts will have two or more correct PINs.
  - Furthermore, about 0.5% of accounts have five or more correct PINs

- In practice, this weakness of the algorithm is of limited practical value; however the **legal implications** of having multiple correct PINs for an account are interesting, and completely uncharted territory.

PIN Verification - Offsets

Customer PIN = Constant PIN (IPIN) + Variable PIN (PIN Offset)

Allows the user to select his own PIN and change it easily

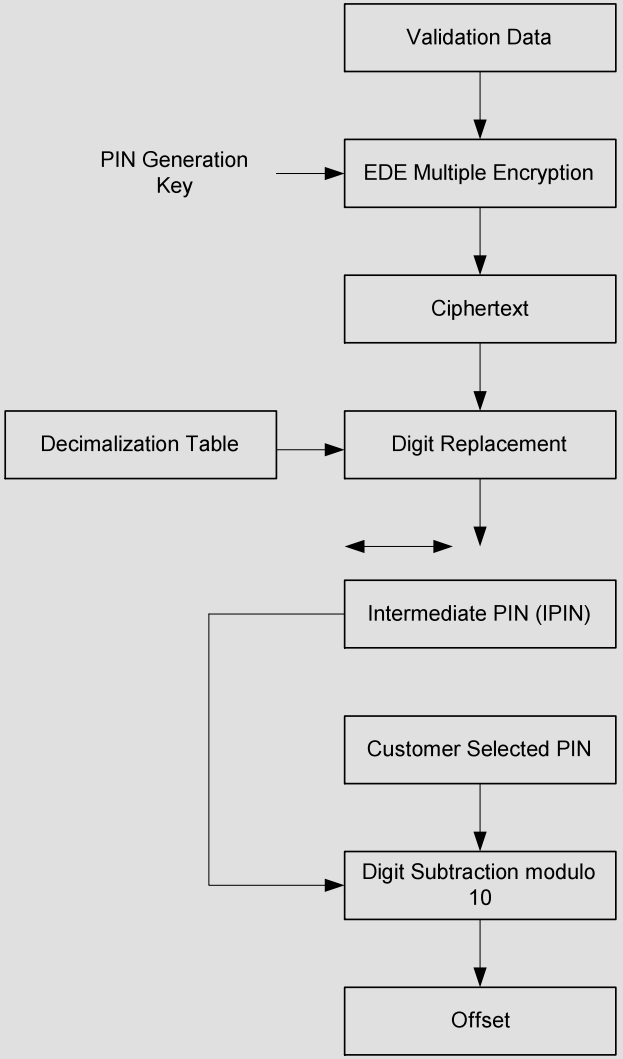
- IPIN
  - Depends on client information (PAN) which gets encrypted using the PIN generation (verification) key.
  - The cipher text is 'decimalised' using the following table

Input	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Output	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**

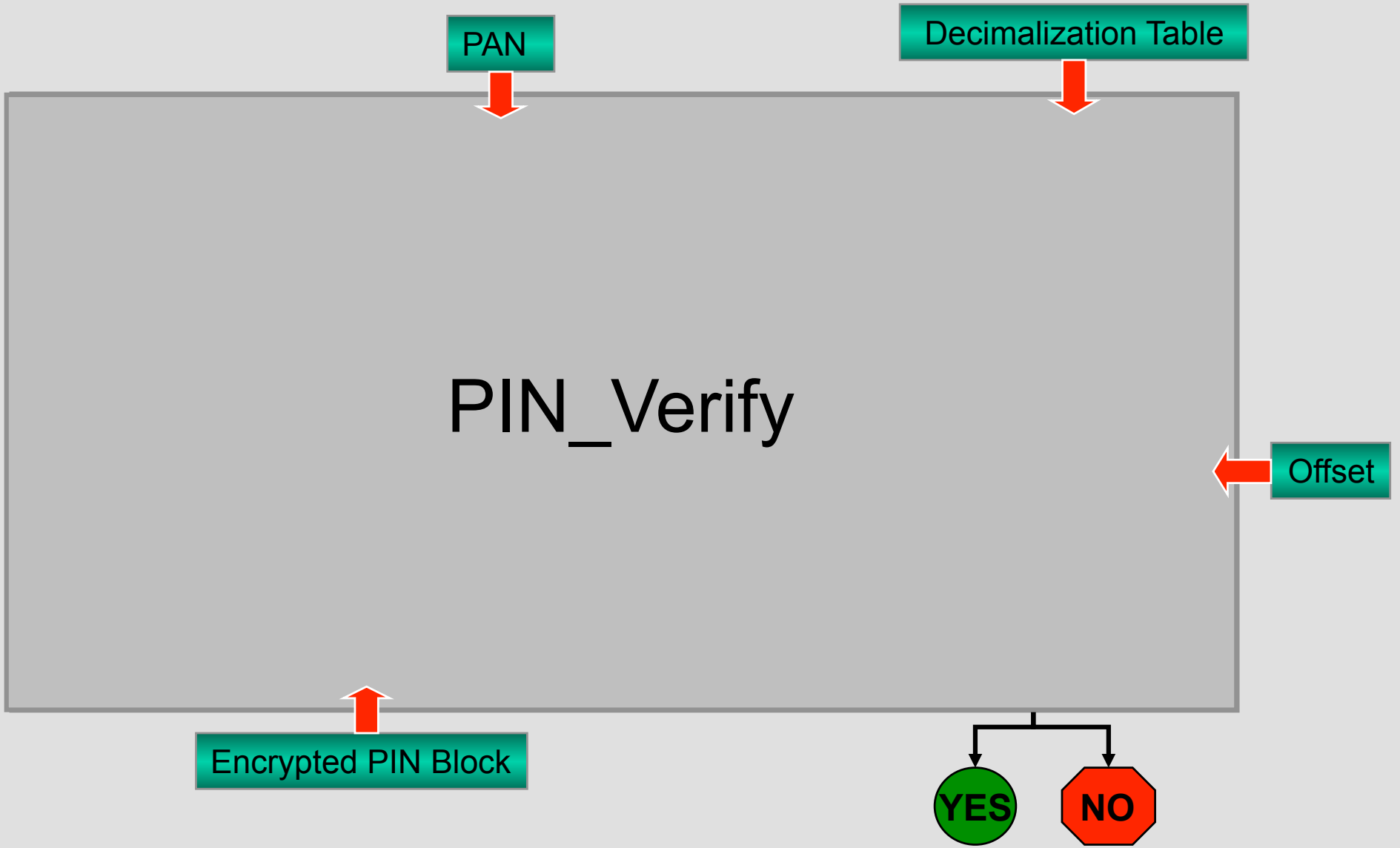
- OFFSET
  - When the client changes PIN the OFFSET changes
  - OFFSET = PIN-IPIN ('-': subtraction modulo 10)

PIN Verification - Offsets

- Validation data is encrypted under PIN generation (verification) key.
- Ciphertext is 'decimalised' to form IPIN by means of a table.
- Calculate the offset as OFFSET = PIN-IPIN (where '-' is subtraction modulo 10)



PIN Verification (Offsets) [2]



PIN Attack Characteristics

- Internal attacks or following metastasis from other compromised infrastructure providing internal access
- Require HSM access
  - Physical Access (stolen device?) or
  - Access to the network which carries transactions (message injection is required)
- Ultimate goal is PIN discovery
- Not time-consuming
- No special knowledge or hardware requirements
- Vendor-independent
- HSM network security is not a solution since the standard functions necessary for the attack should be exposed & available for the whole system to work properly

- ***Inactivated PINs can also be discovered***

XOR-to-null key attack

Attack Background:

- Top-level crypto keys are exchanged between banks in two or three parts, carried by separate couriers and combined using the exclusive-OR function

Host -> HSM : $\{KP_1\}_{KM}$, $\{KP_2\}_{KM}$

HSM -> Host : $\{KP_1 \oplus KP_2\}_{KM}$

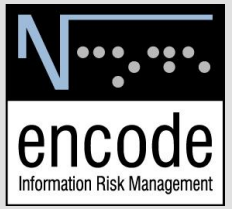
Attack Preparation:

- A single operator could feed in the same part twice, which cancels out to produce an 'all zero' test key. PINs could be extracted in the clear using this key

Host -> HSM : $\{KP_1\}_{KM}$, $\{KP_1\}_{KM}$

HSM -> Host : $\{KP_1 \oplus KP_1\}_{KM}$ (= $\{0\}_{KM}$)

XOR-to-null key attack [2]



Attack Execution:

- Use a transaction that enables a programmer to encrypt the PIN key under a terminal master key
  - Available so that an ATM can verify customer PINs while the network is down.
- Now we can obtain the PIN key encrypted under the all-zero key.
- We can decrypt it using our own computer and are then able to compute any customer's PIN.

Now you know why dual control in key management is important!...

‘Two-time’ attack

- HSMs have multiple keys
  - Local Master Keys (LMK)
  - Terminal Master Keys (KMT)
  - PIN Derivation Keys (KPD)
  - Terminal Communication Keys (KCT)
  - …
- HSMs provide many functions
  - Encryption
  - Translation
  - …

'Two-time' attack

- Recall that a customer PIN is, in effect, their *Primary Account Number* (PAN) encrypted under the PIN derivation key:

  PIN = $\{PAN\}_{KPD}$

- So an attacker will enter the PAN into the system as a KCT, by encrypting it under KMT:

  Host –> HSM : "Encrypt Comms Key" , *PAN*

  HSM –> Host: $\{PAN\}_{KMC}$

- The second step is to get the HSM to take the encrypted PAN (which is now considered to be a KCT) and re-encrypt it under a terminal master key. However, instead of supplying $\{KMT\}_{LMK}$, we supply the PIN key $\{KPD\}_{LMK}$:

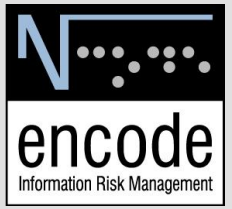
  Host –> HSM : "Translate Comm Key to KMT", $\{PAN\}_{KMC}$, $\{KPD\}_{LMK}$

  HSM –> Host: $\{PAN\}_{KPD}$

- The answer, $\{PAN\}_{KPD}$, is just the PIN.

Break for Panadol

Meet-in-the-Middle Attack



Attack Background:

HSMs use/store many different types of keys (e.g. ZMKs, LMKs, TMKs. KPDs, KCTs, etc.)

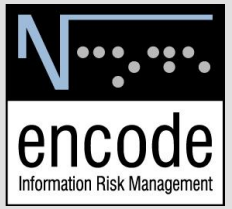
Attack Preparation:

- One test pattern is encrypted under all HSM keys and the different results are recorded

Attack Execution:

- Same test pattern is encrypted under a trial key and the result is compared against all encrypted test patterns
  - Comparison takes slightly longer
  - Much faster than having to do one encryption per comparison
  - Using a hash table comparison is almost instantaneous

Decimalization Attack [1]



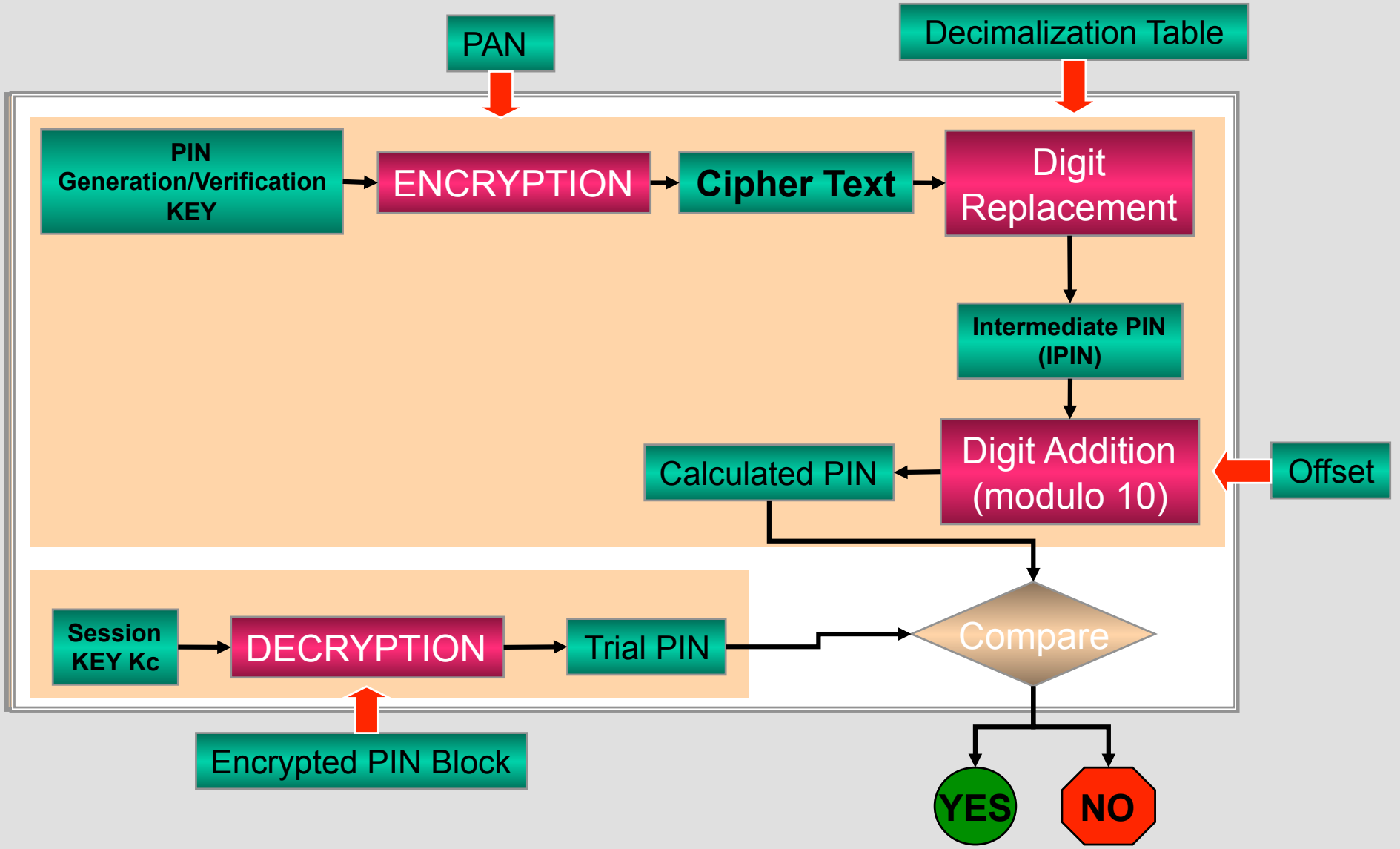
- Remember the raw PIN is converted from hex to decimal using the decimalisation table
- Most HSM APIs allow the decimalisation table to be specified with each PIN verification command
- A normal verification command eliminates one of 10,000 possible PINs for the attacker.
- If the table is altered, the effects can leak much more information about the PIN

Decimalization Attack [2]

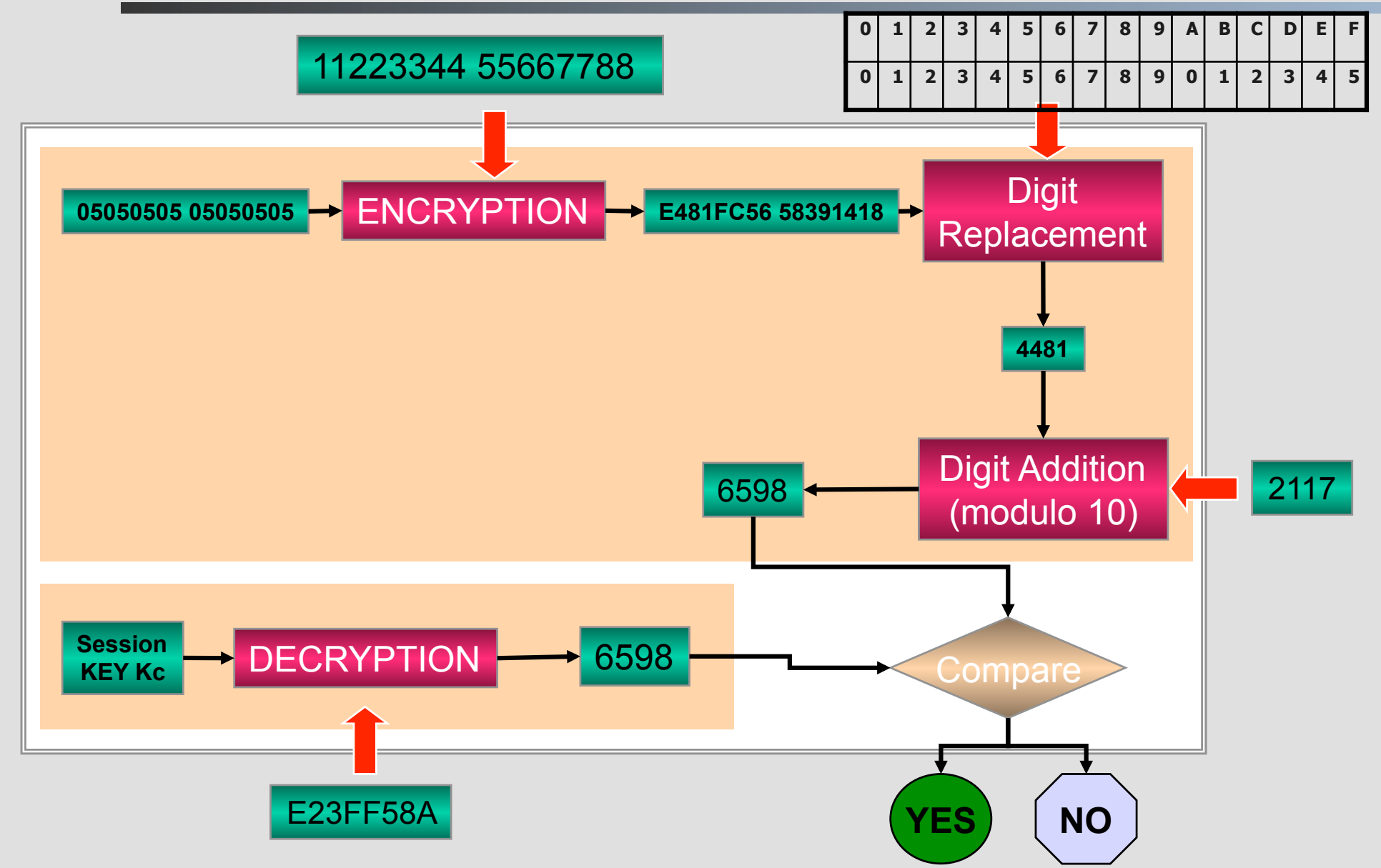
- Input Parameters
  - Encrypted PIN Block (EPB)
  - Validation Data (PAN)
  - Decimalization Table
  - Offset

- **Attack Strategy**: Repeatedly changing one entry in the decimalisation table and observing the results.
  - Phase 1: PIN digit identification
  - Phase 2: PIN digit position identification

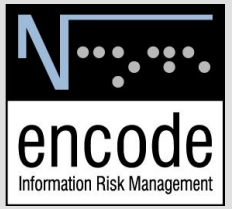
Normal Operation



Normal Operation [2]

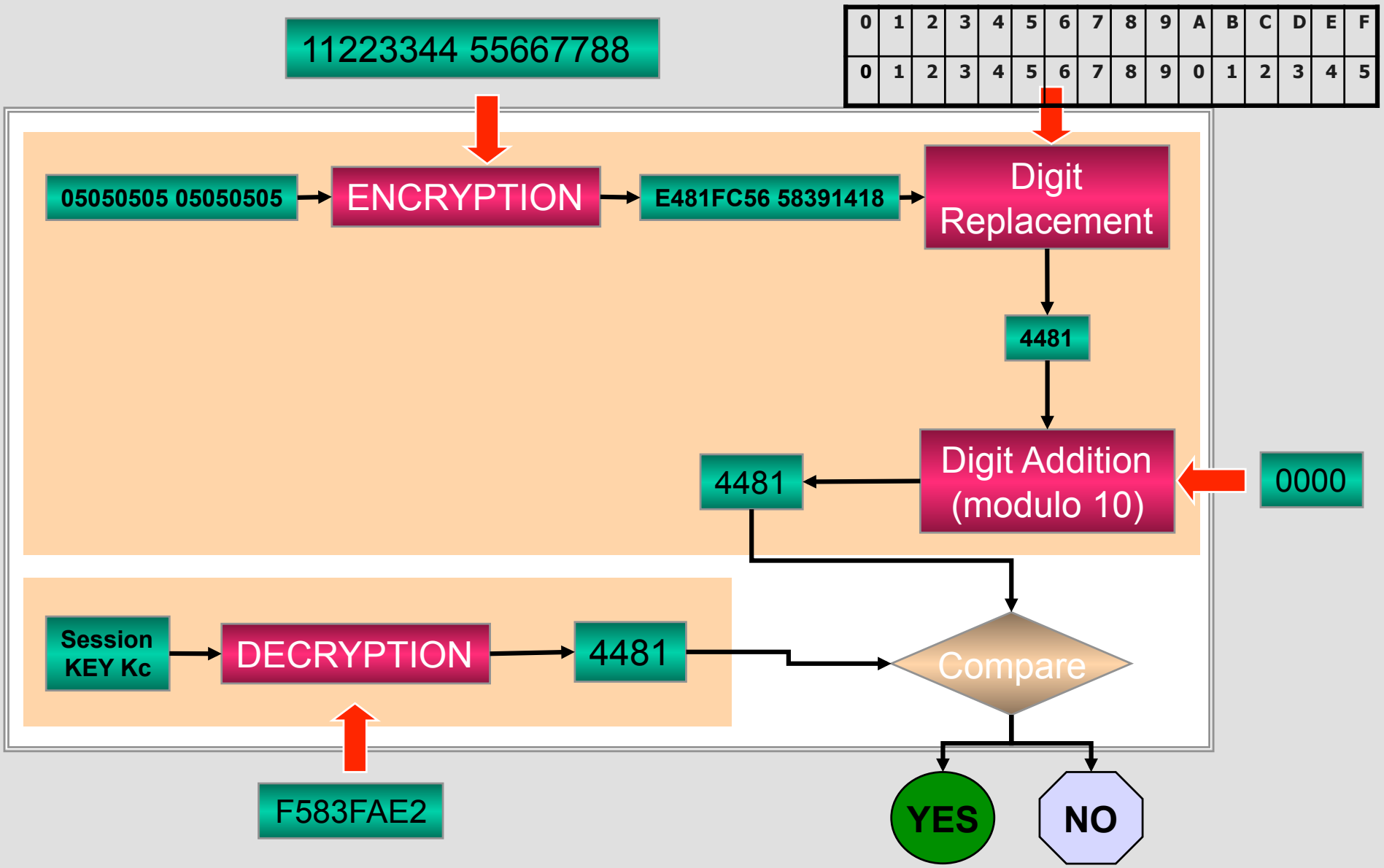


Assumptions

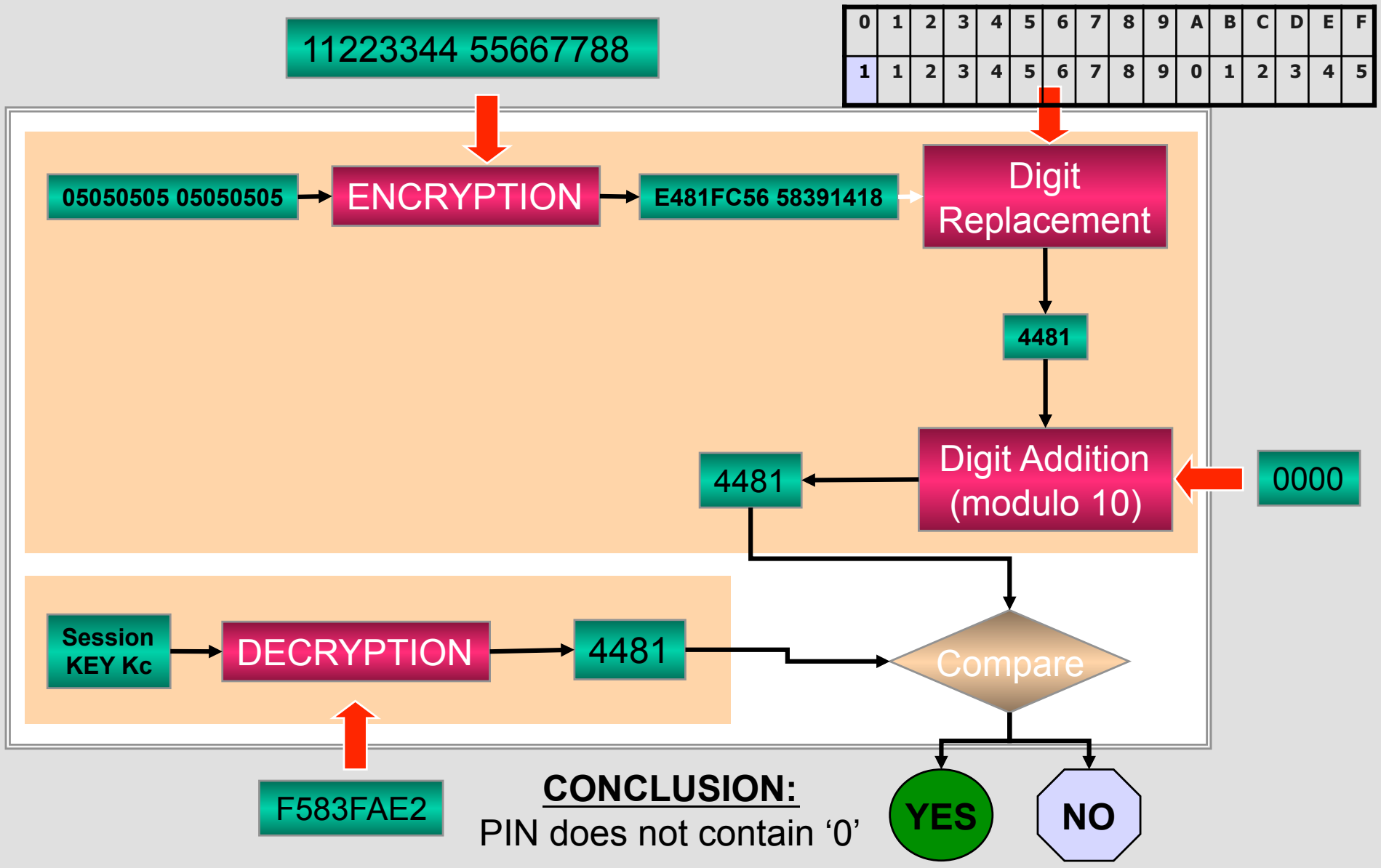


- The Encrypted PIN Block is available to the attacker (e.g. via network sniffing - relatively easy for users internal to the network)
- For simplicity's sake let's assume that the client has not changed his PIN
  - Offset = 0000

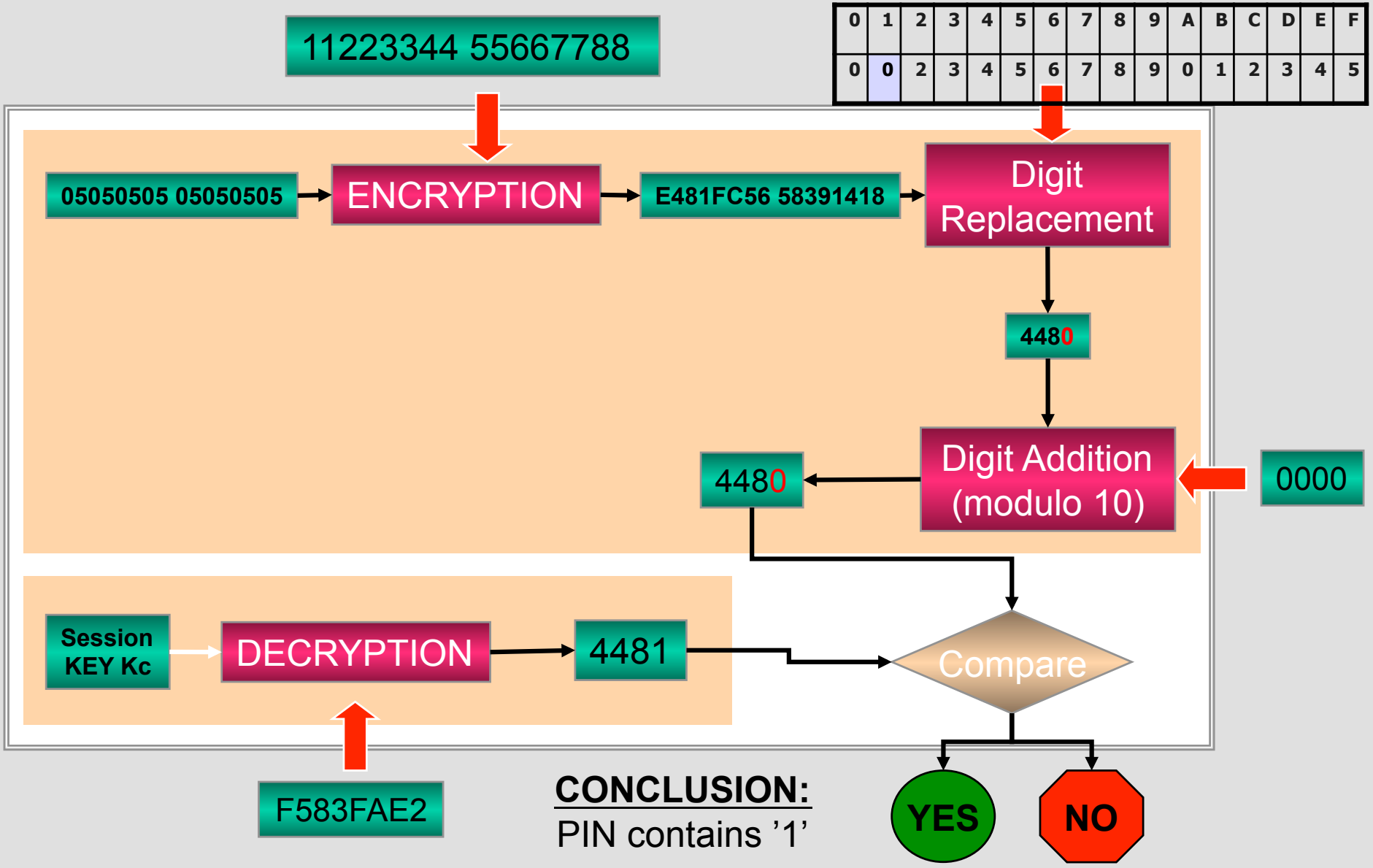
PIN Attack – Normal Flow



PIN Attack - Phase 1



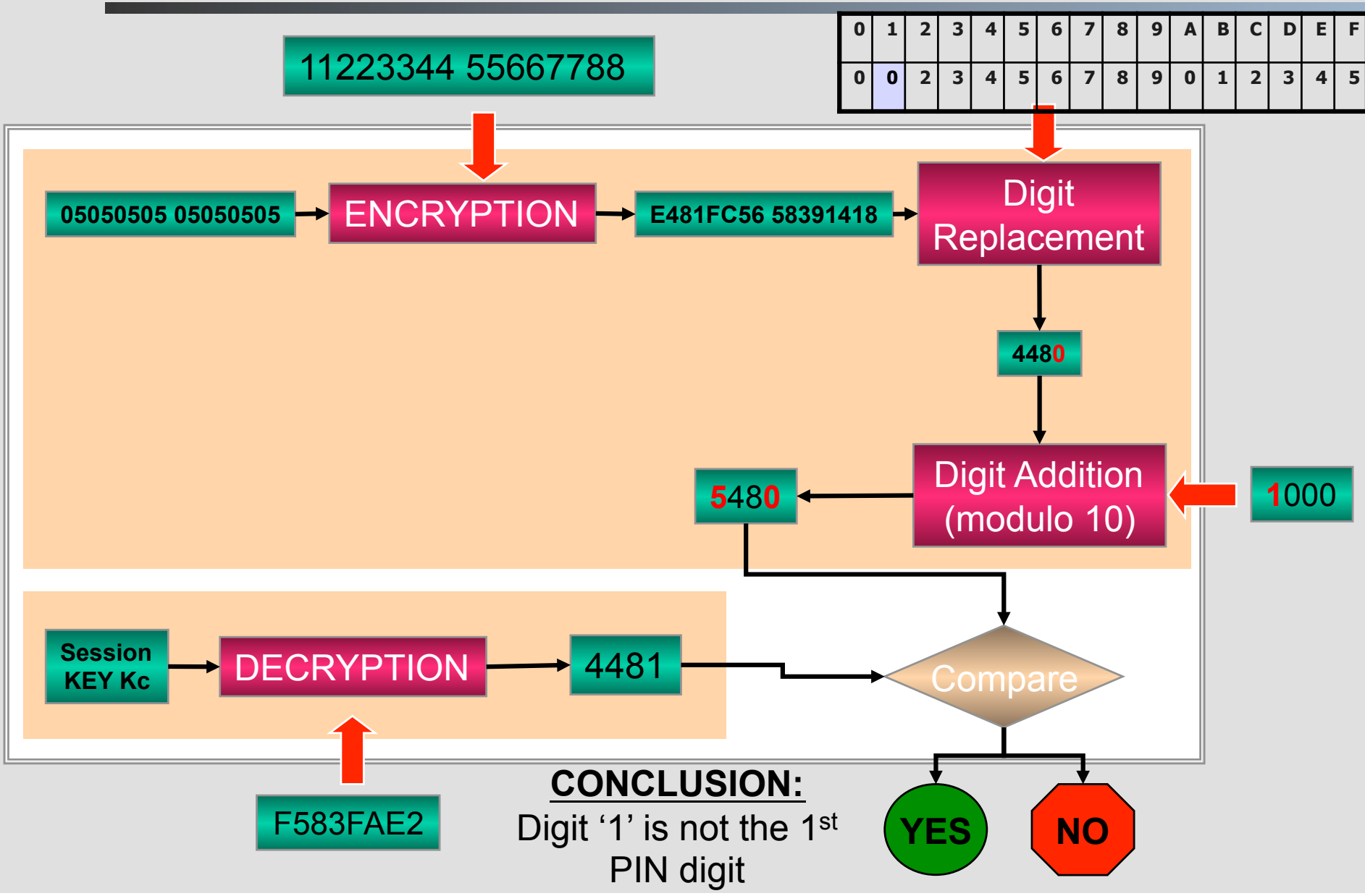
PIN Attack - Phase 1



CONCLUSION:

PIN contains '1'

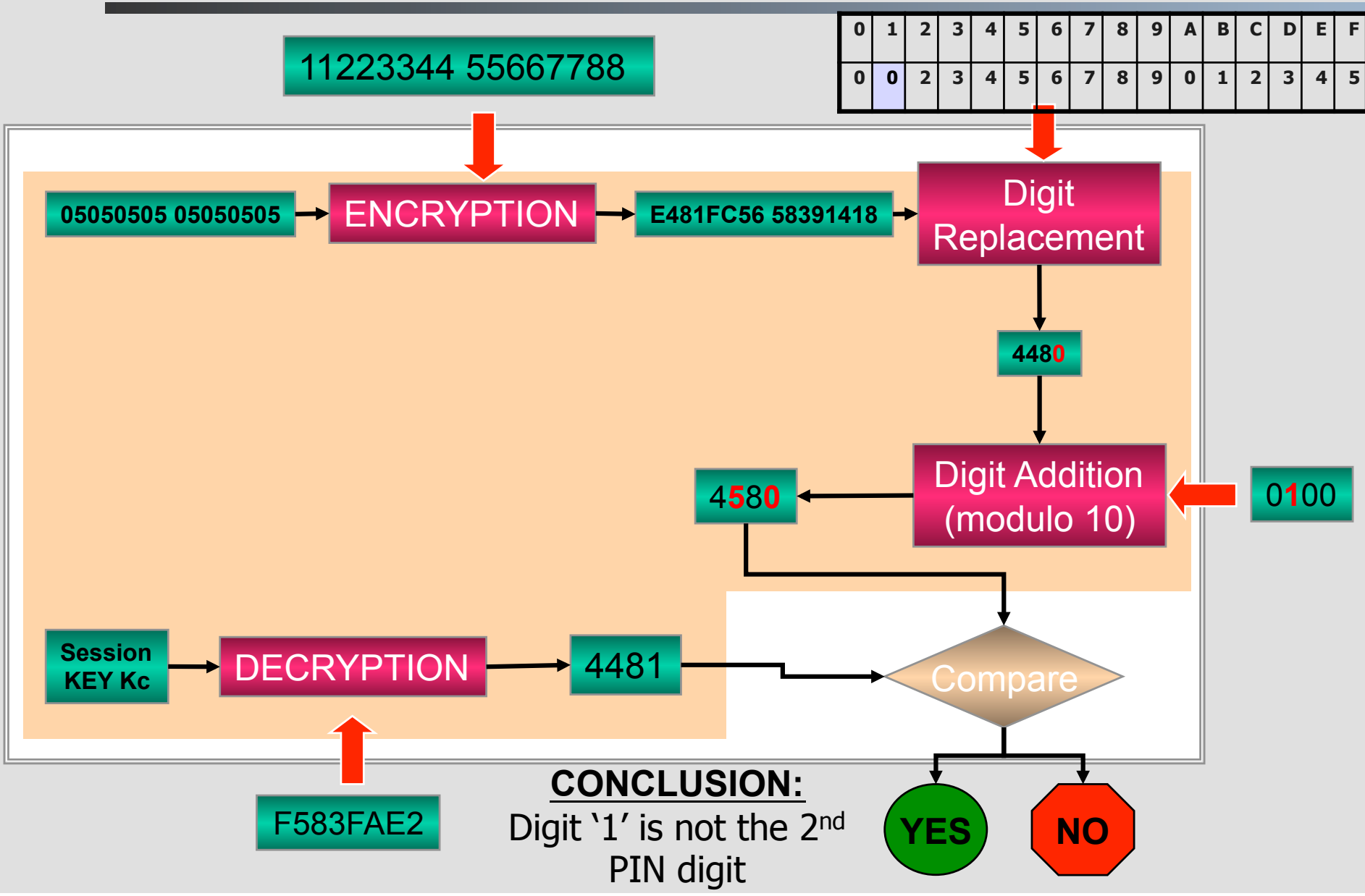
PIN Attack - Phase 2



CONCLUSION:

Digit '1' is not the 1st PIN digit

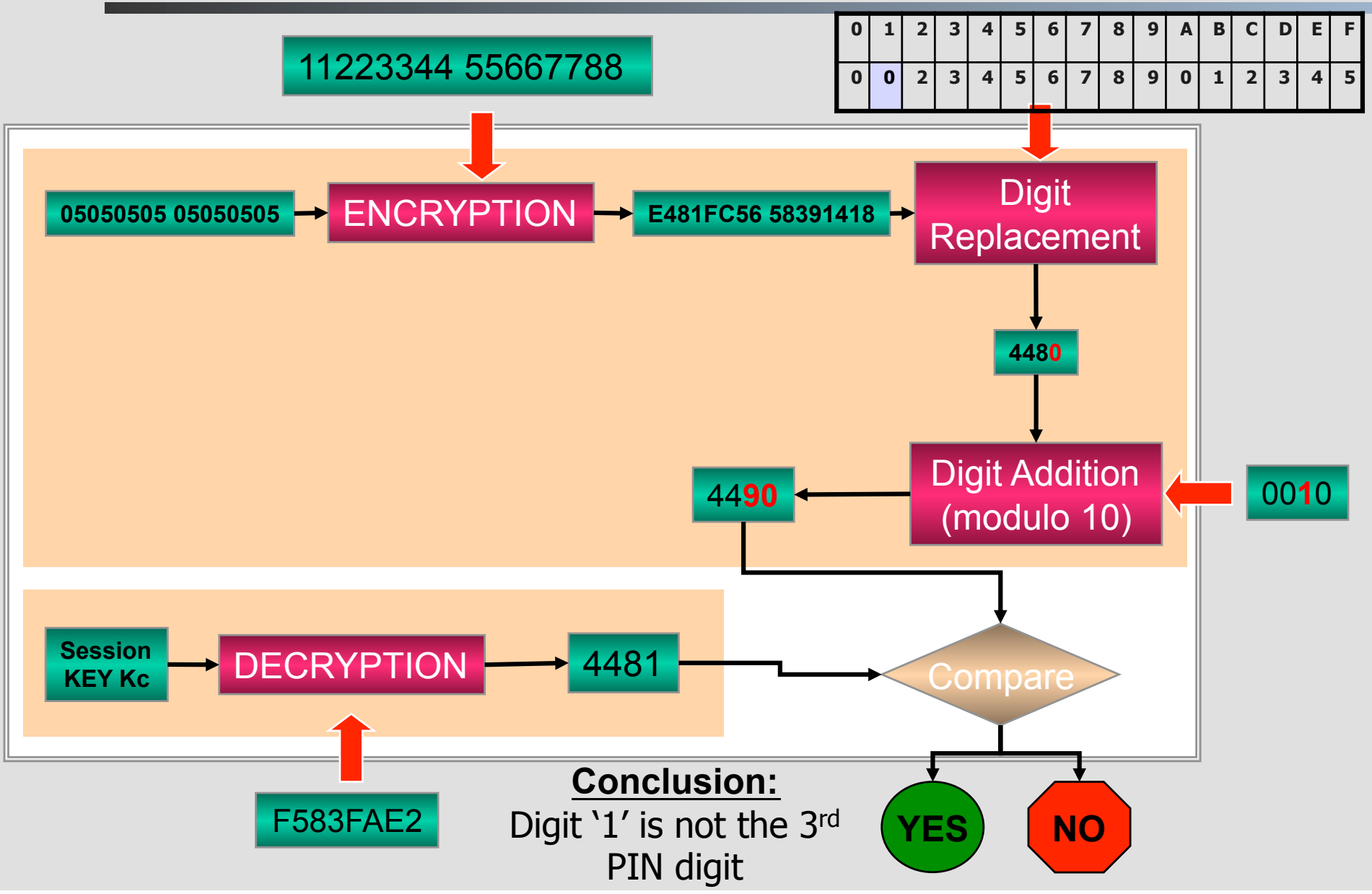
PIN Attack - Phase 2



CONCLUSION:

Digit '1' is not the 2nd PIN digit

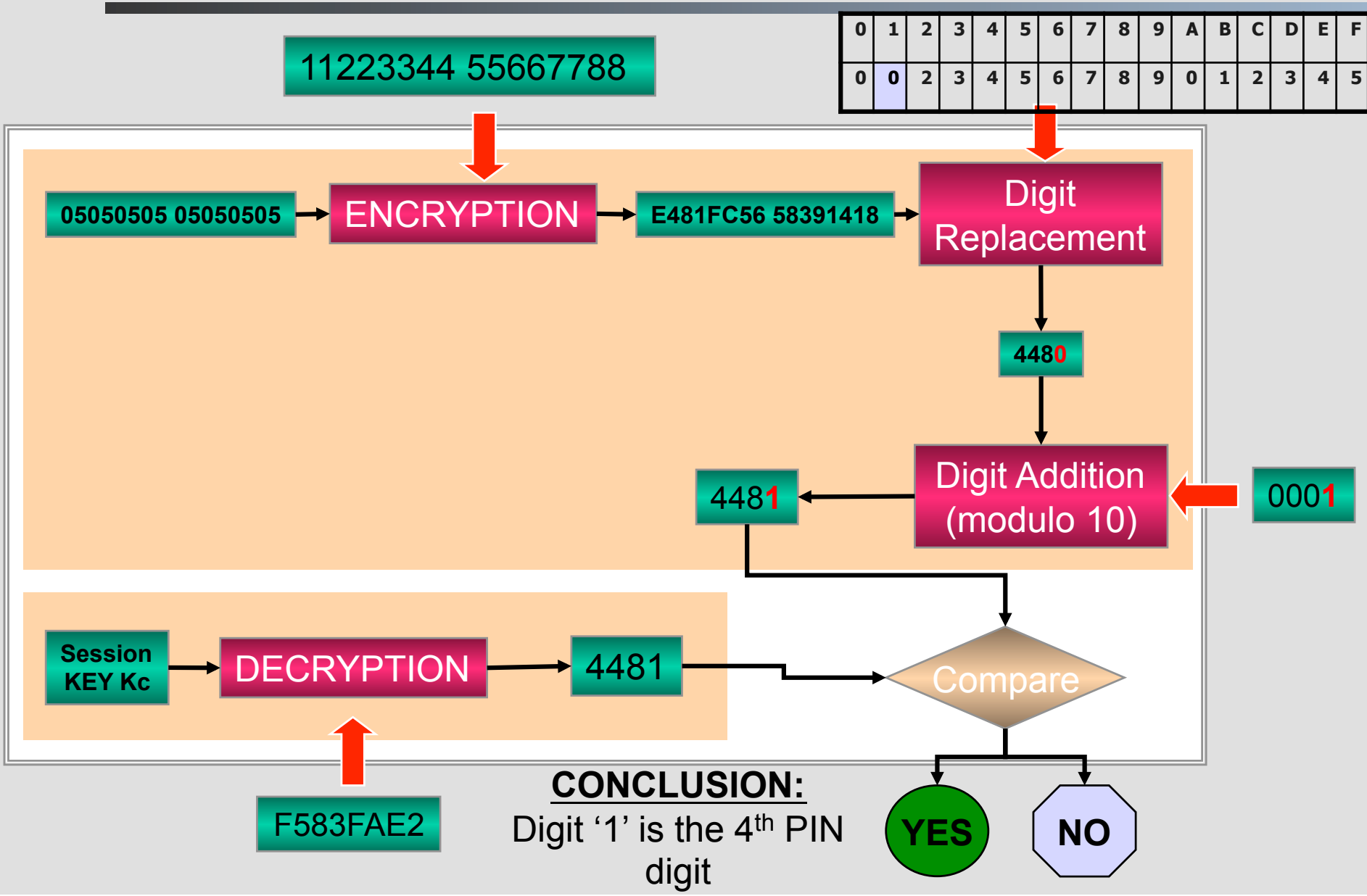
PIN Attack - Phase 2



Conclusion:

Digit '1' is not the 3rd PIN digit

PIN Attack - Phase 2



CONCLUSION:

Digit '1' is the 4th PIN digit

Decimalization Attack Work factor

- The time required to complete the attack depends of the HSM processing speed.

- Typical time required:
  - Known offset: 1 – 20 sec.
  - Unknown offset:10 - 1000 sec.

Translation Attack [1]

Attack Background:

- Translation function is used on edges of keying zones to translate the EPB between zones
- May perform PIN-block reformatting in case entitles on the two zones support different PIN -block formats

Attack Preparation:

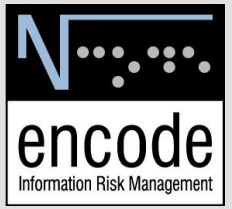
- We precompute a table of 10,000 EPBs using ISO-0 format, using the same, known, PAN for all EPBs
  - The i^{th} entry corresponds to PIN *i* (0000<=i<=9999)

Translation Attack [2]

Attack execution:

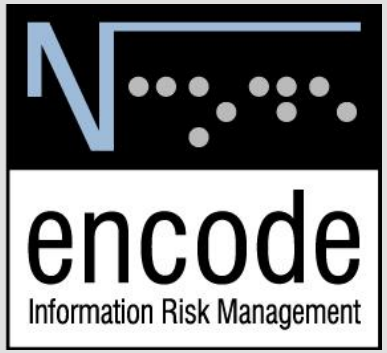
- Given any EPB we use the 'Translate' function to convert it to ISO-1 and then to ISO-0, substituting the PAN with our known value
  - hence breaking the link between the original –unknown- PAN and the PIN and creating a link between the PIN and a known value
- We look up the resulting EPB in our tables of 10,000 EPBs created with known PAN and PINs ranging from 0000-9999

Points to ponder…



- What if we combine the Translation Attack with a XOR-to-null attack and create a dummy keyzone with a known zone key?

Answers on a postcard are welcome…



Conventional IT Attacks …

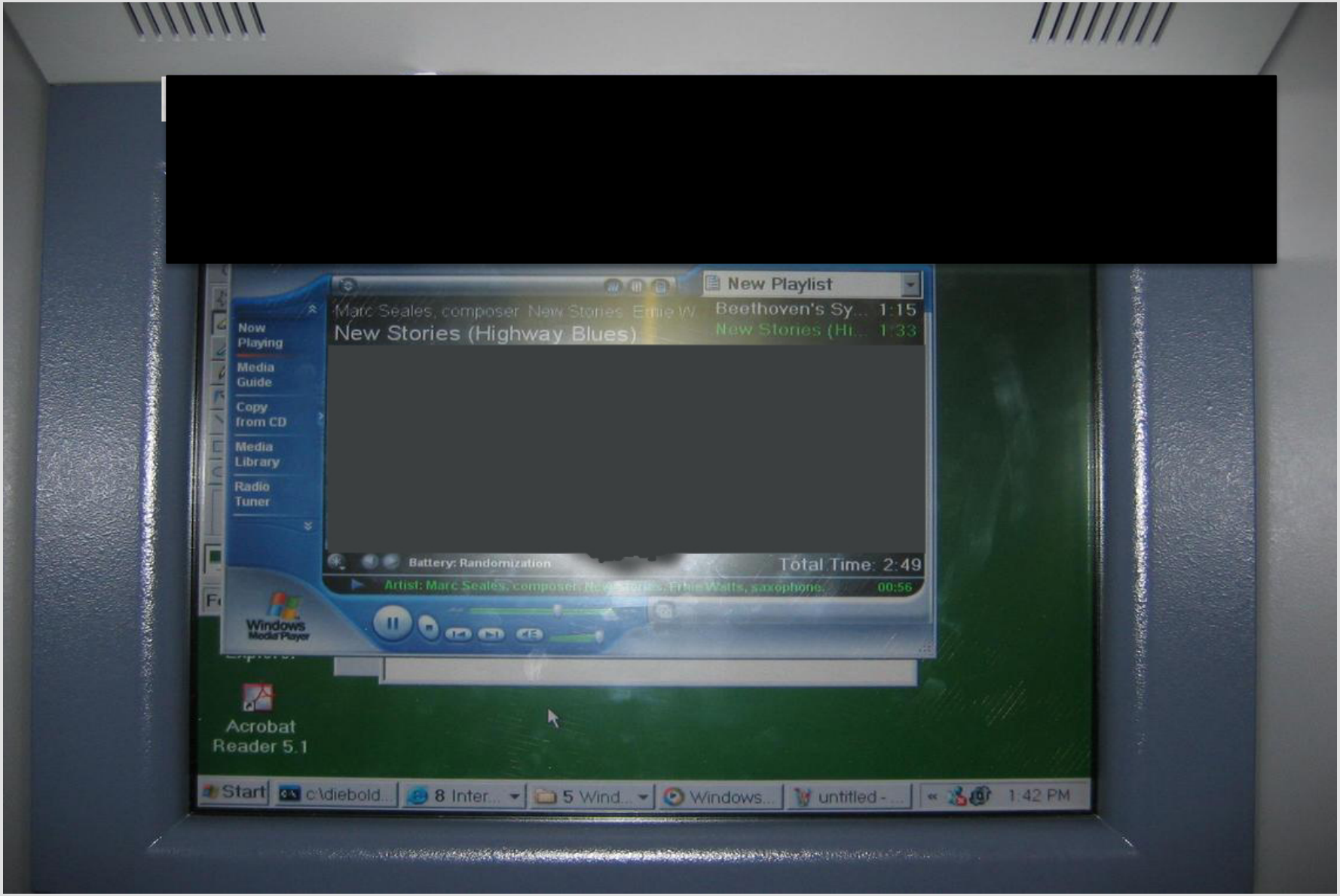
Conventional IT Attacks

encode
Information Risk Management

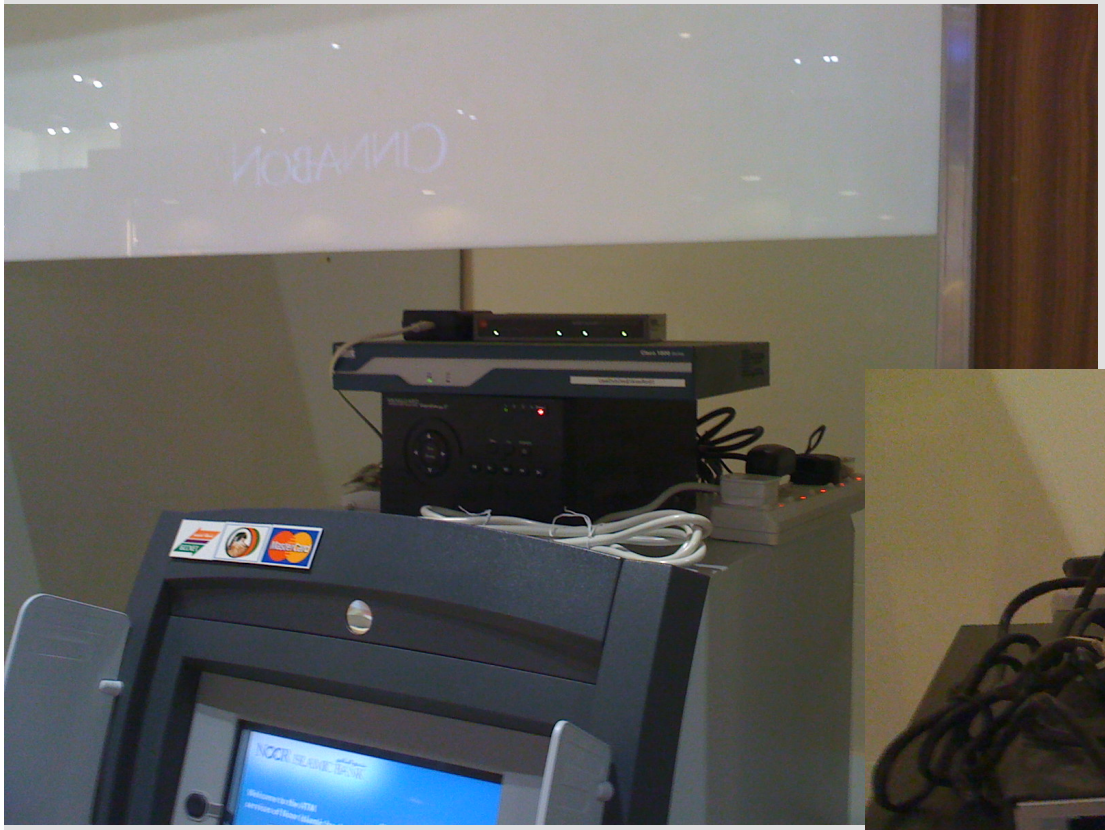
- The need for:
  - New services
  - Processing speed
  - System Integration
- Leads to the adoption of "mainstream" technologies (Windows, TCP/IP …)
- And changes dramatically the threat model

- New technologies must be adopted (but care should be taken)!

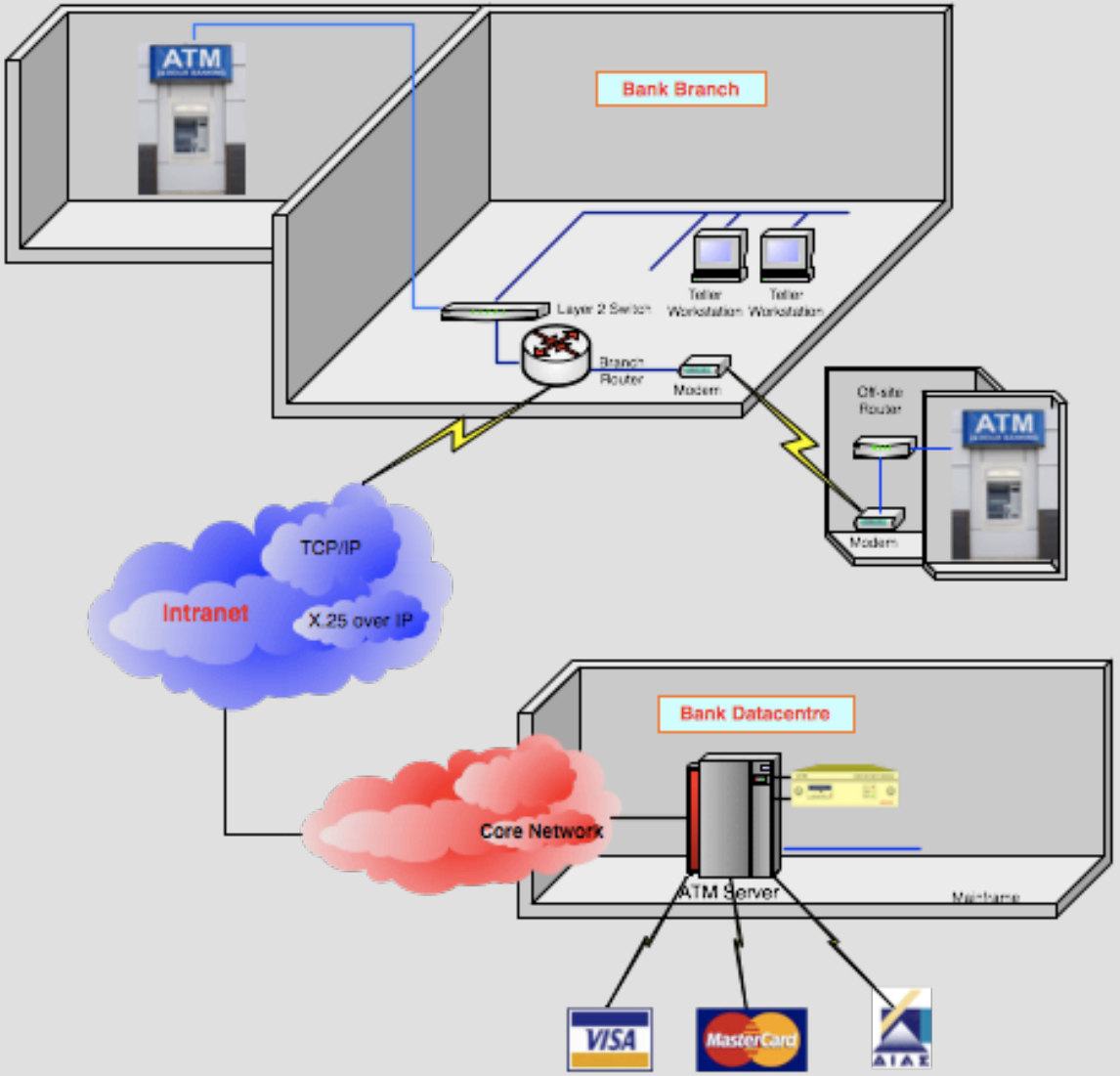
What can go wrong?



What can go wrong?

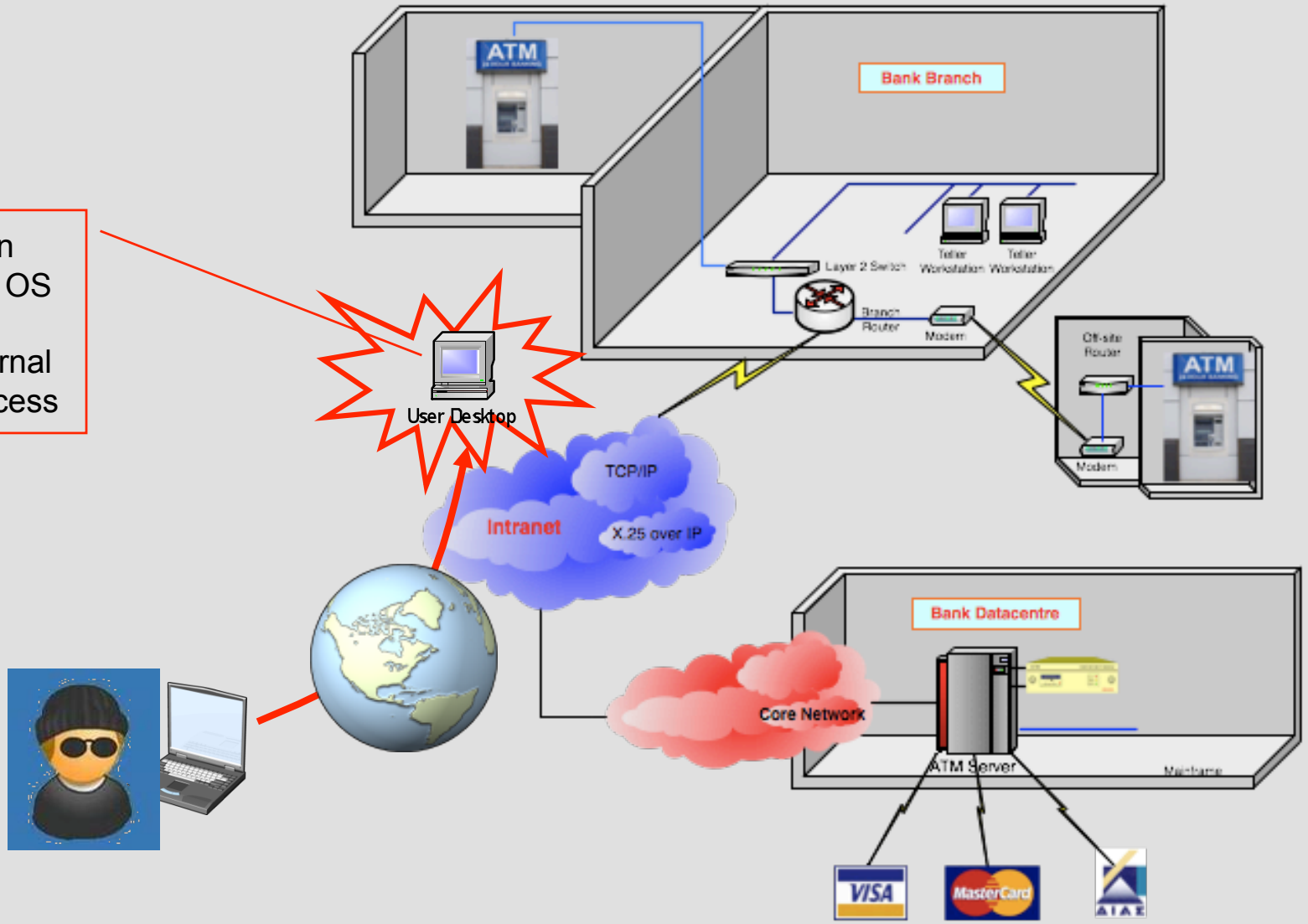


TCP/IP ATM Networks



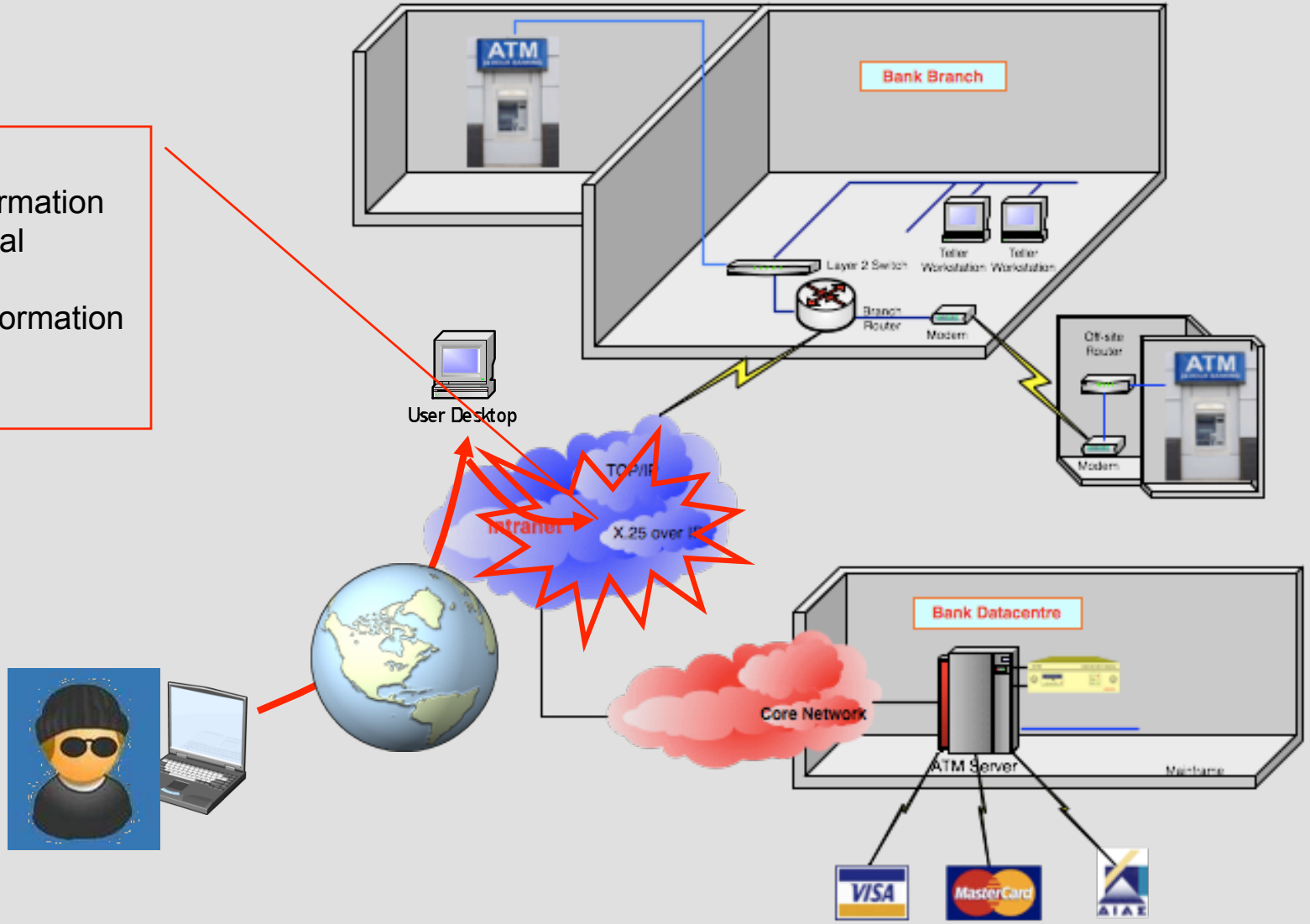
Attacks [1]

- Send Trojan
- Obtain Full OS Access
- Obtain Internal Network Access



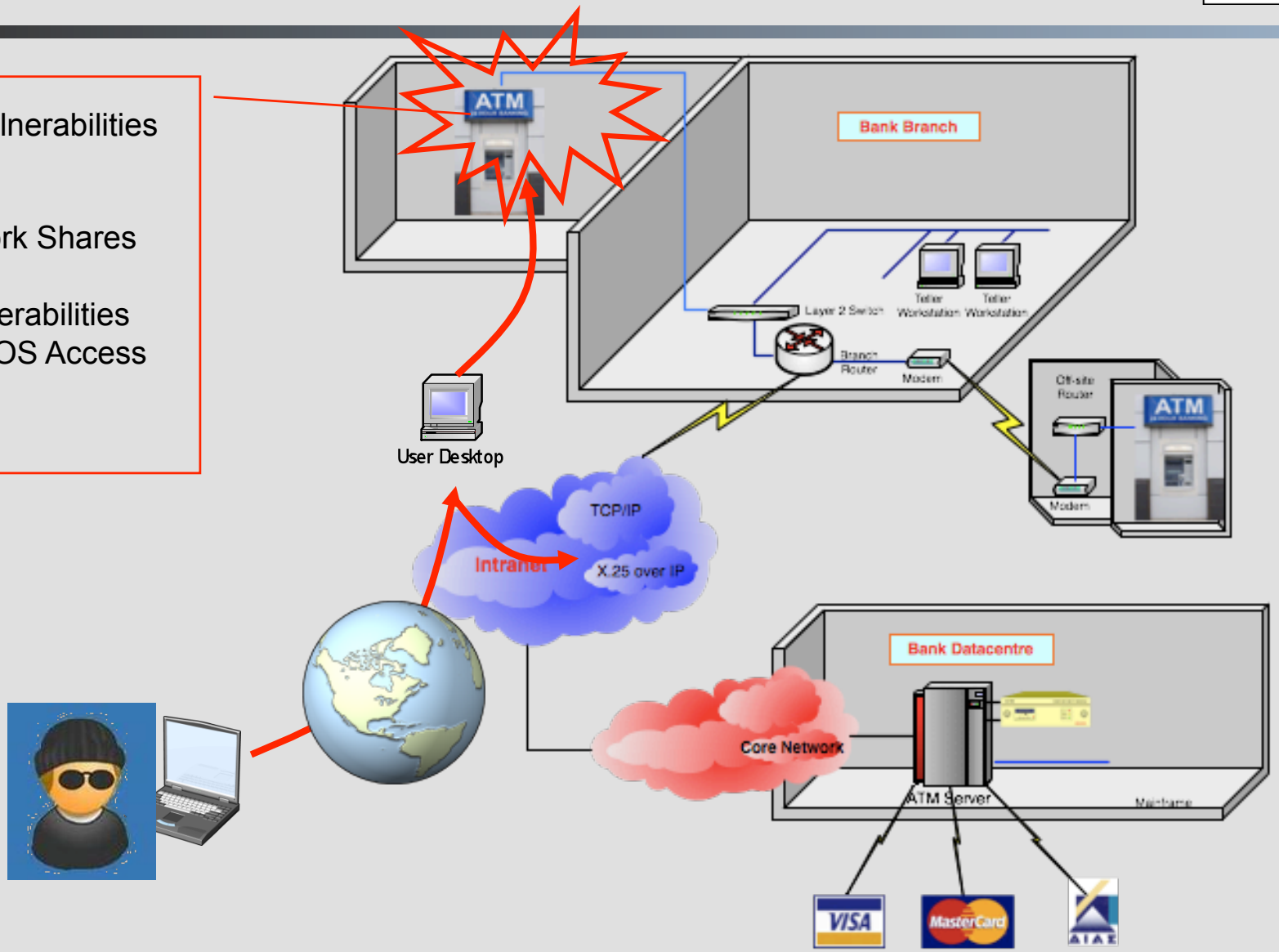
Attacks [2]

- Obtain Information about Internal Network
- Analyze Information
- Target ATM

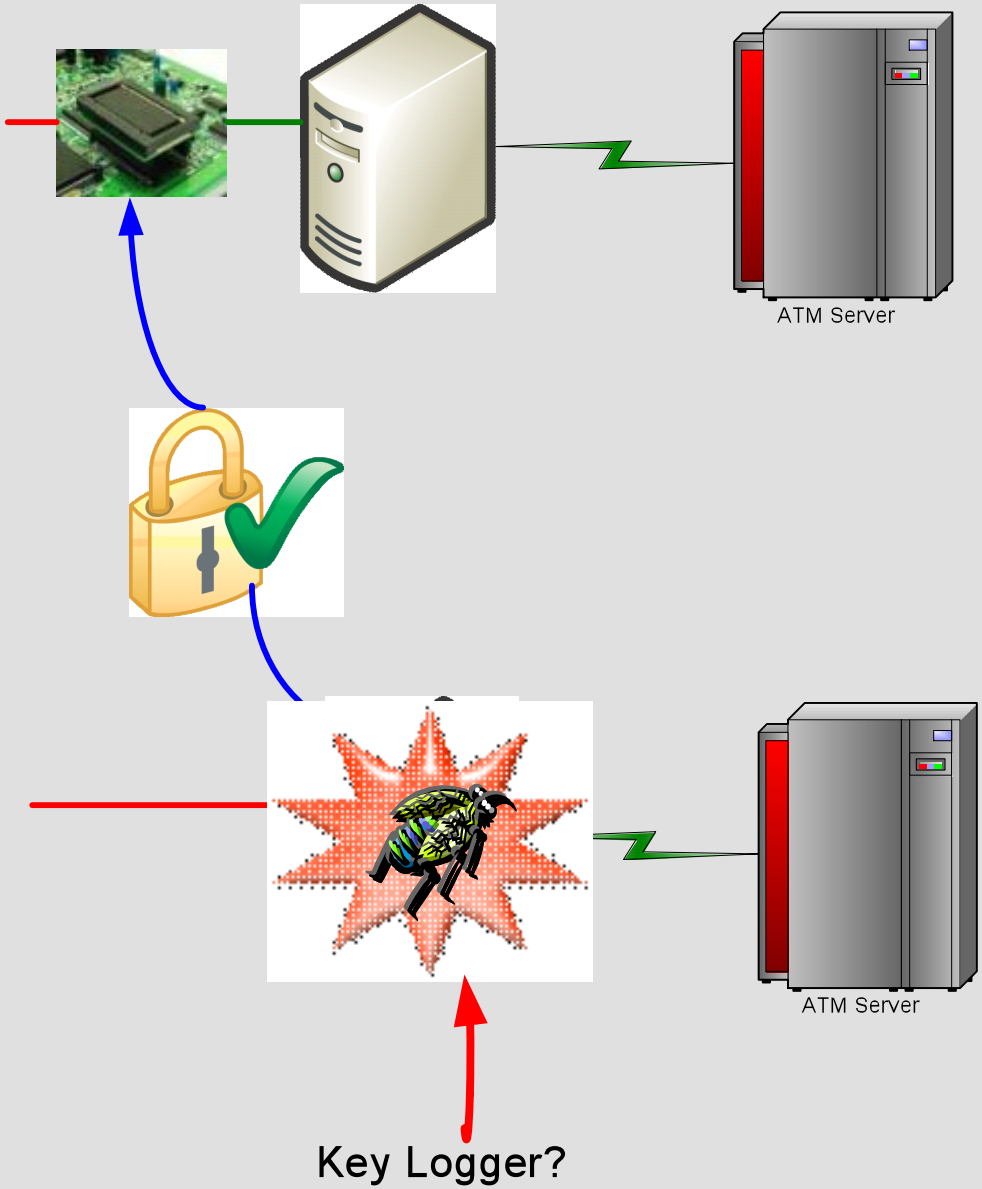


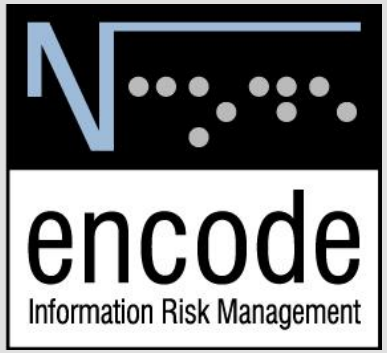
Attacks [3]

- Discover Vulnerabilities
  - OS
  - SQL
  - Network Shares
  - …
- Exploit Vulnerabilities
- Obtain Full OS Access on ATM
- ….?



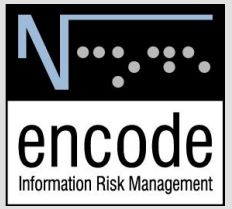
Attacks [4]





Some parting thoughts…

Facts…



- The security of the online PIN transaction APIs and protocols leaves a lot to be desired
  - Finger-pointing is futile as a number of reasons has led to current situation
- Attacks described in this presentation were in the realm of academia a couple of years back; today they ***are*** *reality* (documented cases)
- We'll see more & more of them in the near future

…& Fiction…

encode
Information Risk Management

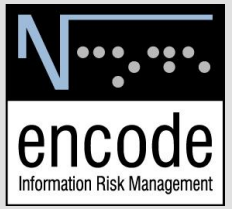
"Our Bank uses industry best practices; we implement and enforces secure processes & procedures"

<insert Bank name here>

May very well be true, but:

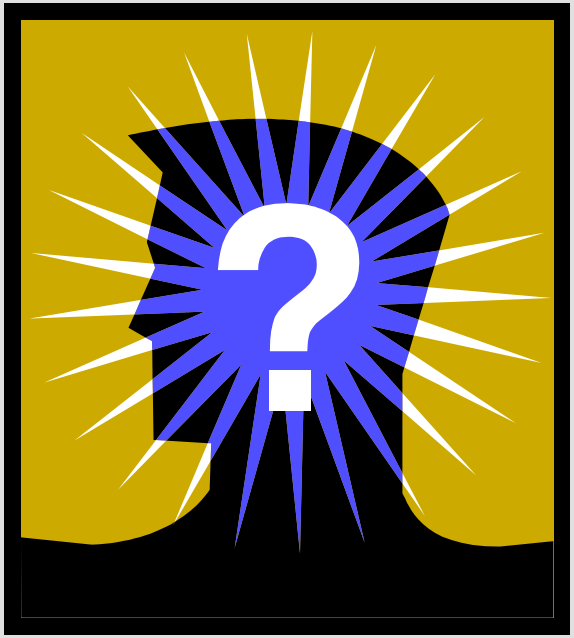
- Ever heard of the 'weakest link'?

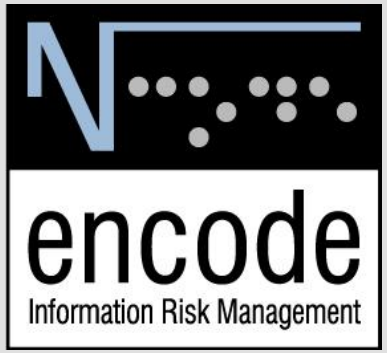
Further Reading



- Mike Bond & Jolyon Clulow, "Encrypted? Randomised? Compromised?", University of Cambridge
- Mike Bond & Ross Anderson, "API-Level Attacks on Embedded Systems", University of Cambridge
- Graham Steele, "Formal Analysis of PIN Block Attacks", University of Edimburgh
- Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov, "Cryptographic Processors—A Survey", IEEE Proceedings
- Omer Berkman and Odelia Moshe Ostrovsky, "The unbearable lightness of PIN cracking", Tel Aviv University
- Trustwave Report, "Automated Teller Machine (ATM) Malware Analysis Briefing"

Any questions?





Thank you for your time…

d.petropoulos@encodegroup.com