CYBERCOM GROUP

Local Presence Global Reach

Encryption of cardholder information

Torbjörn Lofterud
Cybercom Sweden East AB

Torbjörn Lofterud

- Information security consultant at Cybercom Sweden AB
  - QSA
  - PA-QSA
  - PFI

PCI DSS

- Common information security standard
  - MasterCard
  - VISA
  - American Express
  - Discover
  - JCB
- Released late 2004 / early 2005
- Current version is version 2.0
- Contains 12 chapters

PCI DSS - Encryption requirements

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads
- Strong cryptography with associated key-management processes and procedures

“industry-tested and accepted standards and algorithms for encryption”

"a recommended practice, but not specified requirement, that a salt be included"

Homegrown crypto solutions

- "Unique requirements"
- "The standard doesn't address our needs"
- "Our bank requires this"

Threat analysis

- Hashing
  - MD5 / SHA1
  - No or global salt
- 3DES-ECB
  - Electronic codebook format (ECB)
- RSA without random padding
  - Known or no padding

Sample dataset

- Three databases
  - ten thousand (10k) cards representing a smaller merchant
  - one hundred thousand (100k) cards representing a medium size merchant
  - one million cards (1m) representing a large merchant or a small payment service provider

IIN	Brand	Market penetration
910001	Bank A	25%
920002	Bank B	14%
930003	Bank C	7%
940004	Bank D	7%
950001 – 950021	Bank E-Z	47%

Attacking hashed PANs

CYBERCOM GROUP

Database schema

PAN (SHA-1)	Expires	CustomerID
e0b18e3d978fc06354f610bcb4f40915c6ab59f4	09/09	1
70da34d2c94426a5858165e0f24b6fea6ebc86e9	09/08	2
8b19dc6f5b7ef58b7f135dbc0492e0df6d1ff304	09/07	3

Attacking hashed PANs

- Partial known plaintext attack
  - 13 to 19 digits
  - The first 6 digits are predictable (IIN/BIN)
  - Last digits is a checksum (luhn-10)

A brute force attack can be reduced from 16 unknown bytes to roughly 9 unknowns for each IIN attacked. The conclusion is that 10^9 (1 billion) SHA-1 computations has do be done for each IIN

Attacking hashed PANs

- John the ripper – patched to support RAW sha1
- Wordlist-generator that calculates the checksums

```
./wordlist 950001 | ./john --stdin hashlist10k.txt
Loaded 10000 password hashes with no different salts (Raw SHA1)
```

DB Size	Algorithm	Time / IIN
10k	SHA-1	8 minutes
100k	SHA-1	47 minutes
1M	SHA-1	525 minutes

Protecting hashed PANs

- Dont use hashing to protect cardholder data
- Select a slower algorithm
- Use a unique salt for each cardnumber
- Consider global salts as cryptographic keys and protect them in compliance with PCI DSS chapter 3.5 and 3.6

Attacking ECB-mode 3DES PANs

CYBERCOM GROUP

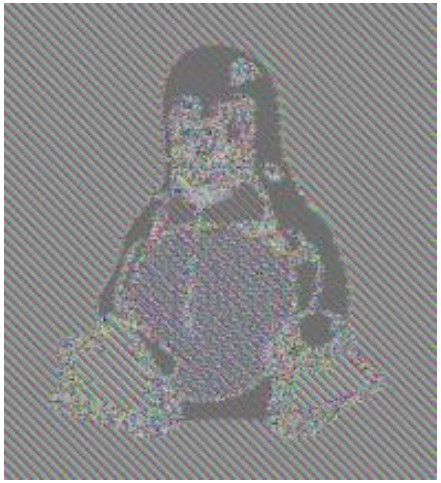
Database schema

Encrypted PAN (3DES-EDE-ECB)	Truncated PAN
52b62426fb218e20:077d02e0e7c0b9b1	910001xxxxxx9377
68319cffbd7a08a1:f3247ac60cb4124d	950021xxxxxx9370
17fed566f5578160:96e17f2a4fdb9569	910001xxxxxx3163
318de67deb17f32a:e8e1a9416342b185	930003xxxxxx6889
52b62426fb218e20:2141378868234976	910001xxxxxx2839
bbe72f0cd8a91665:72b8f67694727019	910001xxxxxx7626

Attacking ECB-mode 3DES PANs

- Attacking cards encrypted with 3DES-ECB
  - (3)DES uses 64bit blocks
  - 16 bytes fits in two blocks
  - 16 byte PAN get divided into two half's
  - Each half of the PAN are encrypted separately

95002171
615122c94fc0ae15



55078534
2991bcd9ff95dab3

Attacking ECB-mode 3DES PANs

Encrypted PAN (3DES-EDE-ECB)	TruncatedPAN
d08a47587775c53d:**76b7617a1def7f8a**	910001xxxxxx0107
76b7617a1def7f8a:e3846577160958 3a	910001xxxxxx3582

Attacking ECB-mode 3DES PANs

Encrypted PAN (3DES-EDE-ECB)	TruncatedPAN
d08a47587775c53d:**76b7617a1def7f8a**	910001xxxxxx**0107**
76b7617a1def7f8a:e3846571609583a	**910001**xxxxxx3582

910001**xx**91000107
91000107**xxxx**3582

Attacking ECB-mode 3DES PANs

910001 91000107

Protecting 3DES PANs

- Don't use electronic code book mode (ECB)
- Use cipher block chaining (CBC)
- Use a standard (PKCS #5)

- Use a cipher with a larger block size (AES)

Attacking RSA-encrypted PANs

CYBERCOM GROUP

```
9100016891000107
```

Attacking RSA-encrypted PANs

9100016891000107

000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000
000000000000**9100016891000107**

Attacking RSA-encrypted PANs

9100016891000107

```
EUNpuFS8ZdcbWFPjsAHuJt8wRr+8v6IFVaGrniuB0l6DQAYDRWIWjd/0X
HIPPh72+KnwCc1yaIWPDPthu+BLHboy48kCUTBnU0cGPjRmCSLsHB1Qrf
NAUxuMyj3YsnvSQe3kekA/GZSK7UBR2CwOIQNsBiS58oT470aKCj+XLuZ
h9zxod41INBzqUKt7v64TZnE6BB9zm3BQVwxvqj9BHWX3HPDrJ8lWJh7u
JVtBtv2wjhl040rwIRxuwh6Y0xYzx+5CVra3APXCG1vsVQxbCCnT1BTjC
FCtch1WddYZ7Iy2LFLpa+moCUb4drcDNSNTmAKM3oUsd5Oc5UwpceWDxQ
==
```

Attacking RSA-encrypted PANs

CYBERCOM GROUP

Database schema

Encrypted PAN (RSA 2048)	Truncated PAN
EUNpuFS8ZdcbWF...Oc5UwpceWDxQ==	910001xxxxxx0107
RqbTx9HpiJ/y4o...oltekI7NKWFg==	950021xxxxxx9370
jsbn2XovfX9TCE...rE0RBflW6c+g==	950020xxxxxx2538

Attacking RSA-encrypted PANs

CYBERCOM GROUP

Database schema

Encrypted PAN (RSA 2048)

```
EUNpuFS8ZdcbWF...Oc5UwpceWDxQ==
RqbTx9HpiJ/y4o...oltekI7NKWFg==
jsbn2XovfX9TCE...rE0RBflW6c+g==
```

Attacking RSA-encrypted PANs

CYBERCOM GROUP

- Proper padding is critical for RSA
  - RSA encryption is a deterministic encryption algorithm
  - RSA encryption without randomized padding is basically a glorified hashing algorithm
  - Properly formatted and randomized padding is referred to as armor
  - Armoring is not an optional feature, its an absolute requirement.

Attacking RSA-encrypted PANs

CYBERCOM GROUP

- Partial known plaintext attack
  - 13 to 19 digits
  - The first 6 digits are predictable (IIN/BIN)
  - Last digits is a checksum (luhn-10)

A brute force attack can be reduced from 16 unknown bytes to roughly 9 unknowns for each IIN attacked. The conclusion is that 10^9 (1 billion) RSA-encryption computations has do be done for each IIN

Protecting RSA-encrypted PANs

CYBERCOM GROUP

- Use a standard
  - PKCS #1

Where to encrypt?

Presentation (first layer)
It is responsible for communication with the client (browser) in a manner understandable by clients (HTTP).

Logical (second layer)

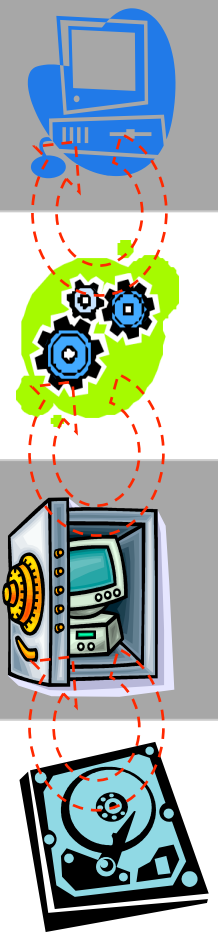
This layer takes commands from the user in tier one and makes logical decisions based on user requests.

Database (third layer)

Customer information is stored and retrieved from the database in a structured way (SQL).

Storage

The database needs a file system and a storage device to store its data. Data is available and addressed as files or raw disks.



Thanks!

- Torbjörn Lofterud
  - torbjorn.lofterud@cybercomgroup.com
  - +46-708-451818