Padding Oracle Attacks on CBC-mode Encryption with Secret and Random IVs

Arnold K. L. Yau

Kenneth G. Paterson

Chris J. Mitchell

22 Feb 2005

Royal Holloway University of London

Overview

- Introduction
  - ISO standards
  - CBC review
- Attacks on ISO padding methods
- Conclusions

Royal Holloway
University of London

ISO CBC-Mode Standard

- ISO/IEC 10116 standardises modes of operation for block ciphers including CBC mode
- New version of standard under development
- Earlier draft (2nd CD)
  - Refers to padding methods in ISO/IEC 9797-1 and ISO/IEC 10118-1
  - Padding oracle attacks paper by Paterson and Yau presented at CT-RSA 2004

ISO CBC-Mode Standard

- Final Committee Draft (FCD)
  - No padding method specified (due to CT-RSA 2004 paper)
    - Same methods assumed
  - Secret and random IVs recommended
- This paper
  - Attacks on FCD
  - New attack strategy or adaptation of old attacks
- Main findings: ISO padding methods are still weak in presence of padding oracle!

CBC-Mode Encryption

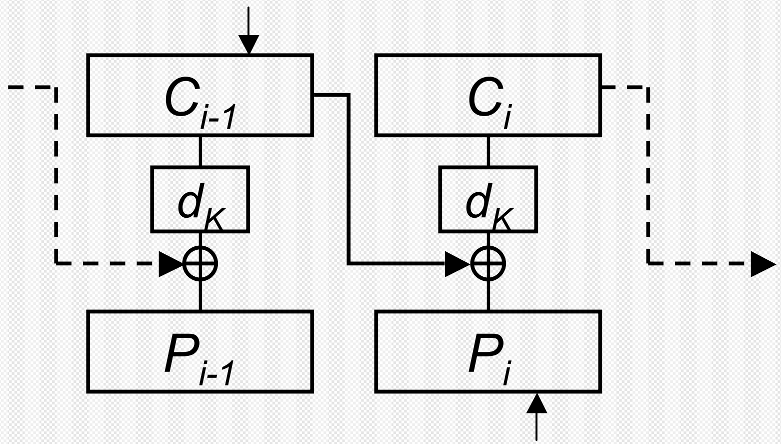
- Data D of length L_D
- Padded to P divided blocks $P_1, P_2, \ldots, P_q$
- Block size n, key K, IV ($= C_0$)
- Encryption/decryption defined by

$$C_i = e_K(P_i \oplus C_{i-1})$$

$$P_i = d_K(C_i) \oplus C_{i-1}$$

CBC-Mode Decryption

- Bit flipping
  - Flipping a bit in C_{i-1} causes the corresponding bit in P_i to flip as well



Royal Holloway University of London

Padding Oracles

- Decrypts in CBC-mode submitted ciphertexts under fixed key K
- Indicates whether padding of plaintext is VALID or INVALID
  - w.r.t. specific padding method
- Padding oracle attacks first proposed by Vaudenay (Eurocrypt 2002)
  - Practical implementation of attack on SSL/TLS by Canvel et al. (Crypto 2003)

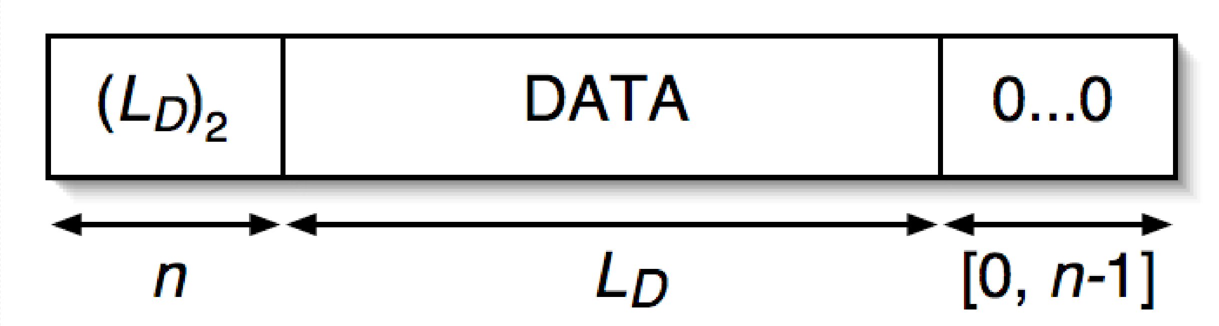
Royal Holloway University of London

Two Models of Secret IVs

- How to ensure both parties share the same IV?
- Model 1
  - ECB encryption or decryption of some *V*
  - Pre-shared list of value
  - Generalised as IV determining information *I* sent alongside ciphertext
- Model 2
  - No information sent
  - e.g. synchronised PRNG

ISO/IEC 9797-1 Attack Padding

- Method 3
  - Left-pad data with a block containing data length in binary, right-pad with as few ‘0’s as necessary to complete a block



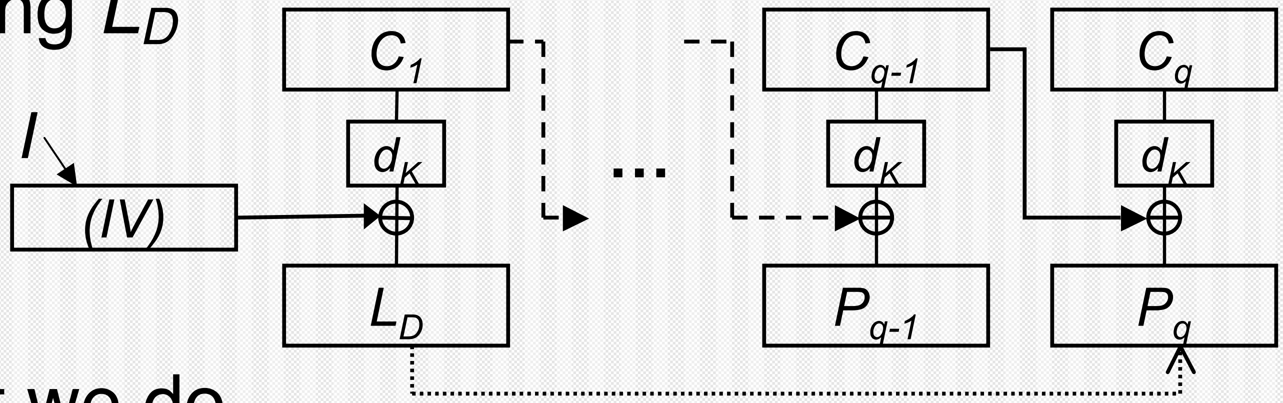
- Previous attack from CT-RSA 2004 fails
  - Requires IV manipulation

Attack Overview

- Attack in Model 1
- Target ciphertext $C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_q$
  - Target block C_k
- Auxiliary ciphertexts $C^1, C^2, \ldots, C^m$
  - IV determining info $I^1, I^2, \ldots, I^m$
- Phase 1: determines lengths of plaintexts corresponding to auxiliary ciphertexts
- Phase 2: decrypts C_k in segments using length info from Phase 1

ISO/IEC 9797-1 Attack - Phase 1

- Finding L_D



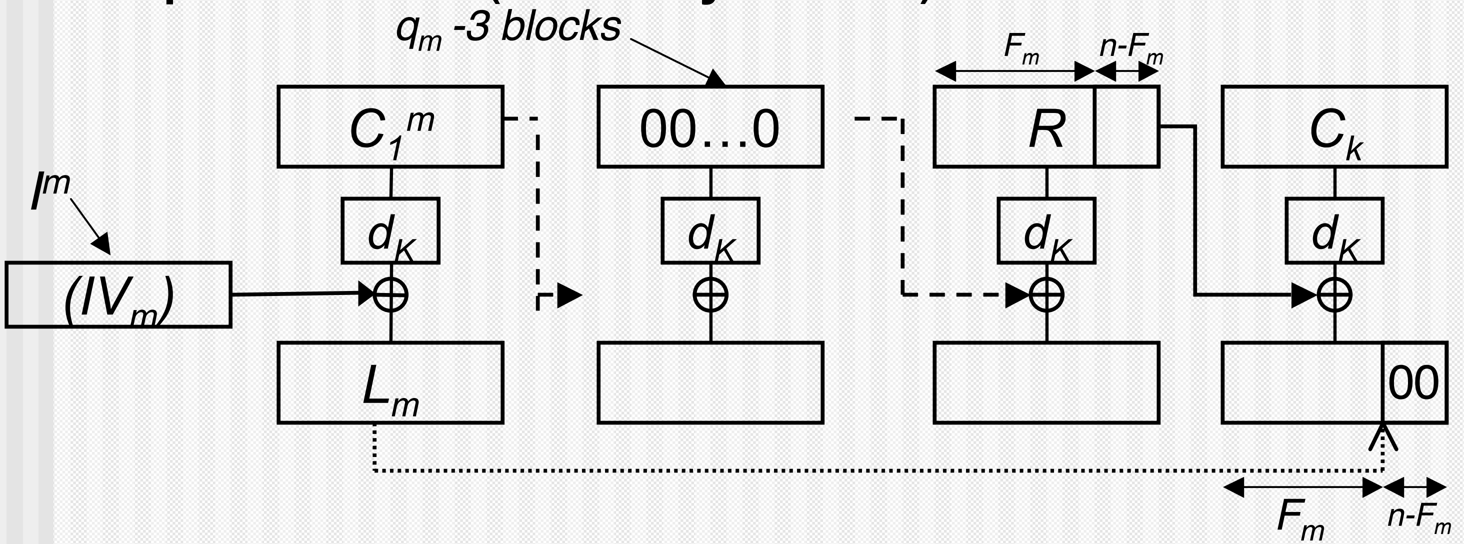
- What we do
  - Flip a bit in block C_{q-1}, submit to oracle
  - VALID means boundary to right
  - INVALID means boundary to left
  - Hence find L_D using binary search
    - $\log_2 n$ oracle queries

ISO/IEC 9797-1 Attack - Phase 1

- Apply this to auxiliary ciphertexts $C^1, C^2, \ldots, C^m$ to find lengths
  - Lengths $L_1, L_2, \ldots, L_m$
  - Lengths mod n: $1 \le F_1 < F_2 < \ldots < F_m \le n-1$

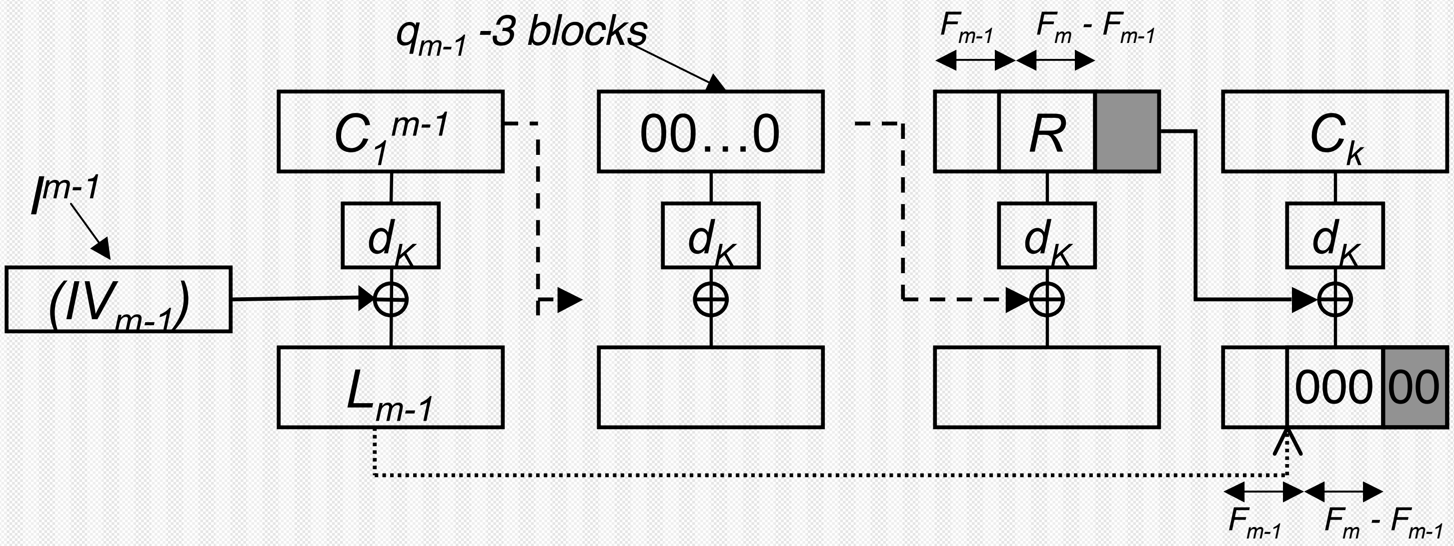
ISO/IEC 9797-1 Attack - Phase 2

- Now attempt to decrypt ciphertext block C_k from target ciphertext
- Try all values of R in rightmost $n - F_m$ positions
- VALID implies bits are all ‘0’s in corresponding positions (exactly once)



ISO/IEC 9797-1 Attack - Phase 2

- Fix R at these positions, continue with C_{m-1} and so on



ISO/IEC 9797-1 Attack - Phase 2

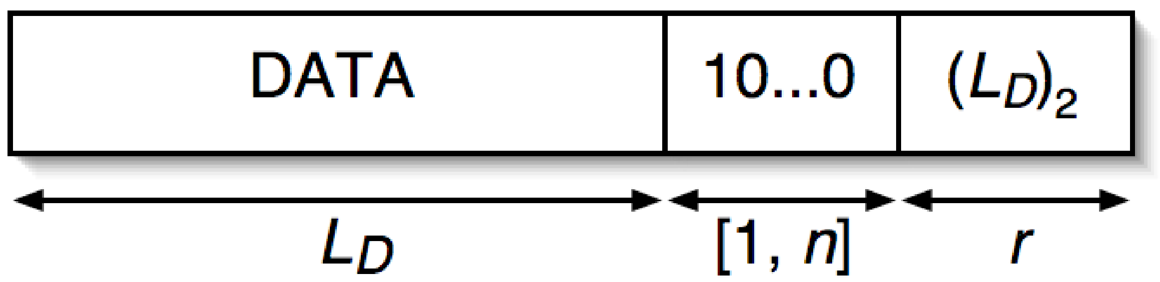
- Rightmost n-F_1 bits of P_k equals final value of $R \oplus C_{k-1}$
- Average complexity $\sum_{j=1}^{m} 2^{F_{j+1}-F_j-1}$
  - Depends on spread of auxiliary ciphertext lengths
  - Byte oriented data, n=64, lengths mod n = 8,16,..,56
    - about 900 queries to extract 56 out of 64 bits

ISO/IEC 9797-1 Attack Summary

- Limitations
  - Attack does not extract leftmost $F_1 \geq 1$ bits of plaintext
  - Auxiliary ciphertexts have to be at least 3 blocks in length
- Secret and random IV recommendation in ISO/IEC 10116 FCD does not enhance security greatly against padding oracle attacks

ISO/IEC 10118-1 Padding

- Method 3
  - Choose parameter $r \leq$ n
  - Encode L_D in r bits (base 2 assumed)
  - Right-pad a single ‘1’ bit, followed by as few ‘0’s as possible to push the encoded L_D to the end of a block



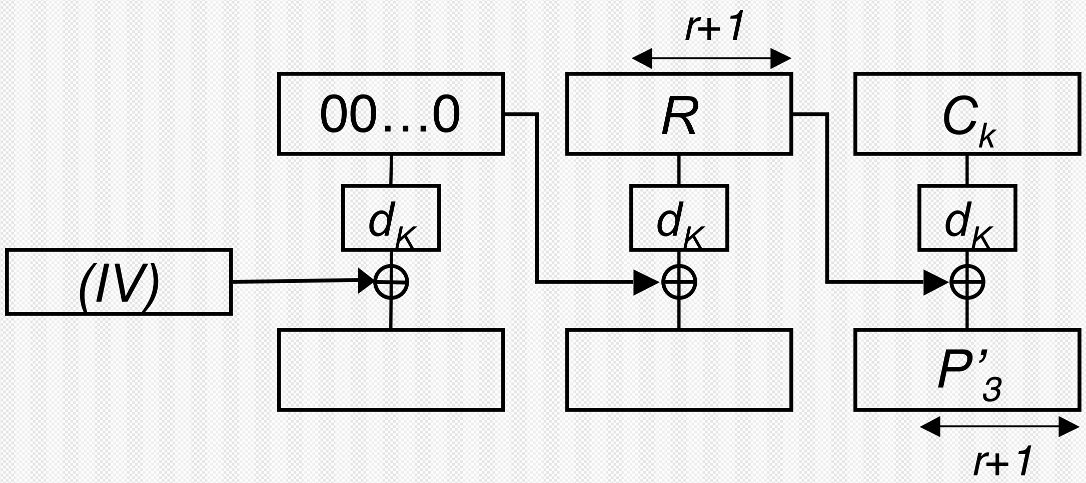
ISO/IEC 10118-1 Attack Overview

- Attacks in (tougher) Model 2
  - Adaptations of CT-RSA 2004 attacks
- First attack: targets arbitrary ciphertext block C_k
  - Construct a valid 3 or 4 block ciphertext having C_k as final block
- Second attack: efficiently decrypts last block of any ciphertext
  - Firstly determines L_D efficiently
  - Secondly decrypts remaining bits in last block efficiently
  - Similar to L_D -finding attack on ISO/IEC 9797-1
  - Details in the paper

Royal Holloway University of London

ISO/IEC 10118-1 First Attack

- Case $r < n$, we construct and submit 3 block ciphertexts
- Go through all settings of rightmost $r+1$ bits of R until oracle returns VALID



Royal Holloway University of London

ISO/IEC 10118-1 First Attack

- Average case complexity of first attack
  - case $r < n$: 2^{r-1} oracle queries
  - case $r = n$: 2^{r} oracle queries
- Second attack determines plaintext efficiently
- Recovers all n bits of a block (except for first block) many orders faster than exhaustive key search in most cases
- Secret and random IV restrictions do not hinder attack significantly

Conclusions (1)

- Secret and random IVs do not prevent padding oracle attacks
- FCD of standard does not specify any padding methods
  - Dangerous if implementer chooses unsafe methods
- OZ-PAD 10…0 also specified in both ISO/IEC 9797-1 and 10118-1
  - Appears to resist padding oracle attacks
  - We recommend use of OZ-PAD
  - Now adopted in latest version of ISO/IEC 10116 (FDIS)

Royal Holloway University of London

Conclusions (2)

- Attacks easily prevented by proper use of strong integrity checks when appropriate
  - Feasibility - constrained in memory or processing power
  - Careful choice of padding method when MAC is not used