Cryptanalysis of White-Box DES Implementations

Brecht Wyseur

COSIC – K.U.Leuven (Belgium)
Paris, March 2007
Orientation

White-Box Attack Context

• Fully privileged attack software shares host
  => Complete access to the implementation of algorithms
• Dynamic execution can be observed
• Internal details both completely visible and alterable at will

Attacker's objective: extract the embedded cryptographic key
Outline

- State-of-the-art
- White-box DES implementations
- Cryptanalysis
- Demo
- Results and Conclusions
State-of-the-art

WB DES
Chow et al. 2002

Naked variant
Fault injection attack
Jacob et al. 2002
Statistical attack
Neumann et al. 2004
Improved variant

Encoded variant

WB AES
Chow et al. 2002

Cryptanalysis
Billet et al. 2005

Cryptanalysis
Goubin et al. 2007

Cryptanalysis
Wyseur et al. 2007
DES (Data Encryption Standard)

Overview
- Feistel structure
- 16 rounds
- Per round:
  - Expansion
  - RoundKey addition
  - 8 S-boxes
  - Permutation
White-box transformation
White-box transformations

- **T-boxes**
  - 8 T-boxes with internal S-box
  - 4 Linear T-boxes (by-pass T-boxes)
White-box transformations

- Internal encodings
White-box transformations

External encodings

- Protection against implementation extraction
- Protection against first and last round attacks

“Encoded variant”
White-box transformation
Cryptanalysis

Input encoding

Round 1

Round 2

Round 3

Round 4

Round 16

Output encoding

Input

12 byte state

12 byte state

12 byte state

12 byte state

Output

Difference propagation

Difference knowledge

S-box input recovery

S-box identification

Key recovery
Cryptanalysis

Detect single R-bit flips

- Change the input to a T-box in round 1
- Observe difference propagation at the input of round 3

Observe: 2 different T-boxes affected
Cryptanalysis

Distinguish X-bit flips and Restricted bit flips
Cryptanalysis

Finding single bit flips

Permutation-Expansion design:

<table>
<thead>
<tr>
<th>S-box</th>
<th>Inputs</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>Ex</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>6</td>
<td>8</td>
<td>3</td>
<td>7</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>7</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>4</td>
<td>8</td>
<td>7</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
### Cryptanalysis

#### Overview

<table>
<thead>
<tr>
<th>ROUND</th>
<th>INFORMATION</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Restricted bit flips</td>
<td>Restricted bit flips</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Middle bit flips, T-box type</td>
<td>Middle bit flips, T-box type</td>
</tr>
<tr>
<td>4</td>
<td>Single bit flips, T-box type</td>
<td>Single bit flips, T-box type</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cryptanalysis

Obtaining the inputs to the S-boxes

Knowledge:
- Single bit flips
- Middle bit flips
- T-box types

Idea:
- Guess S-box
- Guess Input
- Test differences
Cryptanalysis

Key recovery

- Via expansion function
- 3 round approach

Result: 2 complementary keys (DES complementation property)
Demo

- Demo
Conclusion

• Result
  − An efficient tool to extract the secret key from a white-box DES implementation
  − Time complexity: $2^{14}$!

• Conclusion
  − Components and design choices that make DES “strong” in a black-box environment, make it weak in a black-box environment
  − Extending the idea to general 're-trust' white-box implementations (diffusion property etc.)
Uh oh!