White-Box Cryptography

Brecht Wyseur

K.U.Leuven - COSIC
brecht.wyseur@esat.kuleuven.be

Re-TRUST quarterly meeting
Trento, December 2006

Attack Context

- Black Box - Pure external information
  - Conventional model
  - Linear, differential cryptanalysis
- Grey Box - Side channel information
  - Time analysis
  - Power analysis
  - Electromagnetic analysis
- White Box - Internal behaviour

Attack Context

- Black Box - Pure external information
  - Conventional model
  - Linear, differential cryptanalysis
- Grey Box - Side channel information
  - Time analysis
  - Power analysis
  - Electromagnetic analysis
- White Box - Internal behaviour

Attack Context

- Black Box - Pure external information
  - Conventional model
  - Linear, differential cryptanalysis
- Grey Box - Side channel information
  - Time analysis
  - Power analysis
  - Electromagnetic analysis
- White Box - Internal behaviour

The White-Box Attack Context

Definition

- Fully-privileged attack software shares host
  $\Rightarrow$ Complete access to the implementation of algorithms
- Dynamic execution can be observed
- Internal details both completely visible and alterable at will.

Attacker's objective is to extract the embedded cryptographic key.

[Chow *et* al., SAC'02]

Problem statement - Attacks

- Entropy attack

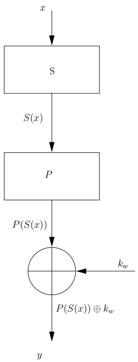
Use of randomness property of keys: good keys have more entropy than the surrounding code and are thus identifiable.

- Post-compilation information leaks
  - Traces of Object Oriented code
  - Function names
- Code section theft or replacement

Key whitening attack

"A Cautionary Note on Weak Implementations of Block Ciphers", T. Kerins and K. Kursawe, WISSec 2006.

- An easy way to mount an attack on software binaries of block ciphers.
- Attack target: SPN block ciphers with a *key whitening* and static S-boxes
- Identify and overwrite S-boxes in static binary.
- $y = (P(0) = 0) \oplus k_w$

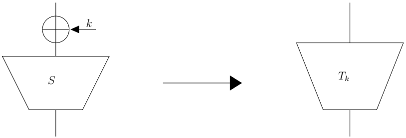


White-Box Cryptography

- Goal: Prevent extraction of key information
- Main Idea
  How to make it as difficult as possible for an attack to extract any key information?
  - Transform into a network of key dependant lookup tables
  - Randomised behaviour of all network nodes.
  - Extend the cryptographic border

Techniques - Partial Evaluation

Replace the standard S-Boxes with key-specific S-Boxes
$T^r_{i,j}(x) = S(x \oplus k^{r-1}_{i,j})$



- Protection against Kerins *et* al. attack
- Provides no real security, but is a necessary building block

Techniques - Encodings

External encodings

Shielding of the white-box implementation by embedding it within random bijections $F, G : GF(2^n) \rightarrow GF(2^n)$.

$$X' = G \circ X \circ F^{-1}$$

Internal encodings

Injections of random bijections in order to randomize the data flow between consecutive lookup tables.

$$L_2 \circ L_1 \Rightarrow (L_2 \circ F^{-1}) \circ (F \circ L_1)$$

$\Rightarrow$ Notion of local security

Techniques - Encodings

External encodings

Shielding of the white-box implementation by embedding it within random bijections $F, G : GF(2^n) \rightarrow GF(2^n)$.

$$X' = G \circ X \circ F^{-1}$$

Internal encodings

Injections of random bijections in order to randomize the data flow between consecutive lookup tables.

$$L_2 \circ L_1 \Rightarrow (L_2 \circ F^{-1}) \circ (F \circ L_1)$$

$\Rightarrow$ Notion of local security

Security

Local security

$$L \Rightarrow E(L) = G \circ L \circ F^{-1}$$

Encrypted L is provable secure

Problem: partial / global security

Metrics

- White-box diversity
- White-box ambiguity

State of the art

- Data Encryption Standard (DES)
  - Presented by Chow *et* al. 2002
  - Improved by Link *et* al., Wyseur *et* al.
  - Cryptanalysis of naked version by Jacob *et* al.
    → Fault injection attack
  - Implementation size: 728 kB
- Advanced Encryption Standard (AES)
  - Presented by Chow *et* al.
    → Implementation size: 752 kB (instead of 4.25 kB for the original black box implementation)
  - Cryptanalysed by Billet *et* al.
    → Algebraïc extension of square attack
  - A new attempt by Bringer *et* al., 2006 → 142 MB ...

Related Research Topics

- Code obfuscation
- Encrypted functions
  $y = E(f)(x)$
  - Homomorphic functions
  - Encrypted code execution
- Encrypted data processing $E(y) = f'(E(x))$
- Observable cryptography
- Traitor tracing

ReTRUST WBC interest

- Protection of keys embedded into software running on the untrusted host;
- Research to use hardware to assist into further improved security;
- Use of white-box techniques to strenghten code obfuscation and the 're-trust protocol';
- Replacement of white-box code

Future directions

- Research for improved white-box techniques
- Implementation and proof of concept
- Re-TRUST applicability

SNIP

WBC is **NOT** an alternative to the Re-TRUST approach, but only a building block.