Timing attack against a DES implementation

Alessandro Menduni

April 23, 2015

1 Introduction

A timing attack is a side channel attack, which consists in exploiting information given by the time taken by the hardware to execute a cryptographic alghoritm. In particular, it is taken into account the dependancy between the input provided to the system and the time required to complete the operation, thus, by the use of precise measurements, an attacker can procede backwards from the output to the input. In this report it will be considered the attack against a poor implementation of the P permutation of the DES library.

2 The attack target: the P permutation

As stated in the introduction, the main target of the attack will be the implementation of the P permutation that is performed on the output of the SBoxes; this stage of the algorithm is implemented in such a way that it makes it feasible to exploit time measurements to deduce the input key of the 16th round of the DES; in fact, as we can see in the snippet below, the time needed by the hardware to perform the permutation depends on the number of bits set to 1, since it procedes bit by bit and, everytime it encounters a bit to 0 in the input string, it skips all the loops and it copies directly such bit to the result string.

```
// Permutation table. Input bit #16 is output bit #1 and
// input bit #25 is output bit #32.
p_table = {16, 7, 20, 21,
          29, 12, 28, 17,
           1, 15, 23, 26,
           5, 18, 31, 10,
           2,  8, 24, 14,
          32, 27, 3,  9,
          19, 13, 30, 6,
          22, 11, 4, 25};

p_permutation(val) {
  res = 0;                  // Initialize the result to all zeros
  for i in 1 to 32 {        // For all input bits #i (32 of them)
    if get_bit(i, val) == 1 // If input bit #i is set
      for j in 1 to 32      // For all 32 output bits #j (32 of them)
   if p_table[j] == i  // If output bits #j is input bit #i
         k = j;             // Remember output bit index
       endif
      endfor                // output bit #k is now input bit #i
      set_bit(k, res);      // Set bit #k of result
    endif
  endfor
  return res;               // Return result
}
```

3 What's the Brundtland Report?

The Brundtland report is actually officially called "Our Common Future", the document was the result of 900 days of interactions between international exponents from the scientific world, experts, research institutes, non-governmental organizations, senior government representatives and everything was held at public hearings throughout the whole world. The main objectives of the Commission were: study and reconsider critical issues and formulate innovative and concrete proposals to deal with them; ensure and enforce international cooperation on the matter and actively push towards a much needed change in current collaboration policies; raise awareness and understanding in both individuals, organizations and governments, so that it could be possible to work together in order to achieve the expected results. In fact it was plain and evident that such a big issue could be faced and solved only with the participation of every party involved in a phenomenon that stretches from energy problems to loss of species and genetic resources, from industry in general to human settlements.

4 A vague definition

Criticisms have been received by this report, especially for its vague way of expressing concepts; in fact, it has been argued that the famous definition of sustainable development given in that instance is better a slogan than it is a basis for theory and has resulted in lots of parties using such term for attempting to capturing attention of the public without actually knowing or considering the complexity of the whole debate. On one hand, environmentalists use it to put the accent on considering environmental issues while planning, without treating explicitly political economy; on the other hand, politicians and theorists have started hiding themselves behind the concept sustainable development to gather consent suggesting radical reform, forgetting to specify what needs to change or expressing specific viable courses of action. In summary, the indefinite definition results in a vague concept meaning different things to different people. Several definitions have been given by other parties, like:

> *"the expansion of the substantive freedoms of people today while making reasonable efforts to avoid seriously compromising those of future generations" (UNDP, 2011, p.18)*

which didn't actually solve the problem because it is difficult to interpret equally what "reasonable efforts" are. Anyways, the concept it's so broad and wide that it's unlikely that a good and short denotation of it could be formed without using words that make it sound more like a principle that a guideline.