Attacks on RSA

Cryptography and Protocols

Andrei Bulatov

Attacks on `Textbook' RSA

- Short message – small key attack
- Small key – several copies
- Quadratic improvement
- Common modulus
- Dependency between plaintexts

Practical Schemes

- PKCS #1 : Public Key Cryptography Standard RSA Cryptography Standard
- **Encryption**:

  P – plaintext, $seed$ – a random seed, PS – a string of zeroes,

  MGF – a pseudorandom function (Mask Generation Function)

  set $DB := PS \parallel 01 \parallel P$

  set $maskedDB := DB \oplus MGF(seed)$

  set $maskedseed := seed \oplus MGF(maskedDB)$

  set $EM := 00 \parallel maskedseed \parallel maskedDB$

  set $C := RSA(EM)$

Practical Schemes (cntd)

- **Decryption**:

  set $EM := RSA^{-1}(C)$

  set $00 \parallel maskedseed \parallel maskedDB := EM$

  set $seed := maskedsed \oplus MGF(maskedDB)$

  set $DB := maskedDB \oplus MGF(seed)$

  set $PS \parallel 01 \parallel P := DB$

An Attack on PKCS#1

- We use two facts:
  - the message being encrypted always starts with 00
  - in many implementations there is a check for that, and if the decrypted message does not satisfy this condition, a specific error message `not PKCS conforming' is issued.

- Suppose Alice uses RSA with keys n of length k, e and d, the message encrypted is m, and the ciphertext is $c = m^e \pmod n$
- We use a simple mathematical fact $(m \cdot s)^e \equiv c \cdot s^e \pmod n$
- The main tool of the attack is a query to Bob (oracle) whether or not for a chosen s, $(c \cdot s^e)^d$, that is $m \cdot s$, is PKCS conforming. In other words, if $m \cdot s \leq 2^{k-8}$

An Attack on PKCS#1 (cntd)

- Set $B = 2^{k-8}$
- **Bit 1.**

  Try $s = 2,4,8, \ldots, 2^i$ until the oracle returns $\geq$ B on $c \cdot s^e$.

  For such s set $s_1 = \frac{s}{2}$

  Then we know that $\frac{B}{2} \leq s_1 \cdot m < B$, or $\frac{B}{2s_1} \leq m < \frac{B}{s_1}$

- **Bit 2**.

  Thus we have found the first significant bit of m.

  To find the second bit we should distinguish two cases:

  $\frac{B}{2s_1} \leq m < \frac{B+B/2}{2s_1}$ and $\frac{B+B/2}{2s_1} \leq m < \frac{B}{2s_1}$

An Attack on PKCS#1 (cntd)

- To do that we query the oracle about $c \cdot \left(\frac{2}{3} \cdot 2s_1\right)^e$
- If $\frac{B}{2s_1} \leq m < \frac{B+B/2}{2s_1}$ then $\frac{2}{3}B \leq \frac{2}{3} \cdot 2s_1 \cdot m < B$
- If $\frac{B+B/2}{2s_1} \leq m < \frac{B}{2s_1}$ then $B \leq \frac{2}{3}s_1 \cdot m < \frac{4}{3}B$
- In a similar way find the remaining bits of m
- For real protocol requires from 2^{16} to 2^{20} oracle queries.

Fix

- Include integrity check!!!
- Do not give away information (see also version-rollback attacks)
- Include timestamp (not good, actually)
- Mask actual processing time (especially if integrity check is performed) to prevent timing attacks