On the Importance of Checking Cryptographic Protocols for Faults

Toon Nolten

Outline

- Hardware Faults
- RSA Signatures
- Fiat-Shamir Identification Scheme
- Defending Against Fault Based Attacks
- Summary

Hardware Faults

- *Transient faults*
- Latent faults
- Induced faults
- *Register faults*

RSA Signatures

- $N = pq$, p and q large primes
- $x^s \bmod N$, where s is a secret exponent
- x in range 1 to N, usually after hashing
- Security relies on the fact that factoring N is hard

Computation of Exponentiation

- Expensive part of computation is modular exponentiation
- Calculate $E_1 = x^s \bmod p$ and $E_2 = x^s \bmod q$ by repeated squaring
- $E = x^s \bmod N$ can be computed using the Chinese remainder theorem
- More efficient than repeated squaring modulo N because the numbers involved are smaller

E by CRT

- a, b precomputed integers s.t.:
$$\begin{cases} a & \equiv 1 \pmod{p} \\ a & \equiv 0 \pmod{q} \end{cases} \text{and} \begin{cases} b & \equiv 0 \pmod{p} \\ b & \equiv 1 \pmod{q} \end{cases}$$
- Such integers always exist
- $E = aE_1 + bE_2 \pmod{N}$

RSA's Vulnerability

- $E = M^s \bmod N$, correct signature
- $\hat{E}$, faulty signature
- Suppose: $\hat{E} = a\hat{E}_1 + bE_2 \pmod{N}$
- Observe: $E - \hat{E} = a(E_1 - \hat{E}_1)$
- If $E_1 - \hat{E}_1$ is not divisible by p then:
  $gcd(E - \hat{E}, N) = gcd(a(E_1 - \hat{E}_1), N) = q$

Fiat-Shamir Identification Scheme

- Efficient method whereby Alice can authenticate her identity to Bob
- Both parties agree on an n-bit modulus N which is a product of two large primes and a security parameter t
- Secret key: $s_1, \ldots, s_t \bmod N$
- Public key: $v_1 = s_1^2, \ldots, v_t = s_t^2 \pmod{N}$

Fiat-Shamir Protocol

1. Alice picks a random $r \in \mathbb{Z}_N^*$ and sends r^2 to Bob.
2. Bob picks a random subset $S \subseteq \{1, \ldots, t\}$ and sends the subset to Alice.
3. Alice computes $y = r \cdot \prod_{i \in S} s_i \bmod N$ and sends y to Bob.
4. Bob verifies Alice's identity by checking that $y^2 = r^2 \cdot \prod_{i \in S} v_i \pmod{N}$.

Fiat-Shamir Identification Scheme

- Attack based on register faults that occur while Alice is waiting for a challenge
- Given t faulty runs $s_1, \ldots, s_t$ can be recovered in the time it takes to perform $\mathcal{O}(nt + t^2)$ modular multiplications

Fiat-Shamir Vulnerability

- Suppose one bit of r is flipped while waiting for S, $E = \pm 2^i$, Bob receives correct value $r^2 \bmod N$ but y is computed incorrectly
$$\hat{y} = (r + E) \cdot \prod_{i \in S} s_i$$
- Bob knows $\prod_{i \in S} v_i$ and can compute
$$(r + E)^2 = \frac{\hat{y}^2}{\prod_{i \in S} v_i} \pmod{N}$$
- Bob can guess the n possible values of E and recover r from
$$(r + E)^2 - r^2 = 2E \cdot r + E^2 \pmod{N}$$

Fiat-Shamir Vulnerability

- Using r and E Bob can compute
$$\prod_{i \in S} s_i = \frac{\hat{y}}{r + E} \pmod{N}$$
- To find $s_1, \ldots, s_t$ Bob constructs suitable sets S, singleton sets or sets that result in a set of equations for the s_i

Defending Against Fault Based Attacks

- Verify the output of a computation
- Protect internal state across rounds using CRC
- Random padding of the message to be signed

Summary

- Signature schemes using CRT, e.g. RSA and Rabin, are especially vulnerable
- Other implementations of RSA signatures are also vulnerable but require many more faults
- Identification schemes are vulnerable as well, e.g. Fiat-Shamir, Schnorr and Guillou-Quisquater
- Verifying the computation and using error detection bits for the internal state are necessary for *security reasons*

References

Dan Boneh, Richard A. DeMillo, Richard J. Lipton:
On the Importance of Checking Cryptographic Protocols for Faults
(Extended Abstract). EUROCRYPT 1997: 37-51