Title: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1

Author: Daniel Bleichenbacher

Conference: Crypto '98

**Background:**

The Bleichenbacher attack, named after its discoverer Daniel Bleichenbacher in 1998, is a cryptographic attack primarily targeting implementations of the RSA cryptosystem that rely on PKCS #1 v1.5 padding. This attack is a form of adaptive chosen ciphertext attack (CCA) that exploits vulnerabilities in the padding scheme to decrypt ciphertexts and ultimately recover the RSA private key.

**Bleichenbacher's Attack and Its Foundation**

Daniel Bleichenbacher first described the attack in 1998. He demonstrated that an adversary could exploit differences in error messages generated by decryption oracles to extract information about the plaintext. By sending specially crafted ciphertexts and analyzing the responses from the decryption oracle, an attacker could iteratively deduce the private key and ultimately decrypt the encrypted messages.

In 2002, Serge Vaudenay built upon Bleichenbacher's work and introduced a refinement to the attack in his paper titled "Security Flaws Induced by CBC Padding—Applications to SSL, IPSEC, WTLS...". Vaudenay's contribution extended the Bleichenbacher attack to cipher block chaining (CBC) mode padding, expanding the potential attack surface to a broader range of cryptographic protocols beyond RSA.

**Bleichenbacher Attack Evolution Over the Past 20 Years:**

Initial Discovery (Late 1990s): Daniel Bleichenbacher first described the attack in a paper titled "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1" in 1998. The attack exploited subtle differences in error messages returned by RSA decryption oracle when processing improperly padded ciphertexts.

**Practical Exploitation (2000s):** The Bleichenbacher attack gained practical relevance as researchers demonstrated its effectiveness against real-world implementations. Notably, the attack was successfully applied to break SSL/TLS implementations that used RSA encryption with PKCS #1 v1.5 padding, leading to significant security vulnerabilities such as the famous "ROBOT" attack discovered in 2017.

**Refinements and Variants**: Over the years, researchers have developed various refinements and variants of the Bleichenbacher attack, enhancing its efficiency and applicability to different scenarios. These include adaptations for specific encryption schemes, improvements in oracle querying strategies, and optimizations to reduce the number of required ciphertext queries.

**Standardization Efforts (2010s):** The threat posed by the Bleichenbacher attack prompted standardization bodies like the Internet Engineering Task Force (IETF) to revise cryptographic standards. Notably, the RSA PKCS #1 v1.5 padding scheme has been deprecated in favor of more secure alternatives, such as RSA OAEP (Optimal Asymmetric Encryption Padding), which is resistant to Bleichenbacher-type attacks.

**Continued Relevance (Present):** Despite efforts to mitigate its impact through standardization and adoption of more secure padding schemes, the Bleichenbacher attack remains relevant. Vulnerable implementations, legacy systems, and occasional misconfigurations continue to expose systems to this attack vector. Moreover, advancements in cryptanalysis and side-channel attacks may lead to further refinements of the original attack technique.

Bleichenbacher's paper presents a critical vulnerability in RSA-based cryptographic systems utilizing the PKCS #1 v1.5 padding scheme. The attack detailed in the paper demonstrates how adversaries can exploit discrepancies in the error messages produced during RSA decryption to recover plaintext information. By iteratively querying a decryption oracle with carefully crafted ciphertexts, attackers can gradually deduce the plaintext, ultimately compromising the security of RSA-encrypted messages. The paper's findings have profound implications for the security of cryptographic protocols relying on RSA encryption and underscore the importance of robust padding schemes in mitigating chosen ciphertext attacks.

**Technical Analysis:**

1. RSA Encryption and PKCS #1 v1.5 Padding:

- RSA encryption involves exponentiating the plaintext message with the recipient's public key modulus (N) and public exponent (e), yielding the ciphertext.

- PKCS #1 v1.5 padding is applied to the plaintext before encryption, ensuring proper formatting and randomness. The padding consists of fixed bytes followed by random padding, ensuring uniqueness and integrity of the message.

2. Oracle-Based Attack:

- The attack leverages an oracle that provides different error responses based on the validity of the padding in the decrypted ciphertext.

- By submitting carefully crafted ciphertexts to the oracle and observing its responses, attackers can deduce information about the decrypted plaintext.

3. Mathematical Principles:

- The attack exploits subtle variations in the decryption behavior of incorrectly padded ciphertexts.

- Through a series of adaptive chosen ciphertext queries, the attacker can infer information about the plaintext based on the oracle's responses.

- By iteratively refining their knowledge of the plaintext, attackers can ultimately recover the entire message.

4. RSA Decryption and Error Messages:

- During RSA decryption, the presence of incorrect padding can result in different error messages from the decryption oracle.

- These error messages leak information about the decrypted plaintext, allowing attackers to infer details about its structure and content.

- By analyzing the oracle's responses to carefully crafted ciphertexts, attackers can iteratively narrow down the possible plaintext values until successful decryption is achieved.

The "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1" paper, published by Daniel Bleichenbacher in 1998, describes a chosen-ciphertext attack against the PKCS #1 v1.5 padding scheme used in the RSA encryption standard. This attack can lead to the complete recovery of the plaintext message from a given ciphertext without knowing the private key.

The attack is based on the fact that the PKCS #1 v1.5 padding scheme has a predictable structure, and the way errors are handled in the decryption process can leak information about the plaintext.

Here's how the attack works:

1. PKCS #1 v1.5 Padding Scheme:

- The plaintext message is padded with a specific pattern before encryption.

- The padding consists of a leading byte 0x00, followed by a non-zero random byte 0x02, and then a sequence of non-zero random bytes 0x03, ..., 0x03 (with at least 8 bytes of 0x03), and finally the plaintext message.

2. Attack Setup:

- The attacker chooses a ciphertext C and sends it to the decryption oracle (the system that decrypts the ciphertext and returns either the plaintext or an error message).

- The decryption oracle decrypts the ciphertext C using the private key, checks the padding structure, and responds with either the plaintext or an error message indicating an invalid padding.

3. Blinding the Ciphertext:

- The attacker blinds the ciphertext C by raising it to a random value ‘r’ (modulo the RSA modulus ‘n’), resulting in a new ciphertext C'.

- The attacker sends the blinded ciphertext C' to the decryption oracle.

4. Observing the Oracle's Response:

- If the decryption oracle returns an error message, the attacker knows that the padding structure is invalid.

- If the decryption oracle returns the plaintext, the attacker knows that the padding structure is valid.

5. Iterative Approach:

- The attacker iterates through different values of the leading bytes of the padded plaintext, modifying the blinded ciphertext C' accordingly.

- For each modification, the attacker sends the modified ciphertext to the decryption oracle and observes the response.

- By analyzing the responses, the attacker can deduce information about the leading bytes of the padded plaintext.

6. Mathematical Analysis:

- The attack exploits the mathematical properties of the RSA encryption scheme and the structure of the PKCS #1 v1.5 padding.

- The attacker uses the blinding factor r and its multiplicative inverse r^-1 (modulo n) to unblind the ciphertext and recover the original plaintext.

- The analysis involves modular arithmetic operations and the properties of the RSA encryption function.

The attack proceeds iteratively, gradually revealing more information about the padded plaintext until the complete plaintext is recovered.

The mathematical details of the attack involve modular arithmetic operations, the properties of the RSA encryption function, and the analysis of the padding structure. The attacker exploits the fact that the decryption oracle leaks information about the padding structure through its error messages, allowing the attacker to iteratively recover the plaintext.

It's important to note that the PKCS #1 v1.5 padding scheme has been superseded by more secure padding schemes, such as OAEP (Optimal Asymmetric Encryption Padding), to mitigate this attack and provide better security guarantees.

**Conclusion:**

Bleichenbacher's attack paper exposes a critical vulnerability in RSA-based cryptographic systems relying on PKCS #1 v1.5 padding. Through a meticulous technical analysis, the paper elucidates the mathematical principles and processes underlying the chosen ciphertext attack, highlighting the exploitation of side-channel information leakage during RSA decryption. The findings underscore the importance of robust padding schemes and secure cryptographic implementations in mitigating chosen ciphertext attacks and preserving the security of RSA-based protocols.

**References:**

Bleichenbacher, Daniel. "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1." Advances in Cryptology—CRYPTO '98. Springer, Berlin, Heidelberg, 1998.

Duong, Thai, and Juliano Rizzo. "Here come the ⊕ ninjas." Black Hat USA 2011.

Bleichenbacher, Daniel. "Bleichenbacher's Attack Strikes Again: Breaking PKCS# 1 v1. 5 in XML Encryption." Cryptology ePrint Archive, Report 2003/052, 2003.

Klima, V., Pokorny, O., & Rosa, T. "Practical padding oracle attacks." Journal of Cryptology, 21(2), 280-289, 2008.

Hanno Böck et al. "Return Of Bleichenbacher's Oracle Threat (ROBOT)." 2017. <https://robotattack.org/>