Security And Forensics Lab

15th October 2024

Assignment - 8

Note: This assignment has to be done by a group of two students.

Objective: Implement a secure file transfer protocol using AES for encryption and Elliptic Curve Digital Signature Algorithm (ECDSA) for signing. Demonstrate tampering detection using ECDSA signatures and a brute force attack on a weak AES key to show/justify the importance of strong key policies. Find the details of the tasks below:

1. Implement a secure file transfer system that uses AES in CBC mode with a 128-bit key for file encryption, ensuring secure transmission between clients and the server.
2. Generate an ECDSA key pair (private and public) and sign the encrypted file with the sender's private key. Send the signed file along with the public key for signature verification.
3. At the receiver's end, verify the authenticity and integrity of the received file using the sender's public key to validate the ECDSA signature.
4. Simulate a tampering attack by modifying the file during transmission. Implement mechanisms to detect tampering through ECDSA signature verification.
5. Conduct a brute-force attack on files encrypted with a weak AES key (e.g., a reduced 16-bit key) to demonstrate the ease of cracking weak encryption. Report the results of this attack.
6. Recommend stronger key policies to prevent such attacks. Discuss the importance of using strong AES keys (128-bit, 192-bit, or 256-bit). Explain how strong key policies enhance security.

The submission should include the following:

1. Code for the server, client, and file transfer protocol with:
    - AES encryption for secure file transfer.
    - ECDSA signing and verification for file integrity.
    - Brute force attack simulation.
2. Logs of file transfers showing encryption, decryption, and signature verification.
3. Logs of tampering detection using ECDSA signatures.
4. Code and report on the brute force attack simulation:
    - Detailed steps of the brute force attack.
    - Explanation of the results.
    - Recommended security improvements.