Hybrid Encryption

Stephen Haunts

@stephenhaunts | www.stephenhaunts.com

Overview

- Applying lessons learnt so far to hybrid encryption
- Encrypting with AES and RSA together
- HMACS for data integrity

Reviewing Security Concepts

Confidentiality

Integrity

Non-Repudiation

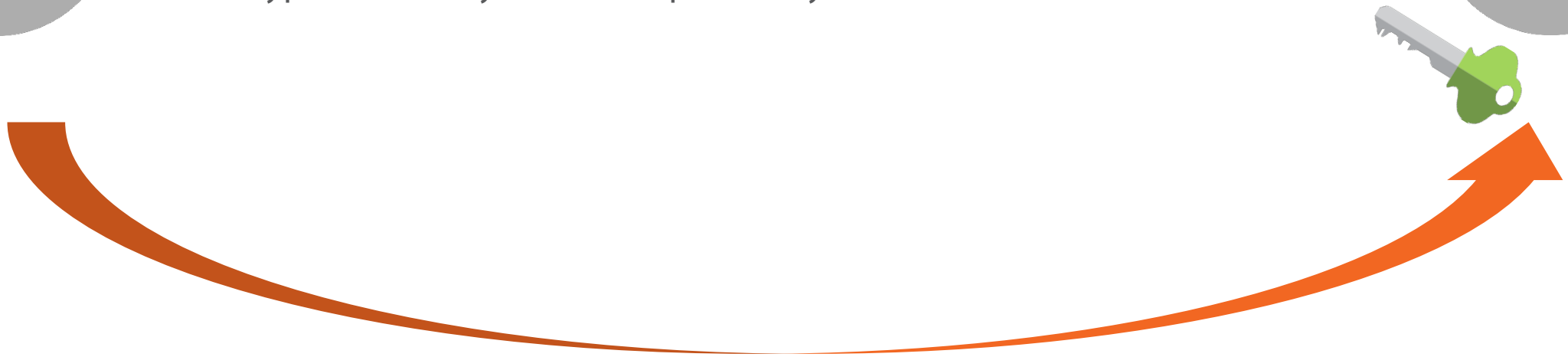
Authentication

Introducing Hybrid Encryption

- Key sharing with symmetric encryption is hard to do securely
- Asymmetric encryption is a lot slower than symmetric encryption
- Asymmetric key sharing is a better solution
- Hybrid encryption combines the best of both worlds
- Symmetric keys are encrypted with asymmetric encryption such as RSA

Introducing Hybrid Encryption

1. Generate AES session key
2. Generate IV
3. Encrypt message with AES key and IV
4. Encrypt session key with Bob's public key



Encrypted Data, encrypted session key, and IV are sent to Bob

Introducing Hybrid Encryption

1. Decrypt AES session key using private key
2. Decrypts message using decrypted key and IV

Encrypted Data, encrypted session key, and IV are sent to Bob

Introducing Hybrid Encryption

1. Generate AES session key
2. Generate IV
3. Encrypt message with AES key and IV
4. Encrypt session key with Alice's public key

Encrypted Data, encrypted session key, and IV are sent to Alice

Introducing Hybrid Encryption

1. Decrypt AES session key using private key
2. Decrypts message using decrypted key and IV

Encrypted Data, encrypted session key, and IV are sent to Alice

Code Demonstration

Encrypting with AES and RSA Together

Adding Integrity Checks

- Add integrity checks to guard against data tampering or corruption
- The easiest way is by standard hashing like MD5, SHA1 or SHA2
- Hash of the encrypted data is sent to the recipient with the message
- Before decryption the recipient hashes encrypted data and compares hashes
- The hash could be regenerated by an attacker
- Better solution is to use a Hashed Message Authentication Code

Adding Integrity Checks

1. Generate AES session key
2. Generate IV
3. Encrypt message with AES key and IV
4. Encrypt session key with Bob's public key
5. Calculate HMAC of encrypted data using AES session key

Encrypted Data, encrypted session key, IV and HMAC are sent to Bob

Adding Integrity Checks

1. Decrypt AES session key using private key
2. Recalculate HMAC for encrypted data
3. Decrypts message using decrypted key and IV

Encrypted Data, encrypted session key, IV and HMAC are sent to Bob

Code Demonstration

Adding in Integrity Checks with HMACs

Code Demonstration

```
private static bool CompareUnSecure(byte[] array1, byte[] array2){
    if (array1.Length != array2.Length){
        return false;
    }
    for (int i = 0; i < array1.Length; ++i){
        if (array1[i] != array2[i]){
            return false;
        }
    }
    return true;
}
```

Code Demonstration

```
private static bool Compare(byte[] array1, byte[] array2)
{
    var result = array1.Length == array2.Length;

    for (var i = 0; i < array1.Length && i < array2.Length; ++i)
    {
        result &= array1[i] == array2[i];
    }

    return result;
}
```

Module Summary

- Public key cryptography doesn't require sharing a common key
- Asymmetric encryption is based on mathematical computations
- Hybrid encryption uses best of symmetric and asymmetric

Module Summary

- Hybrid encryption is based on two separate cryptographic systems
  - Key encapsulation scheme
  - Data encapsulation scheme
- Added additional integrity checking
- HMACS used for integrity

Module Summary

- Recipient needs the AES key to recalculate the HMAC