Review: Plaintext Recovery Attacks against SSH

Introduction to Cryptographic Algorithms '12/'13

Raoul Estourgie
Ben Brücker

Institute for Computing and Information Sciences
Radboud University Nijmegen

Outline

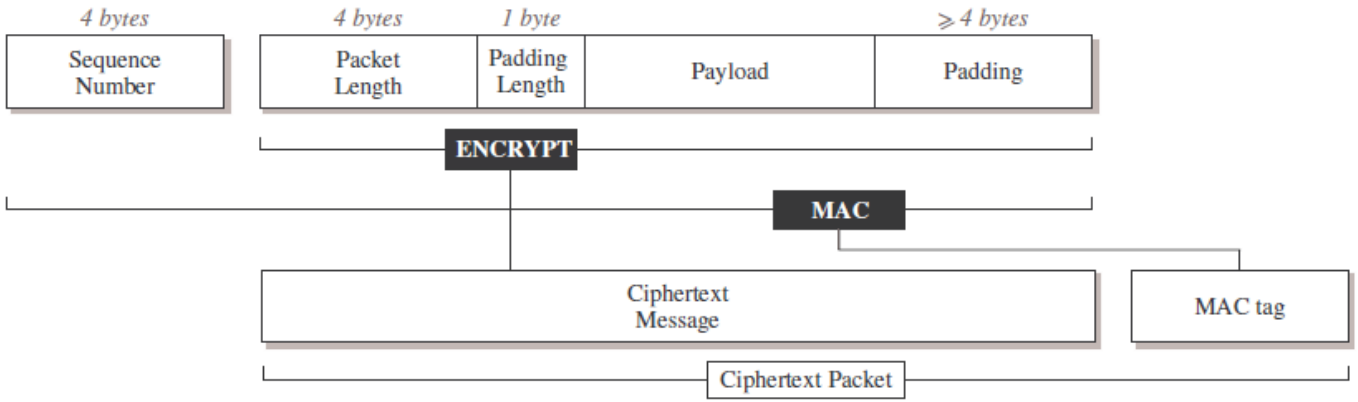
What is SSH?

- Secure Shell (SSH) connects computers securely over insecure network connections.
- It was released in 1995 and was designed to replace rlogin, rsh, Telnet and similar insecure protocols.
- The SSH protocol covers authentication, confidentiality and integrity.
- Our review article "Plaintext Recovery Attacks against SSH" paper focuses on the OpenSSH implementation.

What is the SSH-BPP protocol?

- The Binary Packet Protocol (BPP) of SSH encrypts a plaintext and then protects it's integrity by appending a MAC value.
- Prefixed with 4 byte packet-length, 1 byte padding-length
- Suffixed with 4 to 255 bytes of padding
- The message is then encrypted with a cypher of choice, for example aes128-cbc.
- MAC is calculated over this message and a 32-bit packet sequence number
- Mac is appended to the message

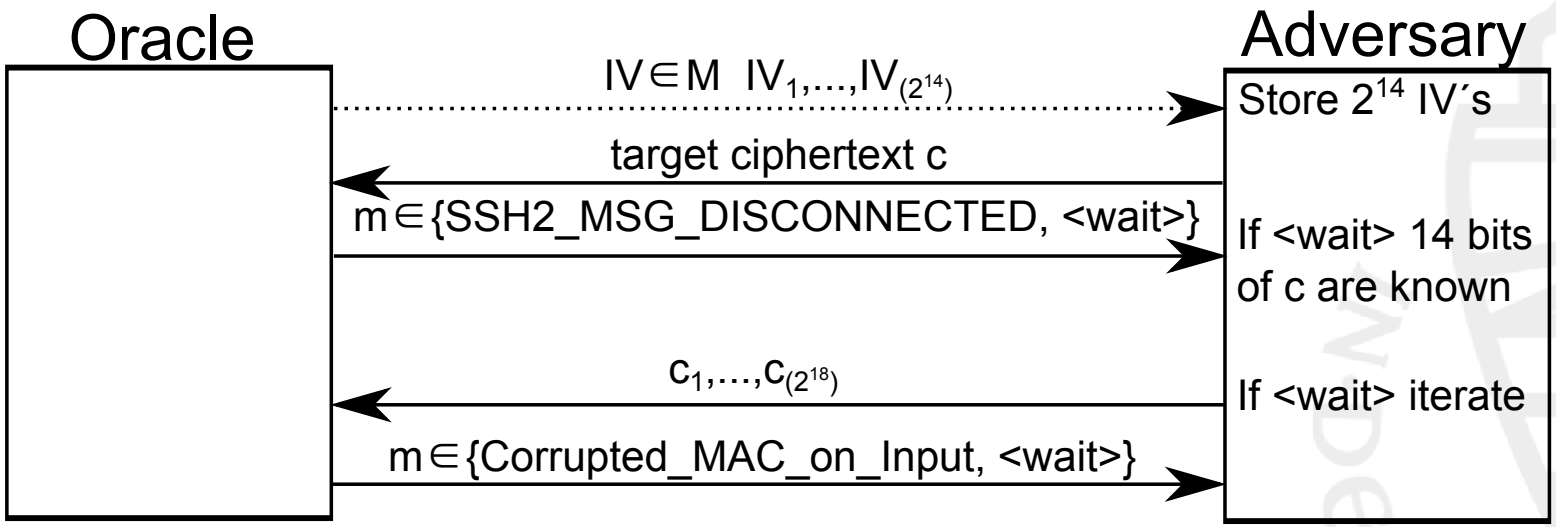
Schematic of a BPP block



Test

- The packets then form a data stream since the encryption is in CBC mode.
- Every packet $i-1$ on a connection will be the initialization vector (IV) for packet i on the same connection.
- For decryption it is essential that the receiver decrypts the first ciphertext block to be able to read the length field.
- The SSH protocol also specifies error handling for the BPP protocol. The connection should terminate whenever a transmission error occurs or MAC verification fails. When such a termination happens,the connection should be re-established. Implementations are free to send error messages to their peer when an error occurs.

Security game



Questions

Questions?