Phil Rogaway observed that CBC mode is not secure against chosen-

plaintext attack if the IV is known or can be predicted by the attacker

before he choses his plaintext [1]. Similarly, CBC mode is not secure if

the attacker can observe the last ciphertext block before choosing the

next block of plaintext, because the last block of ciphertext

essentially serves as the IV for the rest of the message.

The attack itself is very simple. Remember that in CBC mode, each

plaintext block is XOR'ed with the last ciphertext block and then

encrypted to produce the next ciphertext block. Suppose the attacker

suspects that plaintext block might be, and wants to test whether

that's the case, he would choose the next plaintext block to be

. If his guess is correct, then , and so he can confirm his

guess by looking at whether C\_j = C\_i.

The SSH2 protocol, when used with a block cipher in CBC mode, does allow

the attacker to observe the last ciphertext block of a packet, which is

then used as the (implicit) IV of the next packet. [...]

From: <https://www.openssl.org/~bodo/tls-cbc.txt>

See:

<https://derekwill.com/2021/01/01/aes-cbc-mode-chosen-plaintext-attack/>

<https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2023_04_18!10_54_07_PM.pdf>