Hack The Box Write Up

Info:

Name:	Nuclear Sale
Type:	Challenge
Category:	Crypto
Difficulty:	Easy
Date:	31 Jul 22

Description:

Plutonium Labs is a private laboratory experimenting with plutonium products. A huge sale is going to take place and our intelligence agency is interested in learning more about it. We have managed to intercept the traffic of their mail server. Can you find anything interesting?

Analysis:

In this challenge, we are only provided a Wireshark file "*challenge.pcap*". Upon inspection, a stream of email conversation between the Sales Department and Management can be found and it is shown below:

Sales: *Hello everyone, a potential buyer approached us asking for a huge amount of plutonium. Are we even allowed to sell this much?*
Management: *We are very XORry but the management does not approve such a sale. It may damage our business. Who is the buyer?*
Sales: *He is a high-profile individual. His information is encrypted below: <Ciphertext1>. You know what you have to do.*
Management: *Here is the ciphertext encrypted with our key: <Ciphertext2>.*
Sales: *Encrypting again with our key: <Ciphertext3>.*
Management: *Oh my. This changes everything. We cannot refuse selling to this guy. He can literally destroy us. Move the process.*
Sales: *Alright, we will process the order. Thanks!*

Exploit:

It seems that they are using XOR encryption and the same key is being used multiple times, specifically,

$$C1 = P \oplus S$$
$$C2 = C1 \oplus M$$
$$C3 = C2 \oplus S,$$

Where P is the plaintext, S is the Sales key and M is the Management key.

In this way, when Management encrypts C3 with their own Management key, they get the original plaintext.

However, since C3 = C2 ^ S, if we XOR C3 and C2, we get the Sales key, which we can then use to get the plaintext by XORing it with C1.

The above is implemented in "*attack.cpp*".