“Bye, Bye, Bye” to AES ECB Mode

Early last month, a group operating out of the University of Toronto released a report highlighting some of the security flaws found in the popular online meeting app Zoom. Their report highlighted a few concerning things. However, the one area I want to highlight is the type of encryption Zoom is currently using to encrypt the audio and video portions of the meeting: AES-128 in ECB mode.

What is AES-128?

AES is short for the Advanced Encryption Standard that was standardized back in 2001 by National Institute of Standards and Technology (NIST). It’s an extremely popular encryption protocol that is used in everything from encrypting web traffic to encrypting hard drives. The 128 of AES-128 is the size of the key used to encrypt the data; in this case, the key size is 128 bits. The larger the key, the more security AES has. AES can come in 3 flavors of key sizes: AES-128, AES-192, and AES-256. AES-256 has better security properties than AES-128. However, AES-128, if done correctly, cannot be broken (unless you have a working quantum computer) and can be relied on to securely store or transmit encrypted data.

What is ECB mode?

In addition to different key sizes, AES can operate in different “modes of operation” that help give AES a lot of flexibility in how it encrypts data. For instance, the AES mode of operation used in Wi-Fi networks is different than the AES mode of operation to encrypt a hard drive. These modes give AES a lot of flexibility to meet different security requirements.

The ECB mode is short for Electronic Code Book mode. When it first came on the scene, ECB looked like a good choice for encryption. It takes the data, chops it up into 128 bit blocks, and runs the AES encryption (or decryption) process over those chunks. At the time, ECB mode seemed secure and it was fast and easy to implement – all properties that are great for cryptography.

Why do Security Analysts’ have an extreme dislike for ECB mode?

As time went on, Cryptographers realized that ECB mode is not semantically secure. That is a fancy way of saying that, while you may not be able to read what the original information was, you can still gain information about how the original text was structured by comparing different data that was encrypted with the same key.

If the length of the data is the same, and if the same data is repeated over and over, then this can be discovered just by looking at the encrypted data. In other words, ECB mode leaks information about your data. Sometimes this will not lead to any sort of significant break. Other times, malicious attackers can get creative and be able to recover some of the encrypted data as in the case of the 2013 Adobe break (different algorithm, same ECB mode).

Does this mean that hackers can listen to my meetings on Zoom?

Probably not. AES-128 in ECB mode is not broken (i.e. you still need the key to decrypt the data), and no one has proven they can recover any data just by looking at the Zoom call encrypted text. (Zoom published a writeup of their security here.) Since the publication of the original report, Zoom has also updated their encryption to AES-256 in GCM mode. GCM mode has some solid security properties that make encrypting video and audio streams much more secure.

How do I know if any applications in my organization are using AES in ECB mode?

You will need to gather your software engineers and look at the cryptography libraries that your applications are using. Some of the older libraries use ECB mode as a default, and **that should be changed as soon as possible**. If your application is using custom-written cryptography code, the chances of there being a serious bug in that code is extremely high.

Should I still use AES-128 in ECB mode?

Is it 2001?

Do boy bands still roam the earth?

Do you want to risk that someone can recover "leaked data" from your encrypted information?

If your answer to any of those questions is "No", then you have your answer.

There are new cryptography standards and libraries that are faster and have great security properties for whatever your use case is. The new algorithms do a much better job at encrypting the data so it appears to not leak information like ECB does. To use Zoom as an example, switching to GCM mode means that not only do you avoid leaking as much data, but GCM also safeguards your data against tampering so any malicious attacker cannot alter the data without the algorithm detecting it.

What do I do if I have applications that rely on AES in ECB mode?

Contact us. Changing the cryptography in an application is not a straight-forward process. You need to work with experts who:

- Thoroughly understand regulatory requirements
- Know how to manage a security project
- Can help choose a quality cryptography design for your use case
- Write code that is secure by design

Together, we can help your organization say "Bye, Bye, Bye" to AES in ECB mode.