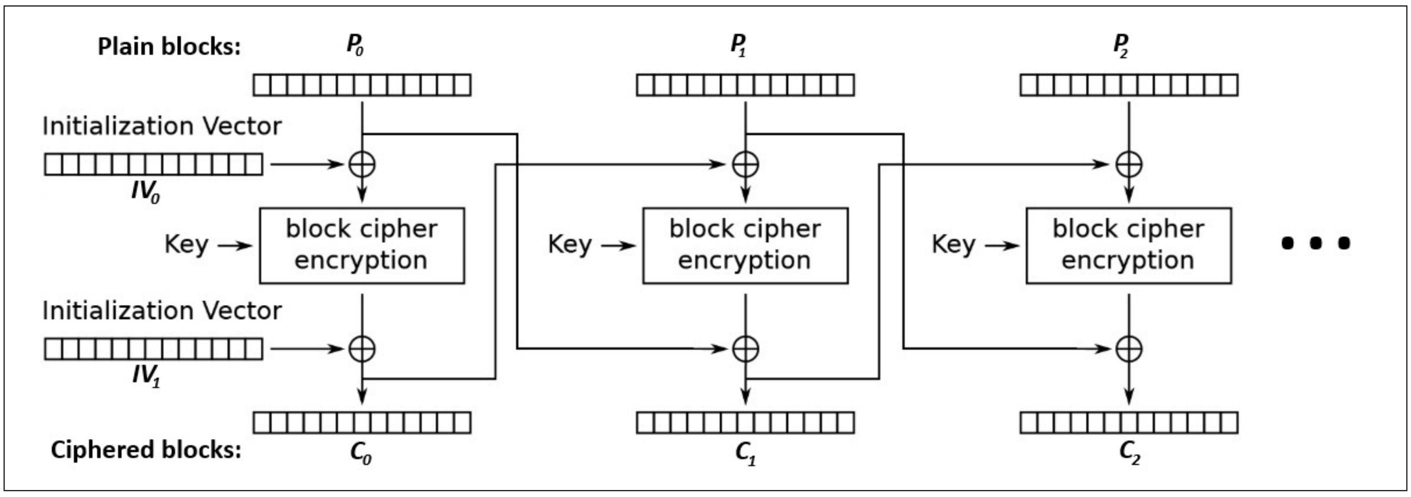
AES-IGE Malleability with user-controlled IV

NiwdEE

for: RootMe XMAS 2025

Context

Quick reminder of how AES-IGE works:



We will use the following symbols and definitions:

$AES_{k,IV}, AES^{-1}_{k,IV} : (\mathbb{F}_2^{128})^n \longrightarrow (\mathbb{F}_2^{128})^n$	AES-IGE cipher encrypt/decrypt using key "k" and Initialization Vector "IV"
$E_k, D_k : \mathbb{F}_2^{128} \longrightarrow \mathbb{F}_2^{128}$	Block cipher Encrypt/Decrypt using key "k" ($D_k = E_k^{-1}$)
$(X_n) : [\![0..l-1]\!] \longrightarrow \mathbb{F}_2^{128}, X \in (\mathbb{F}_2^{128})^l$	Sequence of l blocks of 128 bits with $X = X_0 \parallel X_1 \parallel \ldots \parallel X_{l-1}$
$\vert\vert$	Bitwise concatenation ($e.g.\, 111 \parallel 000 = 111000$)
$\oplus$	Binary XOR

Assumptions

From now on, we will assume that the server uses the secret key k, the initialization vector $IV = IV_0 \parallel IV_1$ and will not change these parameters later.

Let's also say that we know a plaintext P, of any length, and its corresponding ciphertext C obtained from $AES_{k,IV}$.
I.e. $AES_{k,IV}(P) = C \Leftrightarrow AES^{-1}_{k,IV}(C) = P$

By definition, we have: $(C_n)_{n\in\mathbb{N}} : \begin{cases} C_0 = E_k(P_0 \oplus IV_0) \oplus IV_1 \\ C_{n+1} = E_k(P_{n+1} \oplus C_n) \oplus P_n \end{cases}$ and $(P_n)_{n\in\mathbb{N}} : \begin{cases} P_0 = D_k(C_0 \oplus IV_1) \oplus IV_0 \\ P_{n+1} = D_k(C_{n+1} \oplus P_n) \oplus C_n \end{cases}$

Exploit

1. Find values of D_k

We have a target plaintext T, our goal is to forge a malicious ciphertext M and initialization vector $mIV = mIV_0 \parallel mIV_1$ such as $AES^{-1}_{k,mIV}(M) = T$ only knowing a couple (P, C) such as $AES_{k,IV}(P) = C$ (without knowing k or IV of course).

By definition, we have: $(T_n)_{n\in\mathbb{N}} : \begin{cases} T_0 = D_k(M_0 \oplus mIV_1) \oplus mIV_0 \\ T_{n+1} = D_k(M_{n+1} \oplus T_n) \oplus M_n \end{cases}$ and $(M_n)_{n\in\mathbb{N}} : \begin{cases} M_0 = E_k(T_0 \oplus mIV_0) \oplus mIV_1 \\ M_{n+1} = E_k(T_{n+1} \oplus M_n) \oplus T_n \end{cases}$

Without knowing the secret key k, we will never be able to directly calculate arbitrary values of D_k, so we should force a value of D_k we need to a value of D_k we know. In fact, we do know some values of D_k since the equation of P_{n+1} directly implies $D_k(C_{n+1} \oplus P_n) = P_{n+1} \oplus C_n$ and we assumed that the values of (P_n) and (C_n) are known. Then, in the definition of (T_n), we have to calculate the value $D_k(M_{n+1} \oplus T_n)$, but we cannot.

Let's force: $D_k(M_{n+1} \oplus T_n) = D_k(C_{n+1} \oplus P_n) = P_{n+1} \oplus C_n$

$\Leftrightarrow \quad M_{n+1} \oplus T_n = C_{n+1} \oplus P_n$ Because D_k is bijective

$\Leftrightarrow \quad M_{n+1} = C_{n+1} \oplus P_n \oplus T_n$ $\Rightarrow$ We have an expression of M based on known values

2. Deduce values of M

We can calculate, using the previous expression, $M_k\ \forall k \geq 1$, but we still miss M_0. So let's dive into $M_{n+1} = C_{n+1} \oplus P_n \oplus T_n$ to learn more.

For $n = 0$:

$$\begin{aligned}
& M_1 = C_1 \oplus P_0 \oplus T_0 \\
\text{but} \quad & T_1 = D_k(M_1 \oplus T_0) \oplus M_0 \\
\Leftrightarrow \quad & M_0 = D_k(M_1 \oplus T_0) \oplus T_1 \\
& \quad = D_k(C_1 \oplus P_0 \oplus T_0 \oplus T_0) \oplus T_1 \\
& \quad = D_k(C_1 \oplus P_0) \oplus T_1 \\
\Leftrightarrow \quad & M_0 = P_1 \oplus C_0 \oplus T_1
\end{aligned}$$

For $n \geq 1$:

$$\begin{aligned}
& T_{n+1} = D_k(M_{n+1} \oplus T_n) \oplus M_n \\
\Leftrightarrow \quad & M_n = D_k(M_{n+1} \oplus T_n) \oplus T_{n+1} \\
& \quad = D_k(C_{n+1} \oplus P_n \oplus T_n \oplus T_n) \oplus T_{n+1} \\
& \quad = D_k(C_{n+1} \oplus P_n) \oplus T_{n+1} \\
& \quad = P_{n+1} \oplus C_n \oplus T_{n+1}
\end{aligned}$$

$$\text{let } i = n - 1 \Leftrightarrow n = i + 1 \Rightarrow i \geq 0$$

$$\begin{aligned}
& M_{i+1} = P_{i+2} \oplus C_{i+1} \oplus T_{i+2} \\
\Leftrightarrow \quad & C_{i+1} \oplus P_i \oplus T_i = P_{i+2} \oplus C_{i+1} \oplus T_{i+2} \\
\Leftrightarrow \quad & P_i \oplus T_i = P_{i+2} \oplus T_{i+2}
\end{aligned}$$

$$\text{let } j = i + 2 \Leftrightarrow i = j - 2 \Rightarrow j \geq 2$$

$$\Leftrightarrow \quad T_j = T_{j-2} \oplus P_j \oplus P_{j-2}$$

We found the value M_0 must have for this to work, but we also see that T_n must verify a property based on a previous block $\forall n \geq 2$. In other words: Only T_0 and T_1 can be arbitrary, each of the following blocks necessarily derives from the preceding ones.

3. Find cIV

In the first part, we forced the value of D_k appearing in the definition of T_{n+1} to the one appearing in P_{n+1}. Now let's extend this to the expressions of T_0 and P_1 (not P_0 because it depends on IV, that we don't know).

$$\begin{aligned}
\text{Let's force:} \quad & D_k(M_0 \oplus mIV_1) = D_k(C_1 \oplus P_0) = P_1 \oplus C_0 \\
\Leftrightarrow \quad & M_0 \oplus mIV_1 = C_1 \oplus P_0 && \text{Because } D_k \text{ is bijective} \\
\Leftrightarrow \quad & mIV_1 = C_1 \oplus P_0 \oplus M_0 && \Rightarrow \text{We have an expression of } mIV_1 \text{ based on known values}
\end{aligned}$$

And then,

$$\begin{aligned}
\text{By definition:} \quad & T_0 = D_k(M_0 \oplus mIV_1) \oplus mIV_0 \\
& \quad = P_1 \oplus C_0 \oplus mIV_0 && \text{Because of what we forced} \\
\Leftrightarrow \quad & mIV_0 = P_1 \oplus C_0 \oplus T_0 && \Rightarrow \text{We have an expression of } mIV_0 \text{ based on known values}
\end{aligned}$$

4. Verifications

Now we expressed explicitly the values of M and mIV, we can check if it really decodes to T.

So, let R the result of the decoding. I.e. $R = AES^{-1}_{k,mIV}(M) \quad \Leftrightarrow \quad (R_n)_{n\in\mathbb{N}} : \begin{cases} R_0 = D_k(M_0 \oplus mIV_1) \oplus mIV_0 \\ R_{n+1} = D_k(M_{n+1} \oplus R_n) \oplus M_n \end{cases}$

For R_0:

$$\begin{aligned}
R_0 &= D_k(M_0 \oplus mIV_1) \oplus mIV_0 \\
&= D_k(M_0 \oplus C_1 \oplus P_0 \oplus M_0) \oplus mIV_0 \\
&= D_k(C_1 \oplus P_0) \oplus P_1 \oplus C_0 \oplus T_0 \\
&= P_1 \oplus C_0 \oplus P_1 \oplus C_0 \oplus T_0 \\
&= T_0
\end{aligned}$$

For R_1:

$$\begin{aligned}
R_1 &= D_k(M_1 \oplus R_0) \oplus M_0 \\
&= D_k(M_1 \oplus T_0) \oplus M_0 \\
&= D_k(C_1 \oplus P_0 \oplus T_0 \oplus T_0) \oplus M_0 \\
&= D_k(C_1 \oplus P_0) \oplus P_1 \oplus C_0 \oplus T_1 \\
&= P_1 \oplus C_0 \oplus P_1 \oplus C_0 \oplus T_1 \\
&= T_1
\end{aligned}$$

For $(R_n)_{n\geq 1}$:

$$\text{suppose } R_n = T_n$$

$$\begin{aligned}
R_{n+1} &= D_k(M_{n+1} \oplus R_n) \oplus M_n \\
&= D_k(C_{n+1} \oplus P_n \oplus T_n \oplus T_n) \oplus M_n \\
&= D_k(C_{n+1} \oplus P_n) \oplus M_n \\
&= P_{n+1} \oplus C_n \oplus M_n
\end{aligned}$$

$$\text{let } i = n - 1 \Leftrightarrow n = i + 1 \Rightarrow i \geq 0$$

$$\begin{aligned}
R_{i+2} &= P_{i+2} \oplus C_{i+1} \oplus M_{i+1} \\
&= P_{i+2} \oplus C_{i+1} \oplus C_{i+1} \oplus P_i \oplus T_i \\
&= P_i \oplus P_{i+2} \oplus T_i \quad \text{as predicted}
\end{aligned}$$

5. Summary

If we know a plaintext P and a ciphertext C such as $AES_{k,IV}(P) = C$, we can forge a ciphertext M and an initialization vector mIV such as $AES^{-1}_{k,mIV}(M) = T$ with the first two blocks of T (T_0 and T_1) being arbitrary and without having any information about k or IV using these expressions:

$$(M_n)_{n\in\mathbb{N}} : \begin{cases} M_0 = P_1 \oplus C_0 \oplus T_1 \\ M_{n+1} = C_{n+1} \oplus P_n \oplus T_n \end{cases} \qquad mIV = mIV_0 \parallel mIV_1 : \begin{cases} mIV_0 = P_1 \oplus C_0 \oplus T_0 \\ mIV_1 = C_1 \oplus P_0 \oplus M_0 \end{cases} \qquad (T_n)_{n\in\mathbb{N}} : \begin{cases} T_0 : \text{as you want} \\ T_1 : \text{as you want} \\ T_{n+2} = T_n \oplus P_{n+2} \oplus P_n \end{cases}$$