Checklist de Segurança para Projetos com ESP32

Por Fábio Souza

2025

EMBARCADOS

Checklist de Segurança para Projetos com ESP32

Por Fábio Souza - 2025

Introdução

A segurança é um aspecto fundamental no desenvolvimento de dispositivos IoT. Ciente das ameaças crescentes no ambiente conectado, a Espressif implementou uma série de medidas robustas de segurança no ESP-IDF, visando proteger projetos baseados no ESP32.

Os métodos de segurança apresentados possuem como objetivo:

- Garantir que **apenas código confiável** seja executado.
- Proteger a **identidade e integridade do código** armazenado na flash externa.
- Proteger a **identidade do dispositivo**.
- Assegurar **armazenamento seguro** de dados confidenciais.
- Estabelecer **comunicação autenticada e criptografada** com dispositivos remotos.

A seguir, apresentamos um checklist prático para você avaliar e fortalecer a segurança do seu projeto com ESP32, baseado na Documentação Oficial da Espressif.

Boot Seguro (Secure Boot)

O **Secure Boot** garante que apenas firmware autenticado e confiável seja executado no dispositivo, estabelecendo uma **cadeia de confiança (chain of trust)**. Ele verifica a assinatura digital do firmware durante o boot e nas atualizações OTA.

- ☐ O recurso Secure Boot está habilitado no dispositivo?
- ☐ O Secure Boot foi implementado para garantir que apenas software autenticado seja executado?
- ☐ A chave de assinatura privada foi gerada em um sistema com fonte de entropia confiável?
- ☐ A chave privada de assinatura foi mantida em sigilo absoluto, sem exposição a terceiros?
- ☐ O processo de geração e uso da chave foi protegido contra ataques de canal lateral, como ataques de tempo (timing attacks)?
- ☐ Todos os eFuses de segurança relacionados ao Secure Boot foram corretamente programados?
- ☐ As interfaces de debug (JTAG, UART) e modos de boot desnecessários (ex: UART Download Mode) foram desabilitados?
- ☐ O Secure Boot foi ativado em todos os dispositivos de produção, conforme recomendação oficial?

Checklist de Segurança para Projetos com ESP32

Por Fábio Souza - 2025

Criptografia da Memória Flash (Flash Encryption)

A **Flash Encryption** protege o conteúdo da memória flash externa (firmware, dados e chaves), garantindo que apenas o próprio dispositivo consiga acessar essas informações. Utiliza criptografia **AES-XTS**.

- ☐ A Flash Encryption foi ativada em modo Release no dispositivo?
- ☐ Todos os dados armazenados na flash, incluindo firmware e dados sensíveis, estão criptografados?
- ☐ Os eFuses de configuração da Flash Encryption foram devidamente queimados, impedindo alterações futuras?
- ☐ As interfaces de debug e acesso físico (UART/JTAG) foram desabilitadas após a ativação da Flash Encryption?

Armazenamento Seguro de Dados (Secure Storage / NVS Encryption)

O **Armazenamento Seguro de Dados** garante que informações sensíveis (como credenciais, chaves e dados privados) sejam armazenadas de forma criptografada na flash, utilizando **NVS Encryption**, com chaves protegidas pelos **eFuses** do dispositivo.

- ☐ As partições NVS com criptografia está habilitado para armazenar dados confidenciais?
- ☐ As chaves de criptografia do NVS são gerenciadas automaticamente pelo hardware?

Comunicações Seguras

A **Comunicação Segura** garante a privacidade e integridade dos dados transmitidos entre o dispositivo e servidores ou outros dispositivos. O ESP-IDF oferece suporte a **TLS/SSL** via **esp-tls**.

- ☐ Todas as comunicações do dispositivo utilizam TLS/SSL para garantir confidencialidade e integridade?
- ☐ Foi implementada autenticação mútua (Mutual Authentication), quando necessário, entre cliente e servidor?
- ☐ O recurso esp-tls ou outras APIs seguras do ESP-IDF foram utilizados para estabelecer conexões protegidas?

Checklist de Segurança para Projetos com ESP32

Por Fábio Souza - 2025

Atualização de Firmware (OTA) Segura

As atualizações OTA permitem atualizar o firmware do dispositivo remotamente. Para garantir a segurança, é necessário validar assinaturas digitais e proteger o transporte dos pacotes de atualização.

- ☐ As atualizações OTA são assinadas digitalmente e verificadas antes de serem aplicadas?
- ☐ O dispositivo realiza a validação da assinatura digital durante o boot para qualquer firmware atualizado?
- ☐ A comunicação durante o processo OTA é protegida com TLS/SSL, garantindo integridade e confidencialidade?

Proteção de Interfaces e Acesso Físico

A desativação de interfaces de depuração e modos de acesso não utilizados é fundamental para evitar que atacantes acessem o dispositivo fisicamente.

- ☐ As interfaces de depuração JTAG e UART foram desabilitadas em produção?
- ☐ Os eFuses de segurança relacionados a Secure Boot, Flash Encryption e restrição de debug foram queimados permanentemente?
- ☐ O Download Mode (UART boot) foi desabilitado quando não há necessidade de suporte em campo?

Auditoria e Documentação

Documentação detalhada das práticas de segurança implementadas no projeto e auditoria contínua para garantir conformidade e integridade.

- ☐ Documentou todos os procedimentos de segurança adotados no projeto?
- ☐ Registrou a configuração dos eFuses queimados para cada dispositivo?

Checklist de Segurança para Projetos com ESP32

Por Fábio Souza - 2025

Boas Práticas

Práticas recomendadas que aumentam a segurança geral do dispositivo e reduzem riscos operacionais e de segurança.

- ☐ As bibliotecas e SDKs (ESP-IDF) utilizados estão atualizados com as últimas correções de segurança?
- ☐ Foram implementadas políticas de senha seguras para todas as interfaces de configuração?
- ☐ Não existem credenciais padrão nos dispositivos de produção?
- ☐ Existe um plano de resposta a incidentes, incluindo atualização de firmware rápida em caso de vulnerabilidades?

Política de Segurança e Atualizações (Security Policy & Updates)

A Espressif fornece informações importantes sobre vulnerabilidades e políticas de atualização através do GitHub e canais oficiais.

- ☐ Consultou a Security Policy Brief disponível no repositório oficial ESP-IDF no GitHub?
- ☐ Acompanham-se regularmente os Security Advisories publicados pela Espressif (hardware e software)?
- ☐ Estão sendo aplicadas as correções de segurança em componentes ESP-IDF e bibliotecas de terceiros, conforme as atualizações lançadas pela Espressif?
- ☐ Está sendo seguido o procedimento recomendado de atualização periódica para a última versão de correção de bugs (bugfix release) do ESP-IDF, garantindo a aplicação de todas as atualizações críticas de segurança?