wolfSSL Tuning Guide

2024-11-08

Contents

1 イントロダクション

このガイドは、wolfSSL 組み込み SSL/TLS ライブラリのパフォーマンスとメモリ使用量を調整および最適化するためのリファレンスをエンジニアのみなさまに提供します。「ガイド」として考慮されるべきものであり、今後も随時更新します。何か不足していると感じた場合は、ぜひお知らせください。より使いやすくすることも、wolfSSL の主な目標の 1 つです。

1.1 対象読者

このガイドは、wolfSSL 組み込み SSL/TLS ライブラリのパフォーマンスとメモリ使用量を最適化することに関心のあるエンジニアを対象としています。

1.2 概要

wolfSSL チューニングガイドは、wolfSSL 組み込み SSL/TLS ライブラリのパフォーマンスとメモリ使用量を最適化するために設計されています。このドキュメントは、さまざまな環境に適応できるように包括的なガイドと説明を提供することを目的としています。このガイドは、メモリフットプリント、パフォーマンス、およびセキュリティを特定の要件に応じて調整することで、SSL/TLS 処理の効率を高めることに関心のある開発者を対象としています。

2 考慮事項

2.1 予想される要件

wolfSSL を環境に最適化する最初のステップは、予想される要件を文書化することです。最高レベルでは、SSL/TLS の設計目標は通常以下に集約されます：

- **メモリフットプリント（ROM）**
- **セッションごとのメモリ使用量（RAM）**
- **SSL ハンドシェイクのパフォーマンス**
- **データフローパフォーマンス（大量データ転送）**
- **望ましいセキュリティレベル（以下の図 1 を参照）**

2.2 望ましいセキュリティレベル

セキュリティレベル	レベル名	説明
1	緩やか	カジュアルな覗き見を防ぐことができればよい
2	適度	攻撃者が存在するが、彼らはそこまで高いモチベーションがない
3	企業向け	プロフェッショナルな攻撃に対して安全
4	軍用グレード	軍事レベルの保護
5	量子コンピュータ耐性	量子コンピュータによる攻撃に耐えることができる

図 1：望ましいセキュリティレベル

これらのトップレベルの目標の各々は、設計を進める中で他の目標とトレードオフが発生します。

あらかじめ定義する必要のある重要な変数は次のとおりです：

1. 利用可能なハードウェア：
   a. SSL/TLS に利用可能なメモリ（ROM / RAM）
   b. CPU の種類とクロック速度
2. 必要な SSL/TLS プロトコルレベル（例：TLS 1.0、TLS 1.1、TLS 1.2 など）
3. 必要な暗号スイート。要件に暗号スイートが定義されていない場合は、パフォーマンス目標に合った暗号スイートを自由に選択できます：
   a. 公開鍵アルゴリズムとキーの長さ（RSA、ECC、NTRU、PSK など）
   b. ブロック / ストリーム暗号（AES、DES、3DES、RC4、HC-128 など）
   c. ハッシュ関数（SHA、SHA2、MD5、Blake2b など）
4. 接続のどちら側にいるか：クライアント、サーバー、またはその両方？
5. クライアント認証？
6. SSL 接続の反対側は定義されていますか？
   a. どの SSL 実装を使用していますか？
   b. どの SSL/TLS プロトコルバージョンですか？
   c. キーの長さは？
   d. クライアントまたはサーバーですか？
7. 一度に必要なアクティブな SSL/TLS 接続/セッションの最大数は？
8. SSL ハンドシェイクのパフォーマンス要件は？
9. SSL ハンドシェイク完了後の大量データ転送のパフォーマンス要件は？
10. ハードウェア暗号化は利用可能ですか？もしそうなら、どの暗号がハードウェアで利用可能ですか？
11. 編集者注：このドキュメントを実用的な範囲内に保つために、オペレーティングシステムと TCP/IP スタックのチューニングについては本ドキュメントのスコープから外しています。

上記の変数をすべて考慮すると、多くのことを考慮する必要があることがわかります。したがって、このガイドでは参考として 3 つの最適化レシピを提示します：

1. 最小フットプリントサイズ（ヒープ、スタック、静的データ、コード）のための最適化
2. 最高速度を実現するための最適化
3. 最高のセキュリティ性能を保つための最適化

他の最適化レシピも利用可能です。info@wolfssl.jp までご連絡ください。追加の参考レシピには以下が含まれます：

1. 大量の接続数に対応するための最適化
2. 特定のオペレーティングシステム/チップセット環境における最適化
3. 特定のアプリケーション向けの最適化
4. 最高のセキュリティと最小のフットプリントの組み合わせなど、複数の目標に向けた最適化
5. 低消費電力のための最適化
6. セキュリティレベル 1,2 のための最適化 # レシピ

2.3 レシピ #1 最小フットプリント

多くのユーザーは、メモリリソースが限られている深く組み込まれたシステムを使用しています。このセクションでは、wolfSSL のフットプリントサイズを削減する方法を説明します。

1. 必要なプロトコルバージョンのみをサポートするように制限します。たとえば、TLS 1.2 接続のみを許可します。
2. コンパイル時に不要なライブラリ機能を削除します - wolfSSL マニュアルの2.4.1 節を参照してください。
3. 限定されたセットの暗号スイートを選択します：
   a. RSA、ECC、PSK のメモリ使用量の違い。
   b. 小さい鍵サイズを選択します - wolfSSL マニュアルの4.3 節を参照してください。
4. ハードウェア暗号が利用可能であればそれを活用します - wolfSSL マニュアルの4.4 節を参照してください。
5. コンパイラとツールチェーンの最適化を利用します。
6. 接続の両端を制御できる場合は、最大 SSL レコードサイズを減らします。

2.4 レシピ #2 最高速度

接続に SSL/TLS を追加すると、パフォーマンスの低下は避けられません。私たちの目標は、そのパフォーマンス低下をできるだけ小さくすることです。このセクションでは、ハンドシェイク中およびハンドシェイク後の wolfSSL の速度を向上させる方法を説明します。

パフォーマンスに関して懸念される主な分野は 2 つあります：

1. SSL/TLS ハンドシェイク速度。
2. データフロー速度（SSL ハンドシェイク後の大量データ転送）。

SSL ハンドシェイクのパフォーマンスを最適化する際に考慮すべき項目は次のとおりです：

1. より速い数学ライブラリを使用します（big integer vs. fastmath）。
2. ハードウェア暗号が利用可能であればそれを活用します - wolfSSL マニュアルの4.4 節を参照してください。
3. 鍵サイズ - wolfSSL マニュアルの4 章を参照してください。
4. 鍵タイプ（例：RSA vs ECC）。
5. ハンドシェイク速度とセキュリティレベルのトレードオフ（例：クライアント/サーバー証明書検証 - wolfSSL マニュアルの4.8 節を参照）。
6. PSK（事前共有鍵）を使用することを検討します - wolfSSL マニュアルの4.7 節を参照してください。

ストリーミングメディア環境での**最大データフロー速度**（例：ビデオゲーム、VoIP アプリケーション、クラウドインフラストラクチャ）では、暗号スイートの選択が重要です。このレシピでは、ハードウェア環境や接続数に応じて多くのオプションがあります。レシピをシンプルにするために、典型的なクラウドベースのサーバーで動作する単一接続環境に焦点を当てます。

最大データフロー速度を最適化する際に考慮すべき項目は次のとおりです：

1. ストリーム暗号、Rabbit、HC-128 など、遅いアルゴリズムよりも速いアルゴリズムを優先する暗号スイートを選択します。
2. より良いコンパイラの最適化を利用します。（これはユーザーにとって実用的なオプションではないかもしれません）
3. ハードウェア暗号が利用可能であればそれを活用します。

2.5 レシピ #3 最高のセキュリティ

SSL/TLS 接続のセキュリティは非常に重要です。プロジェクトに SSL/TLS を追加する主な理由は、安全な通信チャネルを確保することだからです。

すべての暗号ベースのプロトコルと同様に、新しい攻撃や脆弱性が発見され公開されると、SSL/TLS のセキュリティ推奨事項は変更されることがあります。最高のセキュリティを最適化すると、構成に応じてメモリ使用量とパフォーマンスの両方に悪影響を及ぼす可能性があります。

1. 現在利用可能な最高の情報に基づいた、暗号スイートの選択。
2. 現在利用可能な最高の情報に基づいた、鍵サイズの選択。
3. その他の考慮事項

上記の基本レシピからわかるように、SSL/TLS の最適化は複雑な多変量問題であり、初期環境に関するさまざまな前提に大きく依存します。wolfSSL チームは、これらの選択に際し多くのお客様にサポートを提供してまいりました。シンプルなご質問のほか、短期間のプロフェッショナルデザインコンサルティング、さらには SSL/TLS プロジェクト全体の実装管理まで、さまざまな方法でサポートいたします。ご興味がありましたら、ぜひ info@wolfssl.jp までお問い合わせください。# 追加情報

wolfSSL ポーティングガイド: https://wolfssl.jp/docs/

wolfSSL のダウンロード: https://wolfssl.jp/download/

wolfSSL サポートフォーラム (英語): http://www.wolfssl.com/forums

ご不明な点がございましたら、info@wolfSSL.comまでお問い合わせください。導入支援や最適化コンサルティングのご案内も可能です。