MATLAB EXPO

セキュアコーディングを実践する
ー セキュリティ関連のソリューション紹介 ー

アプリケーションエンジニアリング部
田中 康博

セキュリティ関連のソリューション紹介

セキュリティ関連のソリューション紹介 - モデリングガイドライン

モデルのセキュリティ標準への準拠性を検証 (1)

■ 概要:

- セキュアコーディングのためのモデリング標準からの逸脱を特定

■ モデルアドバイザーでのチェック:

- CERT C, CWE, ISO/IEC TS 17961

■ 結果:

- 基本的な欠陥の削除
- 生成コードのセキュリティ標準への準拠性を低下させる可能性のあるブロックの削除やパラメーターの見直し

モデルアドバイザー

The screenshot shows the Model Advisor interface. On the left, a tree view lists various modeling standards, with 'Check for bitwise operations on signed integers' highlighted in red. On the right, the 'Check for bitwise operations on signed integers' panel displays a warning: 'Warning: The following bitwise operations on signed integers were found: Location: .../Bit to Integer Converter'. Below this, the 'Recommended Action' is 'Change data type to unsigned integer.' A red arrow points from the warning location to a Simulink block diagram below. In the diagram, a 'Bit to Integer Converter' block is highlighted in red with the text '欠陥!' (Defect!). The diagram shows two 'C2806x GPIOx' blocks connected to a 'Bit to Integer Converter' block, which outputs a 'uint8' signal to a 'mod' block, followed by a '1-D T(u)' block, and finally a 'Velocity_Command' output.

セキュリティ関連のソリューション紹介 - モデル解析

モデルのセキュリティ標準への準拠性を検証 (2)

- 概要:
 - モデルの潜在的な設計エラーを特定
- 検出される設計エラー:
 - ゼロ除算, 整数オーバーフロー, 範囲外配列アクセス
 - デッドロジック
 - 浮動小数点の問題 (NaN / 非正規浮動小数点)
 - 指定された最小値と最大値の違反
 - データストアのアクセス違反
- 結果:
 - 設計エラーの削除 / 正当化

設計エラー検出

Results: focVelocityEncoder_F28069

Design error detection in progress.
10/254 objectives valid
233/254 objectives in progress
11/254 objectives are dead logic

Results:

- Detailed analysis report: ([HTML](#)) ([PDF](#))

Simulink Design Verifier Results Summary: focVelocityEncoder_F28069

Progress	<div style="width: 80%;"></div>
Objectives processed	21/254
Valid	10
Falsified	11
Elapsed time	0:41

セキュリティ関連のソリューション紹介 - コード生成

セキュリティ標準のためのコードを生成

- モデルアドバイザーによるEmbedded Coderのパラメーターの提案
 - 浮動小数点演算子、再帰検出、オーバーフロー処理など
- ユーザーの希望がセキュリティ標準から逸脱する可能性がある
 - 既定のパラメーター動作: 調整可能 (ファイルスコープ)
 - CERT-C DCL19-C. (関数スコープ)
 - Minimize the scope of variables and functions
- ユーザーはモデルに手書きコードを含めることができる
 - セキュリティ標準に準拠していない可能性がある

CERT C: Rec. DCL19-C

変数と関数のスコープは最小化する

説明

ルール定義

変数と関数のスコープは最小化します。^[1]

例

[すべて展開する](#)

> static 指定子なしで宣言され、1つのファイル内でのみ参照される関数またはオブジェクト

> 必要なスコープを超えて定義されたオブジェクト

Polyspace Bug Finder ヘルプドキュメント

セキュリティ関連のソリューション紹介 - コード解析

コードのセキュリティ標準への準拠性を検証 (1)

- コードレベルで最終チェック
 - ルールはコードに対してのみ定義される
 - 手書きコード (S-function など)
- セキュアコーディングチェッカー
 - CERT-C/C++
 - ISO/IEC TS 17961
 - MISRA-C:2012 Amendment 1
- CWEチェックのための解析フィルター

コードのセキュリティ標準への準拠性を検証 (2)

検証結果の詳細

SEI CERT C ARR30-C (Rule)
Do not form or use out-of-bounds pointers or array subscribers. Attempt to dereference pointer at index 10. Valid range: [0..9]

イベント	ファイル	スコープ	行
1 Dynamic allocation	staticmemory.c	bug_outboundptr()	77
2 Assignment to local pointer 'ptr'	staticmemory.c	bug_outboundptr()	77
3 Not entering if statement (if-condition false)	staticmemory.c	bug_outboundptr()	78
4 Assignment to local variable 'i'	staticmemory.c	bug_outboundptr()	79
5 ARR30-C: Do not form or use out-of-bounds pointers or array subscribers	staticmemory.c	bug_outboundptr()	82

```

staticmemory.c
72 *=====*/
73 void bug_outboundptr(void) {
74     char* ptr;
75     int i;
76
77     ptr = (char*)malloc(SIZE10);
78     if (ptr == NULL) return;
79     for (i = 0; i <= (SIZE10-1); i++) /* After the loop, i is outside the buffer */
80         ptr[i] = 43;
81
82     ptr[i] = 4; /* Defect: Out of bounds access */
83
84     free(ptr);
85 }
86
  
```

デバッグ情報

- 欠陥の原因特定、トレースバック
- 変数の範囲/値

Polyspace Code Prover

- No False Negative
 - ランタイムエラーを検出
 - コードの安全性を証明

コードのセキュリティ標準への準拠性を定量化

未対応モデルのコード例： ルール別の SEI CERT C 違反 (上位10件のみ)

違反総数: 67件が見つかりました

セキュアコーディング準拠への逸脱を削減

推奨モデルのコード例： ルール別の SEI CERT C 違反 (上位10件のみ)

違反総数: 35件が見つかりました

モデルとコード間のトレーサビリティ

Result Details
 Variable trace | fx focVelocityEncoder_F28069.c / focVelocityEncoder_F28069_step1()
 Status: Unreviewed | Enter comment here...
 Severity: Unset

SEI CERT C INT13-C (Recommendation)
 Use bitwise operators only on unsigned operands
 Right operand of | is negative.
 A | operation on negative value may alter the sign bit and lead to the result misinterpretation.
 Use unsigned integer type or avoid negative values.

Event	File
1	INT13-C Use bitwise operators only on unsigned operands focVelocityEncoder_F28069.c f

Source
 focVelocityEncoder_F28069.c × c2806xSchedulerTimer0.c ×

```

1426 tmp_0 = (int16_T)((real32_T)fmod((real_T)rtb_SignA
1427 )
1428 }
1429 /* Switch: '<S65>/Switch' incorporates:
1430 * Constant: '<S65>/Constant1'
1431 * DataTypeConversion: '<S65>/DataTypeConv1'
1432 * DataTypeConversion: '<S65>/DataTypeConv2'
1433 * Logic: '<S65>/AND3'
1434 * RelationalOperator: '<S65>/Equal1'
1435 */
1436 if (rtb_NotEqual && (((((uint16_T)tmp) & 128U) != 0)
1437 & 127)) == (((((uint16_T)tmp_0) & 128U) != 0)
1438 (tmp_0 & 127)))) {
1439 rtb_IntegralGain = 0.0F;
1440 }
1441
  
```

Model Diagram
 A block diagram showing a 'single' input (1) entering a 'postSat' block. The output of 'postSat' goes to an 'AND' block. The 'AND' block also receives a 'boolean' input (0). The output of 'AND' goes to an 'equal' block. The 'equal' block also receives an 'int8' input. The output of 'equal' goes to a 'boolean Ts:Sample' block. The 'boolean Ts:Sample' block also receives a 'boolean' input (P). The output of 'boolean Ts:Sample' goes to an 'int8' output block.

source-to-model link
 +

3 single → postSat → boolean
 4 boolean → boolean Ts:Sample → boolean

- コードからモデルへジャンプできるハイパーリンク
- 双方向のトレーサビリティを確保

まとめ:セキュリティ関連のソリューション紹介

- モデルからコードまでのセキュアコーディングのサポート

- 開発の早期段階での設計チェック

Simulink
Check

Simulink
Design Verifier

- セキュアコーディングのためのコード生成の設定

Embedded
Coder

Polyspace
Bug Finder / Polyspace
Code Prover

✓コードレベルで最終チェック

- コード品質の定量化
- 生成コード、S-Function、デバイスドライバなどの手書きコードなど

Accelerating the pace of engineering and science

© 2020 The MathWorks, Inc. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See www.mathworks.com/trademarks for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.