平成24年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	三浦功也
卒業研究題目	組込みシステム向け仮想化環境を用いた汎用OSの監視機構	

近年, 組込みシステムは, オープン化が進むとともに, ネットワークに接続する機会が多くなってきており, 従来から使用されてきたリアルタイム OS(RTOS) に加えて,Linux などの汎用 OS が使われる機会が増加してきている. そのため, 組込みシステムが外部からの攻撃にさらされる機会が増加しており, セキュリティ対策が必要となってきている. 組込みシステムは, 主に機器を制御する目的でつかわれることが多く, 機器が誤作動すると, 人命にかかわる事態が起こりうる. 汎用 OS のセキュリティソフトを用いることで, 汎用 OS が自身を監視することはできるが, ゼロデイアタックなどにより, 汎用 OS が乗っ取られてしまうことがある. 乗っ取られてしまった汎用 OS 上のセキュリティソフトは信頼できるソフトウエアとは言えない. そのため, 汎用 OS のみで監視機構の信頼性を確保することは難しく, 信頼性向上のためには汎用 OS 外部の信頼できるソフトウエアから汎用 OS を監視する方法が考えられる. われわれの研究室では, 組込み分野で求められるリアルタイム性と, 多機能性を両立させるために, 組込み向け仮想化環境 SafeG を開発してきた. SafeG を用いることで,RTOS と汎用 OS は独立に動作させることができ, かつ汎用 OS から RTOS への不正なアクセスを保護できる. 逆に,RTOS にはこのような制限がないため,RTOS から汎用 OS の監視が実現できる.

そこで本研究では, 信頼性のある監視機構実現のために,SafeG を用いて,RTOS から汎用 OS を監視する機構の提案と実装を行った. 汎用 OS を監視する手法として, シーケンス監視, 汎用 OS 上の監視機構の監視, 汎用 OS の割込み頻度の監視を提案した. そのうち, 汎用 OS への非依存性, 実装の容易さ, オーバーヘッドの小ささからシーケンス監視を実装した. シーケンス監視のために, 汎用 OS から RTOS へシーケンス番号を送り,RTOS でその値を確認する必要があった. 汎用 OS から RTOS にシーケンス番号を送信する方式として, ポーリング方式, 直接番号通知方式, 間接番号通知方式を提案し, オーバーヘッドの小ささと, 監視機構の実現の容易さから直接番号通知方式を実装した. この方式を実現するために,SafeG,RTOS, 汎用 OS に機能の追加を行い, 監視機構のフレームワークを構築した. 汎用 OS には, シーケンス番号の送信を SafeG に依頼するための機能を追加した. SafeG には, 汎用 OS から送られたシーケンス番号と, 汎用 OS のコンテキスト情報を RTOS に通知する機能を加えた. RTOS では,SafeG によって得られた情報から, 汎用 OS の動作状況を確認する機能を追加した. また, ユーザの記述コード量削減のために, 以上で述べた監視機構の自動コンフィギュレーションを行うフローについても提案を行った.

評価実験として,SafeG のプログラムサイズ増加量, 監視を行う際に生じる汎用 OS と RTOS のオーバーヘッド, 異常検出時間, コンフィギュレーションによる記述コード削減量を測定した. その結果, 汎用 OS から RTOS へシーケンス番号を送信する時間は 23μs 以内, シーケンス番号が異なるときや, 送信元アドレスが異なるときの異常検出時間は 21μs 以内,RTOS で汎用 OS から送信されたシーケンス番号確認に要する時間は 17μs 以内であることが確認でき,SafeG のプログラムサイズの増加量は.text セクションの 160 バイトであった. これらの結果より, 検証容易性やリアルタイム性を十分確保できることが確認できた. また, 監視機構作成の自動コンフィギュレーションを行うことで, ユーザが記述するコード行数が 165 行減少することが確認でき, ユーザによる機能の追加や修正が容易であることが確認できた. 以上より,SafeG を用いて RTOS から汎用 OS を監視することが可能なことを示した.