動的コード書き換えによる組込み Linux の セキュリティ向上技術の開発

○大原　衛[*1)]、岡野　宏[*2)]

１．はじめに

近年、ネットワークに接続される組込み機器が急速に普及している。本研究では、組込み機器のためのバッファオーバフロー攻撃対策技術を開発した。図１に示したように、バッファオーバフローは、最もよく見られるソフトウェア脆弱性の 1 つである。

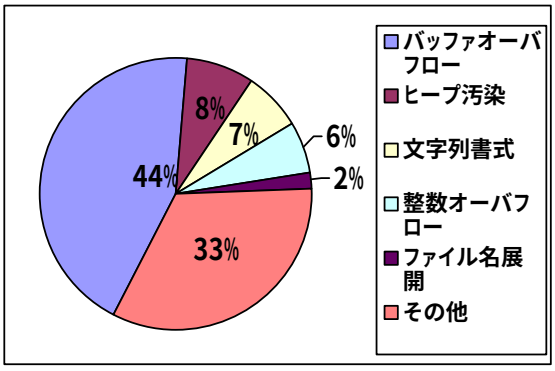

図１　2000-2003 年 CERT 報告に見られる脆弱性の分類

２．開発手法によるバッファオーバフロー対策

バッファオーバフロー攻撃は、以下のようにして行われる。一般に、ソフトウェアはサブルーチンの集合として構築される。サブルーチン S_A がその作業途中でサブルーチン S_B を利用するとき、S_A は作業の途中経過 X をメモリ内の領域 R_X に保存し、S_B に制御を移す。S_B は、R_X に隣接した領域を作業領域として用いる。ここで、S_B が外部からの入力を受け取ると仮定する。攻撃者は、S_B に多量の入力を与えることで、S_B の作業領域をあふれさせ、X を上書きする。S_B は、作業を完了すると、R_X に X が保存されているものとして S_A に制御を戻そうとする。しかし、R_X が不正に書き換えられているために、正しく処理を継続できない。

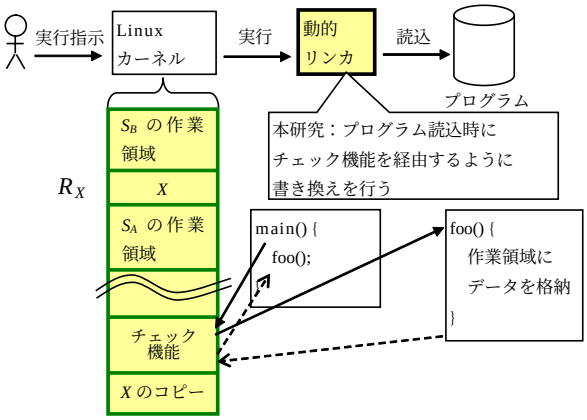

図２　開発手法の概要

このような攻撃に対応する手法として、X の上書きを防止する方法と、X が上書きされた際に対応を行う方法が考えられる。本研究では、S_A が S_B を呼び出す際にメモリ内の別領域に X のコピーを保存し、S_B が S_A に制御を戻す際に X の整合性チェックを行うことで、上書きに対応する手法（図２）を開発した。このチェック機能の実装には、ソフトウェアの動的書き換えを利用した。動的書き換えを用いることで、新規に開発するソフトウェアだけでなく、既存のソフトウェア資産の脆弱性にも対応することができる。

３．結果・考察

ネットワークに接続される組込み機器では、英 ARM 社のプロセッサと Linuxを組み合わせた環境が頻繁に利用されている。本研究では、この環境向けに試験的な実装を行い、評価を行った。１回のサブルーチン呼び出しに対して、チェックのために必要な追加的な命令量は、約 20 語であった。また、チェックを行うことによる時間オーバヘッドは、全体の１割弱であり、リアルタイム性の低い応用には適用可能であると考えられる。

４．まとめ

組込み機器向けのセキュリティ向上技術を開発した。今後、試験実装を発展させ、より多くの環境に対応させるための移植性と、性能の向上について検討する。

---

*1) IT グループ、*2) エレクトロニクスグループ