L-004

Packet Filtering Unit の評価

Evaluation of Packet Filtering Unit

○齊藤圭介† 伊丸岡修哉† 佐藤友暁‡ 深瀬政秋†

Keisuke Saito Shuya Imaruoka Tomoaki Sato Masa-aki Fukase

1. はじめに

近年、インターネットは回線の高速化や無線 LAN の普及など、接続環境の拡大と多様化が進んできた。それに伴いインターネットを利用した犯罪も増加し、大きな問題となっている。代表的なものは、コンピュータウィルスや不正アクセスによる情報漏えいなどである。

不正アクセス対策として IDS (Intrusion Detection System)と IPS(Intrusion Protection System)がある。現在主にコンピュータにおいて使用されているのはソフトウェアの IDS/IPS であるが、CPU やメモリのリソースを消費してしまう問題がある。そこで我々の研究室では、ハードウェア上で不正アクセスを処理することによりリソースの消費から CPU やメモリを解放し、また低消費電力で動作することによってモバイルコンピュータにおいても利用可能な H-HIPS (Hardware-based Host Intrusion Protection System)の開発に取り組んでいる。

本研究の目的は、H-HIPS の検知シグネチャの削減である。Packet Filtering Unit は H-HIPS に既存のファイアウォールユニットを改良したものである。従来のファイアウォールユニットは動作が高速であるが、対象とするポート番号を変更する度に回路を合成しなくてはならない。しかし、Packet Filtering Unit は基本的にホワイトリスト以外の通信を許可せず、ポートの開閉を動的に行うので従来よりも多くの危険からコンピュータを防御する。今回はこの Packet Filtering Unit の評価を行う。

2. H-HIPS

H-HIPS は、従来のソフトウェアベースなホスト型 IPS をハードウェアベースにしたものである。ハードウェアベースにすることにより、監視対象とするコンピュータ自身に導入する必要が無くなるため、各々のコンピュータは CPU やメモリのリソース消費の問題から解放される。また、機能面でも従来のホスト型やネットワーク型の IDS の問題点を解消している。

H-HIPS は、ハードウェアとして回路の書き換えや更新が容易な FPGA(Field Programmable Gate Array)を用いている。そのため、今後出現する新たな不正アクセスやコンピュータウィルスに対しても防御ユニットを追加することで柔軟に対応する。H-HIPS の構成を図 1 に、H-HIPS と従来のソフトウェアベースな IDS との比較を表 1 に示す。

†弘前大学大学院理工学研究科 Graduate School of Science and Technology, Hirosaki University

‡弘前大学総合情報処理センター Information Processing Center, Hirosaki University

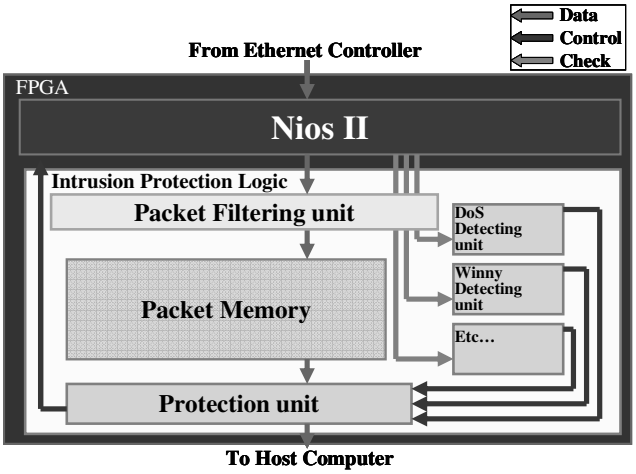

図 1.H-HIPS 構成

表 1.H-HIPS と従来の IDS の比較

	監視対象	リアルタイム検知	LAN内部での検知	パケットレベルの詳細な分析	CPUリソースの消費
NIDS	パケット	可	不可	可	なし
HIDS	OSのログ etc.	不可	可	不可	あり
H-HIPS	パケット	可	可	可	なし

3. 従来の H-HIPS 用ファイアウォールユニット

現在、H-HIPS に搭載されているファイアウォールユニットは、シンプルな回路で実現しているので動作が高速である。しかし、ポートの開閉は静的であり、変更する場合はその度に回路の論理合成が必要となる。そのため、回路の書き換えが容易な FPGA 以外での利用は難しく、汎用性に欠けるという問題がある。

4. Packet Filtering Unit

Packet Filtering Unit は、クライアント側での使用を想定している。通信要求の際の送信元ポート番号と応答の際の宛先ポート番号とに着目し、図2のアルゴリズムを作成した。Packet Filtering Unit の挙動を以下に示す。

まず、通信の要求を行った際に、送出したパケットの TCP ヘッダから送信元ポート番号を記憶し、それと同時に時間計測を始める。次に、応答の際に受信したデータのパケッ

トから宛先ポート番号を記憶する。この宛先ポート番号と通信を許可するポート番号が記載されたホワイトリストとを比較し、一致しなかった場合は通信要求の際に記憶された送信元ポート番号と比較を行う。

比較の結果、このどちらの比較にも一致しなかった場合は、不正な通信であると判断して通信を防御する。逆に、どちらか一方で一致すれば正常な通信であると判断され、H-HIPS に搭載されている他の防御ユニットへと渡される。また、記憶されたそれぞれの送信元ポート番号が、設定した時間閾値を超えていた場合には時間超過であると判断され、宛先ポート番号との比較の際に比較対象としないため通信は防御される。これにより、一度通信を許可されたポートがそのまま開放状態を維持することを防ぐので、セキュリティホールは減る。Packet Filtering Unit の開発環境を表 2 に示す。

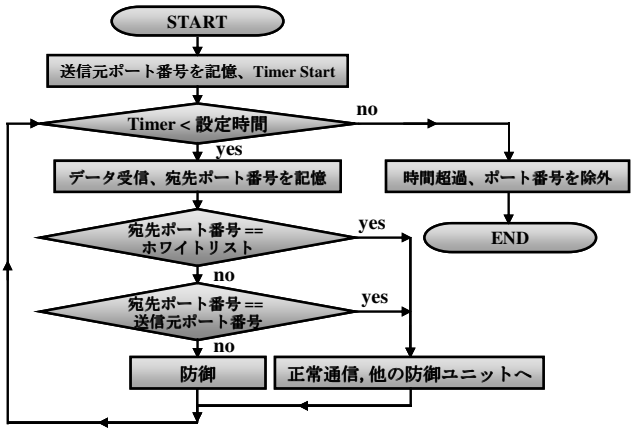

図 2.Packet Filtering Unit アルゴリズム

表 2.開発環境

OS	Microsoft Windows XP
CPU	Intel Pentium4 (3.0GHz)
Main Memory	1 Gbyte
CAD	Altera QuartusII v5.0
FPGA	Cyclone EP1C20F400C7

5. シミュレーション

QuartusⅡを用いて、作成した Packet Filtering Unit のシミュレーションを行った。シミュレーションの実行結果を図 3 に示す。比較において、ホワイトリストに記載されたポート番号と一致した場合、送信元ポート番号と一致した場合、そのどちらのポート番号とも一致しなかった場合、送信元ポート番号が設定した時間を超過していた場合のそれぞれの場合で正常な結果が出力されていることが図 3 から確認出来る。

6.評価

Packet Filtering Unit のスペックを表 3 に示す。最大遅延時間より、Packet Filtering Unit は 80MHz での動作が可能である。これは、NIC(Network Interface Card)で用いる PCI バスの動作周波数である 66MHz を満たしている。また、現在の H-HIPS 用ファイアウォールユニットは通常 50MHz で動作しているため、Packet Filtering Unit は従来よりも高速な動作が可能である。

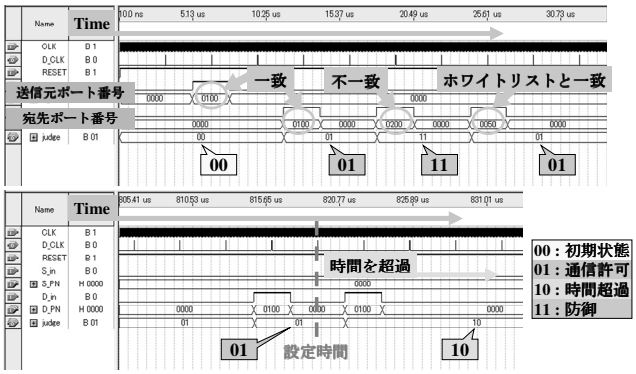

図 3.シミュレーション実行結果

表 3.Packet Filtering Unit のスペック

	Packet Filtering Unit
Total logic elements	**409 / 20,060**
Total pins	**39 / 301**
Total memory bits	**0 / 294,912**
Clock frequency	**80MHz (12.5ns)**
Maximum time delay	**11.904 ns**

7.まとめ

本研究では、動的なポートの開閉によりセキュリティホールの削減や他の防御ユニットの処理を効率化する Packet Filtering Unit の作成、及び QuartusⅡ上でのシミュレーションを行い、その評価を行った。今後の課題としては、Packet Filtering Unit の FPGA 上での実機検証等が挙げられる。

8.参考文献

[1] T.Sato and M.Fukase, ”Reconfigurable Hardware Implementation of Host-Based IDS,” Proc.of IEEE The 9th Asia-Pacific Conference on Communicat -ions,Vol.2, pp849-853,2003.

[2] 菊池一平、佐藤友暁、深瀬政秋 「ハードウェア化不正アクセス防御システムの開発」 平成 19 年度電気関係学会東北支部連合大会,p106,2007.

[3] 菊池一平、佐藤友暁、深瀬政秋 「不正アクセス防御システムのハードウェア実装」情処研報,2007-CSEC-39,pp. 13-18,2007.

[4] T.Sato, K.Kikuchi, S.Imaruoka, and M.Fukase, ”DoS Attack Analysis for H-HIPS,” Proc. of IMETI, Vol.Ⅱ,pp.110-115,2008.