様式 C-19

科学研究費補助金研究成果報告書

平成２１年　６月　１日現在

研究種目：若手研究　(B)
研究期間：2007　～　2008
課題番号：19700050
研究課題名（和文）　高検知精度アノマリ分析機能を有する高速・低消費電力動作ホストベースＩＰＳの開発
研究課題名（英文）　Development of High-Speed, Low-Power and High Detection Accuracy HIPS with Anomaly Analysis Function
研究代表者
佐藤　友暁（SATO TOMOAKI）
弘前大学・総合情報処理センター・准教授
研究者番号：00336992

研究成果の概要：
本研究は，モバイルコンピュータを安全・安心に使用できるために不可欠な不正アクセス防御システムの開発である。本システムは再構成可能なハードウエアである FPGA (Field Programmable Gate Array)を使用した。本システムの開発に不可欠なノマリ検知方式による DDoS (Distributed Denial of Service)攻撃防御ユニット，システム全体の低消費電力化のためのファイアウォールユニット，情報流出を防ぐファイル交換ソフトウエア検知ユニットの開発を行った。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,300,000	0	1,300,000
2008 年度	1,800,000	540,000	2,340,000
年度			
年度			
年度			
総　計	3,100,000	540,000	3,640,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：セキュアネットワーク，ＩＤＳ，ＩＰＳ，低消費電力

１．研究開始当初の背景

インターネットにおける不正アクセスは今日の重要な問題である。特に個人のパソコンの使用環境においては，以下の理由により不正アクセスの被害，踏み台に利用された被害，情報流出の被害が深刻になっている。
・PC の管理が徹底されていない（セキュリティパッチの不徹底，アンチウィルスソフトウェアのパターンファイル更新の不徹底）
・常時接続・ブロードバンド化の一般化
・公衆無線 LAN アクセスポイント (AP)の普及
・Winny 等の P2P (Peer to Peer)ファイル交換ソフトウェアの普及

これらの問題に対し，IDS (Intrusion Detection System) や IPS (Intrusion Prevention /Protection System)による監視と被害防止が不可欠である。現在の IDS と IPS の問題点を設置場所による分類で整理すると次の通りである。

（１）　ホストベース IDS/IPS

①　　検知処理において CPU を使用するた

め，CPU リソースやバッテリ電力を消費する
② CPU 負荷の高いパケットレベルでの詳細な解析は不可能
③ CPU 負荷が高くなる高精度のアノマリ検知が不可能

（2） ネットワークベース IDS/IPS
① LAN 内部のクライアント間で発生する検知が不可能
② ネットワークを流れるパケット量によっては，すべてのパケットを解析不可能
③ IDS/IPS 処理専用の高性能計算機が必要（ソフトウェアを含め非常に高価です）

従来の IDS/IPS の問題点を解消し，モバイル機器や組込み機器で使用可能な低消費電力で動作する，高検知精度アノマリ分析機能を有する IPS の開発が不可欠である。

２．研究の目的

本研究の目的は，高速・低消費電力で動作が可能であり，高検知精度アノマリ分析機能を有するホストベースの IPS を開発することで，従来の IDS や IPS の問題を解消することである。

３．研究の方法

高検知精度アノマリ分析機能を有するホストベースの IPS を開発することを目的として，以下について取り組んだ。

（1）アノマリ分析機能の開発

ホストベースの利点を生かし，FPGA (Field Programmable Gate Array)のネットリストで構成されたファイアウォール機能を併用し，送受信が許可されたポート以外での通信を遮断することでアノマリベース検知アルゴリズムをシンプルにする。

（2）Winny による情報流出防御ユニットの実装

情報漏洩の主な原因である Winny 利用による情報流出にたいし早急に対処する必要がある。Winny 検知アルゴリズムをハードウエア IPS へ組み込むことで，情報漏えい防御へ対処させる。

（3）ファイアウォールユニットの開発

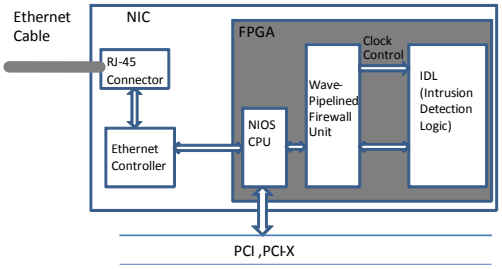
検知ユニットの削減およびハードウエアベース IPS の消費電力の削減を目的としたファイアウォールユニットの開発を行う。また，ファイアウォールユニットで検知ユニットのクロックを制御することで，システム全体の低消費電力化を実現する。

（4）パケットレベルにおける不正アクセスの観測と不正アクセスのパターンの解析

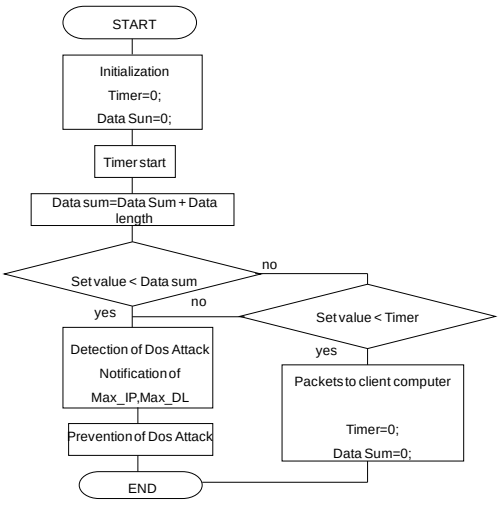
不正アクセスの手法は日々変化している。常に新しい情報を入手する環境を構築することで，パケットレベルにおける不正アクセスの観測と不正アクセスのパターンの解析を行う。

４．研究成果

本研究では，下図に示す H-HIPS (Hardware-based HIPS)の不正アクセスや情報漏洩の防御機能および H-HIPS で使用する LUT の削減および消費電力の削減を目的としたファイアウォールユニットの開発を行った。



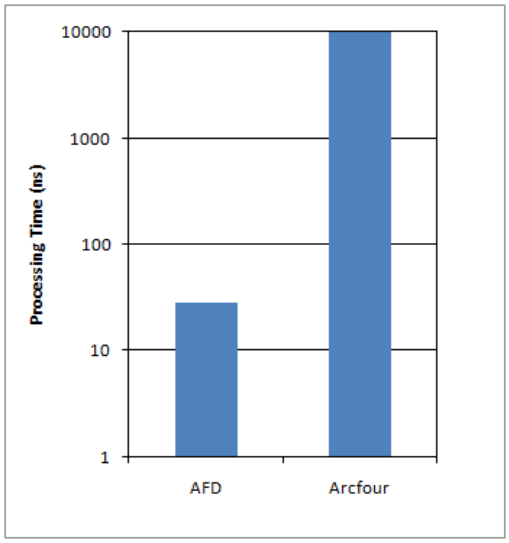
H-HIPS (Hardware-based HIPS)の特徴である FPGA (Field Programmable Gate Array)の特徴を生かし，アノマリ検知方式による DDoS (Distributed Denial of Service)攻撃防御ユニットの開発を行った。DDoS 攻撃への対処方法はこれまで限られているが，本研究の成果によって多様な DDoS 攻撃からコンピュータシステムの防御が可能になる。下図は，本研究で開発した DDoS 攻撃防御ユニットのアルゴリズムである。このアルゴリズムを低消費電力型の FPGA を使用してプログラムした結果，2.6Gbps 動作することが確認された。



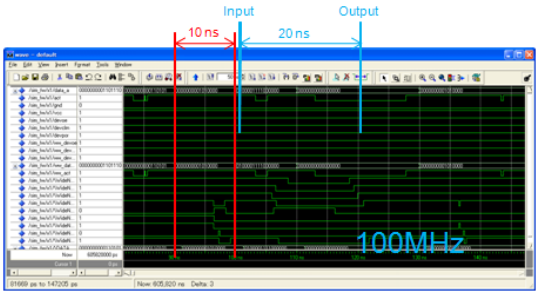
る P2P (Peer to Peer)ソフトウエアによる情報漏えいへ対処するために，ファイル交換ソフト検知ユニットを現在開発中の IPS へ組み込むことを提案し，開発を進めている。ファイル交換ソフトのパケットレベルでの動作を調査するために，ファイル交換ソフト調査用ネットワークを構築した。その結果をもとに，ファイル交換ソフト検知ユニットのビヘービアモデルを開発した。

本機能の実現によって CPU (Central Processing Unit)に負荷をかけることなく，現在個人用パソコンにおいて一般的なギガビットイーサネットにおけるホストベースでのリアルタイム検知が可能になり，アプリケーションの干渉による障害リスクがなくなる。

下図は Winny で使用されている RC4 を低消費電力型の FPGA に実装した AFD と 2.4GHz で動作する CPU を使用した Arcfour の処理時間を示したものである。この結果より，FPGA を使用して処理することで大幅な高速化が達成されることが明らかにされた。



FPGA のリソースを最大限に活用するために，ホストベース IPS で必要とする検知機能を削減することを目的として，LUT で構成するファイアウォール機能を開発した。また，その機能をウェーブパイプライン動作させることに成功した。その結果，IPS 回路全体の高速化および消費電力の大幅な削減に成功した。この結果現在個人用パソコンにおいて一般的なギガビットイーサネットにおけるホストベースでのリアルタイム検知が可能であることを明らかにした。下図はウェーブパイプライン手法によって，２倍速で動作している状態を示したものである。



キャンパスネットワークにおける Winny の利用を検知するための手法を提案した。また，出張先において，公衆無線 LAN (Local Area Network)やインターネットカフェ等のセキュリティ状況についてまとめた。この結果をもとに新たな検知アルゴリズムの検討をおこなうことが可能になった。

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 19 件）

① Tomoaki Sato, Shuya Imaruoka, and Masa-aki Fukase, ″System-Level Control for Low-Power Consumption on Winny Detection System,″ Proc. of ICESIT2009, pp. 10-14, 2009. 査読有

② Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, “Reconfigurable Firewall Unit by Wave-Pipelined Operations,” Proc. IEEE ISPACS2008, pp. 449-452, 2009. 査読有

③ Masa-aki Fukase, Kazunori Noda, and Tomoaki Sato, “Emerging Hardware Cryptography and VLSI Implementation,” Proc. of ISPACS, pp. 445-448, 2009. 査読有

④ Masa-aki Fukase, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, “Design and Chip Implementation of the Ubiquitous Processor HCgorilla,” Proc. of ASP-DAC, pp. 129-130, 2009. 査読有

⑤ Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, “FPGA Implementation of Winny Packets Detection for Mobile Computing,” Proc. of IEEE ISCIT 2008, pp.204-209, 2008. 査読有

⑥ Masa-aki Fukase and Tomoaki Sato, “A Ubiquitous Processor Free from Instruction Scheduling,” Proc. of ISCIT, pp. 75-80, 2008. 査読有

⑦ 佐藤友暁，伊丸岡修哉，深瀬政秋，“キ

ャンパスネットワークにおける Winny 検知手法の FPGA 実装," 学術情報処理研究, No. 12, pp. 68-74, 2008. 査読有

⑧ Masa-aki Fukase and Tomoaki Sato, "Compact FPU Design and Embedding in a Ubiquitous Processor for Multimedia Performance Enhancement," ECTI-EEC Trans. Vol. 6, No. 2, pp. 79-85, 2008. 査読有

⑨ Masa-aki Fukase and Tomoaki Sato, "Compilation Techniques Specific for a Hardware Cryptography-Embedded Multimedia Mobile Processor," Journal of Systemics, Cybernetics and Informatics, Vol.5 No, 6, pp. 13-21, 2008.査読有

⑩ Tomoaki Sato, Kazuhira Kikuchi, Syuya Imaruoka, and Masa-aki Fukase, ″DoS Attack Analysis for H-HIPS,″ Proc. of IMETI, Vol. II, pp. 110-115, 2008. 査読有

⑪ Masa-aki Fukase and Tomoaki Sato, "Development of Parallelizing Compilers of a Ubiquitous Processor," Proc. of WMSCI2008 Vol. II, pp. 220-225, 2008. 査読有

⑫ Masa-aki Fukase, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, "Enhancing Multimedia Processing by Wave-Pipelining Integer Units and Floating Point Units in Whole," Proc. of ECTI-CON 2008, IEEE Xplore, pp. II-681-II-684, 2008. 査読有

⑬ Tomoaki Sato, Kazuhira Kikuchi, Shuya Imaruoka, and Masa-aki Fukase, ″Low-Power Scheme of Portscan Detection Unit by Using Embedded Technology,″ Proc. of ICESIT2008, pp.122-125, 2008. 査読有

⑭ Masa-aki Fukase, Hiroki Takeda, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, "Ad-hoc Cipher by a Ubiquitous Processor," Proc. of ICESIT, pp. 118-121, 2008. 査読有

⑮ Tomoaki Sato, Kazuhira Kikuchi, and Masa-aki Fukase, ″Port-Scan Detection Unit for H-HIPS,″ Proc. of CITSA2007, Vol. II, pp. 250-255, 2007. 査読有

⑯ Masa-aki Fukase and Tomoaki Sato, "A Stream Cipher Engine for Ad-hoc Security," Proc. of CIS'2007, pp. 902-906, 2007.査読有

⑰ Masa-aki Fukase, Kazunori Noda, Hiroki Takeda, and Tomoaki Sato, "Multimedia Performance of a Ubiquitous Processor," Proc. of ISCIT2007, pp. 1464-1469, 2007. 査読有

⑱ Masa-aki Fukase, Hiroki Takeda, and Tomoaki Sato, "Hardware/Software Co-Design of a Secure Ubiquitous System," Computer Intelligence and Security, Springer Berlin/Heidelberg, LNCS Vol. 4456/2007, pp. 385-395, 2007. 査読有

⑲ Masa-aki Fukase and Tomoaki Sato, "Exploiting Design and Testing Methods of High-Speed Power Conscious Wave-Pipelines," Proc. of NASA2007, pp. 5.1.1-5.1.6, June 2007. 査読有

〔学会発表〕(計 16 件)

① 齊藤圭介, 伊丸岡修哉, 佐藤友暁, 深瀬政秋,「不正アクセス検知ユニットの改良」情報処理学会東北支部研究会, 2008 年 12 月 16 日, 弘前. 査読無

② 佐藤友暁,「海外のネット事情」第 20 回情報処理センター等担当者技術研究会, 2008 年 8 月 28 日, 弘前. 査読無

③ 齊藤圭介, 伊丸岡修哉, 佐藤友暁, 深瀬政秋,「ネットワークプロセッサの実用化に関する研究」, 平成 20 年度電気関係学会東北支部連合大会, pp. 98, 2008 年 8 月 22 日, 郡山, 査読無

④ 伊丸岡修哉, 齊藤圭介, 佐藤友暁, 深瀬政秋,「ファイル交換ソフトウェアへのハードウエア対処」pp. 100, 2008 年 8 月 22 日, 郡山, 査読無

⑤ 野田一訓, 横山温子, 武田宏樹, 深瀬政秋, 佐藤友暁,「実行段の多機能ウェーブ化によるマルチメディア機能強化」信学技報, Vol. 107, No. 508 (VLD2007-157, ICD2007-180), pp.7-12, 2008 年 3 月 7 日, 那覇. 査読無

⑥ 武田宏樹, 野田一訓, 深瀬政秋, 佐藤友暁,「ユビキタスプロセッサ HCgorilla の改良」信学技報, Vol. 107, No. 508 (VLD2007-157, ICD2007-180),pp.31-36, 2008 年 3 月 7 日, 那覇. 査読無

⑦ 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エア実装」情処研報 2007-CSEC-39, Vol. 2007, No. 126, pp. 13-18, 2007 年 12 月 14 日, 東京.査読無

⑧ Kazunori Noda, Hiroki Takeda, Masa-aki Fukase, and Tomoaki Sato, "Multimedia Performance of a Ubiquitous Processor," 平成 19 年度電気関係学会東北支部連合大会, p16, 2007 年 8 月 23 日, 弘前, 査読無

⑨ 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 年 8 月 24 日, 弘前, 査読無

⑩ 伊丸岡 修哉，成田 圭一，菊池 一平，佐藤 友暁，深瀬 政秋,「Winny 防御ユニットの実用化」平成 19 年度電気関係学会東北支部連合大会，p107，2007 年 8 月 24 日，弘前，査読無
⑪ 武田宏樹，野田一訓，深瀬政秋，佐藤友暁,「HCgorilla の大規模化に関する研究」平成 19 年度電気関係学会東北支部連合大会，p188，2007 年 8 月 24 日，弘前，査読無
⑫ 横山温子，武田宏樹，野田一訓，深瀬政秋，佐藤友暁,「HCgorilla のハードウェア/ソフトウェア協調設計に関する研究」平成 19 年度電気関係学会東北支部連合大会，p189，2007 年 8 月 24 日，弘前，査読無
⑬ 岩本祐顕，天間僚，武田宏樹，野田一訓，深瀬政秋，佐藤友暁,「マルチメディアストリーム暗号エンジン」平成 19 年度電気関係学会東北支部連合大会，p194，2007 年 8 月 24 日，弘前，査読無
⑭ 伊藤智恵美，深瀬政秋，佐藤友暁,「ユビキタスプロセッサ HCgorilla 用並列化コンパイラの開発研究」平成 19 年度電気関係学会東北支部連合大会，p98，2007 年 8 月 24 日，弘前，査読無
⑮ 野田一訓，武田宏樹，深瀬政秋，佐藤友暁「HCgorilla のマルチメディア機能強化」情処研報（情報処理学会研究報告），Vol. 2007，No. 58，(2007-DPS-131)，pp. 85-90，2007 年 6 月 6 日，盛岡.査読無
⑯ Masa-aki Fukase and Tomoaki Sato，“Design Techniques of Wave Pipelines,” IEICE Technical Report，ICD2007-28，pp. 67-72，2007 年 5 月 31 日，川崎.査読無

〔図書〕（計 1 件）
① 深瀬政秋，佐藤友暁,「組み込み技術の基礎」津軽地域の産業活性化人材養成事業メカトロニクスシステム要素技術研修テキスト，弘前大学消費生活共同組合，2008 10 月

６．研究組織
(1)研究代表者
佐藤 友暁（SATO TOMOAKI）
弘前大学・総合情報処理センター・准教授
研究者番号：00336992

(2)研究分担者

(3)連携研究者