L-001

SHA-1,RC6 復号ユニットによる Share 検知

Share detecting by SHA-1 and RC6 decrypting Unit

伊丸岡 修哉† 佐藤 友暁‡ 深瀬 政秋†
Imaruoka Syuya Sato Tomoaki Fukase Masaaki

1．はじめに

近年のファイル共有ソフトは非常に有用である反面、ウイルスによる個人情報や機密情報の漏洩が深刻な問題となっている。さらに P2P(peer-to-peer)ネットワークがトラフィックを増大させることによる帯域の圧迫、流通するファイルのほとんどが著作権を侵害している問題についても議論されている。そのためシステム管理者側はファイル共有ソフトについて適切に対処する必要がある。

本研究では、その普及とともに情報流出事件の原因に挙がる機会が増加している Share を取り上げる。我々は既に国内で最も広く使われている Winny に対して、H-HIPS (Hardware-Base Host Intrusion Prevention System)に検知ユニットを組み込むことによる対策を提案しており、同様に Shar 検知ユニットを H-HIPS に組みこむ。暗号化されている Share の通信を復号して検知を行うためには SHA-1、RC6 復号ユニットが必要となるため、この制作を行った。

2．H-HIPS

ソフトウェアによる IPS や IDS では、ネットワーク型では回線速度や高性能な専従機を、ホスト型ではコンピュータリソースを消費するというデメリットが存在する。当研究室で開発されている H-HIPS は高速な処理が可能であるハードウェアの利点を生かし、前述のデメリット無しにリアルタイム処理を行う IPS である。図 1 に示すように H-HIPS は NIC(Network Interface Card)上に組み込むことを想定している。Nios プロセッサにより検知部分を抽出し、複数の検知ユニットが並列して検査することでそのパケットに含まれる攻撃の有無を判断し、通過の可否を判定・実行する。各不正アクセスの特徴をとらえた検知ユニットを開発することで、取りこぼしの無い正確な検知が可能である。検知ユニットを FPGA 上に設計することで、搭載するコンピュータの用途に応じた構成の変更が容易であり、新たな検知対象に対しても防御回路を追加することで柔軟に対応することが可能である。

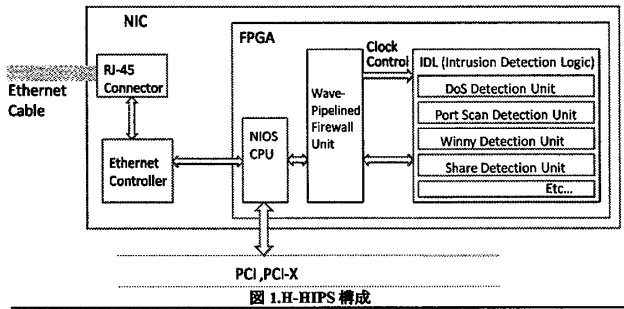

図 1.H-HIPS 構成

†弘前大学理工学研究科電子情報システム工学専攻
Graduate School of Science and Technology, Hirosaki University
‡弘前大学総合情報処理センター
C&C Systems Center, Hirosaki University

3．Share

Share は Winny の後継を目指して開発されたファイル共有ソフトである。Winny の作者逮捕以降に利用者を拡大するとともに、Share を原因とする情報漏えい事件の件数も増加している。H-HIPS はパケットに含まれる情報から検知を行うが、Share では使用する通信ポートは任意に設定されること、通信は公開鍵方式で暗号化されることからそれぞれ決定的な検知法とはなりえない。Share で接続される側のノードとなった場合に限れば、接続要求ノードからのポートスキャンを受けるため、H-HIPS にすでに組み込まれている Port Scan Detection Unit での検知が可能である。我々は接続の方向に関わらない検知を可能にすべく、Share のネットワークに参加する際、起動中のノード少なくとも 1 つとコネクションを張る必要がある点に注目した。検知アルゴリズムを下図 2 で示す。

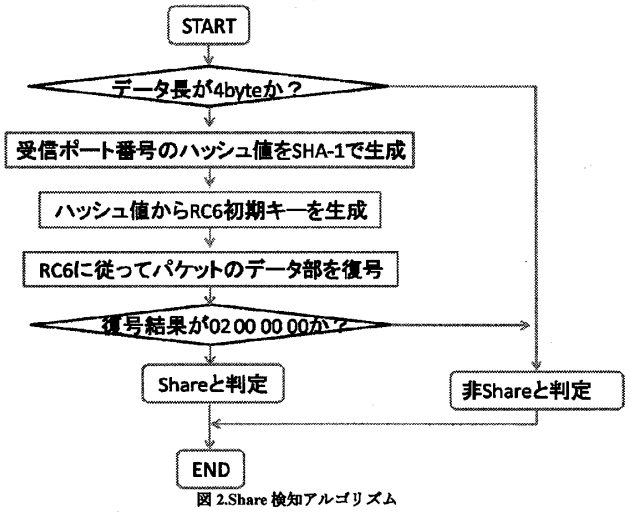

図 2.Share 検知アルゴリズム

4．SHA-1

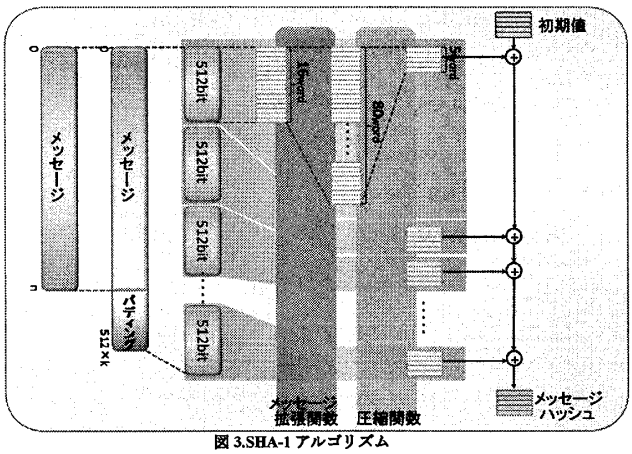

図 3.SHA-1 アルゴリズム

SHA-1[1]アルゴリズムは TLS/SSL・PGP・IPSec・SSH 等に

広く使われているハッシュアルゴリズムである。図 3 で示すように、可変長のメッセージを拡張・圧縮することで、最終的に 160bit のハッシュを生成する。Share においては、RC6 復号・暗号キーに必要な、ポート番号のハッシュ値を求めるために用いられている。

今回作成した検知ユニットでは、メッセージはデータ長一定の受信ポート番号(16bit)であるため、パディングの処理を省略した構成となっている。また、拡張メッセージを格納する領域として FPGA のプリミティブな記憶領域であるブロック RAM を割り当てた。図 4.は作成した SHA-1 ユニットに対する既知の入力データによる動作確認、ポート番号を入力したシミュレーション結果である。

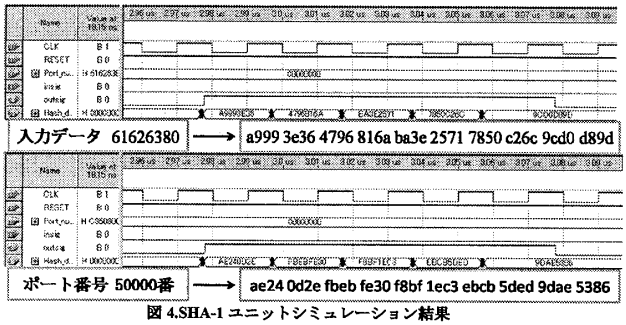

図 4.SHA-1 ユニットシミュレーション結果

5．RC6

RC6はRonald Rivestら[2]によって1998年に開発された共通鍵暗号方式である。NIST(National Institute of Standards and Technology)によるAES (Advanced Encryption Standard)選定の最終候補の 1 つになったが採用されなかった。しかし、ビットローテートを基調としたその高速な暗号化[3]には定評があり、Shareにおいても暗号アルゴリズムに採用されている。

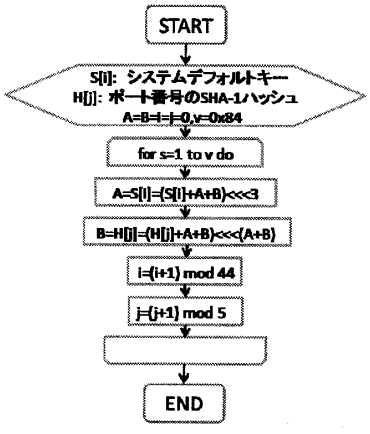

図 5.RC6鍵生成アルゴリズム

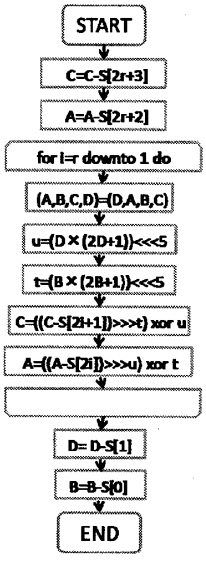

図6.RC6復号アルゴリズム

ポート番号のSHA-1ハッシュ値と、Shareのマジックナンバーから図5に示したRC6鍵生成アルゴリズムに従ってRC6ラウンド鍵S[i]を得る。次に、得られたS[i]を用いて図6.で示すRC6復号アルゴリズムに従って4byteのパケットデータ部を復号する。A,B,C,Dには開始時には暗号文が、終了時には平文が格納される。Shareのネットワーク接続のためのパケットである場合、復号されたデータ部は02 00 00 00となる。

	Logic Element数	memory bit数	Time	消費電力
SHA-1 Unit	1107	2048	3.1μs (50MHz)	120.04mW
RC6 Decryption Unit	3754	512	15.2μs (66MHz)	160.14mW
Share Detection Unit	5123	2560	23.4μs (50MHz)	192.26mW

図 7.シミュレーション結果

SHA-1 ユニット、RC6 復号ユニットおよび二つを組み合わせた Share 検知ユニットのシミュレーション結果を図 7 に示す。この検知ユニットのスループットは以下の式で求められ、

$$TP = f \times W \times \frac{L_{Frame}}{L_{Data}}$$

f : クロック周波数(=50MHz)

W : Share 検知ユニットのワード幅　(=16bit)

L_{Frame} :　フレームのデータ長 (64byte*)

L_{Data} : 検知対象のデータ長 (20byte)

TP=2.560 (Gbit / sec) が得られる。これはギガビットイーサへの対応が可能であることを示している。

6．おわりに

今回 Share の通信方式に注目し、SHA-1 ユニット・RC6 復号ユニットを組み合わせることで Share 検知ユニットを作成した。作成したユニットに実際のパケットデータを入力することで正常な検知が可能であることを確認した。今後の課題としては、SHA-1 ユニットの動作周波数がボトルネックになり、全体が 50MHz での動作になっている点について、PCI バスの動作周波数である 66MHz を超えるように改良を加えること。および、ネットワーク環境で検証することで、既成のソフトウェア IPS と比較した際の検知率・通信速度の比較が挙げられる。

参考文献

[1] National Institute of Science and Technology, "Secure Hash Standard", Federal Information Processing Standard (FIPS) 180-1, 1993 年

[2] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin , "The RC6 Block Cipher", RSA, The Security Division of EMC,1998年

[3] 鈴木裕信,『AESファイナリストをめぐって～暗号最新動向/鈴木裕信』, 共立出版 Bit 2000年4月号 (pp17-pp24),2000年

[4]長谷川揚平,山田裕,出口勝昭,安生健一郎,粟島亨,天野英春『リコンフィギャラブルプロセッサ上でのブロック暗号RC6の実装』,情報処理学会報告.SLDM 2004(5) (pp29-34),2004年

[5]鵜飼祐司,『P2PソフトShareの暗号を解析，ネットワーク可視化システムを開発』,ITmedia,2007年