スイッチ間の連携による内部ネットワークセキュリティ向上機構

佐川昭宏† 高橋ひとみ‡ 斉藤匡人‡ 間博人‡ 徳田英幸†,‡

† 慶應義塾大学 環境情報学部, ‡ 慶應義塾大学大学院 政策・メディア研究科
{sagawa, hitomi, masato, haru, hxt}@ht.sfc.keio.ac.jp

インターネットなど外部ネットワークから企業などの内部ネットワークに対する攻撃が増加し，情報の改竄や，管理者権限の奪取などさまざまな問題を引き起こしている．そこで，それらを防ぐファイアウォールや侵入検知システム (IDS) などの解決策が広く使われている．しかしこれらの対策は内部ネットワーク内の攻撃を想定していないため，内部ネットワークにおいても安全性を向上させる必要がある．そこで，ネットワークスイッチに変更を加え，安全性を向上させる機構 Dynamic DeFense Switch (DDFS) を提案する．DDFS によって，この問題を解決し，より安全なネットワークを提供する．

A Local Network Security Improvement System Using Cooperation Between Switches

Akihiro Sagawa† Hitomi Takahashi‡ Masato Saito‡ Hiroto Aida‡ Hideyuki Tokuda†,‡

†Faculty of Environmental Information, Keio University
‡Graduate School of Media and Governance, Keio University

Increasing computer security attacks from external networks like the Internet to internal local area networks (LAN) like office networks, lead to some problems such as falsification of information and loss of administrative right. There are some widely used defense systems against these attacks — firewall and an Intrusion Detection System (IDS). However, these defense systems do not assume any attacks between LAN hosts. We should pay attention to security for LAN and its hosts. We propose Dynamic DeFense Switch (DDFS) which improves existing LAN switches. DDFS solves the LAN security problems and realizes the more secure LAN.

1 はじめに

インターネットの拡大に伴い，企業やキャンパスネットワークなどの内部ネットワークがインターネットに接続する機会が増加し，高速・安価な回線の普及によってインターネットに常時接続することが可能となった．しかし，インターネット利用の機会が増加するとともにインターネットを経由した不正アクセスや脆弱性の事前調査などに接する機会も増加している．

不正アクセスなどによって，組織内ネットワークのホストに外部から侵入された場合，侵入者は外部からは直接侵入できない内部ネットワークに侵入ホストを介して接続できる．その結果侵入者は内部ネットワークを調査し，より機密性の高い別のホストを攻撃することが可能である．しかし，現在の防御システムであるファイアウォールや侵入検知システム (IDS) は，主に内部ネットワークと外部ネットワークの境界で動作するため，内部ネットワーク内で行われる侵入者の調査や攻撃を防げない．また，内部ネットワークにはホストだけでなく，ネットワークプリンタなども存在すると考えられるため，機器ごとに対策を取るのは難しい．

そこで，本研究ではホスト間の通信を中継するネットワークスイッチ (以下，スイッチ) に注目する．通常のスイッチは，イーサネット上の集線装置や無線アクセスポイントとして機能し，OSI 参照モデル第 2 層の MAC アドレスを用いて転送先のインタフェースを決定する．しかし，本稿で提案するスイッチ Dynamic DeFense Switch (DDFS) では，第 2 層に加え第 3 層および第 7 層の解析や DDFS 間の連携情報を組み合わせ，転送先のインタフェースを決定する．スイッチは内部ホスト間の通信を中継するため，DDFS は境界に設置されたファイアウォールや IDS よりもホストに近い位置でネットワーク利用を監視できる．監視の結果，攻撃者と思われるホストが判明した場合，その情報を必要に応じ他の DDFS に通知する．通知を受けた DDFS は以後そのホストからの通信を廃棄する．DDFS はホストごとに特別なソフトウェアを導入する必要はない．したがって，DDFS によってこれまで困難だったほぼすべての内部ネットワークでの攻撃や調査を監視・防止できる．

本稿では，まず第 2 節で内部ネットワークでの攻撃事例について述べ，第 3 節でそれら攻撃の前段階とな

るブロードキャストパケットを用いた予備実験の結果を示す．そして，第4節でDDFSの概要と設計について述べ，第5節でまとめと今後の課題を述べる．

2 内部ネットワーク内における攻撃と調査

初期の内部ネットワークは組織内の固定ホストが接続し，インターネットなど外部ネットワークへの接続はほとんど行われなかった．このため内部ネットワークに侵入するには，施設内への物理的な侵入が必要でありその遂行は困難であった．

しかし，今日の内部ネットワークでは一部の環境では内部者が部外から持ち込んだラップトップの接続を許容し，インターネットをはじめとする外部ネットワークと常時接続されている．さらに，無線LANの普及により建物外でも電波が届く範囲内であれば機器に直接接続することなく，内部ネットワークへ参加できる．

また，ファイアウォールを通過したワームやトロイの木馬などによって利用者のホストを乗っ取り，外部の人物が内部ネットワークに参加することも可能である．

これらの手法により内部ネットワークに接続した悪意ある人物が内部ネットワーク内に接続されたホストに攻撃や調査をする代表的手法として以下の3つが挙げられる．

- ARP応答の偽造による盗聴
- ブロードキャストパケットの解析
- ワームの侵入

以降では，これらの行為を行う悪意のある人物を攻撃者と呼び，一般の利用者である内部者とは区別して扱う．また，攻撃者には侵入や攻撃の下準備となる調査を行う者も含むこととする．

2.1 ARP応答の偽造による盗聴

Address Resolution Protocol (ARP) [7] は，IPアドレスに対応するデータリンク層のMACアドレスを求めるために利用されるプロトコルである．

ARPによって対象ホストのMACアドレスを取得する手順は以下の通りである．

1. 対象ホストのMACアドレスを取得するため，要求ホストは自身のIPアドレス，MACアドレスと対象ホストのIPアドレスを含んだブロードキャストパケットを送出する．(ARP要求)
2. 同一セグメント上の全ホストはARP要求を受信する．各ホストはARP要求に含まれる対象ホストのIPアドレスが自身のIPアドレスと一致するか調べる．
   一致する場合は要求元のIPアドレス，MACアドレスに加え，自身のIPアドレスとMACアドレスを含んだパケットを生成し要求ホスト宛に送信する．(ARP応答)
   一致しない場合，そのホストは応答せずパケットは破棄される．
3. ARP応答を受け取ったホストは自身のARPテーブルを更新し，IPアドレスとMACアドレスの組み合わせを一定時間保存する．

しかし対象ホストではないホストが，自身のMACアドレスと対象ホストIPアドレスを含んだ偽のARP応答を生成し，要求元に送付した場合，要求元は新たな応答を優先し，実際とは異なったIPアドレスとMACアドレスの組み合わせをARPテーブルに保存する．このため，対象IPアドレス宛のパケットは別ホストに送付される．偽のARP応答を用いた場合，スイッチによって他ホスト宛の通信が盗聴できない環境であっても誘導によって盗聴が可能である [8]．この様子を図1に示す．

(1) ホストAとホストBがスイッチを介し通信を行っている．スイッチを用いているためリピータハブと異なり，ホストAB間の通信は攻撃者であるホストCには到達しない．

(2) ホストCがホストAとホストBに対し，ホストCのMACアドレスを含んだ偽のARP応答を行うと，ホストAとホストBのARPテーブルに誤った組み合わせが登録される．

(3) その結果，ホストAはホストCをホストBだと思い，ホストBはホストCをホストAだと思いパケットを送信する．したがってホストCは，ホストA，ホストBの送出するパケットを入手できる．この状態でホストCが誘導したパケットを正しい宛先に再送すると，存在を隠したまま通信内容を盗聴できる．

2.2 ブロードキャストパケットの解析

ブロードキャストパケットは，ホストの探索や自身の情報を通知するためにネットワークスイッチなどを介して同一セグメント上のすべてのホストを対象として送出されるパケットである．通常ブロードキャストパケットを受信したホストはパケット内容を判断し，必要なければソフトウェア内でその内容を廃棄する．しかし，攻撃者が受信したブロードキャストパケットを解析した場合，ホストやネットワーク構成を把握できる．

ブロードキャストを利用するプロトコルとしてDynamic Host Configration Protocol (DHCP) [4] が挙げられる．DHCPはホストに対しIPアドレスやDNSサーバ，ゲートウェイなどホスト環境に必要となる設定値をやりとりするプロトコルである．DHCPによって個別のネットワーク設定をする必要がなくなるため，情報コンセントを用いたオープンエリアのように端末が頻繁に入れ替わる環境や，多数の端末が存在するネットワークなど多くの環境で使われている．

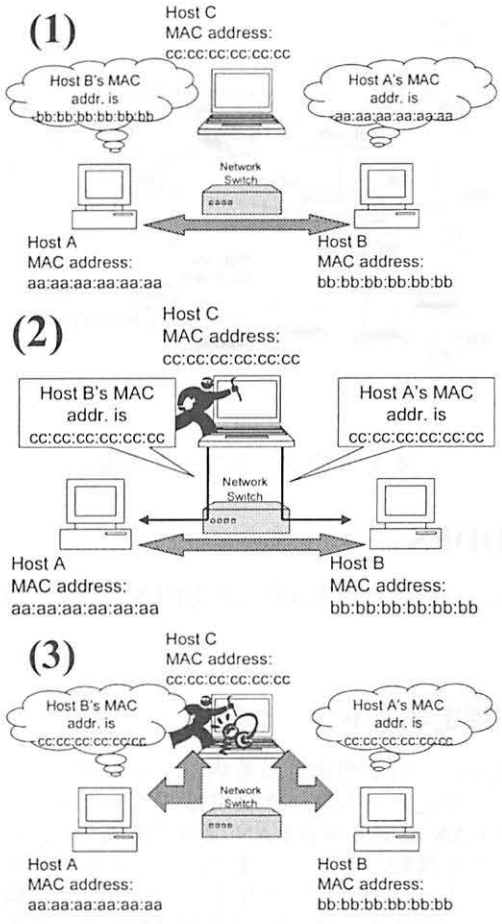

図 1: ARP 応答の偽造による盗聴例

DHCP による設定は以下の流れで行われる．

1. DHCP による環境設定を要求する DHCP クライアントは，要求する設定項目を列記した DHCPDISCOVER メッセージをブロードキャストし DHCP サーバを検索する．

2. DHCPDISCOVER メッセージを受け取ったすべての DHCP サーバは DHCPOFFER メッセージによってクライアントに DHCP サーバの存在をブロードキャストし，設定値を返答する．

3. DHCPOFFER メッセージを受け取った DHCP クライアントは応答のあった DHCP サーバを 1 つ選び DHCPREQUEST メッセージによって設定を要求する．

4. DHCPREQUEST メッセージを受け取ったサーバは設定値を調べ IP アドレス重複などの問題がなければ DHCPACK を送り設定を反映する．

これらクライアントからの通信はブロードキャストを用いて行われるため，攻撃者をはじめとする同一セグメント上のホストは対象ホストの要求内容を傍受できる．攻撃者は DHCP サーバの存在を知ることで，設定の要求や以下に示すホスト詐称行為が可能である．

クライアントの詐称　DHCP サーバは DHCPOFFER の送信元 MAC アドレスによって応答の有無や IP アドレスなどの設定値を変更できる．クライアントが DHCPOFFER メッセージを送信し，サーバが DHCPOFFER メッセージを応答した場合，クライアントの MAC アドレスは有効なアドレスとして DHCP サーバに登録されているといえる．攻撃者はこれらの通信を追跡し，DHCP が有効な MAC アドレスを収集できる．攻撃者は攻撃者ホストの MAC アドレスを記録したアドレスに変更することで，そのクライアントになりすまし，有効な設定値を取得できる．

DHCP サーバの詐称　攻撃者のホストに対しても，DHCPDISCOVER メッセージが送られてくるため，要求クライアントに対し攻撃者が用意した偽の DHCP サーバも応答できる．攻撃者の用意した偽の DHCP サーバは，要求クライアントに対し偽のゲートウェイアドレスと偽の DNS サーバを設定値として与える．偽のゲートウェイを指定することで，被害者ホストを攻撃者のホストに誘導し，送信内容の盗聴が行える．また，偽の DNS サーバがあるドメイン名に対して別の IP アドレスを返答することで，ドメインを利用した利用者を別のホストに誘導できる．

2.3 ワームの侵入

一般に組織内部などの内部ネットワークでは外部からのアクセスは境界のファイアウォールによって制限されることが多い．このため内部ホストでのアクセス制限は比較的緩く設定されていることが多く，ネットワークプリンタやセンサなどアクセス制限機能を持たないホストも存在する．

しかし，MS-Blaster[2] に代表されるワームに感染したホストが組織内部に持ち込まれた場合，境界部の防御システムでは対処できない組織内部にワームが蔓延する可能性がある．さらに，攻撃者がトロイの木馬を設置した場合や無線 LAN の盗用によって，攻撃者が内部のホストに対し情報収集活動を行った場合でも，同様に境界部の防御システムでは検知できないという問題がある．

3 予備実験

本機構の有用性を検討するために，予備実験を行った．予備実験の内容は，あるネットワーク構成の調査を目的とし，端末にてネットワークを流れるブロードキャストパケットを受信し，その内容解析から構成を把握するという内容である．

実験対象となるネットワークとしてキャンパス内の研究ネットワーク(ネットマスクが255.255.254.0のネットワーク)を利用した．また，パケットの受信・解析にはFreeBSD上で動作するEthereal[5]を用いた．

調査時間を1時間とし，午前2時10分から午前3時10分にかけて計測を行った．その結果，4325パケットのブロードキャストフレームを受信した．受信したフレーム数の内訳を図2に示す．

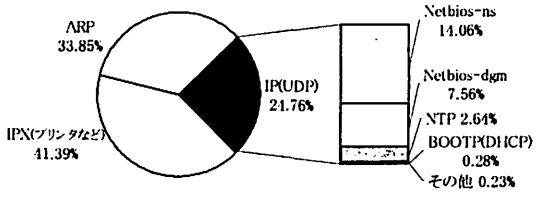

図 2: 受信したブロードキャストフレームの内訳 (N=4325)

受信フレームを解析することで以下の情報を得た．

- MACアドレスの調査から，対象ネットワークには少なくとも68ホストが存在する．
- MACアドレス中の先頭3バイトで構成されるOUI(ベンダコード)の調査から，PC/AT互換機以外に，Sun Microsystems社製のホストやApple Computer社製のホスト，ネットワークプリンタが存在することが伺える．
- ARP要求パケットの観察からあるホストはEtherLeak[1]の問題を抱えたドライバを利用していることがわかる．
- 多数のNetBIOS over TCP/IPのパケットが受信されていることから，多くのWindowsホストが稼働するネットワークと推測される．
- NetBIOSによってそれぞれのIPアドレスとホスト名の対応付けができる．
- DHCPパケットを受信したため，ネットワーク内にはDHCPサーバが存在する．

この実験によって，内部ネットワークではブロードキャストが多用され，多くの情報を攻撃者に与えることが確認できた．情報が入手されることを防ぐためにブロードキャストを防ぐことも有用だが，ブロードキャストの全く使えないネットワークは，クライアントの多い内部ネットワークに適さない．DDFSのブロードキャスト制限機能では不用意なブロードキャストの伝搬を防ぎ，ネットワークに接続した攻撃者に多くの情報を与えない環境を提供する．

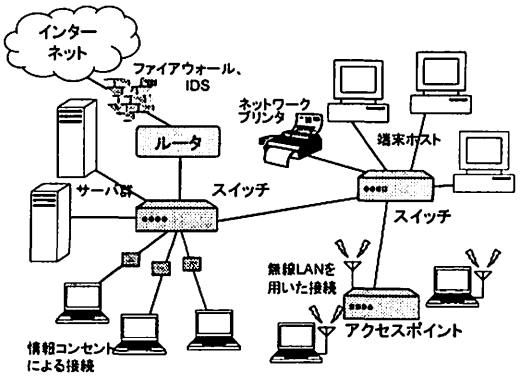

図 3: 想定ネットワーク環境

4 DDFS

本節ではスイッチを改良したDDFSの概要と設計を述べる．

4.1 想定ネットワーク環境

DDFSの利用が想定される内部ネットワークを図3に示す．想定ネットワーク環境はスイッチを中心とする有線LAN環境と無線LAN環境で構成され，同一セグメントで接続している．また，ネットワークを構成するホストにはPCだけでなくプリンタなどの機器も存在する．情報コンセントや無線LANによって内部者は部外から持ち込んだラップトップPCを接続できる．

また，想定ネットワーク環境では以下の条件が成り立つと仮定する．

- 有線LAN環境上のすべてのホストはスイッチ上のインタフェースに直接接続されており，ホストとスイッチ間にはリピータやブリッジなど他の中継機器は存在しない．
- 無線LAN環境ではアクセスポイントを介してすべての通信が行われるインフラストラクチャモードにて通信が行われている．ただし，現在の無線LANの実装ではWEPを用いてデータリンク層で暗号化した場合でも共通のWEPキーが使われ，クライアントごとに異なるキーを用いた暗号化は行えない．このため他のホストが送信したフレームや，他ホストに宛てられたフレームを傍受し内容解読が可能であるという問題がある．DDFSではこの問題は解決できないため，IPSec[6]など上位層の暗号化により特定ホスト宛の通信は傍受が行えても解読できないものとする．

これらの仮定によって，想定ネットワーク環境に接続するホスト間の通信は，すべてスイッチもしくはアクセスポイントを1度以上経由した上で行われる．また，各ホストは他ホスト宛のフレームを受信することはない．

4.2 システム概要

図3のような想定ネットワークには攻撃者が2節で述べた各種攻撃や調査を行えるという問題がある．そこで，図3に示したスイッチおよびアクセスポイントに攻撃を防ぐ以下の機能を追加する．

- **偽造 ARP 応答防止機能**
  ARP 応答の偽造によって通信の誘導が行われる可能性がある．そこで偽造された ARP 応答を検出し，廃棄する．
- **ブロードキャスト転送先限定機能**
  ブロードキャストフレームが不必要なホストに伝達されることを防ぐため，ブロードキャストフレームの送信先を限定する．
- **ファイアウォール機能**
  ウィルスが組織内に蔓延することや，内部ホスト間の攻撃を防止するため，それらの行動を検知し，遮断する．

これらの機能がスイッチとして独立動作した場合でも多くの場合は問題なく動作する．しかし，機器ごとに必要となる設定は管理者にとって大きな負担となる．また，各スイッチ間の持つ情報に偏りが起き，攻撃アクセス過多のホストも他のスイッチを介してネットワークに再び参加できてしまう．

そこで DDFS では以上の3機能に，以下の機能を加えシステムを構成する．

- **連携機能**
  DDFS 上の設定や攻撃アクセス回数などの情報を収集し，他の DDFS と共有する．

4.3 設計

DDFS 内のシステム構成を図4に示す．

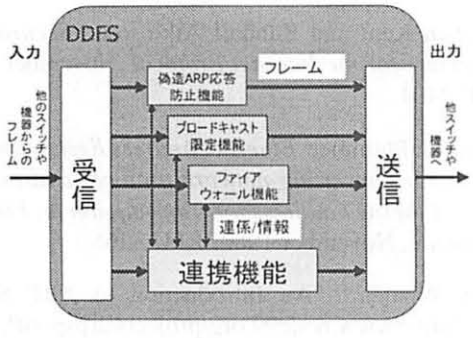

図4: システム構成図

DDFS は受信したフレームの種類によって，内部の処理を振り分ける．既存の情報から受信フレームが攻撃であるか判断し，攻撃であるとした場合受信フレームを廃棄する．廃棄されなかったフレームは MAC アドレスに基づいて別の機器に転送される．

以下に各機能の設計を述べる．

偽造 ARP 応答防止機能

偽造 ARP 応答伝達防止機能は，偽の ARP 応答中継を防ぐ．ARP 応答によってある IP アドレスに対応する MAC アドレスが変更される場合はホストが移動したか，ARP 応答が偽造されたと判断できる．偽造と判断された場合，攻撃者の送信した ARP 応答は DDFS 内で廃棄され，宛先への送信を防ぐ．

ブロードキャスト限定機能

ブロードキャスト限定機能はスイッチでブロードキャストフレームの宛先を限定し特定のインタフェースにのみ送信する．このことにより，ブロードキャストフレームが到達するホストを限定し，不必要な転送を防ぐ．

ファイアウォール機能

ファイアウォール機能はホストから送信されたフレームがワームや内部攻撃でないかを DDFS 内のファイアウォールで判定する．ワームやフィルタリングルールによって内部攻撃と判定された場合 DDFS は対象フレームを廃棄し，問題の拡大を防ぐ．

連携機能

連携機能は，DDFS 間で情報共有を図るために使われる．たとえば，ブロードキャスト限定機能では DHCP サーバにつながるインタフェースの情報を与え，ARP 応答の伝達防止機能では他の DDFS に接続した情報と自ホストの情報を交換する．

効率よい連携を図るために同一ネットワーク上の DDFS 間で木構造を作成し，この木構造を用いて情報の収集・配信を行う．また，この木構造作成により他の DDFS につながるインタフェースを特定できる．

4.4 動作概要

偽造 ARP 応答防止機能

各 DDFS の偽造 ARP 応答防止機能は，IP パケットが到着するとその送信元 MAC アドレスと IP アドレス，到着インタフェースを ARP テーブルに記録する．

DDFS が ARP 応答を受信すると ARP テーブルを検索し，応答に含まれる IP アドレス，MAC アドレス，到着インタフェースの対応が正しいかを確認する．IP アドレスの登録が確認されたにもかかわらず，MAC ア

ドレス，接続インタフェースが異なる場合，当該ARP応答は偽造されていると判断しフレームを廃棄する．

ARPテーブルは連携機能によって定期的にRoot DDFSに送信される．Root DDFSは各DDFSのARPテーブルを他のDDFSに配信する．配信されたARPテーブルを元に各DDFSは自身のARPテーブルを更新する．

ブロードキャスト限定機能

DDFSを用いてブロードキャストの転送先を限定する例としてDHCPを挙げる．DHCPはブロードキャストパケットによってDHCPサーバを探し出す．

DDFSを用いてDHCPクライアントがDHCPサーバにアドレスを要求する様子を図5に示す．まず，左下のホストがDHCPサーバにDHCPDISCOVERメッセージを送信する．ラップトップが接続されたDDFSはDHCPパケットを送信したホストを記憶した後，ブロードキャストフレームをDHCPサーバの接続された上流DDFSにのみ送信する．同様に，上流DDFSは送信元を記録し，転送先をDHCPサーバのつながるインタフェースに限定する．この振る舞いにより，他のホストが傍受することを防止する．

DHCPサーバのつながる上流インタフェースは連携機能によって検索される．

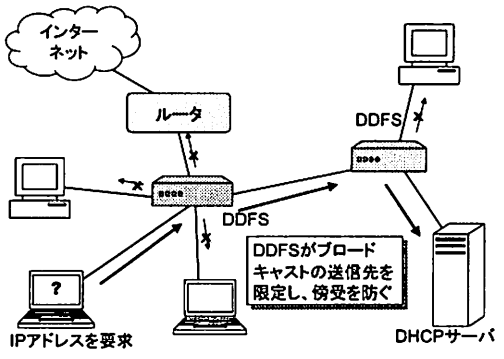

図5: DDFSによるDHCPパケットの限定

ファイアウォール機能

DDFS内部のファイアウォールは既存のIPパケットフィルタリング機能に加え，既知の攻撃パターンやワームを検出し通信を遮断する機能を持つ．問題がない場合ファイアウォールの接続するスイッチから宛先ホストに向けて再送される．問題があったパケットはスイッチ内で廃棄され，送信先に送られることはない．

あるDDFSが特定ホストから問題のあるパケットを短時間に大量に受信した場合，連携機能ですべてのDDFSにおいて当該ホストとの通信を禁止させる．

5 まとめと今後の予定

本稿では，スイッチ間の連携によって内部ネットワークセキュリティの向上を図るスイッチDDFSを提案した．DDFSは，偽造ARP応答防止機能，内部攻撃防止機能，ブロードキャストパケット制限機能を持つ．これら機能により現在セキュリティ対策がほとんど行われていない内部ネットワークをより安全にできる．

今後はDDFSの実装を行い，対象とする攻撃が防御可能か，本機構によるオーバーヘッドはどの程度かを評価し，本機構の有用性を証明する．また，ブロードキャストフレームのうちDHCPのようにホストの検索を行うのではなく，ホストの情報を伝達する目的で使われるフレームや，イーサネットを用いるプロトコルであっても，IPv6[3]などARPの存在を前提としないプロトコルへの応用を検討する．

参考文献

[1] Ofir Arkin and Josh Anderson. @Snake, Inc. Security Advisory, EtherLeak: Ethernet frame padding information leakage, January 2003.

[2] CERT Advisory CA-2003-20 W32/Blaster worm, August 2003. http://www.cert.org/advisories/CA-2003-20.html.

[3] Stephen E. Deering and Robert M. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*, December 1998. RFC 2460.

[4] Ralph Droms. *Dynamic Host Configuration Protocol*, March 1997. RFC 2131.

[5] Ethereal free network protocol analyzer for Unix and Windows. http://www.ethereal.com.

[6] Stephen Kent and Randall Atkinson. *Security Architecture for the Internet Protocol*, November 1998. RFC 2401.

[7] David C. Plummer. *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Etherne t address for transmission on Ethernet hardware*, November 1982. RFC 826.

[8] Sean Whalen. An Introduction to ARP Spoofing. http://www.node99.org/projects/arpspoof/, April 2001.