WIDE 合宿における DNS 攻撃実験
– Monkey in the middle attack 実験報告 –

藤原 和典 (fujiwara@jprs.co.jp), 関谷 勇司 (sekiya@wide.ad.jp), 石原 知洋 (sho@sfc.wide.ad.jp)

2005 年 1 月 31 日

概 要

インターネットの普及にともない DNS の重要度は増しているが、現在の DNS プロトコルには、いくつかの攻撃対象となりうる部分がある。そのうち、DNS データを改竄する攻撃では、利用者を別サイトに誘導することができ、容易に Phishing 型詐欺を行うことができるため、金銭的利益を得る目的の攻撃が行われる可能性がある。

本実験では、盗聴可能なネットワークに対し、中間者攻撃を行い、DNS データの改竄ができることを示した。

具体的には、無線ネットワークでパケットを監視し、適度に偽の名前解決応答を正しい応答の前に返すという攻撃プログラムを試作し、影響を観察する実験を行った。その結果、ほとんどのユーザを騙しサイトへ誘導することができた。

第 2 章にて実験の目的を定義し、第 3 章にて開発したソフトウェアの説明、第 4 章にて実験環境を紹介する。第 5 章にて実験手順を示し、第 6 章に結果を分析する。また、第 7 章にて考察を行ない、第 8 章に今後の課題をまとめる。

1 DNS への攻撃実験

DNS はインターネットにおける唯一で不可欠な分散データベースであり、インターネットの普及にともない重要度を増している。ところが、現在の DNS プロトコルには、いくつかの攻撃対象となりうる部分があり、RFC3833 Threat Analysis of the Domain Name System にまとめられている。DNS への攻撃のうち、サーバへの DoS 型攻撃では、機会の損失を与えることはできるが、それ以上の被害を与えることは困難である。DNS データを改竄する攻撃では、利用者を別サイトに誘導することができ、容易に Phishing 型詐欺を行うことができるため、金銭的利益を得る目的の攻撃が行われる可能性がある。

また、共有ネットワーク型の無線 LAN が普及しているが、このネットワークではユーザが出すパケットを容易に盗聴できるため、ユーザとサーバの間のデータを改竄する中間者攻撃を行いやすい。そこで、今回は、中間者攻撃 (Monkey-in-the-middle attack) を行い、DNS データの改竄ができることを示した。

2 実験の目的

本実験は、DNS に対する現状の脅威を明らかにし、DNS の運用者ならびに開発者に対して、改善策の提言ならびに貢献を行うことを最終的な目的とする。

まず、WIDE 研究者に、DNS による名前解決の脆弱性と弊害の大きさを実感させ、攻撃の影響と防御方法に関する議論と研究を促進する。また、WIDE 合宿の無線 LAN 接続環境は大規模なイベント (IETF,InternetWeek,N+I 等) で提供される無線 LAN 環境やホットスポットと同等の環境であり、WIDE 合宿環境で検証できればホットスポットなどでの問題点を指摘できる。

そのために、影響を受けた OS の種類、人数、被害の状況等の情報を収集する。さらに、より効率的で致命的な悪影響を与える攻撃方法や、被験者が攻撃を受け、別サイトに誘導されたことに気づかないようにする方法等について、意見の募集を行う。

3　攻撃に用いたソフトウェア

攻撃ソフトウェアは、pcap ライブラリ経由で BPF や Raw ソケットを用いて共有ネットワークを流れる DNS 問い合わせパケットを監視し、問い合わせを解釈し、攻撃応答パケットを生成し、それをネットワークに送る。

今回は主に Linux で動作する Raw ソケットを用いた uso800d と、主に BSD 系の OS で動作する BPF を用いた dnsattack という二つのツールを試作した。また、従来から dnshijack/dnshijacker というツールが出回っているが動作原理は同じである。

3.1　uso800d

pcap ライブラリを用いて DNS 問い合わせパケットを拾い、生成した攻撃応答を raw ソケットを用いてネットワークに出力している。Linux にて動作する。

3.2　dnsattack

pcap ライブラリを用いて DNS 問い合わせパケットを拾い、生成した攻撃応答を BPF を用いてネットワークに出力している。FreeBSD, NetBSD, MacOSX で動作確認を行っている。

4　実験環境

本章では、実験を行った環境について述べる。今回の実験は WIDE 合宿にて行った。WIDE 合宿は 200 人以上の WIDE 研究者が集まる場であり、多くの被験者を得ることができる。なお、実験は前述の通り無線 LAN のネットワークセグメントにて行った。

4.1　トポロジ

今回の実験環境となる WIDE 合宿ネットワークの無線セグメントは、一つの Layer-3 ネットワークセグメントにて構成された。すなわち、ユーザはすべて同一セグメントに存在している。 また、WIDE 合宿地において DHCP にて指示されるリゾルバ DNS サーバは、無線 LAN セグメントとは別のネットワークに存在している。

前述の通り、無線 LAN は一つのネットワークセグメントで構成されている。しかし、複数の会議場もしくは部屋にて無線 LAN を提供するため、無線 LAN 基地局は複数台設置され、ローミング接続を利用してサービスが提供された。

そのため、実際には複数の無線 LAN 基地局をスイッチで接続した形態となっている。 また、ユーザに 802.11a 方式と 802.11b 方式という、二つの無線 LAN 方式を提供した。 さらに、広い部屋、複数の部屋をサポートするため、一つの方式でも複数のチャンネルを用いて無線ネットワーク間のローミング接続を提供している。

無線 LAN にて盗聴型攻撃を行う場合、一つの無線 LAN 基地局にアソシエーションして盗聴するだけでは、その無線 LAN 基地局にアソシエーションしているクライアントの通信のみしか盗聴することができない。

特に、最も広い Plenary 部屋では、複数のチャンネルを用いて複数の場所に無線 LAN 基地局を設置しているため、攻撃するためにも複数のホストが必要となる。

4.2　使用機器

今回の実験のために、次の機器を使用した。

- 802.11a

  攻撃マシン NotePC(Linux)

  計測兼誘導先マシン miniPC(Linux)

  誘導先で提供したサービス http, ssh, telnet, pop3, imap, smtp, ftp

- 802.11b

  攻撃マシン 1 MacOSX(11b - channel 6)

  攻撃マシン 2 FreeBSD(11b - channel 1)

  計測兼誘導先マシン FreeBSD(11b - channel 1)

  誘導先で提供したサービス http, ssh

また、使用する無線 LAN カードによって、クライアントから無線 LAN 基地局へのパケットを盗聴できる場合とできない場合があった。特に 802.11a の無線 LAN カードにて盗聴できない場合が多く発生した。

これは、Linux や FreeBSD の無線 LAN カードのドライバに依存することがわかった。そのため、今回の実験では、無線 LAN カードドライバに手を加え、クライアントから無線 LAN 基地局への通信も盗聴できるよう改造したドライバを利用した。

5 実験

攻撃の効果を段階を経て見極めるため、今回は三段階にわけて実験を行った。

まず、dns-wg の BoF の時間に、実験を行うことを周知した上で、dns-wg BoF 参加者を対象に実験を行った。これを第一回実験とする。その結果をふまえ、第二回実験として、Plenary 部屋にて被験者を増やし実験を行った。この際は、開始時間を告げずに、Plenary 開催中のどこかの時間帯にて 15 分間攻撃を行うことをあらかじめ告知した。さらに、第三回実験として、何も周知せずに Plenary 部屋にて実験を行った。

それぞれの実験について述べる。

5.1 第一回実験 (BoF)

この実験では、BoF に参加した DNS 有識者を対象とした。BoF 部屋の中で実験したため、部屋にいる約 40 名の人を攻撃の対象とした。実験開始をアナウンスし、すべての IPv4 アドレス問い合わせ (A 問い合わせ) を 203.178.136.57(www.wide.ad.jp) に、IPv6 アドレス問い合わせ (AAAA 問い合わせ) を ::1 に誘導した。なお、二つの攻撃プログラムのうち、uso800d を用いて 802.11a の攻撃を行い、dnsattack を用いて 802.11b の攻撃を行った。

その結果、全参加者約 40 中 6 名を除き、85 れなかった 6 名は、違う部屋に設置されている無線 LAN 基地局を利用していたか、Proxy を利用していた人であることがわかった。誘導されなかった 6 人の環境を次に示す。

被験者 1 Windows XP, 802.11a(atheros)

被験者 2 Windows XP, 802.11b, using Web Proxy

被験者 3 Windows XP, 802.11b

被験者 4 Linux(RedHat-9.0), 802.11b

被験者 5 Windows 2000, 802.11a

被験者 6 Windows XP + VMware(NetBSD), 802.11b

この実験の結果、攻撃によって多くの人を誘導できることがわかった。次に、この攻撃方法のスケーラビリティを確認するため、より広い範囲を対象として実験を行うこととした。

5.2 第二回実験 (Plenary)

第二回実験は、ほぼ参加者全員が集まる Plenary の時間帯を選び、参加者全員を被験者として行った。参加者には実験開始時間を明確に告げずに、15 分間実験を行った。

また、誘導先となるホストを用意し、Web サーバ、ssh サーバなどを動作させ、誘導されたことを被験者にわかるようにした。さらに、別のマシンで無線セグメントのパケットを tcpdump にて記録し、本来の DNS 応答よりも攻撃ツールが素早く偽応答を送れているか検証した。

実験環境では、802.11a 1 チャンネルと、802.11b 3 チャンネルの無線セグメントが使用されていたが、そのうちの 802.11a と 802.11b のうちの 2 チャンネル分を攻撃した。今回は、すべての A 問い合わせに対して誘導先マシンの IP アドレスを答えた。

この実験でも、第一回実験と同じく、uso800d を用いて 802.11a の攻撃を行い、dnsattack を用いて 802.11b の攻撃を行った。

なおこの実験においては、攻撃ホストの台数の制限から、すべての無線 LAN 基地局にアソシエーションすることができなかった。そのため、参加者全員を被験者とすることができなかった

すなわち、この攻撃を効率的に行うためには、無線 LAN 基地局一台に対して一台の攻撃ホストが必要であることがわかった。この実験結果の詳細については、6 章にて述べる。

5.3 第三回実験 (Closing)

第三回実験は、特に実施のアナウンスをせずに、ゲリラ的に行った。合宿最終日の Closing にて、ほぼ参加者全員が集まっている環境にて実施した。今までの

実験と同じように、uso800d を用いて 802.11a の攻撃を行い、dnsattack を用いて 802.11b の攻撃を行った。

今回の実験では、次の名前の問い合わせに対してのみ嘘の応答を行うよう、攻撃ツールを設定した。

- www.asahi.com
- www.yahoo.co.jp
- www.zakzak.co.jp
- www.2ch.net
- slashdot.jp

誘導先の偽サーバには Web サーバを動かし、実在するニュースサイトに類似したデザインのページが表示されるよう設定した。

この実験の結果、参加者に対して、詐欺目的での誘導の怖さを体験してもらうことができた。

6 第二回実験の詳細

本章では、被験者数が最大で、パケットキャプチャを行った第二回実験の詳細結果について述べる。

第二回実験においては、802.11b では、1,6,11 チャンネルの 3 波のうち、1 チャンネルと 6 チャンネルに属しているクライアントを攻撃した。また、802.11a では、61 チャンネルに属しているクライアントを攻撃した。

そのため、すべての参加者を被験者とできたわけではなく、攻撃ホストがアソシエーションしていた無線 LAN 基地局にアソシエーションしていたユーザのみを被験者として実験を行った。

6.1 攻撃による影響

802.11a へアソシエーションしていた人への攻撃結果を、表 1 に示す。これは、誘導先の偽ホストにて tcpdump を行い、コネクションを張ろうと試みてきたホストのソース IP アドレスを集計した。なお、誘導されたクライアントがコネクションを試みたプロトコルの内訳を 2 に示す。

これらの結果から、92.3% の被験者が一度は騙されたことがわかる。

表 1: 偽ホストに誘導された被験者の統計

被験者	65
一度でも誘導された人	60

表 2: 偽ホストに誘導された被験者の統計

http	55
ssh	12
telnet	1
pop3	10
imap	1
smtp	3

802.11b では、攻撃は二つのチャンネルを対象としたが、機材の都合でパケットダンプを取ることができたのは 1 チャンネルのみであるため、1 チャンネルでの分析を詳細に行なった。802.11b において騙された被験者数を 3 に示す。被験者数はユニークな IP アドレス数で数えている。

これらの結果から、802.11b 1 チャンネルでは 65.3% の被験者が一度は騙されたことがわかる。

表 3: 偽ホストに誘導された被験者の統計 (802.11b)

一度でも誘導された被験者数	53
http サーバに誘導された被験者数	51
ssh サーバに誘導された被験者数	11
1 チャンネル以外の誘導された被験者数	17
1 チャンネルの被験者数	52
1 チャンネルで誘導された被験者数	34
1 チャンネルで誘導されなかった被験者数	18

6.2 DNS パケットの分析

次に、攻撃ホストとは別のホストにて tcpdump コマンドによるパケットキャプチャを行い、本来の DNS サーバの返答と、攻撃ホストによる攻撃の返答の時間差の分析を行った。

802.11a における結果を図 1 に、802.11b における結果を図 2 に示す。

この図において、横軸は問い合わせパケットの時刻、

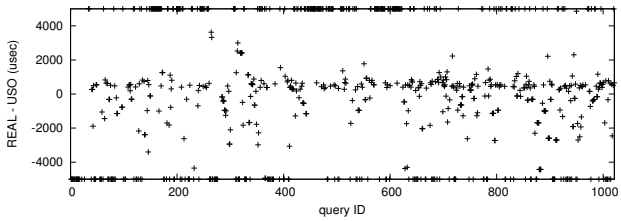

図 1: DNS 応答の分析 802.11a

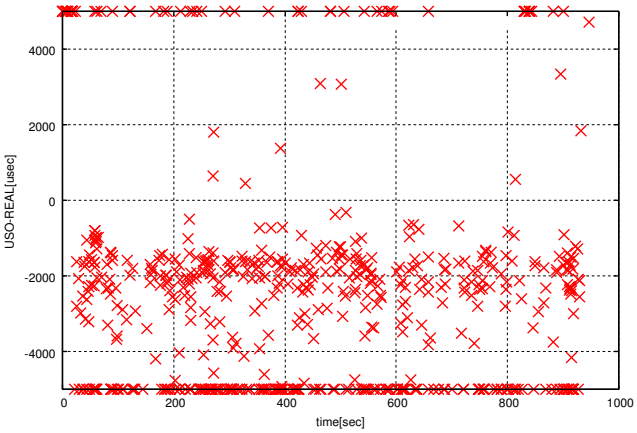

図 2: DNS 応答の分析 802.11b channel 1

縦軸は、問い合わせに対して攻撃ホストが答えた時刻から、本来の DNS サーバからの応答が得られた時刻を差し引いたものである。すなわち、0 より下に位置する点は、攻撃ホストの応答が本来の DNS サーバよりも早かった場合を示す。逆に 0 より上に位置する点は、本来の DNS サーバの応答の方が早かった場合を示す。

また、-5000usec の横軸に張り付いている点は、攻撃ホストからの応答しか観測できなかった場合を示し、5000usec の横軸に張り付いている点は、本来の DNS サーバからの応答しか観測できなかった場合を示す。

表 4、表 5 に、内訳を示す。

6.3 被験者へのアンケート

今回の実験についてのアンケートを実施し、38 人からアンケートを回収した。質問項目は以下のとおりである。

影響がなかった被験者 7 名のうち、3 名は実験中に

表 4: DNS 応答の内訳 802.11a

観測された問い合わせ数	1021
攻撃ホストの方が早く応答した場合	654
本来の DNS サーバの方が早く応答した場合	330
応答が観測されなかった場合	37

表 5: DNS 応答の内訳 802.11b channel 1

観測された問い合わせ数	599
攻撃ホストの方が早く応答した場合	535
本来の DNS サーバの方が早く応答した場合	64
本来の応答が観測されなかった場合	6
攻撃ホストの応答が観測されなかった場合	53

DNS 検索を伴う新しい接続を行なっていなかったというコメントがあった。

1. 実験にて名前解決が騙されましたか？
2. 1. にて騙されたと応えた方は，どんなアプリケーションが騙されましたか？
3. 1. にて騙されなかったと応えた方は，リゾルバにどの DNS サーバを指定されていましたか？ (IP address)
4. お使いになっている環境を差し支えない範囲で教えて下さい。(OS, 無線 LAN)
5. その他，コメント，不思議な挙動，要望等ありましたらご記入お願いいたします。

アンケート結果を表 6 に示す。

7 実験の考察

本章では、第二回の実験結果をもとに実験結果の考察を行う。

まず、図 1、図 2 に示した DNS 応答の分析に関して、同一無線 LAN 基地局にアソシエーションしているホストでの tcpdump による結果なので、無線の電波状況による取りこぼしが発生していることが考えら

表 6: アンケート結果

ホスト数			39
誘導された	総数		32
	OS 別	WindowsXP/2000	20
		MacOSX	4
		NetBSD/FreeBSD	5
		Linux	3
	DNS サーバ設定	localhost	2
		DHCP	30
影響なし	総数		7
	OS 別	WindowsXP/2000	3
		MacOSX	1
		NetBSD/FreeBSD	2
		Linux	1
	DNS サーバ設定	localhost	1
		DHCP	6

れ、誘導先ホストでの記録と合わせて結果を出さないと、正確な結果とはならないと考えられる。また、無線 LAN の基地局はブリッジとして動作しているが、別の無線チャンネルのパケットがもれてきている場合があるという報告があり、すべてのチャンネル・イーサネットセグメントで記録をとり、つきあわせないと正確な分析はできない。

11a の場合、パケットダンプからは応答の 65% において攻撃が成功しているが、誘導先サーバにおける観測結果から見ると、90%以上を誘導できたという結果となった。11b 1 チャンネルの場合、パケットダンプからは応答の 90%で攻撃が成功しているが、誘導先サーバにおける観測結果から見ると、65%の被験者を誘導できたという結果となった。

本実験にて誘導することができなかったユーザが存在したのは、次の理由があると考えられる。

- 無線 LAN 基地局問題
  無線 LAN 基地局の数だけ攻撃ホストを準備することができなかった。また、攻撃に利用した一部の OS では、確実にねらった無線基地局にアソシエーションさせることが難しかった。

- 問い合わせパケットが見えない
  OS の無線 LAN カードドライバの特性により、クライアントから基地局へのパケットを盗聴できないものが存在した。

- 本来の DNS サーバより速く攻撃応答を返せなかった場合
  本来の DNS サーバにキャッシュされているデータの場合、十分速く応答を返せるため、それよりも速く誘導応答を生成できない場合があった。

- IPv6 トランスポートでの問い合わせに非対応
  今回使用したツールが IPv6 トランスポートに非対応だったため、IPv6 による名前問い合わせを利用していたユーザを誘導することができなかった。

また、表 6 より、OS による明らかな差異はない。ただし、UNIX 系 OS を使用されているかたで、DNS 問い合わせに IPv6 トランスポートを使用している場合や AAAA を検索している場合は今回の実験の対象としていないため、誘導することができていない。

以上の考察から、広範囲な無線 LAN ネットワークにおいて、すべてのユーザを誘導するのは困難であるが、一部のユーザを一度でも誘導することは容易であることがわかった。

8 今後の課題

これらの実験結果をふまえ、データからのさらなる分析結果を導き出すことが今後の課題である。また、この攻撃を防ぐための有効な手法も同時に検討していく。