2W-03

DHCPv6クライアントの実装差を利用したDNSサーバアドレス詐称攻撃

高木 聖也† 長谷川 皓一†† 山口 由紀子††† 嶋田 創†††
†名古屋大学工学部電気電子情報工学科 ††名古屋大学情報戦略室 †††名古屋大学情報基盤センター

1 はじめに

ネットワーク通信にIPv6が使用されるようになっており，IoT機器のようなネットワークに接続される機器や人々が所有するデバイスが増加することでより多くのアドレスが必要になることから，IPv6の使用がさらに増加しつづけることが予想される．このように導入が進んでいるIPv6は，ネットワークの発展とともに改良されてきたIPv4とは違い，既に成熟したネットワークに導入されるため高い安全性と信頼性が必要とされている[1]．しかしその一方で，IPv6の仕様の変更によりその変更に対応出来ていない機器の間で実装に差が存在していることが示されている[2]．そこで，本研究ではそのような実装差のひとつであるDHCPv6とRDNSSの対応の差を利用したDNSサーバアドレス詐称攻撃が可能であるかどうかを検証する．

2 DNSサーバアドレス詐称攻撃

クライアントからのDNSクエリに対し，なんらかの手法により本来のDNS応答とは異なる偽の情報を返す，DNSスプーフィングという攻撃が存在する．本研究では，IPv6においてDNSサーバアドレスをDHCPv6とRDNSSの2つの方法で設定可能なことに着目し，その実装差を利用して偽のDNSサーバアドレスを設定することによりDNSスプーフィングを行なうDNSサーバアドレス詐称攻撃を検証する．

DHCPv6はアドレスやDNSサーバアドレスなどをクライアントに通知するためのプロトコルで，ルータとは別にDHCPv6サーバを必要とする．一方RDNSSはルータ広告（以下，RA）のオプションでありDNSサーバアドレスを通知することができる．

この攻撃はDHCPv6を使用してDNSサーバアドレスを配布しているネットワーク環境を想定している．このような環境下で，RDNSSオプションが付与されていること以外は正規のRAと同じオプション，パラメータを持つ偽のRAをネットワークに送信することで，RDNSSオプションで指定した任意のDNSサーバアドレスをクライアントに設定させることが可能であると考えられる．これにより，DHCPv6が実装されていないAndroid 5.1/6.0では偽のDNSサーバアドレスが設定されてしまうことが予想される．

3 攻撃実験

本研究では，実験環境を構築し，クライアントごとの実装差と攻撃の可否を検証した．この実験では正規DNSサーバと正規Webサーバ，偽DNSサーバとクライアントが誘導される偽Webサーバをそれぞれ用意した．DHCPv6サーバは正規DNSサーバのアドレスを通知し，RDNSSは偽DNSサーバのアドレスを通知するようにした．それぞれのDNSサーバでは特定のドメインに対し別のアドレスを返すようにした．攻撃の成否はどちらのWebサーバに接続されるかで判断する．

3.1 実験環境

検証する対象は，この攻撃が有効であろうと予想されるAndroid 5.1/6.0および，それ以外にWindows 10ビルド1709，Linux 4.8.0-53，macOS Sierra 10.12.6，iOS 11.2の6種類のOSとした．実験環境を図1に示す．DNSサーバとWebサーバにはそれぞれbind9とnginxを使用した．ルータはCisco Catalyst 3560-CGを使用し，攻撃者とクライアントが接続するネットワークと，Webサーバと DNSサーバが接続するネットワークを分け，互いに通信可能な設定とした．DHCPv6サーバは，ルータのDHCPv6機能を使用した．無線LANで接続する必要のあるクライアントは，スイッチモードにしたBuffalo WZR-AMPG300NHを介しネットワークに接続させた．

ルータはMフラグをオフとし，Oフラグをオンにした RAを，クライアントからの要求があった際に加えて常時4秒間隔で送信する．これによりIPv6アドレスはステートレス設定，DNSサーバアドレスはDHCPv6を用いて設定するようにした．攻撃者が送信する偽RAは，正規RAにRDNSSオプションとして偽DNSサーバのアドレスを追加したものとした．

DNS server address spoofing attack using DHCPv6 client implementation difference

Seiya TAKAGI† Hirokazu HASEGAWA†† Yukiko YAMAGUCHI††† Hajime SHIMADA†††
†School of Engineering Electrical Engineering, Electronics, and Information Engineering, Nagoya University
††Information Strategy Office, Nagoya University
†††Information Technology Center, Nagoya University

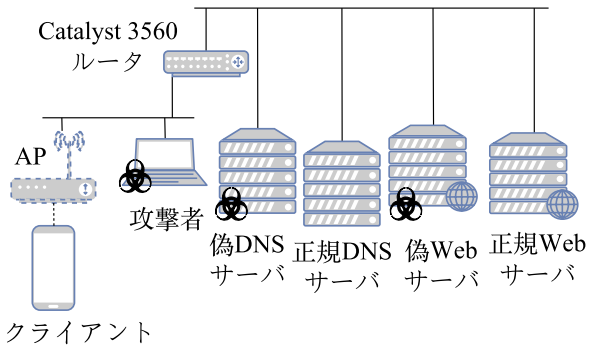

図 1: 実験環境

3.2 実験手順

偽の RA を送信する攻撃者をあらかじめネットワークに接続した状態で実験を行なった．偽 RA を流す際に先に正規 RA を受け取り次に偽 RA を受け取る場合（DHCPv6 先行実験）と，先に偽 RA を受け取り次に正規 RA を受け取る場合（RDNSS 先行実験）について実験を行なった．

3.2.1 DHCPv6 先行実験

1. クライアントをルータに接続する．
2. アドレスの設定が完了したことをネットワーク設定から確認する．
3. 攻撃者が偽 RA を 0.5 秒間隔で数秒間送信する．
4. ブラウザから実験用ドメインへアクセスし，どちらの Web サーバへ接続されたか確認する．
5. ネットワーク設定を確認し，設定された DNS サーバアドレスを確認する．

3.2.2 RDNSS 先行実験

1. 攻撃者が偽 RA を 0.5 秒間隔で送信する．
2. クライアントをルータに接続する．
3. アドレスの設定が完了したことをネットワーク設定から確認し，攻撃者の偽 RA の送信を止める．
4. ブラウザから実験用ドメインへアクセスし，どちらの Web サーバへ接続されたか確認する．
5. ネットワーク設定を確認し，設定された DNS サーバアドレスを確認する．

3.3 実験結果

実験結果を表 1 に示す．複数回実験を行い，一度でもクライアントが偽 Web サーバにアクセスした場合は攻撃は成功，一度も偽 Web サーバにアクセスせず正規 Web サーバにのみアクセスした場合は失敗とみなす．

Android 5.1/6.0 では DHCPv6 機能が実装されていないため，いずれの場合も RDNSS により偽 DNS サーバが設定され，攻撃が成功した．Windows 10 では RDNSS によって行なわれた設定は，後から受信した DHCPv6 による設定で上書きされ，攻撃は失敗した．Linux は，他の OS と異なり，複数の DNS サーバアドレスが設定され，名前解決の際は応答が早かった DNS サーバの結果が採用されるため，攻撃が成功する場合と，失敗する場合があった．macOS および iOS では 1 度設定が行なわれると変更されることはなく，RDNSS 先行の場合は攻撃が成功した．

表 1: DNS サーバアドレス詐称攻撃実験結果

クライアント OS	DHCPv6 先行	RDNSS 先行
Android 5.1	成功	成功
Android 6.0	成功	成功
Windows 10	失敗	失敗
Linux	成功	成功
macOS Sierra	失敗	成功
iOS	失敗	成功

4 おわりに

本研究では，クライアント毎の IPv6 実装差を利用した DNS サーバアドレス詐称攻撃の検証を行なった．実験結果より，クライアント毎の実装差によりこの攻撃が可能であることがわかった．偽 RA による攻撃の危険性は指摘されており [1]，RA Guard や SeND などルータにおける対策や，L2 スイッチ上での NDP Guard という対策も提案されている [3]．しかし，全ての機器の更新が困難であるなど，様々な理由からこれらの対策を適用できない場合も考えられるため，ネットワーク機器における対策のみならず，クライアントにおける対策も必要であると考えられる．今後は，クライアントサイドで攻撃状態を確認可能とする方向での対策について検討していく．

参考文献

[1] IPv6 技術検証評議会, “セキュリティ評価･対策検証部会最終報告書,” http://ipv6tvc.jp/documents/20121023Report.pdf, 2012.

[2] 北口ほか, “クライアント OS の IPv6 実装検証とネットワーク運用における課題,” 情報処理学会研究報告, 2017-IOT-36, No.13, pp.1-8, 2017.

[3] 衛藤ほか, “IPv6 通信の学習に基づく NDP 悪用攻撃対策手法の提案,” コンピュータセキュリティシンポジウム 2014 論文集, pp.199-206, 2014.