平成29年度 情報工学コース卒業研究報告要旨

村瀬(勉) 研究室	氏　　名	高 木　聖 也
卒業研究題目	DHCPv6クライアントの実装差を利用した 詐称攻撃とその対策に関する研究	

近年ではネットワークに接続する機器の増加に伴ない、IPv6の普及が徐々に進んでいる。しかし普及するにつれIPv6の仕様に改訂が行なわれて、追従しきれていない機器の間に実装差が存在してしまっている。このような実装差を悪用することで、悪意あるクライアントが他のクライアントに対して危害を加える可能性がある。

本研究では、IPv6の近隣探索プロトコルに関連する機能であるDHCPv6とRDNSSの実装差を利用した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。DNSサーバアドレス詐称攻撃はIPv6におけるDNSサーバのアドレスを通知する2つの方法に実装差が存在することを利用して、クライアントに偽のDNSサーバアドレスを設定させる攻撃である。図に示した実験環境を利用して、Windows、Linux、macOS、iOS、Android5.1/6.0の6種類のOSに対して実際に攻撃し、どのOSに対してどのような場合に攻撃が可能であるかを検証した。検証は、攻撃者がRDNSSを付加したルータ広告を送信することで攻撃するものとし、クライアントがネットワークに接続する前に攻撃が始まっている場合とクライアントが既にネットワークに接続している場合の2つの場合について検証した。その結果、両方の場合で攻撃が有効であったのはLinuxとAndroid5.1/6.0、既に攻撃が始まっている場合のみで攻撃が成功してしまう可能性があるのはmacOS、iOSであることが分かった。

本研究ではさらに、攻撃可能性の検証結果から対策が必要であると判断し、ネットワークの機器の設定が不適切で十分な安全性を保証できない場合を想定し、クライアントが自ら行なうことができる対策を提案した。複数のDNSサーバが存在するとき全てのサーバが正当であるとは限らないと仮定し、それぞれの応答を相互比較することで不正な応答が存在しているかどうかを調べる。不正な応答が存在していればそれを警告することで不正なDNSサーバを検知したとする。

この対策の有効性を確かめるためにLinuxにおいて対策検証用のプログラムをPythonで実装した。複数のDNSサーバアドレスがクライアントに設定されている場合に、それぞれについて名前解決を行ない、異なる応答が確認されれば攻撃されていると判断する。検証の結果、攻撃が成功していることを検知することができることが確認できた。