修 士 論 文 概 要 書

Summary of Master's Thesis

Date of submission: ____/____/____ (MM/DD/YYYY)

専攻名（専門分野） Department	情報理工学	氏 名 Name	高田 雄太	指 導 教 員 Advisor	印 Seal
研究指導名 Research guidance	後藤 滋樹	学籍番号 Student ID number	CD 5111B063 - 6		
研究題目 Title	IPv6 アドレス割り当てポリシーの観測に基づく脅威予測とその対策				

概要

Internet Protocol version 6 (IPv6) は，Internet Protocol version 4 (IPv4) よりも大きなアドレス空間を使用できるように設計されている．この広大なアドレス空間のため，IPv6 アドレスを用いてインターネット上のホストを探索するホストスキャンは困難である．しかし，ホストへの IPv6 アドレス割り当てには一定の規則（ポリシー）が存在するため，実際には IPv6 アドレスの空間である 128 ビットよりも小さなアドレス空間しか用いられていない問題が存在する．

本研究は，IPv6 パケットを観測して分析することで，IPv6 アドレス割り当てポリシーの存在を明らかにし，新たに考えられる脅威を予測する．この結果を用いて，IPv6 アドレス割り当てのベストプラクティスを導く．

1．はじめに

IPv4 アドレスの枯渇が問題となっている．この問題への対応策の一つとして，IPv6 アドレスへの移行が挙げられる．IPv6 は，IPv4 よりも大きなアドレス空間を使用できるように設計されており，IPv4 アドレス枯渇問題を抜本的に解決するとして考案された．IPv6 は，典型的なサブネットとして 64 ビット，すなわち 2 の 64 乗（約 1800 京）の範囲をホストが利用でき，IPv4 サブネットと比べて実際に利用するホストの密度が大幅に低下する．この広大なアドレス空間のため，IP アドレスを用いてインターネット上のホストを探索するホストスキャンは困難になった．

しかし，ホストへの IPv6 アドレス割り当てや運用方法には一定のポリシーが存在するため，使用する IPv6 アドレスに偏りが生じ，実際には IPv6 アドレスの空間 128 ビットよりも小さなアドレス空間しか用いられていない問題が存在する [1]．

本研究は，IPv6 パケットを観測することで，IPv6 アドレス割り当てポリシーの存在を明らかにする．その結果を活用して，新たに考えられる脅威を予測し，IPv6 アドレス割り当てのベストプラクティスを導く．提案するベストプラクティスを導入することで，本来外部に公開していないはずのサーバホストやクライアントホストに対するホストスキャンを緩和することができる．

2．IPv6 アドレス割り当て方法

2.1 IPv6 アドレス上位 64 ビット

IPv6 アドレスの上位 64 ビットは，RIR や ISP によって階層的に管理されている．サイトの管理者は，RIR や ISP から割り当てられたプレフィックスを利用して，最終的に 64 ビットのプレフィックスを RA（Router Advertisement）メッセージを用いてホストに通知する．

2.2 IPv6 アドレス下位 64 ビット

IPv6 アドレスの下位 64 ビットは，インターフェース ID と呼ばれる同一サブネット上でインターフェースを特定できる識別子である．インターフェース ID の設定には，ホストによる自動設定もしくはユーザによる手動設定が存在する．インターフェース ID の自動設定方法の一つに，ホストの MAC アドレスを用いてインターフェース ID を生成する方法がある．RA でプレフィックス情報を取得した後，生成したインターフェース ID と組み合わせることで IPv6 アドレスとする．これを SLAAC (Stateless Address Auto Configuration) という．SLAAC による IPv6 アドレスの割り当てを図 1 に示す．

図 1. SLAAC による IPv6 アドレスの割り当て

SLAAC 以外の自動設定による割り当て方法や，手動設定によるアドレス割り当て方法も存在する [1]．これらは一定のポリシーに基づいた割り当て方法であり，IPv6 サブネットのアドレス空間は小さくなることがわかる．SLAAC を含めた IPv6 アドレス下位 64 ビットの割り当て方法とそれぞれのアドレス空間を表 1 に示す．

その他，下位 64 ビットだけでなく上位 64 ビットも含めたアドレス空間におけるアドレス割り当て方法として，単語や連続値を使用したアドレス（Wordy）や移行技術や共存技術を利用する際に割り当てられるアドレス (6to4, ISATAP, Teredo) が挙げられる．また，表 1 の割り当て方法はそれぞれ独立した方法だが，Wordy および 6to4 については，表 1 の割り当て方法と重複して出現する可能性がある．

表 1. IPv6 アドレス下位 64 ビットの割り当て方法

	割り当て方法	割り当て例	アドレス空間
自動設定	MAC アドレスを用いたアドレス (SLAAC)	::1234:56ff:fe78:90ab	OUI を固定すると 2^{24}
	プライバシーアドレス (Privacy)	::1f9a:a208:394b:2b7e	2^{64}
手動設定	下位 64 ビットに IPv4 アドレスを用いたアドレス (IPv4-based)	::192:168:0:1	2^{32}
	末尾 16 ビットを除くすべてにゼロを用いた省略記法のアドレス (Low-byte)	::1	2^{16}
	上記以外のアドレス (Manual)	::db8:db8	2^{64}

3. ポリシー観測

本研究では，APAN (Asia Pacific Advanced Network) の観測点にて 2012 年 7 月 16 日から 2012 年 10 月 15 日までの 3 ヶ月間，送信元ポートもしくは宛先ポートに 25，53，80 が利用されている通信を対象に IPv6 パケットをキャプチャした．観測期間を通して観測した IPv6 アドレスの割り当て方法の割合を表 2 に示す．

表 2. 観測期間中の IPv6 アドレス割り当て方法の割合

割り当て方法	個数	割合 [%]
Privacy	2,436,929	87.40
6to4	233,577	8.38
Manual	171,663	6.16
SLAAC	67,961	2.44
Low-byte	61,350	2.20
Wordy	52,542	1.88
ISATAP	47,310	1.70
IPv4-based	3,075	0.11

Privacy の割合が 90% 弱を占めており，Manual の割合は 6%，SLAAC，Low-byte の割合は 2% 強であった．2008 年 4 月時点での IPv6 アドレス割り当て方法を観測した既存研究 [2] では，SLAAC が 50% を占めているため，大きく異なる結果となった．

ポートごとに観測したユニーク IPv6 アドレス数を表 3 に，ポートごとの IPv6 アドレス割り当て方法の割合を図 2 に示す．eph25，eph53，eph80 はそれぞれポート 25，53，80 と通信しているポートを表す．

表 3. ポートごとに観測したユニーク IPv6 アドレス数

ポート	個数	割合 [%]
25	1,050	0.04
53	17,127	0.61
80	51,725	1.85
eph25	1,623	0.06
eph53	144,065	5.14
eph80	2,587,439	92.31

表 3 と図2の二つの結果から，90% 以上の IPv6 アドレスが eph80 で観測されており，eph80 では Privacy が 90% を占めていることがわかる．すなわち，IPv6 による通信は，プライバシーアドレスが割り当てられたホストによる Web 通信がほとんどであると考えられる．

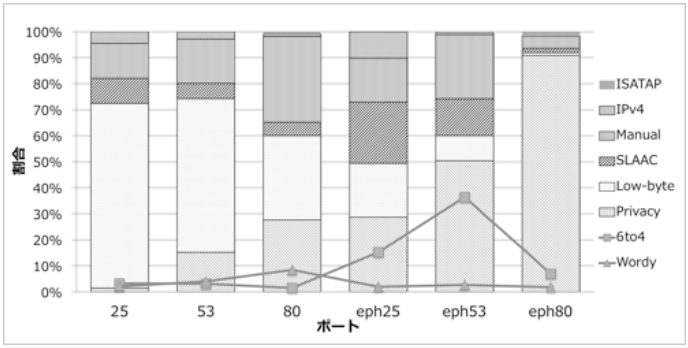

図 2. ポートごとの IPv6 アドレス割り当て方法の割合

4. 脅威と対策

4.1 割り当てポリシーを利用したホストスキャン

観測結果から，ポートごとにアドレス割り当てポリシーが存在することがわかった．

ポート 25，53，80 ウェルノウンポートを使用しているホストは公開サーバホストであると予想でき，Low-byte によるアドレスが比較的多い．すなわち，人間が覚えやすいアドレスを使用していることがわかる．

ポート eph25，eph53 SMTP サーバおよび DNS キャッシュサーバといったサーバホストであると予想でき，SLAAC によるアドレス，プライバシーアドレスが比較的多い．

ポート eph80 ブラウザを使用しているクライアントホストであると予想でき，プライバシーアドレスが多い．

上記ポリシーを利用することで，効率的に非公開のホストを探索することができてしまう恐れがある．

4.2 対策

IPv6 アドレス割り当てのベストプラクティスとして，ホストの利用目的に応じて，IPv6 を次のように適切に割り当てることが推奨される．公開サーバホストに対しては，Low-byte によるアドレスを割り当てる．非公開サーバホストに対しては，SLAAC によるアドレスをオフにし，複雑なアドレスを手動で固定設定する．クライアントホストには，SLAAC によるアドレスをオフにし，プライバシーアドレスを割り当てる．

5. まとめ

本研究では，IPv6 パケットを観測することで，IPv6 アドレス割り当てポリシーの存在を明らかにした．観測結果を活用し，新たに考えられる脅威を予測した上で，その対策法を考案した．対策を施すことで，本来外部に公開していないはずのホストに対するホストスキャンを緩和することが期待できる．

参考文献

[1] F. Gont, T. Chown, “Network Reconnaissance in IPv6 Networks,” Internet- Draft IETF, http://tools.ietf.org/html/draft-ietf-opsec-ipv6-host-scanning-00, Dec. 2012.

[2] D. Malone, “Observations of IPv6 Addresses,” PAM2008, Apr. 2008.