様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 ２３ 日現在

機関番号：６２６１５
研究種目：基盤研究(B)（一般）
研究期間：2021～2023
課題番号：２１Ｈ０３４３８

研究課題名（和文）IPv6ネットワークスキャンの高精度・網羅的な検出に関する研究

研究課題名（英文）Detecting IPv6 network scans with network sensors

研究代表者
福田　健介（Fukuda, Kensuke）

国立情報学研究所・アーキテクチャ科学研究系・教授

研究者番号：９０４３５５０３

交付決定額（研究期間全体）：（直接経費）　　13,300,000円

研究成果の概要（和文）：本研究ではIPv6ネットワークスキャンを効率的に検出するために、既存のセンサーネットワークであるダークネット・ハニーネットを拡張し、ネットワークスキャンを誘引する手法を確立した。手法のキーアイディアは従来のアプローチとは異なり、積極的にセンサーのIPアドレスをネットワーク上に暴露することで、スキャン元にセンサーの存在を認識させる点にある。既存手法および複数のアドレス暴露手法をセンサーネットワークに実装し半年間の観測を行ったところ、既存手法では5件程度のスキャンを検出したのに対して、提案手法では2000件以上のスキャンを検出することに成功した。

研究成果の学術的意義や社会的意義
既存のIPv4インターネットからIPv6インターネットへの移行が進んでいる。IPv6ではアドレス空間が広大なため、ネットワークスキャナーは対象となるIPアドレスを得ることが難しい。同様に、スキャナーを検出するセンサーネットワークにおいてもスキャンが到達しない問題がある。本課題では、センサーアドレスを積極的に広報することで、より多くのスキャンを検出する手法を確立した。これにより、ホスト上の新たな脆弱性が発見された際に、実際の攻撃が始まる前兆である大規模ネットワークスキャンを検出することが可能となった。検出されたスキャンは管理者に対して防御のための重要な事前情報となる。

研究成果の概要（英文）：In this work, we establish a methodology to attract IPv6 network scans, in order to early detect network scans in the wild.
The key idea of the work is to expose IP address block information on sensor networks (i.e, honeynet and darknet) to the Internet so as to detect them by network scanners. We design and implement the proposed sensor networks and deploy to real IPv6 Internet. We confirmed that our proposed method effectively attracts network scans from over the world for more than six months; more than 2000 scans with our method though 5 scans with the traditional method.

研究分野：インターネット工学

キーワード：IPv6　ネットワークスキャン　ハニーネット　ダークネット

様　式　C－１９、F－１９－１（共通）

１．研究開始当初の背景

我々が日常的に使用しているインターネットは、IPv4 および IPv6 プロトコルによって実現されている。IPv4 ネットワークでのセキュリティは従来より議論されているが、ネットワーク全体へのネットワークスキャンは日常的に行われている。これは IPv4 アドレスが 32bit で表現されていることに起因しており、特殊な機器を使用せずとも、全ての IPv4 アドレスへのスキャンは一時間以内に終了可能であることに起因する。そのため、ネットワークスキャンを検出する側においても、ネットワークセンサー(ダークネット、ハニーネット)を設置することで、新たな脆弱性が発表された際に発生するネットワークスキャンを効率良く検出することが可能である。しかし、IPv6 ではアドレス空間が 128bit で実現されており、この広大なアドレス空間を網羅的にスキャンすることは地球誕生からの 50 億年かけても不可能である。これは二つの問題を提起している。ネットワークスキャンを行う側では、いかに効率良く到達可能な IP アドレスの集合を得ることができるか、ネットワークスキャンを検出する側では、いかに効率良くセンサーネットワークへスキャンを誘引するか、となる。スキャンを行う側では、ランダムなアドレスへのスキャンではなく、ヒットリストと呼ばれるアクティブな IPv6 アドレスのリストを用いてスキャンを行う。また、スキャンを検出する側では、ネットワークセンサーが非効率的であることから、CDN (Contents Delivery Network)のようなネットワーク上に大規模分散されたサーバ群におけるスキャンを検出したり、DNS (Domain Name Systems)のようなインダイレクトな通信を用いてスキャンを推定する手法が開発されている。

２．研究の目的

本課題の目的は、上記の「IPv6 ネットワークスキャンを検出する側で、いかに効率良くセンサーネットワークへスキャンを誘引するか」となる。既存研究における IPv6 でのネットワークスキャンの検出は、CDN (Contents Delivery Networks)のようなコンテンツ事業社が多数のサーバーを設置し、そのサーバーに到着するスキャン情報を収集することで実現されている。しかし、この手法は大規模事業者にのみ可能な手法であり、そのような世界規模のセンサーネットワークを持たずとも、より効率の良い検出手法の確立が課題となる。本課題では、IPv6 センサーネットワークの IP アドレスブロックをいかにしてスキャナーに暴露するか鍵となる。先に述べたように、スキャナーはヒットリストを用いてスキャンを行うことから、仮に、スキャナーにセンサーであると認識されることなく、アドレスブロックを暴露し、スキャンを誘引することができれば、脆弱性を攻撃する可能性のある大規模ネットワークスキャンを早期に検出することが可能となる。これはネットワークオペレータにとっては、防御するための時間を得るために重要なステップとなる。センサーネットワークの IP アドレスブロックを暴露する手法はいくつか考えることができるが、どのような手法が最も効果的であるかについての知見は今のところ得られていない。

３．研究の方法

本課題では、IPv6 ネットワーク向けのセンサーネットワークの構築、センサーネットワークの IP アドレスブロック暴露手法の確立、実際に設置したセンサーネットワークに到着するスキャンパケットの振る舞いの同定の三つのステップから構成される。

(1) センサーネットワークの構築では、Virtual Machine 上に Docker によるセンサーネットワークを設計・実装する。対象とするセンサーネットワークとして二つのタイプのセンサーネットワークを想定する。ダークネットは一種のブラックホールであり、アドレスブロックはインターネット上に経路広報されるものの、そのアドレスブロックへのパケットには一切応答しない。ハニーネットは、ダークネットと異なり、到着したパケットに対して返答を行うことで、スキャナーのさらなる反応を引き出す。返答のパターンには単純に Ack を返すものや、より通信プロトコルのセマンティクスに応じた返答を行うものが考えられるが、本課題では、単純に到来パケットに一度のみ返答パケットを確率的に送信する。この二つのセンサーネットワークの違いにより、スキャナーの特徴づけを行うことが可能となる。また、複数のアドレス暴露

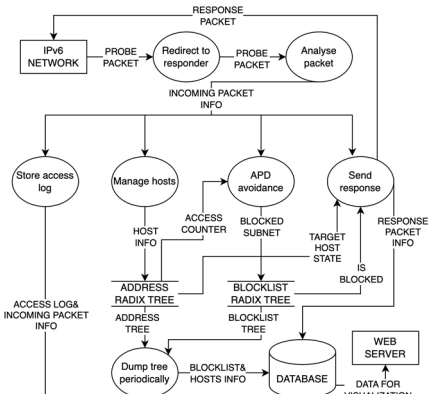

図 1 センサーの反応ロジック

手法を実装する必要があることから、該当する暴露手法に対応するアドレスブロックの割り当てが必要となる。これは一種の A/B テストと考えることができる。そのため、複数のアドレスブロックを自由にセンサーネットワークとして動作させる必要がある。さらに、センサーネットワークに到着するパケットおよび返答を後の解析のために保持するためのデータベースを用意する。センサーネットワークの動作を図 1 に示す。

(2) センサーネットワークの IP アドレスブロック暴露手法として、複数の手法を検討し実際のセンサーネットワークへの実装を行う。

(a) Vanilla: アドレスブロックの暴露を行わない (ベースライン)

(b) IPv4 reverse: IPv4 アドレスは 32bit であり、全てのアドレスの DNS 逆引きを行うことで、それぞれの対応するホスト名を得る。そのホスト名に対して AAAA レコードを調べると対応する IPv6 アドレスが得られる。これは、IPv4/IPv6 のデュアルスタックホストに対応する。これを利用して、暴露したい IPv6 アドレスのホスト名および IPv4 アドレスを DNS 上に設定する。

(c) IPv6 enumeration: IPv6 のアドレス空間を探索することは容易ではない。しかし、DNS の逆引きツリーを網羅的に列挙し検索することで IPv6 アドレスが登録されているホスト名を知ることは可能である。この可能性を調べるために、ランダムな IPv6 アドレスの PTR レコードを登録し、権威 DNS サーバで併せて監視を行うことでこの暴露手法の有用性を調べる。

(d) Special IPv6: ランダムな IPv6 アドレスを人間が認識することは簡単ではない。そのため、ネットワークオペレータはサーバやルータの IP アドレスとして視認性の良いアドレスを設定する傾向にある。その傾向を知るために、視認性の高い IPv6 アドレスを DNS の PTR レコードとして登録する。

(e) Popular service name: ネットワークオペレータはサービス名がわかるようなホスト名を設定する傾向にある。これはユーザにとってもそのサービスに辿りつくことが容易であることから一般的に行われている。そのため、実験ドメインに対して、著名なサービス名をつけたホスト名を DNS に登録することで、そのアドレスを暴露する。

これらの手法をそれぞれダークネット・ハニーネットに独立に適用することで、その傾向を調査する。

(3) センサーネットワークに到着するスキャンパケットの振る舞いの同定では、設置したダークネット・ハニーネットへ到着するパケットを、それぞれの暴露手法を設定・公開した後から、測定しその傾向を調べる。とりわけ、公開されている IPv6 ヒットリストへの掲載のプロセス、ヒットリストへの公開後のアドレススキャンの時系列、どのような組織からのスキャンであるか、等の解析を実データより行う。観測実験は 2023 年 4 月より 2023 年 12 月までの 8 ヶ月行った。

4. 研究成果

	Darknet	Honeynet
Vanilla	5	1
IPv4 reverse	1.7K	2.0K
IPv6 enumeration	2	2
IPv6 special	1	1
Ipv6 popular name	4	2

図 2 到着スキャンパケット数

図 2 に暴露手法の違いによる、センサーネットワークへのスキャンパケットの到着数を示す。図より明らかなように、IPv4 reverse による手法は他の手法と比べて 1000 倍以上のスキャンを誘引することに成功している。他の暴露手法は、Vanilla 設定とほぼ変わらないことから、期待

したような結果が得られていない。これは、IPv4 reverse 以外の手法では、スキャナーが暴露されたアドレスを得るためにより多くの時間が必要であることを示唆している。また、ダークネットとハニーネットの比較では、ハニーネットにより多くのパケットが到来することがわかった。これは、スキャナーがヒットリスト等により、よりアクティブなホストを発見し、スキャンを行っていることを表している。

次に、ハニーネットに対してどのような時系列でパケットが到来するかに着目する。暴露手法およびセンサーネットワークを稼働させた日を起点として、そこから、どのような間隔でパケットが到来するかをプロットする(図 3)。図には AS ごとに初めてパケットが到来した日を示し、同様に、IPv4 Reverse の兆候となる DNS クエリが発生したタイミングを示している。観測開始から数日で、DNS クエリが発生し新しい IPv6 アドレスの存在が暴露され、その数日後には、一般公開されているヒットリストに当該アドレスが掲載されたことがわかる。そして、その後には、異なる AS からスキャンが到来している。これは、アドレス暴露、ヒットリスト掲載、スキャンというスキャナーのライフサイクルをデータより実証できたことを意味する。

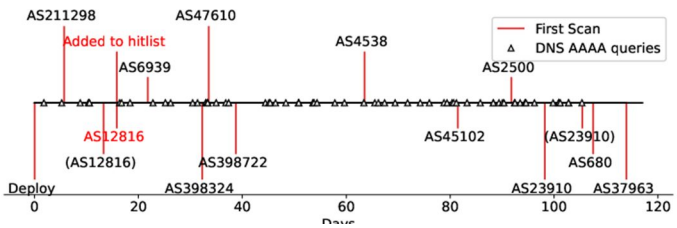

図 3 パケット到着パターン

さらに、スキャナーが公開されているヒットリストを利用しているか、もしくは自分でヒットリストを構築しているかを調査した。公開されているヒットリストはアクティブなホストのみを掲載している。そのため、ハニーネットに登録されているアドレスのみが対象となる。ダークネットに登録されたアドレスは暴露され収集されているものの、到着パケットに対して返答を行わないことから、ヒットリストには掲載されない。つまり、ハニーネットに登録されたアドレスのみにスキャンを行うスキャナーは公開されているヒットリストを利用している確度が高く、ダークネット・ハニーネットの両者にスキャンを行うスキャナーは自分でヒットリストを(IPv4 Reverse の手法で)作成しスキャンを行っている可能性が高い。

図 4 は、横軸にダークネットへの AS ごとのパケット到来数・縦軸にハニーネットのパケット到来数をプロットしたものである。この散布図から、3 つのスキャナーのパターンを検出することに成功した。(1) Honeynet exclusive は公開ヒットリストを用いたスキャン、(2) Balanced は公開ヒットリストでなく独自の IPv4 reverse によるヒットリストを用いたスキャン、(3)Honeynet predominant は Balanced からさらにランダムスキャンを組み合わせたもの、である。この結果より、多くのスキャンは公開ヒットリストもしくは IPv4 reverse を用いた独自ヒットリストを利用していることが明らかとなった。スキャナーの IP アドレスおよび AS 番号を調査したところ、そのほとんどは学術機関もしくはクラウドプロバイダーによるものであった。

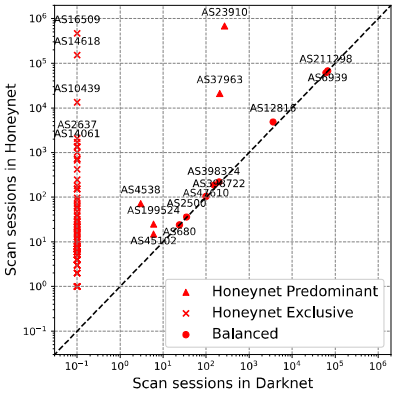

図 4 スキャンパターン分類

図 5 は、上記のスキャンタイプごとの送信パケットのプロトコル別分類である。公開ヒットリストを使用しているスキャナーは ICMP6 のみ、TCP/UDP のみのように、様々なパターンを持つスキャンとなっている。独自ヒットリストを用いたスキャンではほぼ TCP を用いたスキャンとなっており、スキャンを行う側の意図が公開ヒットリストのスキャンとは異なる可能性を示唆している。

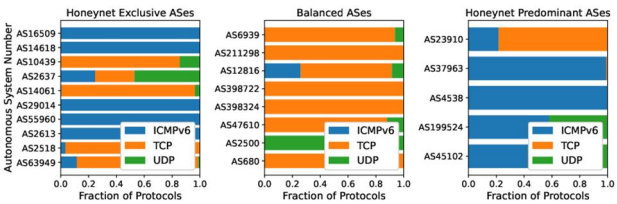

図 5 プロトコル別分類

この他にも、大規模スキャンキャンペーン、プロトコルポート単位での傾向、様々な特徴を解析し、IPv6 ネットワークスキャナーの挙動を明らかにした。

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 L.Zhao, S.Kobayashi, K.Fukuda	４．巻 0
２．論文標題 Exploring the Discovery Process of Fresh IPv6 Prefixes: An Analysis of Scanning Behavior in Darknet and Honeynet	５．発行年 2024年
３．雑誌名 Proc. PAM 2024	６．最初と最後の頁 95-111
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-56249-5_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 G.Hu, K.Fukuda	４．巻 0
２．論文標題 Privacy Leakage of DNS over QUIC: Analysis and Countermeasure	５．発行年 2024年
３．雑誌名 Proc. ICAIIC 2024	６．最初と最後の頁 518-523
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICAIIC60209.2024.10463369	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 L.Zhao, S.Kobayashi, K.Fukuda	４．巻 0
２．論文標題 Design and Implementation of IPv6 Scan Detection System	５．発行年 2023年
３．雑誌名 IEICE General Conference	６．最初と最後の頁 1-3
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 G.Hu, K.Fukuda	４．巻 106
２．論文標題 Characterizing Privacy Leakage in Encrypted DNS Traffic	５．発行年 2023年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 156-165
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2022EBP3014	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 K.Fukuda, Y.Aharen, S.Sato, T.Mitamura	4．巻 0
2．論文標題 Characterizing DNS query response sizes through active and passive measurements	5．発行年 2022年
3．雑誌名 Proc. IEEE ANNET2022	6．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/NOMS54207.2022.9789912	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 G.Hu, K.Fukuda	4．巻 0
2．論文標題 An analysis of privacy leakage in DoQ traffic	5．発行年 2022年
3．雑誌名 Proc. ACM CoNEXT student workshop 2022	6．最初と最後の頁 7-8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3488658.3493782	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
連携研究者	小林　諭 (Kobayashi Satoru) (40824107)	岡山大学・学術研究院環境生命自然科学学域・助教 (15301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関