情報セキュリティ研究用ハニーポット通信データの一般頒布に向けた技術的要件の調査

細井 琢朗 †　　松浦 幹太 †

† 東京大学生産技術研究所
153-8505 東京都目黒区駒場 4-6-1
{hosoi, kanta}@iis.u-tokyo.jp

あらまし ネットワークセキュリティ分野の研究で利用される通信データは、プライバシー情報や危険なデータを含む可能性があるためほとんどの場合公開されず、研究成果の検証や類似研究の推進の壁となっている。本研究では、共通の研究用データセット CCC DATAset 2011 内にも主要なデータとして含まれる、ハニーポットの通信データをセキュリティ研究向けに一般頒布することを考えた場合に、その通信データに求められる技術的要件を、安全性と有用性の観点から調査した。また一例として、CCC DATAset 2011 の「攻撃通信データ」で、通信データ取得ホストの位置特定が目的と疑われる通信の検出を簡便な方法で試みた。

Investigation on Technical Requirements toward Open Distribution of Honeypot Trace Data for Information Security Research

HOSOI Takurou†　　Kanta Matsuura†

†Institute of Industrial Science, The University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo 153-8505, Japan
{hosoi, kanta}@iis.u-tokyo.jp

Abstract Traffic data (traces) which are used in network security researches potentially contain privacy information and hazardous data, so most of them are only used privately, which hinders third-party verification of their results and promotion of their relating researches. In this research, we investigated technical requirements for honeypot traces, such as ones included in the common research dataset CCC DATAset 2011, toward their open distribution for information security researches regarding their security and usefullness. We also tried to detect suspicious host location identification traffic from Attack Traffic Data of CCC DATAset 2011 by simple easy ways as a first step.

1　導入

ネットワーク通信を何らかの形で残したデータ（ログ）は、ネットワークセキュリティ技術の研究、開発、教育に役立っている。例えば、MIT Lincoln Laboratory で製作され Web 上で一般にも公開されている、DARPA Datasets [1] と呼ばれているネットワーク通信データセットの登場により、侵入検知システム（IDS）の研究が非常に活発に進められた。また近年では、CCC DATAset 2008 、2009 、2010 、MWS 2011 Datasets [2]（CCC DATAset 2011 を含む）というデータセットの作成と配布も行われている。こちらのデータセットは提供先を研究者向けに限定することで、主にマルウェア対策の研究に有用なものとなっている。

このように有用なデータセットが共有されることで、異なる研究、技術の性能評価が同じデータセットによって行われ、より客観的な比較が可能になることや、データの容易な入手による研究の促進などが期待される。しかしその共有にはいくつかの解決すべき課題があるため、多くは非公開となっている。まず、インターネット上では危険性のある通信も行われており、それを記録したデータセットは取り扱いに注意が必要になる。次に、ネットワークを流れる通信の記録を作ると、そのネットワークを使用していた利用者の個人的な情報を含んでしまい、プライバシーの観点からそれをそのまま配布することには問題がある。また、場合によってはネットワークの情報、特に各ネットワーク機器の接続情報を隠す必要があるために、データセットを共有できないこともある。

これらの課題の多くは、ネットワークデータセットの匿名化技術により、ある程度解決できる [3]。しかし、その手法はほとんどの場合復元不能な情報の劣化を伴い、匿名化後のデータセットの有用性を損なってしまう。そのため汎用の完全な匿名化手法というものはなく、匿名化の際は、データセットの匿名性と有用性の兼ね合いの中で個別の条件に合うように各種手法を適用することになる。その手法は何をどのような漏洩攻撃から守るのかで決まる。我々は情報セキュリティ技術研究向けのハニーポットの通信データに着目した。この種類の通信データは CCC DATAset 2008 、2009 、2010 、2011 にも「攻撃通信データ」として含まれており、これまで多くの研究を支えてきている。本研究では、ハニーポットの通信データをセキュリティ研究向けに一般頒布することを考え、その通信データに求められる技術的要件を、安全性と有用性の観点から調査した。また一例として、CCC DATAset 2011 の「攻撃通信データ」内で、通信データ取得ホストの位置特定が目的と疑われる通信が検出できるかどうかを簡便な方法で試みた。

2 ネットワークデータの匿名化手法と漏洩攻撃

ネットワークデータの匿名化技術は既に多くの研究がなされ、実用化もされている。また、匿名化されている場合であってもネットワークデータからさまざまな情報を引き出す漏洩攻撃が存在することが知られている [3]。この節では、主な匿名化手法と漏洩攻撃について、既存研究 [3, 4] をもとに簡単に紹介する。

2.1 ネットワークデータの匿名化

ネットワークデータの匿名化とは、ネットワークデータに本来含まれる情報を隠すことで、ネットワークの情報や利用者の情報が漏れるのを防ぐことである。そのために、ネットワークデータ、特に通信データに含まれる各種の情報（MAC アドレス、IP アドレス、ホスト名、ポート番号、プロトコル名、時刻、通信内容など）のいくつかを、データの使用に阻害がない程度に変更する。その主な方法を以下に挙げる。

黒塗り（black marker） 対象とする情報部分を完全に 0 （または意味のない無関係な値）で置き換える。これによりこの情報は完全に秘匿できるが、この情報を必要とする技術では使えないデータとなってしまう（例 : 発信元 IP アドレスを黒塗りすると、攻撃元を特定する技術のほとんどでは使えない）。

一部削除（truncation 、annihilation 、partitioning） 対象とする情報部分を一部分切り詰めること（truncation）や、意味のある部分に一旦分割して、その一部のみを黒塗りする（annihilation 、partitioning）ことで、この情報をある程度秘匿する（例 : IP アドレスの下位 8 ビットのみ残す、時刻情報の日付部分を 0 にする、など）。残りの情報があるため、黒塗りほどにはデータの有用性は損なわれないが、その分の情報漏れが起きる。

置き換え（permutation 、prefix-preserving 、shift 、emuneration） 対象とする情報部分の各ビットを一定の規則（暗号化を含む）に従って一対一に置換する（permutation）、残したい一部分以外をランダムな値で置き換える（prefix-preserving）、値を一定値ずらす（shift）、値の大小は保ったまま値を変更する（emuneration）、などの方法がある。前者二つは匿名化後も個体識別が可能なため、IP アドレスの秘匿によく用いられる。ただし、いくつかの漏洩攻撃は個体識別が可能な場合に成功してしまい、その場合この方法では攻撃を防ぐことができない。後者二つは時刻情報に用いられることが多い。

ハッシュ値（hash 、HMAC）　ハッシュ値や鍵付きハッシュ値に変換することで、対象とする情報を秘匿する。置き換えの一手法と言えるが、負荷の割に、IPv4 の IP アドレス（32 bit）のように短いデータ列に対しては辞書攻撃により秘匿性を破られてしまうという欠点がある。

これらの方法により、対象とした各情報そのものは隠すことができる。ただし、統計的な解析や、フィンガープリントを使った攻撃により、秘匿したかった情報（ネットワークの接続情報、利用者のプライバシー）が漏れることがあるため、条件（秘匿したい情報、秘匿してはいけないデータ部分の特定）と適用する手法の選択には注意が必要である。

2.2　ネットワークデータに対する漏洩攻撃

生のネットワークデータからは、当然多くの情報が漏れる。これに対抗するために匿名化手法が開発されたが、ある使用目的のためにネットワークデータを用意する以上、その中にはさまざまな情報がふくまれており、それを元に情報を引き出す手法（漏洩攻撃）が存在する。主な漏洩攻撃を以下に列挙する。

フィンガープリント攻撃　ポート番号、通信量、サーバやクライアントの振る舞い、ホストの種類（OS や NIC など）に特有の情報をフィンガープリントにして、利用者のプライバシー情報や、ネットワーク構成、接続ホストの種別の情報などを明らかにする。それぞれ使用するフィンガープリントに対応して、攻撃に必要な情報（ポート番号、通信量、時刻情報、ネットワーク遅延量など）がある。また、その多くの手法では、個体を識別できる程度の IP アドレス情報が必要である。

構造認識　一対一に対応する置換方法で IP アドレスを匿名化した場合に一つでも本物の IP アドレスが漏れると残りも分かってしまう、ポートスキャンの通信記録から IP アドレスの並び順がわかる、など、ネットワークデータの情報以外の知識を使ってネットワーク構造の情報を取り出す攻撃方法である。この手法でも、個体を識別できる程度の IP アドレス情報が必ず必要である。

既知情報への写像　例えば、同じネットワークから、通信データを匿名化して、また通信ログ（ヘッダ情報のみ）を匿名化せずに提供した場合に、通信ログと通信データを照らし合わせて、通信データの匿名化を破るような攻撃を指す。この手法では、照合のための匿名化されていないデータが必要である。

暗号学的手法　匿名化手法には、秘匿したい情報を、暗号技術（暗号化、ハッシュ値）で隠す方法がある。これらの方法を対象に、その使用された暗号技術に脆弱性があった場合に、その脆弱性を使って匿名性を破る攻撃がこの手法である。使用した暗号技術そのものに脆弱性がなければこの攻撃は成功しない。一方、前述したように、IPv4 の IP アドレスをハッシュ値に変換した場合などは、この分類の漏洩攻撃の一つである辞書攻撃が成り立つ。これはハッシュ関数を安全に使用する条件（80 ビットセキュリティ）を満たしていないという、暗号技術の運用の間違いのために、ハッシュ関数が本来持つ安全性を発揮できていないことが原因である。

データインジェクション　これには大きく分けて二つの種類がある。一つは送信した通信そのものはネットワークデータに記載されていなくても、その通信の活動が反映されていることを検出して匿名性を破る、probe response 攻撃である。例えば、ネットワークの統計情報（あるポートへの通信量の時間変化のグラフなど）を公開しているホストがあると、見当を付けてそのポートへ多くの通信を送り付けることで、統計情報を収集しているホストの IP アドレスを、その統計量の変化から見つけることができる [5]。

もう一つの手法は、他のパケットと区別しやすい、特徴的なパケットを送り付け、そのパケットをネットワークデータから検出することで、そのネットワークデータを収集しているホストを特定する攻撃である。以降この攻撃をパケットインジェクション攻撃と呼ぶ。

3　ハニーポット通信データの共有化の課題

1 節で述べたように、ネットワークデータの共有にはいくつかの解決すべき課題がある。それはハニーポットの通信データにおいても同様である。この節では、情報セキュリティ研究向けにハニーポットの

通信データを共有することを考え、その有用性と安全性から来る諸条件を整理し、克服すべき課題を明らかにする。

3.1 有用性確保のための条件

MWS 2011 で発表されるような情報セキュリティの研究にハニーポットの通信データを使う場合、そのデータ収集元と使用目的から、通信データに通常求められるものよりも厳しくなる条件と、緩くなる条件がある。以下に、匿名化に関係する条件を列挙する。

1. ICP 、UDP のポート番号はそのまま残す必要がある。
   ネットワーク経由の各種の攻撃は、それぞれのネットワークサービスに対応して行われる。そのため、情報セキュリティ研究に有用な通信データとするには、TCP 、UDP のポート番号を匿名化することはできない。

2. 多くの場合、厳密な時刻情報は必要ない。
   多くのネットワークセキュリティ研究では、通信データのあるパケットが発信、到着した厳密な時刻は必要ない。そのため、時刻情報についてはある程度の匿名化が可能である。ただし、他のデータ（接続ログなど）も提供する場合は、それらとの照会ができるようにしておく必要がある。また、ネットワークセキュリティ技術の一部には、各通信の相対時間を利用するものがある。そこで、時刻情報を匿名化する場合には、単純なシフトを余り大きくないシフト量で使うのが望ましい。

3. 通信内容はそのまま残す必要がある。
   例えば多くのマルウェア検知技術は、パケットに格納されている通信内容のデータを検証することで検知を行っている。また、アプリケーション層での通信内容の再構成が必要なことも少なくない。そのため、情報セキュリティ研究に有用な通信データとするには、通信内容を匿名化することはできない。

4. 上記の条件から、TCP のセッションの再構成ができるよう TCP のヘッダ情報なども匿名化することはできない。

5. 不要な通信（パケット）は削除して構わない。
   ハニーポットの役割は、実際にネットワークに接続してマルウェアに感染されるなどのネットワーク攻撃を受けることで、攻撃に関係する情報を収集することである。また、ハニーポットの通信データを情報セキュリティ研究に用いるのも、この攻撃に関係する情報を使うためである。そこではネットワーク研究のための通信データとは異なり、通信量を実際から少々変えてしまっても問題はない。従って、注目するネットワーク攻撃に関係しないパケットを削除した通信データでも、セキュリティ研究には十分有用なものになる。

これらの条件を満たすことで、情報セキュリティ研究に有用なハニーポット通信データとなる。

3.2 安全性確保のための条件

ハニーポットとその通信データの安全な運用のための条件をここで整理する。

まず、危険な通信が含まれる点について考える。ハニーポットの役割は、実際にネットワーク攻撃を受け、その情報を収集することであるため、その通信データには必ず攻撃の通信を含む。情報セキュリティ研究でこの通信データを用いるのも、この攻撃の通信を利用するためである。従って、危険な通信は必ずこの通信データに含まれる。これが含まれていなければ、情報セキュリティ研究向けの通信データとして有用性が無くなってしまう。そこで、この点については、注意深い運用でその安全性を達成する必要がある。

次に、ユーザのプライバシーについて考える。通常のホストとは異なり、ハニーポットにはユーザがいない末端機器であり、誤って送られる場合を除き、メールの送受信や Web サイトの閲覧などの通信はない。そのため、ユーザのプライバシーが通信データから漏れることはない。すなわち、この点については安全性は達成されている。

最後に、ネットワークの情報について考える。ハニーポットはマルウェアに感染することもあるため、万一の事故の影響を少なくできるように、一般の機器とは別れたネットワーク接続をする。そのためネットワークの構成情報が漏れても問題はない。しかし、ハニーポットはその運用のために、以下の情報を秘匿する必要がある。

- ネットワーク上での位置（IP アドレス）
- 運用情報（収集稼動時間など）

これらの情報が漏れると、ネットワーク攻撃をする者はこのハニーポットを避けて攻撃を行うことができ、ネットワーク攻撃の情報収集というハニーポットの役割を果たせなくなってしまう。そのため、特にハニーポットの位置情報は、頒布されるハニーポット通信データから漏れないよう、匿名化などで手当てしておく必要がある。

3.3 条件を満たす匿名化

この節でのこれまでの議論から、ハニーポットの通信データを情報セキュリティ研究向けに頒布するための技術的要件は、TCP 、UDP ポート番号や通信内容を保持したまま、ハニーポットの位置特定ができないように手当てをすることであることが分かった。そのためには、まずネットワーク内の位置に関する以下の三つの情報を通信データ内で匿名化する必要がある。

a. MAC アドレス。
   これは情報セキュリティ研究においては、パケットの送出と受信を区別する際に使える（実際には IP アドレスで区別することが多い）程度の情報である。そのため、MAC アドレスは黒塗り、もしくは各ハニーポットとその上流の区別をできる程度に変換してしまって構わない。

b. ホスト名。
   いくつかのホスト名は、そこに接続する機器の位置の推定に役立ってしまう。この情報は、下記の IP アドレスとともに匿名化する必要がある。

c. IP アドレス。
   これはインターネットでの位置情報そのものであり、必ず秘匿する必要がある。ハニーポットの IP アドレス自体はプライベート IP アドレス空間のものを使用している場合もあるが、その場合でも、他の機器の IP アドレスを含めて、ホスト名と共に、匿名化による秘匿が必要である。ただし、通信内容の切り分けや通信先の判別が必要なことから、IP アドレスは黒塗りすることはできず、個体識別可能な形に変換することになる。

IP アドレスやホスト名の匿名化には多くの既存研究があり、それらを用いることで、この匿名化は達成できるものとする。

ハニーポットの位置特定を防ぐには、この三つの位置関連情報の匿名化に加え、2.2 節で述べた、データインジェクションも防ぐ必要がある。データインジェクションについては、通信の統計情報を公開するホストを守るために、公開の方法に工夫を加えて耐性を付ける方法（例 : [5]）が既に提案されているが、通信データに対して行われた場合については既存研究を見つけることができなかった。

ハニーポットではその役割から通信が送られてくることを防ぐことはできないため、データインジェクション攻撃を防ぐには、該当するパケットが通信データに含まれた形で攻撃者の手に渡るのを防ぐしか方法はない。probe response 攻撃の場合はある程度の量の通信が送られてくるので、異常検知技術で検出し、それらの通信を取り除くことで攻撃を不成立にさせることが可能と思われる。一方、パケットインジェクション攻撃は、工夫された単一パケットでも漏洩攻撃が成り立つ。この攻撃を防ぐことが、ハニーポット通信データの情報セキュリティ研究向け頒布への残された必要条件となる。

2.2 節で紹介した他の漏洩攻撃のうち、フィンガープリント攻撃と構造認識の方法は、3.2 節の議論により、プライバシー漏洩、ネットワーク構成情報の漏洩、どちらも問題がないため、問題にならない。また、暗号額的手法については、IP アドレスやホスト名の匿名化、もしくはデータインジェクション攻撃への防御の際に用いる場合のみ、考慮が必要となる。

4 位置特定目的が疑われる通信検出の試み

3.3 節での議論から、パケットインジェクション攻撃を防ぐことが課題として残されていることが判った。この攻撃についても、そのパケットを検出して通信データから取り除くことができれば、攻撃を不成立にさせることができる。この攻撃は単一パケットでも可能な点が特徴である。一方、ネットワーク攻撃は、その実行時の負荷や、ネットワーク内に残る痕跡を減らし、攻撃に気付かれにくくするために、通常その通信をなるべく減らして行われる。

そこでこの節では、パケットインジェクション攻撃が単一のパケットで行われると仮定し、そのようなパケットが検出できるかどうかを簡便な方法で試みた。その方法は以下の通りである。

> ある受信パケットの前後一定期間に、同じ発信元（= 同じ IP アドレス）から送信されたパケットがない場合、このパケットを孤立パケットと呼ぶことにする。この孤立パケットを抽出する。
> パケットインジェクション攻撃のパケットはこの孤立パケットの中に含まれていると期待する。

CCC DATAset 2011 に含まれる、期間が連続する 5 個の pcap ファイル群について、前後の一定期間というものを暫定的に 10 分間に設定してこの孤立パケットの抽出を行った結果は、表 1 のようになった。

表 1: 孤立パケットの抽出結果
（前後 10 分間に同一送信元からの受信無し）。

	ハニーポット 1		ハニーポット 2	
	検出数	全パケット数	検出数	全パケット数
2008 年	343	8495403	222	7277796
2009 年	118	1567450	10	1944400
2010 年	261	12364268	395	10122434
2011 年 (1)	535	9521188	501	2889979
2011 年 (2)	468	7735025	503	2863121

全ての pcap ファイル群から、全体に対して小さな割合ではあるが有意な数の孤立パケットを拾うことができた。ただし、これらのパケットのほとんど（九割以上）は、IP datagram として長さが 100 byte 以下のものであった。IP datagram はヘッダ長が 28 byte あるため、これらのパケットは他のパケットと容易に区別できるようなものではないと考えられる。残りの一割弱に実際にパケットインジェクションが含まれているか、今後調査を進める予定である。

また、今回の孤立パケットの抽出の際には、処理を早めるため、受信パケットでのみ抽出を行った。しかし実際には、受信パケットとしては孤立していても、その前後に対応する送信パケットがあることがある。今回もハニーポットから NTP サーバへの時刻合わせの要求に対して帰ってきたパケットの一部を孤立パケットとして抽出してしまっている。これらのパケットは孤立しているとは言えず、孤立パケットとして抽出されるべきではない。この点も改良が必要である。

5 まとめ

本研究では、CCC DATAset 2011 にも攻撃通信データとして含まれている、ハニーポットの通信データを情報セキュリティ研究向けに頒布することを考え、それに必要な技術的要件を調査し、整理した。その結果、多くの要件については、既存技術で対応できる見込みがあることが判った。一方、データインジェクション攻撃、特にパケットインジェクション攻撃への防御が課題として残っていることが判った。今後はこの防御を可能にする方法の研究を進めたいと考えている。

参考文献

[1] DARPA Datasets (1998, 1999, 2000), MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation Data Sets, `http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html`

[2] 畑田充弘, 他, “マルウェア対策のための研究用データセット ～MWS 2011 Datasets～”, コンピュータセキュリティシンポジウム 2011 (CSS 2011), マルウェア対策研究人材育成ワークショップ 2011 (MWS 2011), （2011 年 10 月）

[3] Justin King, Kiran Lakkaraju, Adam Slagell, “A Taxonomy and Adversarial Model for Attacks against Network Log Anonymization”, Proceedings of the 2009 ACM symposium on Applied Computing, pp.1286-1293 (March 2009)

[4] Adam Slagell, Kiran Lakkaraju, Katherine Luo, “FLAIM: A Multi-level Anonymization Framework for Computer and Network Logs”, Proceedings of the 20th Large Installation System Administration Conference (LISA ’06), pp.63–77 (December 2006)

[5] Yoichi Shinoda, Ko Ikai, Motomu Itoh, “Vulnerabilities of Passive Internet Threat Monitors”, 14th USENIX Security Symposium, pp.209-224 (August 2005)