高速化/大容量化する通信下での情報セキュリティのためのデータ処理

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
嶋田 創

概要

- 背景: 近年の情報セキュリティ問題(サイバー攻撃対策)
  - 近年の高度化/拡大するサイバー攻撃
  - サイバー攻撃の防御とその課題
  - サイバー攻撃防御側の希望
- 高速かつ大量な通信データの処理によるセキュリティ向上
  - アノマリ検知
  - ディープニューラルネットワーク応用
- 自分の個人情報をデータサイエンスから守れるか?

Q: なぜサイバー攻撃が行われるのか

- 厳密にはサイバー攻撃を利用した犯罪(サイバー犯罪)
- 疑問
  - その攻撃手段への発想力を活かせば高収入で社会的地位の高い職業につけるのでは?

- A: 金になるから
  - 普通の職業についていたら一生かかっても稼げない金が手にはいるなら?

A: 金になるから

- クレジットカード情報: $4-$20
  - どこで発行されたかによって価値が違う
  - 悪用の他に、ブラックマーケットで売るという手も
- 銀行(オンラインバンキング)決済情報
- 企業秘密
  - 他にも、どうしても手に入らない技術を手に入れるためとか
  - 某国は軍事技術に利用できる技術を一生懸命盗もうとしています
- 脅迫ネタ
  - 機密情報を手に入れた
  - サービス不能(DoS)攻撃をかけるぞ

ブラックマーケット情報や攻撃の相場(の噂)

- 本人認証に使われる情報: $1-$3
  - 社会保障番号、生年月日、など
- Remote Administration Trojan（RAT）: $20-$50
- ウェブサーバ乗っ取り: $100-$200
- DDoS攻撃: $60-$90 / day
- 感染して乗っ取ったコンピュータ: $120-$200 / 1000台

金以外にもサイバー攻撃をする人はいる

- ハクティビスト
  - サイバー攻撃で政治的主張をしたい人
  - Anonymousや某過激化が代表格
- スクリプトキディ(とその亜種)
  - 基本的にネットに転がっているツールを使うだけ
  - 昔ながらの功名心から攻撃をしかけている
  - たいていはツールを使うだけだが、勉強熱心で成長性の高い人も
    - 個人的には、ツールを適切に使いわけて目的を達成できるようになればスクリプトキディを卒業していると思う
- ネットに溢れる情報のおかげで意外とこのような攻撃も馬鹿にならない
  - 仲間を増やそうと熱心に勧誘していたりするし…

金になるサイバー攻撃をする人の分類

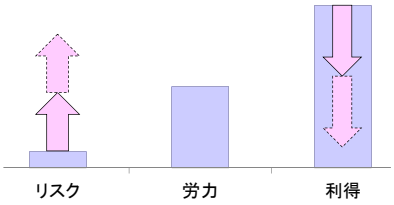
- 無差別型
  - RATなどでボットネットを作って利用権を売りたい
  - RATで侵入した不正クレジットカード利用で換金物を購入
  - ランサムウェアに感染させて脅迫
  - →一般的な防御でまあなんとかなる
- 標的型
  - (D)DoSで業務妨害する
  - 情報窃取をしかける
  - →繰り返し狙ってくるので厳しい

攻撃が目的ではないけど、ある意味攻撃とも言えなくもないもの

- 脆弱性を探してくれるのだけど、そのやり方がアレな所
  - 攻撃者側の手間も減らしていない?
- 「それ、デマだから」な情報をもとに脆弱性を指摘する所

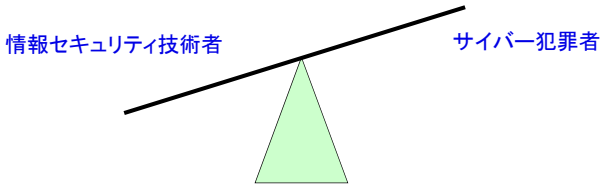
現状のサイバー犯罪

- 現在のサイバー犯罪はリスクに対して利得が大きすぎ
  →リスクを上げて利得を減らす必要がある
- ただし、サイバー犯罪は世界規模なので、リスクを上げれない国家があることを考えておく必要がある



現状の勢力バランス

- 情報セキュリティ技術者の方が分が悪い
- そもそも後手後手に回ることになる
  - 犯罪者側は未発見の攻撃手段を1つ見つければ良い
  - 犯罪者は市販の情報セキュリティ技術を試せる



マルウェアとは

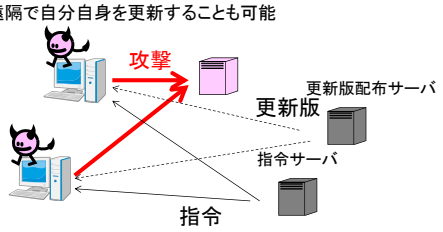
- MALicious softWARE(悪意のあるソフトウェア)の略
- かつてはよくコンピュータウイルスと呼ばれていたが、最近はマルウェアと称すことが多い
- コンピュータウイルスとの違い
  - 愉快犯や技術誇示からサイバー犯罪の道具へ
  - おおっぴらに感染/拡散しない
    - 特定のグループ/ネットワークのコンピュータにのみ感染
    - そもそも、あまりばらまくと発見される可能性が高くなる
  - おおっぴらに怪しい通信したりしない
    - 他の通信にまぎれて通信したりします
  - おおっぴらに破壊活動をしたりしない
    - 発見されると証拠隠滅することもあります

マルウェアの分類

- RAT(Remote Administration Trojan)
  - 遠隔で感染したPCを操作可能な形にする
  - トロイの木馬、ボットネットクライアント、などもこれに分類
  - 自分が加害者になる点が怖い
- スパイウェア
  - 金融関係情報や各種サービス用ユーザ名/パスワードの窃取
  - キーロガーやスクリーンショット取得などの機能
- ドロッパ(ダウンローダ)
  - より高度なマルウェアを送り込む
  - 他のファイル形式の脆弱性を利用した実行ファイルのカプセル化
- 昔ながらのもの
  - ウイルス: 無差別に近い拡散、PCに何らかの異状を発生させる
  - ワーム: 増殖することに特化

RAT(Remote Access Trojan)

- トロイの木馬、バックドア作成、踏み台ツールの発展
- 指令を受け取って攻撃などの動作を取る
  - 昔はIRC経由が多かったが、マークされるようになったので最近はHTTPやHTTPS経由で指令受信
  - DDoS攻撃などにも利用
  - 遠隔で自分自身を更新することも可能



代表的なRAT: Poison Ivy

- バージョンアップしながら今も利用されている
- 機能
  - スクリーンショット、音声、Webカメラの画像の取得
  - アクティブなポートの表示
  - キー入力操作情報の収集
  - 開いているウィンドウの管理
  - パスワードの管理
  - レジストリ、プロセス、サービス、デバイス、インストールされているアプリケーションの管理
  - ファイル検索、同時に多数のファイル移動の実行
  - リモートシェルの実行
  - サーバの共有
  - 自身の更新、再起動、終了

RATを体験してみよう

ShinoBOT Suite

- ドロッパから模擬RATから遠隔操作まで体験できます
  - ただし、操作は全てShinoBOTサイトを経由して記録されます
- お偉いさんへのデモンストレーションとかに使えます
- 最近だと色々とセキュリティ警告が出て体験しづらくなりました

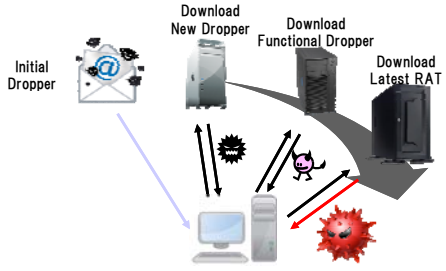
マルウェアの送り込み方

- 昔ながらのメール
  - 本体に添付することは減ってきてウェブからのダウンロードが中心に
  - 複数のダウンロードを繰り返すDrive-by-Download攻撃も
  - 標的化: ビジネス等でやりとりのある相手を装ってメール
- ウェブからのダウンロード
  - 攻略されたウェブサイトから配布
  - ウェブ広告にまぎれて配布
  - 標的化: 水飲み場型攻撃
    - 特定のユーザがよく見るウェブサイトにマルウェアをしかける

マルウェア送り込みのテクニック: Drive-by-Download

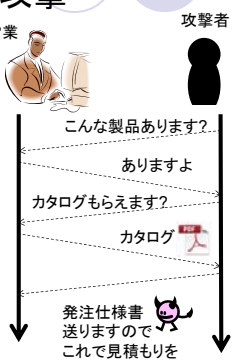
- 複数のサーバを経由して複数のマルウェアを送り込む
- 途中で条件によって攻撃を中止

→アンチウイルス側に検体を提供させない



マルウェア送り込みのテクニック: やりとり攻撃、水飲み場型攻撃

- やりとり攻撃
  - 複数回のメールのやりとりの後にマルウェア送付
- 水飲み場型攻撃
  - 「ある仕事をしている人が頻繁に見るページにマルウェアを仕掛ける」ことによる特定業種の業社への標的型攻撃
  - 例: 政府のある機関のプレスリリース、入札公告ページ
    - その機関に関連する会社に対して攻撃
    - さらにIPアドレスを制限する事例もある



攻撃用メールアカウント準備

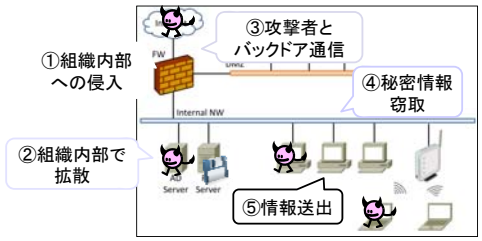
周りから攻撃していくにしろ、攻撃用メールアカウントはあった方が便利(に思える)

- 従来だったら
  - セキュリティのゆるいフリーメールアドレスを利用する
  - 従来同様に無差別攻撃用にspam送信用メールサーバを(乗っ取ったPCを用いて)立てること

  →ただし、あまりにも評判が悪くなると後述のブラックリストで対策される
- 近年では
  - そこそこメジャーな組織のメールアカウントを乗っ取って送信
  - アカウント名の名寄せなどで、外部ウェブサービスなどとアカウント/パスワード共有していたりすると外部が漏らした時に…

標的型攻撃の進行

- 非常にざっくり書くと5段階
  - 侵入前に組織の内部構成を調査することもある
  - 組織内での拡散において、潜伏、索敵を行うこともある
  - 長いものだと攻撃に数ヶ月かけることもある



標的型攻撃の実例(1/3)

三菱重工への標的型攻撃

- 発覚: 2011/8/11にサーバが再起動を繰り返すため
- 影響範囲
  - サーバー 45台、従業員用PC 38台
  - 8種類のウイルスを発見
  - 11の事業所から発見
- 発端: “原発のリスク整理”という添付ファイル
  - 東日本大震災(2011/3)の直後
  - Adobe Flashの脆弱性を利用
  - 送信元は内閣府実在の人物の名前、メールアドレスを騙る
  - 三菱重工は原発を作っている(いた)ので、受け取った人は疑わない

標的型攻撃の実例(2/3)

JAXAへの標的型攻撃[1]

- 特に長期間に渡った例(1年8ヶ月にも及ぶ)
- 発見: 2012/11/21
- 発端: 2011/3/17
  - なりすましメールの添付ファイル

日本年金機構への攻撃[2]

- 短期間に31台の端末が感染、ローカルに保存してあった情報が流出
- 発見: 2015/5/19
- 発端: 2015/5/8
  - メールの添付ファイル

[1] http://www.jaxa.jp/press/2013/02/20130219_security_j.html
[2] https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf

標的型攻撃の実例(3/3)

EmEditorアップデートファイルを利用した攻撃[1]

- 攻撃対象: 名古屋大学、JAXA、ISAS、朝日新聞、農林水産省など
- 以下の様な.htaccessファイルがアップデート配布ディレクトリに置いてあった
  - 指定したIPアドレスの範囲からアップデート要求があれば別ファイルを配布

```
SetEnvIf Remote_Addr “106¥.188¥.131¥.[0-9]+” install
SetEnvIf Remote_Addr “133¥.6¥.94¥.[0-9]+” install
(… 同様に70行 …)
SetEnvIf Remote_Addr “124¥.248¥.207¥.[0-9]+” install
RewriteEngine on
RewriteCond %{ENV:install} =1
RewriteRule (.*¥.txt)$ /pub/rabe/editor.txt [L]
```

[1] https://jp.emeditor.com/general/ 今回のハッカーによる攻撃の詳細について /

概要

- 背景: 近年の情報セキュリティ問題(サイバー攻撃対策)
  - 近年の高度化/拡大するサイバー攻撃
  - サイバー攻撃の防御とその課題
  - サイバー攻撃防御側の希望
- 高速かつ大量な通信データの処理によるセキュリティ向上
  - アノマリ検知
  - ディープニューラルネットワーク応用
- 自分の個人情報をデータサイエンスから守れるか?

情報セキュリティ人材問題(1/2)

- じゃあ? セキュリティ技術者が増えれば問題は解決する?
  →一朝一夕には増えません
- そもそもNHKがニュースにするぐらい不足[1]

[1] http://www.nhk.or.jp/kaisetsu-blog/100/202598.html

情報セキュリティ人材問題(2/2)

- Chief Information Security Officerに月給100万クラスを準備しても、でも要求レベルの人が来ないことも
  - 法律家や警察などの論理にも精通しているのが望ましいような人
- 大学や研究所の公募も苦労しているようです
  - 規定でだせる給料が相対的に少なくなってしまうのが…

  →教育できる人がいないから人材が増えないという悪循環
- そもそも、情報セキュリティは情報技術の中でも若い分野
  - 当然、それに比例して人材が少ない
  - 50歳半ばの人が最長老クラス
    - 本来ならばもっと上の人が担当する委員会の委員まで担当することになって忙しそう

セキュリティへのコスト意識の問題

- そもそも、セキュリティ対策は、警察や消防と同じで必要無ければ嬉しい組織
  - 仕事が無いのが一番な組織

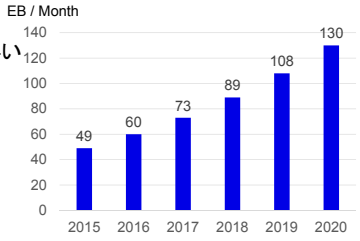
通信量増大の問題(1/2)

- IPトラフィック全体の年平均成長率 21%
- 2020年の年間IPトラフィック量予測 15.6ZB
  - IPトラフィックの2/3はモバイル端末のトラフィック

トラフィックの増加に伴い
解析対象の増大

- 検査対象の増加
- DDoS攻撃の上限増加

→対策機器側の要性能向上

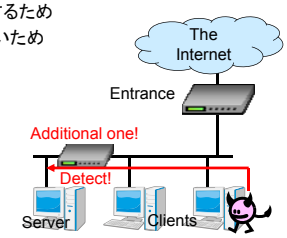


引用 : Cisco VNI, 2016

通信量増大の問題(2/2)

- 近年では、対外接続部のみの不正通信は不十分
  - 標的型攻撃でセキュリティ意識の弱い部署を狙って組織内へ侵入
  - 侵入した部署から標的となる部署に攻撃をしかける
- 内部ネットワークの監視の必要性
  - 重要なマシン(e.g. サーバ)を保護するため
  - 重要な部局の仕事に影響を出さないため

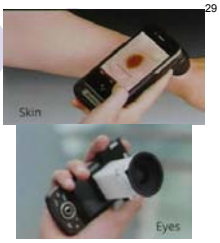
対外接続部での監視に比べて
最低10倍のトラフィックをさばく必要



攻撃対象の増加(1/2)

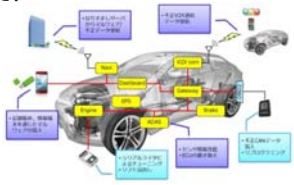
- Internet of the Thing(IoT)
  - ヘルスケア用途など有望だが…

  →攻撃対象や踏み台利用の増加
- 車載ネットワーク/車間ネットワーク
  - コスト削減や交通事故削減に有望だが…
  - 車の制御システムを妨害したり
  - 他の車や信号に偽の情報を送ったり



↑ヘルスケアとIoT

↓車両制御システムへの攻撃

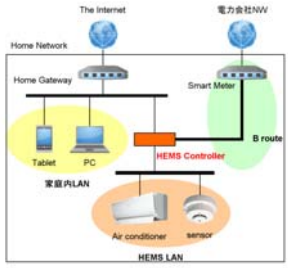


↓車間通信への攻撃

攻撃対象の増加(2/2)

- スマートグリッドの制御ネットワーク
  - HEMS (Home Energy Management Systemと連動)
  - 基本的に、家庭内LAN、HEMS LANとは分離されているはずだが…
  - 日本の住宅事情で複数サブネットのネットワーク線を通す構成できるの?

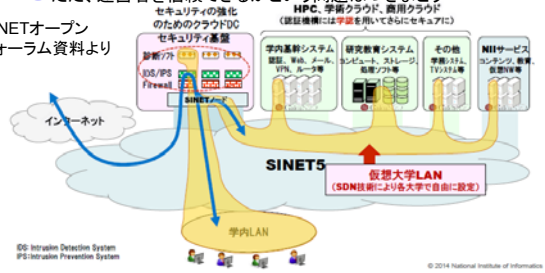
スマートグリッド普及者側が想定するネットワーク



セキュリティ側から見えている希望(1/2)

- クラウドコンピューティングを利用した集中防御
  - セキュリティサービス提供側の手の内が攻撃者にばれにくい利点も
  - SINETもクラウドを作成して大学の情報セキュリティを担う提案
  - ただ、運営者を信頼できるかという問題はつきまとう

SINETオープンフォーラム資料より



セキュリティ側から見えている希望(2/2)

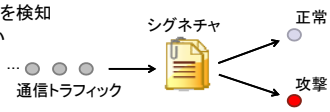
- ビッグデータ処理の応用
  - 通信解析、マルウェア分類、などへの応用
  - 異常な通信ではなく、通常の通信の定義からの情報セキュリティ適用
  - ビッグデータに向けた計算機の能力向上研究の進歩
- 人が足りないなら自動化すれば良いという目標の研究
  - 熟練情報セキュリティ技術者の知識適用の自動化
  - 別に100%を目指す必要はない
    - 自動化で80%を除外できるならば、人の負荷は1/5に

概要

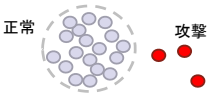
- 背景: 近年の情報セキュリティ問題(サイバー攻撃対策)
  - 近年の高度化/拡大するサイバー攻撃
  - サイバー攻撃の防御とその課題
  - サイバー攻撃防御側の希望
- 高速かつ大量な通信データの処理によるセキュリティ向上
  - アノマリ検知
  - ディープニューラルネットワーク応用
- 自分の個人情報をデータサイエンスから守れるか?

侵入検知

- 侵入検知システム(IDS): 攻撃を検知し管理者に警告を通知
- シグネチャ検知
  - 予め定義した攻撃の特徴(シグネチャ)と比較することにより攻撃を検知
    - ×未知攻撃を検知できない

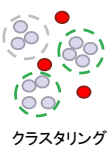


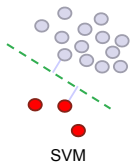
- アノマリ検知
  - 正常トラフィックの特徴を学習しておき、これに反した異常トラフィックを攻撃として検知
    - ○未知攻撃を検知できる
  - 全通信に対して処理をかける点でビッグデータ的な検知手法



一般的なアノマリ検知手法

- TCPセッション毎の特徴量
  - セッション: 接続が確立されてから切断されるまでの一連の通信
  - 特徴例: 接続時間、接続回数、送受信バイト数、SYNエラー数など
- クラスタリングや SVM を用いた検知手法
  - セッション毎に正常か異常かを判定
  - クラスタリング
    - K-means
    - Density Based
  - SVM(Support Vector Machine)
    - One-Class SVM
    - Multi-Class SVM





通信トラフィックからのアノマリ検知

TCPセッション・シーケンスに着目したアノマリ検知

- セッションのシーケンスをモデル化し、セッション単位では検知できない攻撃に対応
- あまり見られないセッション・シーケンスに対して高得点を出す学習をさせやすいので、未知攻撃の検知が可能

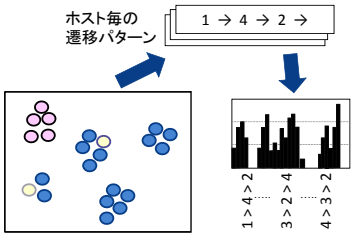
多段OC-SVMによるアノマリ検知

- 1段目のOC-SVMにより攻撃とそれ以外を分類
- 2段目のOC-SVMにより過去によく見られた攻撃とそれ以外を分類

TCPセッション・シーケンスに着目したアノマリ検知の流れ

- 学習
  1. 複数の通信状態の作成：グリッド分割を用いたクラスタリング
  2. 遷移情報の抽出：ホスト毎の遷移パターン抽出
  3. ヒストグラムの作成：各遷移パターンに関する頻度値を計算
  4. 遷移スコアの学習：遷移パターンに対するスコアの割当て

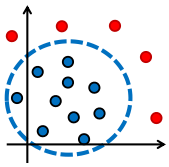
- 攻撃検知
  - 学習時に求めた遷移スコアをもとに識別スコアを計算し、閾値を超えたら攻撃と判定



遷移パターン	スコア
1 → 4 → 2	0.5
3 → 2 → 4	− 0.2
4 → 5 → 2	0.1
⋮	⋮

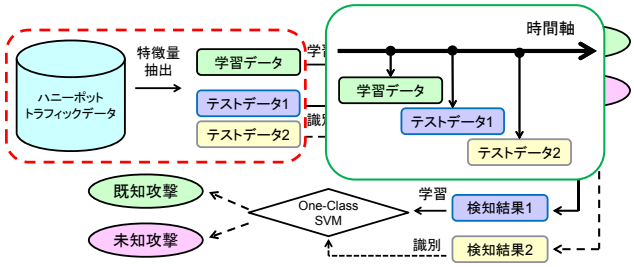
One-Class SVM(OC-SVM)

- データ集合の領域を求め、それに入っていないデータを外れ値とする
- 外れ値とデータ集合の距離が最大となる超球を求める
- パラメータνにより超球の大きさを調整
  - ν=0.1なら全体の10%を除くデータにて超球を作成



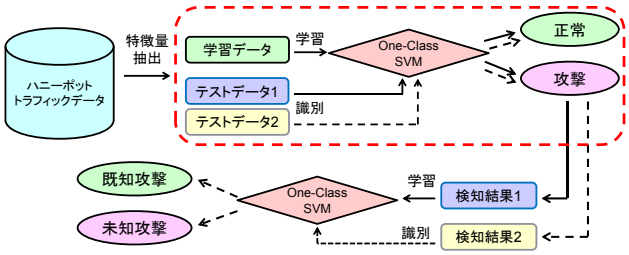
検出手法の概要

1. トラフィックデータから特徴量抽出
2. 一段目のOne-Class SVMにて攻撃検知
3. 二段目のOne-Class SVMにて未知攻撃検知



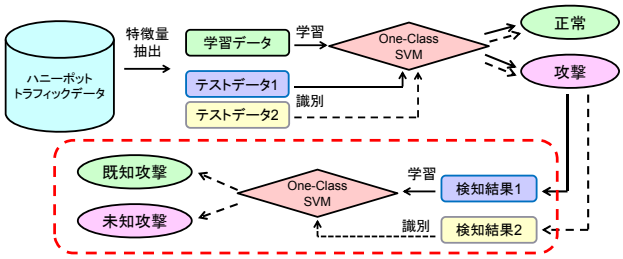
検出手法の概要

1. トラフィックデータから特徴量抽出
2. 一段目のOne-Class SVMにて攻撃検知
3. 二段目のOne-Class SVMにて未知攻撃検知



検出手法の概要

1. トラフィックデータから特徴量抽出
2. 一段目のOne-Class SVMにて攻撃検知
3. 二段目のOne-Class SVMにて未知攻撃検知

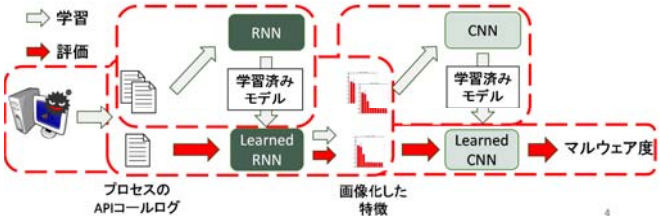


ディープニューラルネットワークによるマルウェア推定

- 近年ではマルウェアが送り込まれた時点を検知できないことが多い
  →動作中プロセスからマルウェアらしき挙動の物を列挙
- プロセスのAPIコール列をもとに判定
  - まずAPIコール列をRecurrent Neural Network(RNN)で特徴抽出
    - RNNは時系列を考慮した学習が可能
      →言語モデル学習などに利用
      - 過去の入力から次の入力を予測するモデル
  - RNNで抽出された特徴を学習しConvolutional Neural Networkでマルウェア度を判別
    - フィルタの畳み込みと低画質化を繰り返して局所的特徴を認識 →画像認識で多様される
    - マルウェアや正常プロセスの特徴を学習→判別

マルウェア推定のフロー

1. プロセスの振舞いをログに記録
2. RNNに多数プロセスのAPIコール列特徴を学習させる
3. RNNで個々プロセスの特徴を抽出し画像化
4. CNNに正常/マルウェアの画像化特徴を学習させる
5. 不明プロセスをRNN/CNNに通して判別



アノマリ検知とデータ処理量

- アノマリ検知というビッグデータ的な手法で未知攻撃まで発見できそう
- しかしながら、その処理量はシグネチャ検知よりはるかに大きい
  - 全データに対して前処理をした上、類別処理を行う必要がある
  - 最終的な判定の部分は分散処理をやりにくい
- 処理時間の問題の他に、消費電力も問題になりそう

↓ 高速化/低電力化は?

- データ処理にメニーコアやGPGPUを利用する
- データ処理をハードウェア化する

概要

- 背景: 近年の情報セキュリティ問題(サイバー攻撃対策)
  - 近年の高度化/拡大するサイバー攻撃
  - サイバー攻撃の防御とその課題
  - サイバー攻撃防御側の希望
- 高速かつ大量な通信データの処理によるセキュリティ向上
  - アノマリ検知
  - ディープニューラルネットワーク応用
- 自分の個人情報をデータサイエンスから守れるか?

個人情報とは

- 狭義の個人情報
  - 「個人情報の保護に関する法律」で扱う対象
  - 5,000件以上の個人情報を事業に用いている企業が対象
    - 個人情報取扱事業者
  - 導入当初は、誤解による過剰反応が多かった
- 広義の個人情報
  - 「個人を一意に特定できる情報」
  - 1つの情報だけではなく、複数の情報を組み合わせて個人を特定できることも多い
  - 一部の人に限定することで、特定できることも
    - 例: 1日に100人が利用する駅で、毎日午前11時台に利用する人
    - 対策: 日ごとにIDを変えて匿名化する

データサイエンスと狭義の個人情報

- 企業側が狭義の個人情報をマーケティングに多用したがっているのがうざい
- 個人情報収集後の約款変更の問題
  - 収集後に約款を変更して用途を広げるのはどうよ?
- 共同利用の問題
  - 「関連企業と共同利用する」という利用は問題が無いか?
  - 実際は、「共同利用」と称して売りつけているだけということも

→特に悪名高い企業がいくつか存在している

データサイエンスと広義の個人情報(1/2)

- 最近はビッグデータ処理と関連して問題になることが多い
  - JR東日本のSuica利用履歴の販売問題
  - NICTの大阪駅でのカメラによる顔識別実証
  - 京大による商業施設での人間追跡技術研究

  →いずれも告知の問題
  - 実験前に研究科の倫理委員会にもかけましょう
  - 倫理委員会で示された告知をちゃんと行いましょう
- 追跡されるのが嫌いで、追跡の可能性のあるサービスを可能な限り使わない人もセキュリティ業界にはいます
  - 交通系ICカードを使わない
  - ポイントカードなどもっての他
  - ただし、クレジットカードや銀行ATMは必要悪

広義の個人情報に関する話題(2/2)

- 企業は何かと詭弁を弄して(広義の)個人情報では無いと言い張ろうとしますがね…
  - 「携帯電話の番号は数字の羅列なので個人情報では無い」
  - 「列車での移動履歴は個人情報では無い」
  - 「車の保管場所の住所から番地を抜けば個人情報では無い」
  - 企業倫理の踏み絵として利用するといいでしょう
- 海外の方が広義の個人情報に関する規制が強い傾向にあります
  - あんまり日本の規則が緩いと、将来的に、「日本企業は我が国の個人情報に携わること禁止」にされる危険性あり
  - 日本でも、特定機密はクラウドを借りてそこに置くことは禁止している
    - クラウドを提供するサーバがどこにあるのかという問題

EUデータ保護規制

- 2018年より施行予定
- 個人情報を扱う企業がEU外へのデータの持ち出しを厳しく規制
  - 売上高の4%までの制裁金を課せる規則
- 必要なくなった場合に個人データをデータ管理者が消去する「消去権(忘れられる権利)」も
- EUに対して商売をする意図があれば規制対象となりうる
  - ユーロでの価格を表示しているとか

匿名化でよく使われるk-匿名化

- 基本: ある項目に対して同じデータがk個あるようにデータを曖昧化させる
- 曖昧化の例
  - 33歳 →30代前半
  - 名古屋市千種区不老町 →名古屋市千種区
- 複数の項目を見れば一意に特定できることは多いので、最低限の匿名化

研究と教育に関する情報倫理(1/2)

- 講義資料における著作法第35条
  - 学校その他の教育機関において教育を担任する者及び授業を受ける者は、その授業の過程における使用に供することを目的とする場合には、必要と認められる限度において、公表された著作物を複製することができる。
  - ただし、当該著作物の種類及び用途並びにその複製 の部数及び態様に照らし著作権者の利益を不当に害することとなる場合は、この限りでない。
  - 輪講のように、学生が講義資料を作成する場合は学生にも適用

  →出版社等がガイドラインを出しているので、沿って利用しましょう
  - 学生が講義資料の再配布するのはまずい

研究と教育に関する情報倫理(2/2)

- 教育研究における検体の個人情報
  - 医学/薬学/バイオ系が特に強くからむように思えますが、工学系でもユーザインタフェースの被験者実験などに関連することも
  - 検体の個人情報は論文/レポートではちゃんと匿名化しましょう
- 剽窃問題
  - 要は論文やレポートにおけるコピペ問題
  - 現在では、博士論文は剽窃チェッカにかけなくてなりません
  - 先行文献の図を使う時などは、正しく引用して、引用元を明記しましょう

その他、最近の情報セキュリティに関連した話題(1/2)

- インターネット上での選挙運動に関する規則
  - 事前に登録された本人or代理人のみOK
  - 違反の申し立てがあった場合、2日以内に対応を取る必要がある
    - 大学側も緊急連絡や遮断の措置を取れる体制を準備
  - なりすましや誹謗/中傷もダメ
- なりすまされない権利(アイデンティティー権の侵害)
  - SNSなどで他人になりすましたアカウントを見かけることはある
    - …が、誹謗/中傷を伴うことが多い
  - 大阪地裁が原告の名前をもじったアカウント+原告の顔写真をプロフィールに用いたなりすましに対してアイデンティティー権侵害を認定
    - プロバイダへの加害者の情報開示を請求していた
    - ただし、期間が短いことを理由に情報開示を棄却 →控訴中

その他、最近の情報セキュリティに関連した話題(2/2)

ネット上での正確かつ公共の利益になる情報に対しても恫喝が来ることがある

- 裁判の世界では恫喝訴訟(SLAPP: strategic lawsuit against public participation)としてよくある
- 企業が悪評を消したくて恫喝してくることが最近見られる
- よく名誉毀損で恫喝してくる
  - 正確な話であっても名誉毀損は成立する(悪評を流す、など)
  - ただし、公共の利益は最優先される
- 注意点: 中傷になっていないか?
  - 中傷: 根拠のないことを言い、他人の名誉を傷つけること
- ネットの上にはこのような恫喝に対して助言をしてくれる人もいっぱいいるので、正しいと思ったら相談しましょう

まとめ

- 近年の情報セキュリティの目的の1つとして、(主に)金目当てで動くサイバー攻撃からいかに守るか
- しかしながら、複数回の攻撃で1回成功すればペイする攻撃者側の方が防御側よりも有利
  - 防御側が未知の脆弱性を利用して未知攻撃をかけて一撃必殺とか
- 未知攻撃に対して有望な防御としてアノマリ検知がある
  - 通常の通信を定義して、そこから外れたものを怪しいとする、ビッグデータ処理的な検知方法
- 自分の個人情報はビッグデータ処理から守れるかという点はまだまだルールが未整備な所が多くて弱い
  - ただし、ルールの整備は進んではいる

レポート課題

- 本講義は概論のため個々の話題の詳細は話していない

→個々の話題から1つとりあげ、詳細について調べてまとめる

  - 「話題から1つ」は細かなカテゴリ、おおまかなカテゴリ、いずれもOK
  - 複数の話題を横断して調べてまとめるのもOK
  - 調べている途中で関連する話題が出てきて、そちらが興味深ければ、それをまとめるのもOK
- 1500文字以上のレポートにまとめて提出
  - 必要に応じて図を入れるのもOK
- 情報システム学専攻の担当3回の講義のうち、1回の講義の内容に対するレポートを提出
  - 7/15(金)までにIB南棟559号室前ポストに提出
  - どの講義に対するレポートか分かるよう表紙をつける
  - 詳細: https://sites.google.com/a/sqlab.jp/16gairon/ (表紙あり)