幸せのトラフィック解析
公開版

園田道夫
(所属ザイオン:いろいろ)

ここで言う

幸せのトラフィック解析とは

トラフィックの裏に潜むネタを炙り出すことかっくいー(笑)

みんなで幸せになりましょう

量的変化という捉え方

- トラフィック（流量、量）の変化を見れば、いろいろなことが見えてくる（人間様の例）
  - 例1：特定の相手先への夜間通話が増えた
  - 例2：これまでの会話とは異なるテーマでの会話が多くなる
  - 例3：特定のキーワードを含む会話トラフィックが少なくなる、多くなる（このあたりはペイロードの中身解析に近いか？）
  - 例4：ノンバーバルコミュニケーションでの特定の動作パターンが増える
  - 例5：怒りのトラフィックが増える
  - 例6：メールが来なくなる

というわけで早速ジッケソ

対象人数	3人（予算の都合（笑））
対象のプロファイル	30代男性、20代女性、60代女性
実験場所	某サテンなど
テーマ	1時間会話して、最低2回嘘をついてくだされ。ダマせたら1万円
記録方法	レコーダー、ビデオ

結果はもちろん・・・

そして3万円放出（苦笑）

- データを解析してわかったこと
  - 嘘モードでは身じろぎが増える（該当3人）
  - 嘘モードでは特定の語彙が増える（該当2人）
  - 嘘モードでは視線の動きにそれまでと違いが出る（合わせる、合わせなくなる＝該当3人）
  - 嘘モードでは会話密度（スピード）に変化が出た（該当2人）
  - 嘘モードでは若干全体の音声ピッチが上がっているようだ（該当1人）
- 特にノンバーバル系の動きに注目すると面白いようですが、ビデオ撮影はインパクトがあるため配慮が必要でしょう（笑）

ソーシャルエンジニアリングへの応用（するなって・・・（苦笑））

- 電話で情報を引き出す場合
  - 引き出す質問とどうでもいい話のトーンを変えないことを意識する（自然な流れ）
    - 会話密度、語彙、スピード、抑揚
    - 埋没させすぎてもいけない（パターンを変えないことが重要）
- 物理的対話で情報を引き出す場合
  - 電話に比べて注意すべきポイントが多い（特に女性相手とベテラン相手（経験則））
  - 特に気をつけるべきなのは、ノンバーバルコミュニケーションのパターン（身じろぎ、目線、手の動きなど）
  - 会話内容に合わせた動きをシミュレートしておく

ついでに社会工学対策(余談)

- 一応対策らしきものを(笑)
  - もし相手が詐欺師もしくは欺術愛読者だったら、という想定をしとくべき
  - 何らかの情報を渡す＝会話を始める前に属性情報の確認くらいはすべき
  - コールバックするときも、大代表あたりからかけていけば良いかと
  - 第三者に確認することを心がける
  - もし相手が詐欺師もしくは欺術愛読者でなければ、トラフィックを解析すれば見破れるかも(ただし、スピードが必要)

もっと実用的な例

- トラブルシューティングとかに使われる考え方
  - 例1：特定の種類のパケットが増える、減る
  - 例2：特定の宛先、送信元が増える、減る
  - 例3：全体量が増える、減る
  - 例4：ありえない時間帯のトラフィック
  - 例5：CPU使用率、メモリ使用率の変化
  - 例6：I/Oの変化
  - 例7：温度の変化
- メーリングリスト観察とか
  - 例1：特定の発言者が増える、減る
  - 例2：流量そのものが増える、減る

もっと黒い？例

- 黒いって何？という話はさておき
  - 例1：Webアプリケーションの脆弱性を突き止める（特定リクエストのパラメタを変化させて、応答の量的変化を見る→部分的な側面にのみ効果があると想定される）
  - 例2：そしてもちろんバッファオーバーフロー（入力値パラメタのデータ量を機械的に増やして送り込み、反応の量的変化を見る）
  - 上記例とも反応のデータ量を測定し、その変化を見るというもの

暗号通信の解析

- すべてのデータが暗号化されてたらお手上げ (例：ハードウエア装置同士) →トラフィック・フロー・セキュリティ
- ルーティング情報が暗号化されていない通信の場合は、そこから各種ステイタスが取得可能送信先、送信元、通信頻度、通信文の大きさなど
  - トンネルの場合もルーティング情報は残る
- メール本文のみの暗号化などの場合はさらに多くの情報が得られる
  - タイトル、ヘッダ、宛先など

通信が暗号であっても わかっちゃうこと（除くトラフィックフローセキュリティ）

- だれとだれが話しているのか
- どの時間帯にやりとりがあるのか
- メッセージの長さはどのくらいなのか
- やりとり総量はどのくらいなのか
- 単位時間あたり量はどのくらいなのか
- 他の情報で補完できれば、上記情報が得られるだけでもいろいろなことが判明する

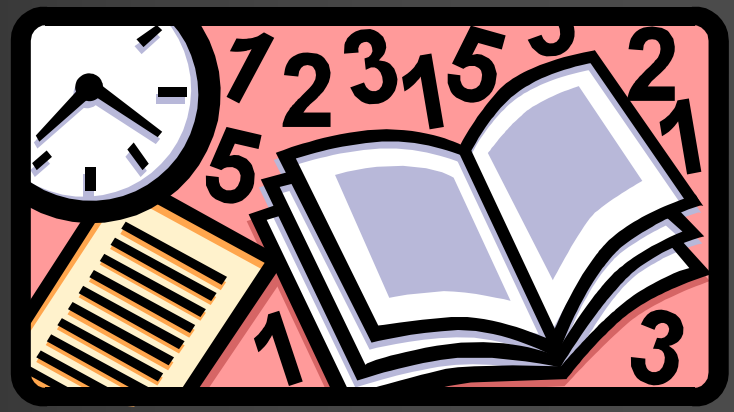
トラフィックの眺め方

- 量的変化を眺めると
  - 対象の行動パターンがわかる（時間帯、パワー、どの相手と仲が良いのか悪いのか、などなど）
  - ステイタスが分かる（組織内の情報が補完できれば、どのようなプロジェクトが動いていそうか推定できたりするのでは（笑））
- 眺め方はこんな感じ？
  - 「急に増えた」「急に減った」（総量）
  - 「通信量の平均値」「1回あたりの通信セッション量（時間、パケット）」「各プロトコルごと」「単位時間あたりの通信量」「通信量の変移グラフパターン」
  - 「平時」「非常時」
  - 実は某天気予報って↑こんな感じ・・・（笑）？
  - 人間系にも応用可能ですな

解析の考え方とか

- データを大きなまとまりのある量的変化として捉える（内容は気にしない）
  - ただし、キイワード解析はデータ内容が関係するかも
- グラフパターンの認識や予測
  - データマイニング手法（相似法、最近隣法など）
  - なにぶん文学部なので（笑）、お勉強ちうです
- 利点
  - システムに実装する場合、実はシンプルにしやすい
  - コンピュータに解析させやすい分野（問題は人間の方）
- 課題
  - 通信が大量になるとノイズの除去が必要
  - データへのスポットの当て方？切り出し方？

研究中の応用例



- インシデントレスポンスシステム（かっくいー（笑））
- 簡易IDS
- 簡易ハニーポットツール
- 嘘ハケーン機（そんな馬鹿な（笑））

・・・詳細はまだ内緒（笑）。

おわり