インターネット
早期広域攻撃警戒システム
WCLSCAN

WCLSCANプロジェクトリーダー
鈴　木　裕　信
hironobu@h2np.net

ひとことであらわすと…

WCLSCAN

危険を自動推定するシステム

JPCERT/CC, IPA, @Police

人間が見るためのデータをまとめるシステム

WCLSCAN

概要

- インターネット上で発生している広域な攻撃を24時間365日自動的に検知し状況を解析し危険度を予測する
  - “広域情報収集／データベース化／自動化分析”の3つの機能からなり独立しているので拡張が簡単
  - 状況を診断するような専任オペレータは不要
  - ベイズ推定（推測統計学）を使い危険度を計算させるので確信度が高い
- いつでもどこでも知ることができる
  - パソコンからだけではなく携帯電話からのチェックも可能なのでいつでもどこでもチェックができる
  - デスクトップ上から常時モニタリングができる

WCLSCAN

ここまでの道のり

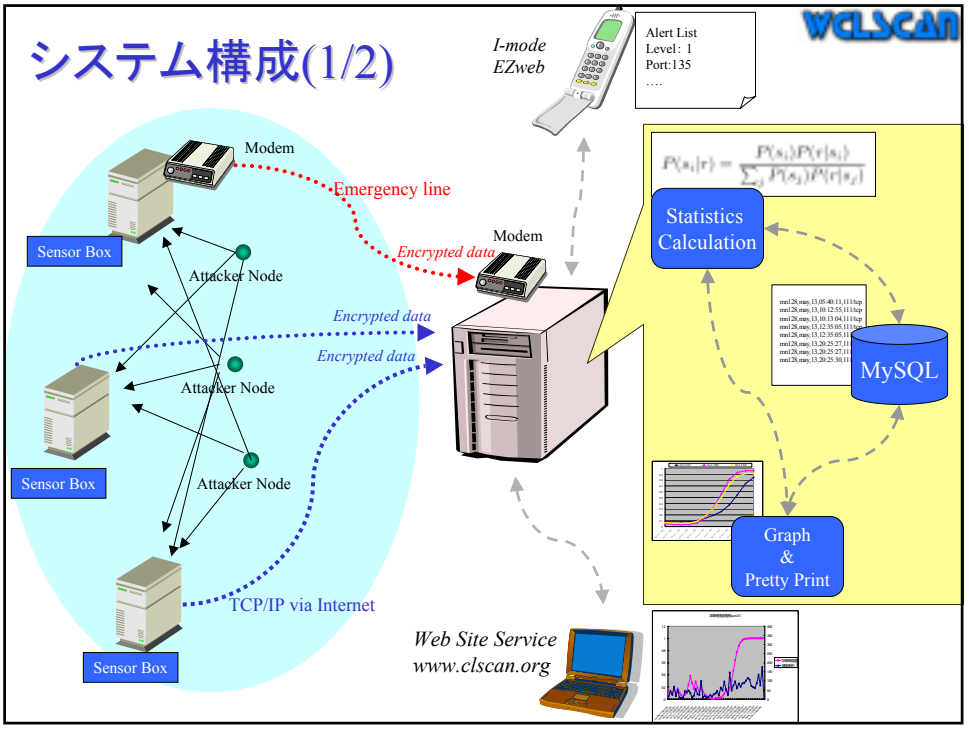
- 1999年: clscanを作成・運用・公開
  - ルータのセキュリティログPretty Printツール
- 2001年: セキュリティログを分析した結果を発表
  - パケット到着とインシデントとの関係、CERT/CCアラートやベンダー脆弱性情報とインシデントアクティビティの関係、Zero-Dayアタックの発見等など
  - ソフトウェアシンポジューム 2001やLinux カンファレンス2001で発表→広域ネットワーク上でのシステムの提案
- 2002年: WCLSCANの開発開始
  - clscanの広域ネットワーク版
- 2003年: ベイズ推定を使った推論部の導入
  - Internet Weather Report aka WCLSCANとなる

ゼロから考えたオリジナルなシステム

最近の状況

- 成果を論文として発表
  - 16th Annual FIRST Conference on Computer Security Incident Handling
  - ソフトウェアシンポジューム 2004
  - ほか2件
- ボランティアベースの研究活動として活発に進められている
  - 2004年10月末現在　参加組織数8
    - 研究所1・大学4・企業3

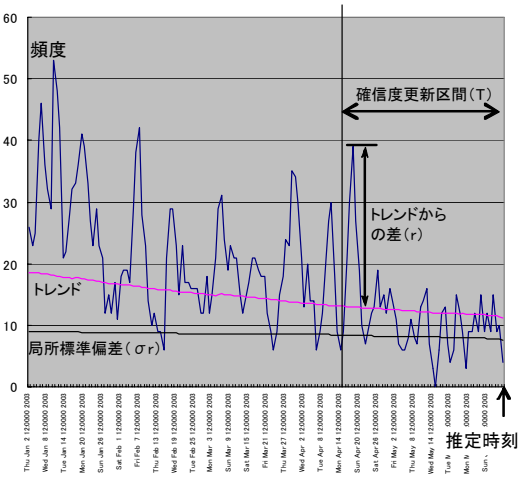
システム構成(1/2)



システム構成(2/2)

- センサーボックスシステム
  - インターネット上に存在し到着したパケットを記録した後、集積サーバへその記録を暗号化した後に転送する
- 集積システム
  - センサーボックスから送られてくる記録を受け取り復号化した後MySQLへ格納する
- 計算システム
  - MySQLから必要なデータを取り出し危険度を計算する
- 表示作成システム
  - 計算サーバから結果を受け取り、グラフや見やすい表に加工し、メールで通知したりWebサイトへ掲載する

ベイズ推定による攻撃検知手法



事前確率　尤度関数

$$P(s_i|r) = \frac{P(s_i)P(r|s_i)}{\sum_j P(s_j)P(r|s_j)}$$

事後確率　　証拠

$$\begin{cases} s_0 & : \text{危険状態} \\ s_1 & : \text{安全状態} \end{cases}$$

r: ポートスキャン頻度のトレンドからの差(観測)

ゆうど
尤度関数

$$P(r|s_0) = \frac{r}{k\sigma_r + r}$$

$$P(r|s_1) = \frac{k\sigma_r}{k\sigma_r + r}$$

石黒氏作成のSCSI2004発表スライドより

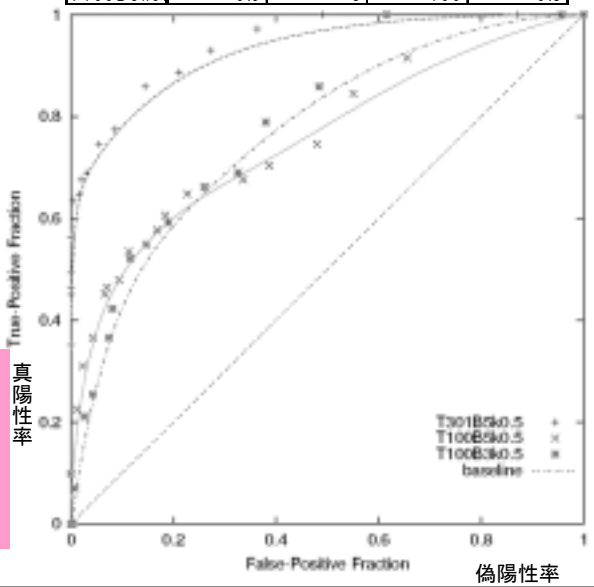
評価実験

- 期間 2003/1/1 ~ 2003/12/1
- ポート25 (smtp) ※変化がダイナミックだったため対象にしてみた
- サイト数　1 ※先行してセンサー単独で動かしていた
- ベイズ推定の結果に対し正しい（真陽性率）と誤り（偽陽性率）のROC (receiver operating characteristic)曲線を作成
- 同じデータで「ベイズ更新区間」「トレンド区間」のパラメータを変化をさせてみた

- y=xよりもROC曲線は上方であるので、有効に危険状態を判別できている
- トレンド区間が大きいほうが精度が出る
- 同じトレンド区間なら更新区間が小さいほうが精度が出る
- 良いパラメータの選び方は職人芸の世界だった！？

石黒氏によるROC曲線評価実験結果より

グラフID	ベイズ更新偏差係	ベイズ更新区間	トレンド区間	Az値
T301B5k0	0.5	5	301	0.95
T100B5k0	0.5	5	100	0.79
T100B3k0	0.5	3	100	0.8



真陽性率

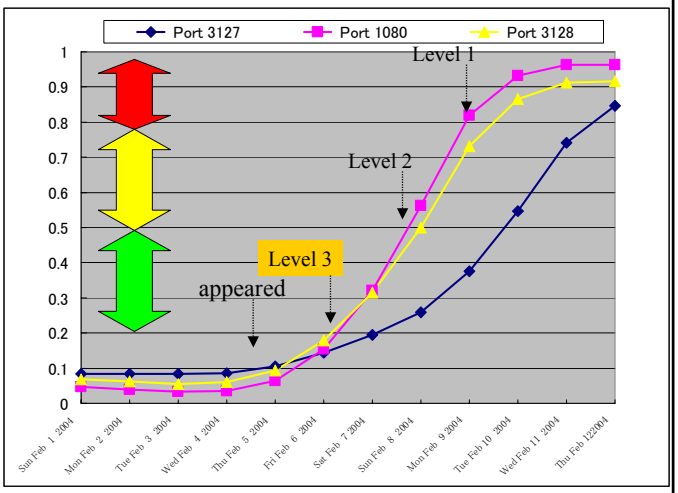
偽陽性率

ケーススタディ(1/2)：Doomjuice

まったく新しい攻撃が発生した場合

- 2004/2/7 （昼ごろ）レベル3に見たことのないポートへのアクセス増加を認知
- 2004/2/7 (午後4時) IWR研究者間メーリングリストへMydoomバックドア狙いのポートスキャンが増えていることを報告
- 2004/2/9(日本時間)ウィルスベンダによるアナウンス
- 2004/2/10 (日本時間)メディアによるアナウンス
- 2004/2/11 @policeによる注意喚起掲示

Graph of Bayesian Estimation Curve

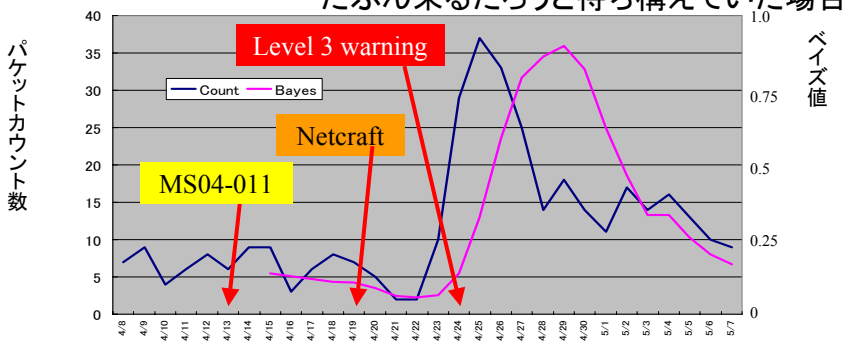


Time Zone is JST

Detected activity of “Doomjuice”

ケーススタディ(2/2):SSL BOMB

たぶん来るだろうと待ち構えていた場合



- SSL BOMB --- MS-IISへのDoSアタック
  - 2004/4/13 MS04-011でTCP/SSLの脆弱性を公表
  - 2004/4/19 Netcraftがexploitコードが公表されていると警告
  - 2004/4/24 IWRでlevel 3にリストアップされる
    - 予想通りの攻撃をセンサーが捕らえた

状況通知(1/2)

詳しくはhttp://www.clscan.orgにアクセス

- Web Brower from PC/PDA
  - www.clscan.org
- I-mode (NTT DoCoMo)
  - www.clscan.org/iwr/i.html
- Ezweb (KDDI)
  - www.clscan.org/iwr/ez.hdml

携帯電話の画面イメージ

```
2004/2/19 19:31
IWR:
L P     B    C
1 80    0.88 117
1 135   0.84 287
2 901   0.69 9
2 443   0.50 2
3 1080  0.50 128
3 3128  0.49 130
3 12345 0.45 4
3 3127  0.42 209
```

- ほとんど場合、携帯電話からのチェックで十分
- レベル1発生時に携帯へメール通知する機能は“ウザイ”ので中止

WCLSCAN

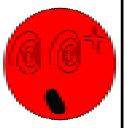
状況通知(2/2)

GNOME2.6ベース
なので注意！

- Facial indicator
  - GNOME アプレットを開発
    - デスクトップ上から常時モニタ
  - Webサイト上のアイコン
    - パソコン上から
    - 携帯電話から

画像ベース

文字ベース

Smiley	Uneasy	Distress	Panic
			
(^_^)v	(-_-;)	(-_-T)	(@o@#)

WCLSCAN

研究プラットフォームとして

- データベースに格納されている大量のログから色々な分析をしてみる
  - ネットワーク上でのウイルス感染パターンの視覚化

時間があれば
デモするよ！

  - www.sco.comへのDoSアタックの痕跡をみつけることもできた

@policeの
元ネタ

オンゴーイングな研究及び開発

大学を
中心にした
取組み

- 新しいデータマイニング手法
- 分散推論エンジン
- 専用ハードウェアを必要としないセンサーボックス
- 計測網の拡大と安定運用に向けての地道な取り組み
- 分析方法の高度化と表現法方法の高度化
- IDMEFサポートとデータ交換
- 新しいアプローチによる新型センサ、データ収集、分析法
- 突発的な異変を感知するSPIKE FINDER
- ディスクトップ・フェイス・インディケータ

色の違いは実施グループの違い

まとめ

- インターネット早期広域攻撃警戒システムWCLSCANの開発と運用を行っている
- 精度の良いベイズ推定による危険度を計算し、その結果を一般に公開しており、その情報はパソコンからだけではなく携帯電話からも確認できる
- 評価実験により有効であることが確認され、ケーススタディ紹介のように現実に役に立っており、また得られた知見も外部へ提供している
- 現システムの拡大・拡張だけではなく、先端的研究プラットフォームとしても位置づけられ、さらに進んだ研究開発に着手
- さらに安定し充実したシステムにするために奮闘中！！