Overview of WCLSCAN, the Automatic Internet Threat Detection System

Hironobu SUZUKI

Waseda Univ.

Agenda

- About WCLSCAN project
  - Project Goal
- System
- Mathematical approach for threat detection
  - Using Bayesian estimation
  - Other method

Our Goals

- Find “new” threats without any human-operator
- Run non-stop, 24-7 system.
- Find threats from huge chaos data
- Show the simple conclusion
- Access easy from anywhere, in anytime

System Overview

Alert List
Level: 1
Port:135
....

WCLSCAN

I-mode
EZweb

TCP/IP via Internet2 (IPv6)

Encrypted data

Sensor Box

Attacker Node

Encrypted data

Encrypted data

Attacker Node

Sensor Box

Attacker Node

TCP/IP via Internet (IPv4)

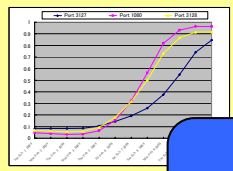
Sensor Box

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

Statistics Calculation

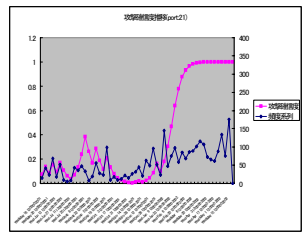
mn128,may,13,05:40:11,111/tcp
mn128,may,13,10:12:55,111/tcp
mn128,may,13,10:13:04,111/tcp
mn128,may,13,12:35:05,111/tcp
mn128,may,13,12:35:05,111
mn128,may,13,20:25:27,111
mn128,may,13,20:25:27,111
mn128,may,13,20:25:30,111

MySQL



Graph
&
Pretty Print

Web Site Service
www.wclscan.org



Sensor Box

- Global IP reached Black-Box
  - To capture reached IP packets
- Linux Box
  - # iptables -A INPUT -i eth0 -j LOG
  - # iptables -A INPUT -i eth0 -j REJECT
- Home-made verbatim data transfer program in Perl
  - Encrypted by GPG
  - Batch style using cron
  - Queue files and send it style

Receive and Archive Server unit

- Receive encrypted data from sensor box
- Decrypt it
- Parse it
- Submit it into Database
  - MySQL

Perl, Ruby, Shell Script and Others

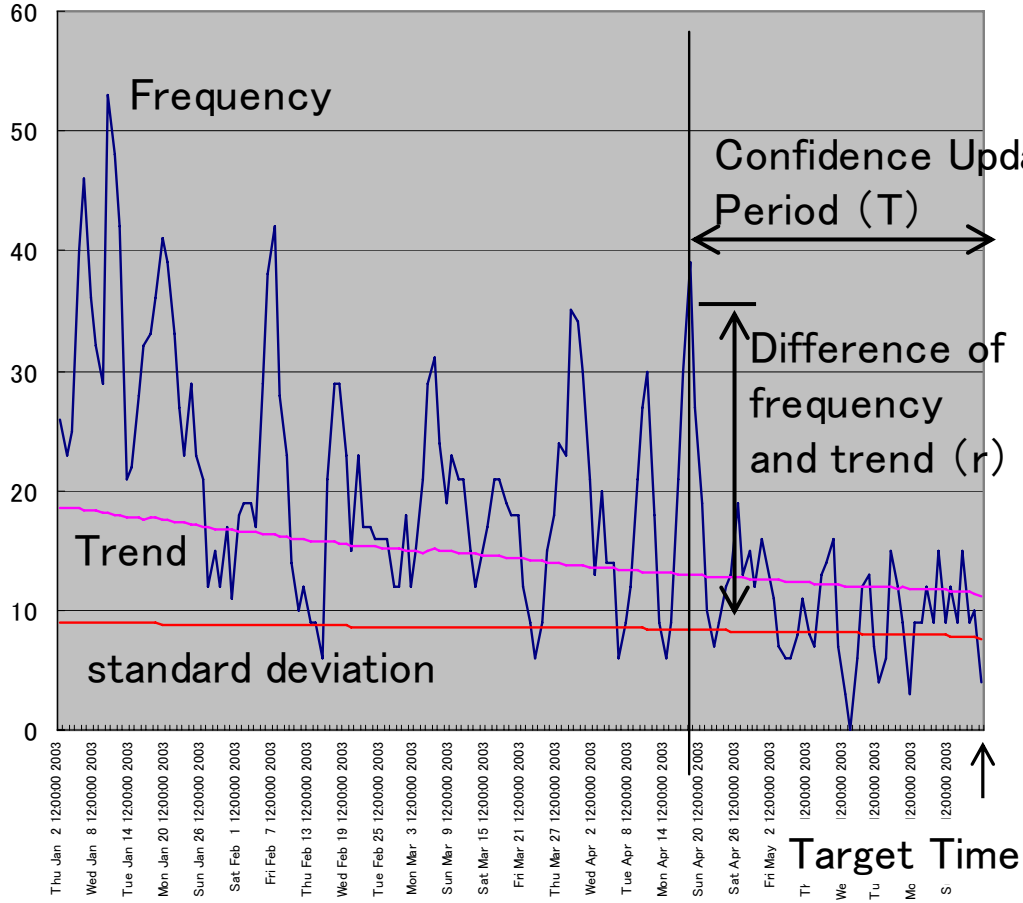
Statistics Calculation Server unit

- Calculate data using intelligent method
  - Bayesian Estimation
  - Graph theory based analysis (coming soon!)
  - Etc.

Presentation Server unit

- Pretty print
  - PC, Mobile phone
- Trend Graph
  - PC, Mobile phone
- Sound warning
  - For PC

Threat Detection Method using Bayesian Estimation



Prio prob. Likelihood

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

Posterio prob.

Evidence

- S_0 : critical state
- S_1 : safe state

r : Difference between frequency of port scans and their trends

Likelihood function:

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

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

k : coefficient of sensitivity

Case Study 1: Doomjuice

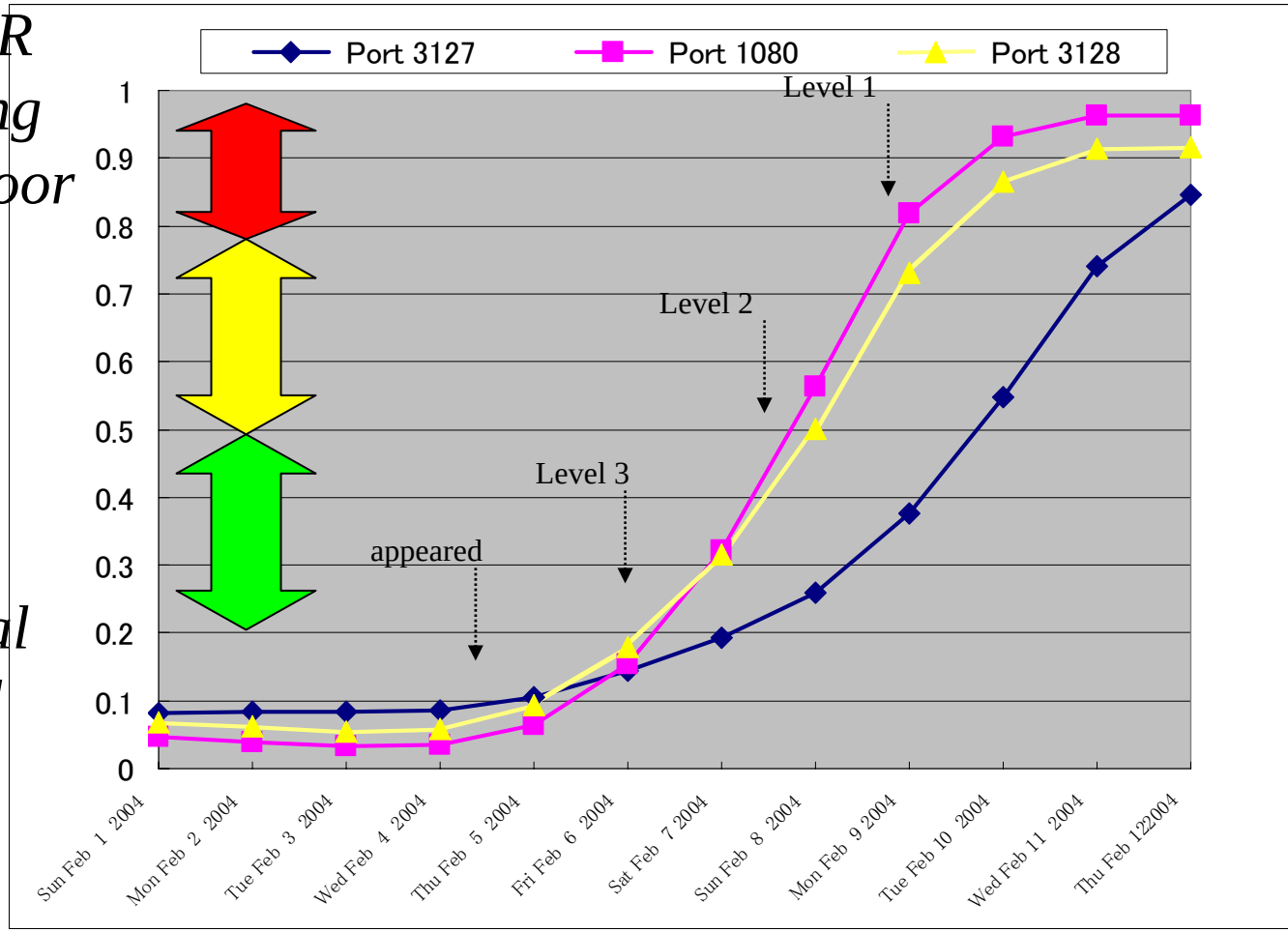
2004-02-07 1pm: *We found Attack Activities*

2004-02-07 4pm: *IWR mailing-list "Scanning for Mydoom's backdoor is increasing".*

2004-02-09 : *Virus benders announced about "Doomjuice".*

2004-02-11 : *National Police Agency issued alert document.*

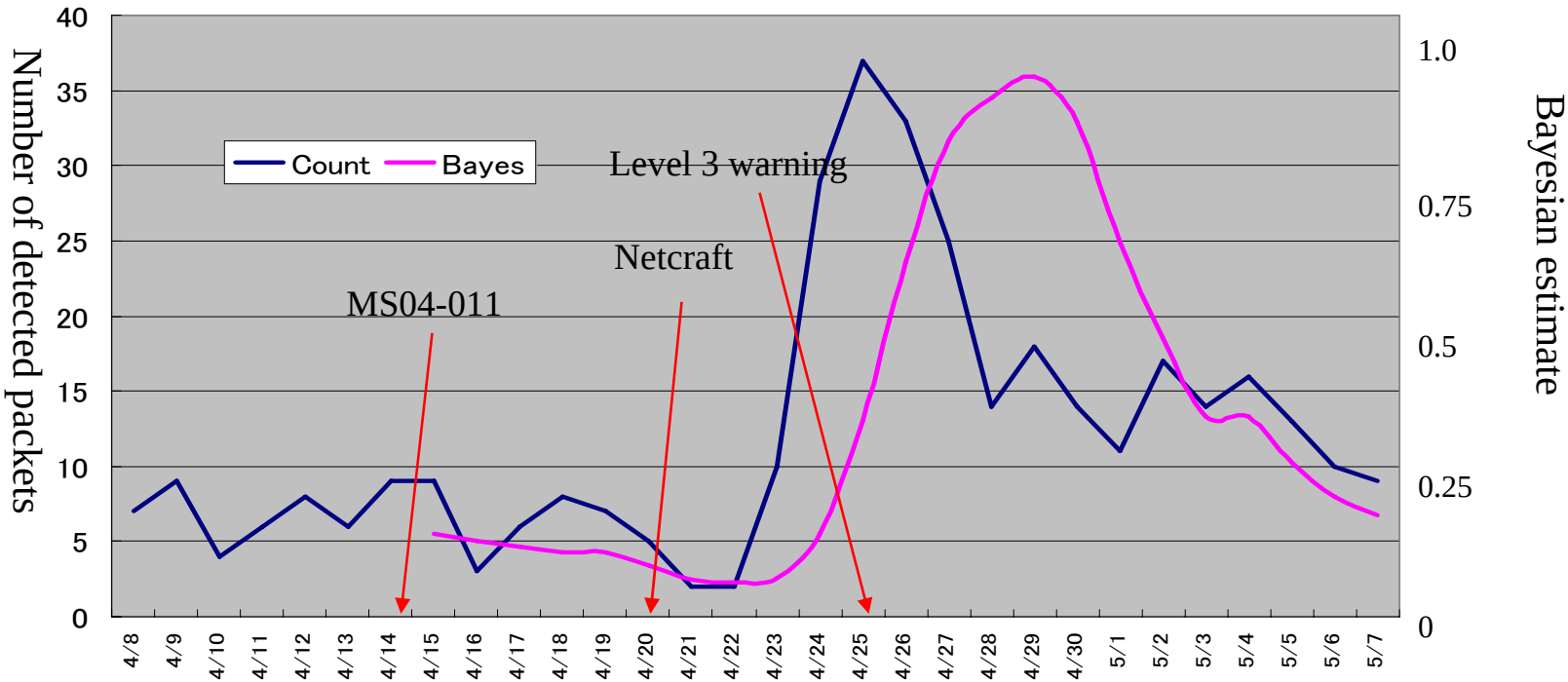
Bayesian Estimation Curve



Case of Zero-day attack

Time Zone is JST

Case Study 2: SSL BOMB



- SSL BOMB, MS-IIS DoS Attack
  - 2004-04-13 MS04-011was issued
  - 2004-04-19 Netcraft reported exploit code
  - 2004-04-24 IWR listed it as level 3

Case of "announcement's effects"

WCLSCAN

WCLSCAN - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.wclscan.org/

移動

WCLSCAN

インターネット早期広域攻撃警戒システム

更新時間

2006-03-23 12:56

インターネット 概況

だいじょうぶ

アイコンの説明

詳細な状況

PC/PDA用表示

現在の状況

ポート別変化グラフ

ベイズ変化グラフ

ポートランキング

国別ランキング

世界地図版

音声による状況報告

各種情報

インターネット上のインシデント情報を解析するシステム

本サイトでは1999年より進めてきたネットワークセキュリティの研究開発成果を公開しています。インターネット早期広域後期攻撃警戒システムWCLSCANはパケット検出しデータベース化した後、統計情報等の抽出、広域ネットワーク上のセキュリティに対する脅威を自動的に検知・発見するシステムです。24時間・356日体制で **ベイズ推定を用いインターネット上でのインシデント危険度を自動的に察知する機能を持つ Internet Weather Report aka WCLSCAN (論文)** を稼働させています。直観的に現在のインターネット上の状況を理解できるようにページ左上にある顔の**アイコンが現在の 状況** を示しています。またiモードやEZWebなどにも対応しており携帯からも確認できます。

システムに組み込まれたベイズ推定により脅威と判断しているため、通常の人間の判断ではむずかしい大量のデータに埋もれて認知できないような脅威もこのシステムはピックアップしてくれます。