# Internet Threat Detection System Using Bayesian Estimation

3-18, 6, 2004
FIRST 16th Annual Conference

Masaki Ishiguro*1) Hironobu Suzuki*2)
Ichiro Murase*1) Hiroyuki Ohno*3)
*1)Mitsubishi Research Institute, Inc
*2)Hironobu SUZUKI Office
*3) National Institute of Information and Communications Technology, Japan

# *Agenda*

- About project and system
  - Goal
  - Background history
  - System overview
- Threat detection method using Bayesian estimation
  - Mathematical method
  - Example ( ftp case ), Evaluation, Real action
- www.clscan.org
  - Web site demo
- Conclusion
- On going project

WCLSCAN

# *This project is …*

- Kind of academic and voluntary based research project

| | |
|---|---|
| National Laboratory (1) | National Institute of Information and Communications Technology, Japan |
| Universities (2) | Osaka University. |
| | Gunma University. |
| Private Companies (3) | Mitsubishi Research Institute, Inc |
| | HIRONOBU SUZUKI OFFICE |
| | One private company |

# *Goals*

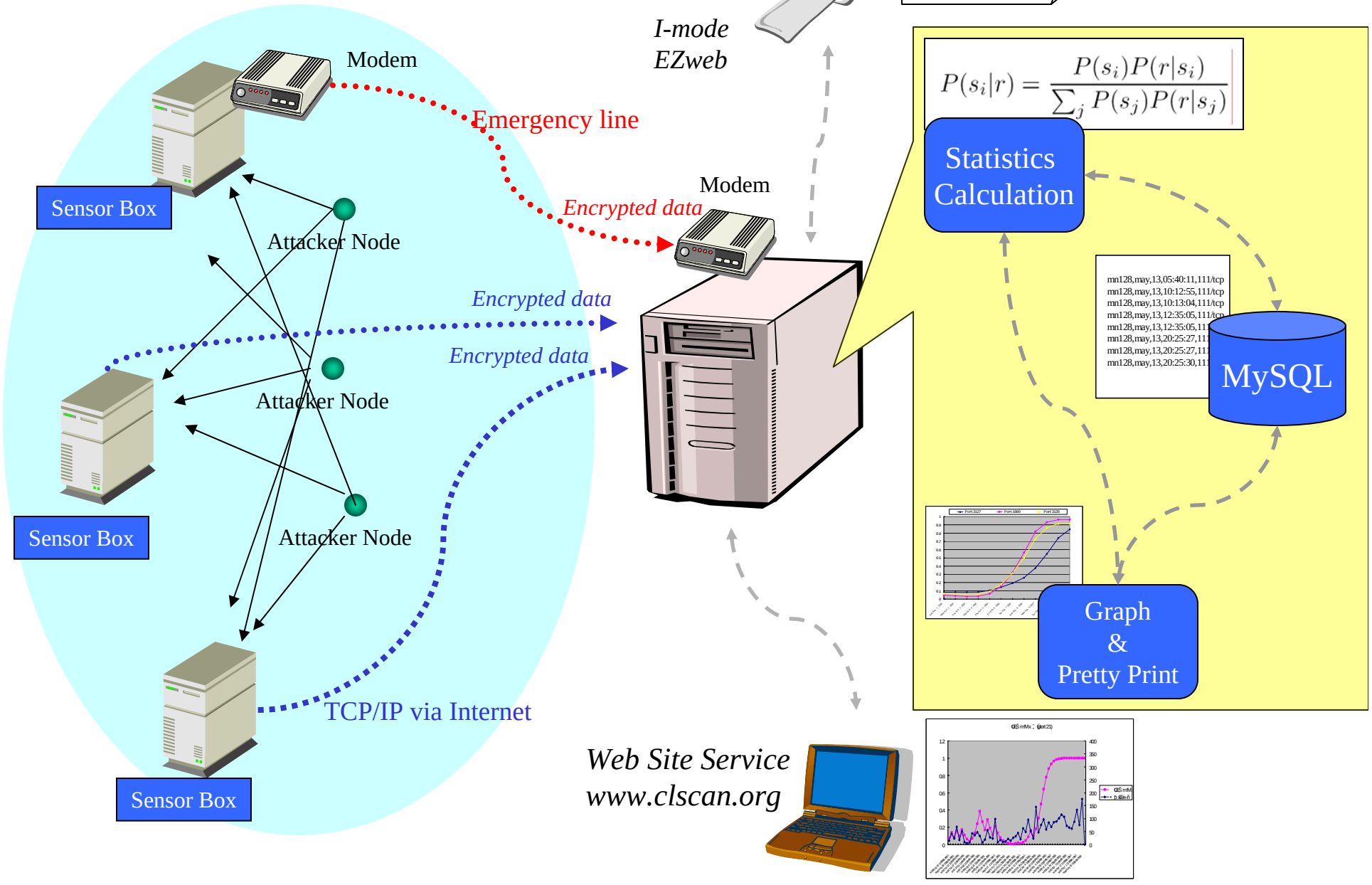

- Find “new” threats without human resources
- System never sleep, 24 hours/7 days
- Find threats from huge chaos data
- Show the simple conclusion
- Access the report in anytime from anywhere

WCLSCAN

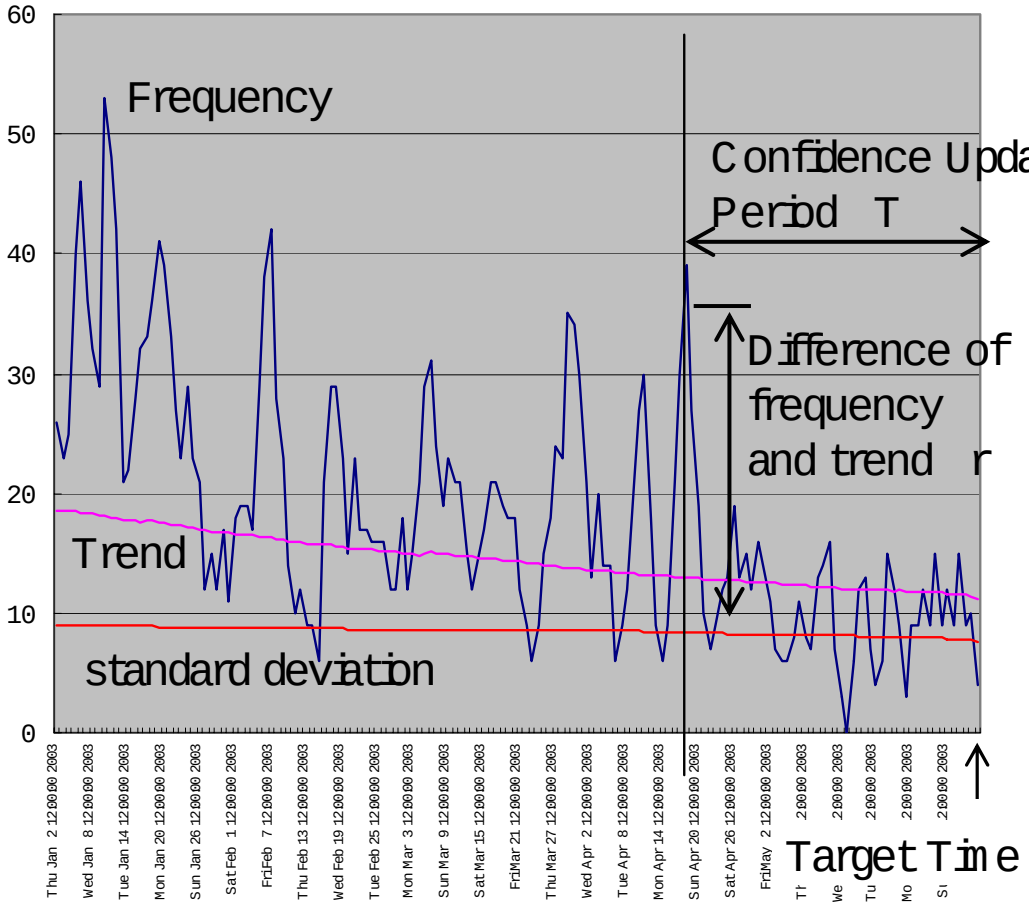
# *Background History*

- 1999 CLSCAN (common log scanner)
  - "pretty print" tool for syslog file of my Internet router
- 2001 Last 12 months log was analyzed
  - "*Internet security analysis using packet filter log*" , SEA software symposium 2001
- 2002 WCLSCAN project was started
  - Wide area version of clscan
- 2003 Internet Weather Report aka WCLSCAN
  - "threat calculation using Bayesian estimation" unit was added to WCLSCAN
- Today, 4 sensor boxes have been running and provide information on www.clscan.org

# System Overview



# 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:

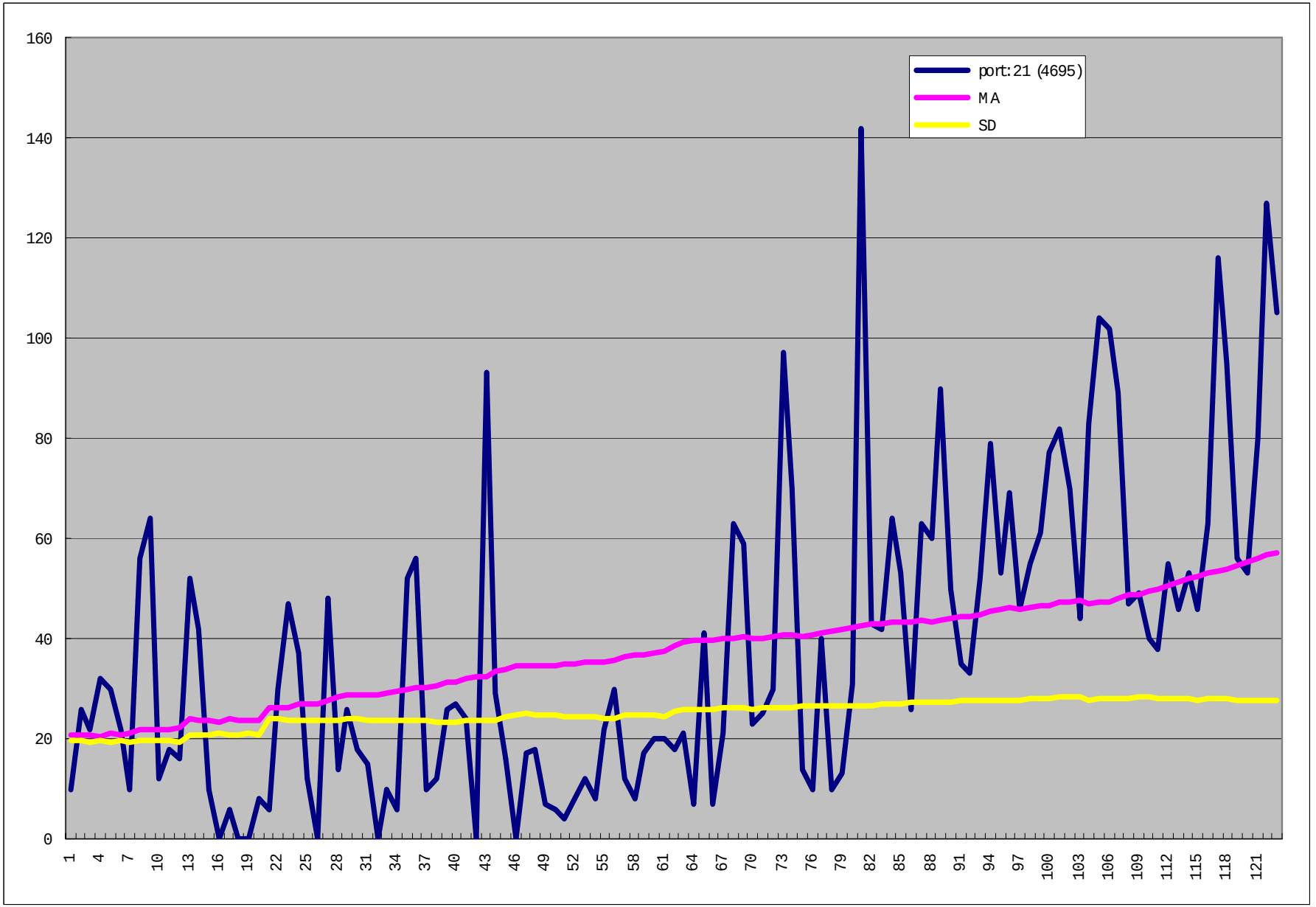
$$\begin{cases} P(r|s_0) = \dfrac{r}{k\sigma_r + r} \\ P(r|s_1) = \dfrac{k\sigma_r}{k\sigma_r + r} \end{cases}$$

k : coefficient of sensitivity

# *Example ( ftp case)*

- ftp case is a typical example to show how the threat levels are output by our system.
- There are appropriate amount of scans to ftp port.
- ftp case illustrate well the transition of threat levels
- We show how is the alert messages of our system like.

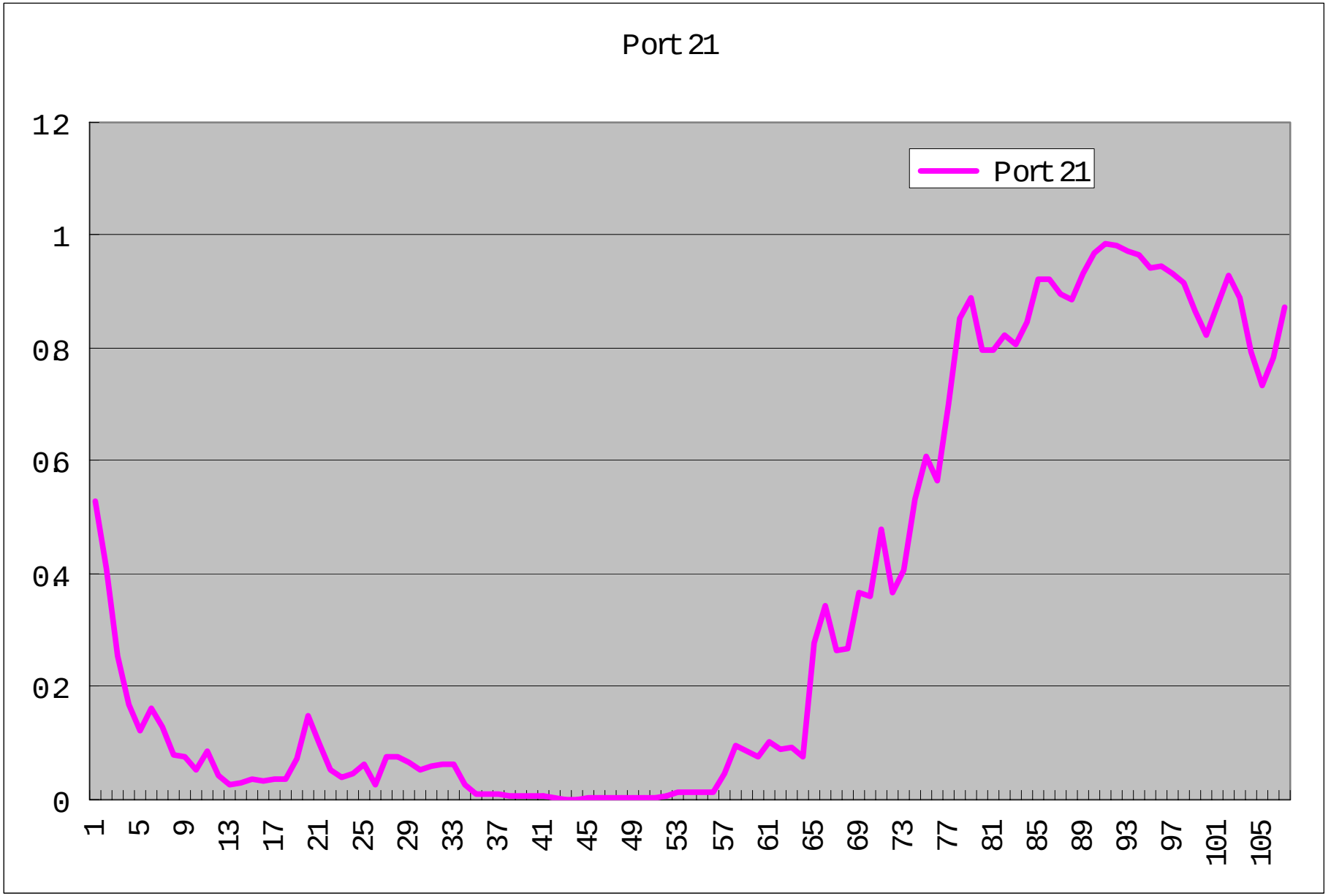
# *Example ( ftp case)* 2001-05-15~2002-05-16 (one year)



# *Example ( ftp case)*

YYYY-MM-DD

2001-05-15~2002-05-16 (one year)



WCLSCAN

# *Example ( ftp case)* 2001-05-15~2002-05-16 (one year)

**Port No.: 21**

**Warning Level: Severe (Level 2)**

**Bayes Confidence: 0.8741**

**Latest Access Amount: 105**

**Latest Moving Average: 57.2**

**Latest Standard Deviation: 27.8**

**(Latest Term: [Tue May 14 00:00:00 2002**

**-- Sun May 19 00:00:00 2002])**

WCLSCAN

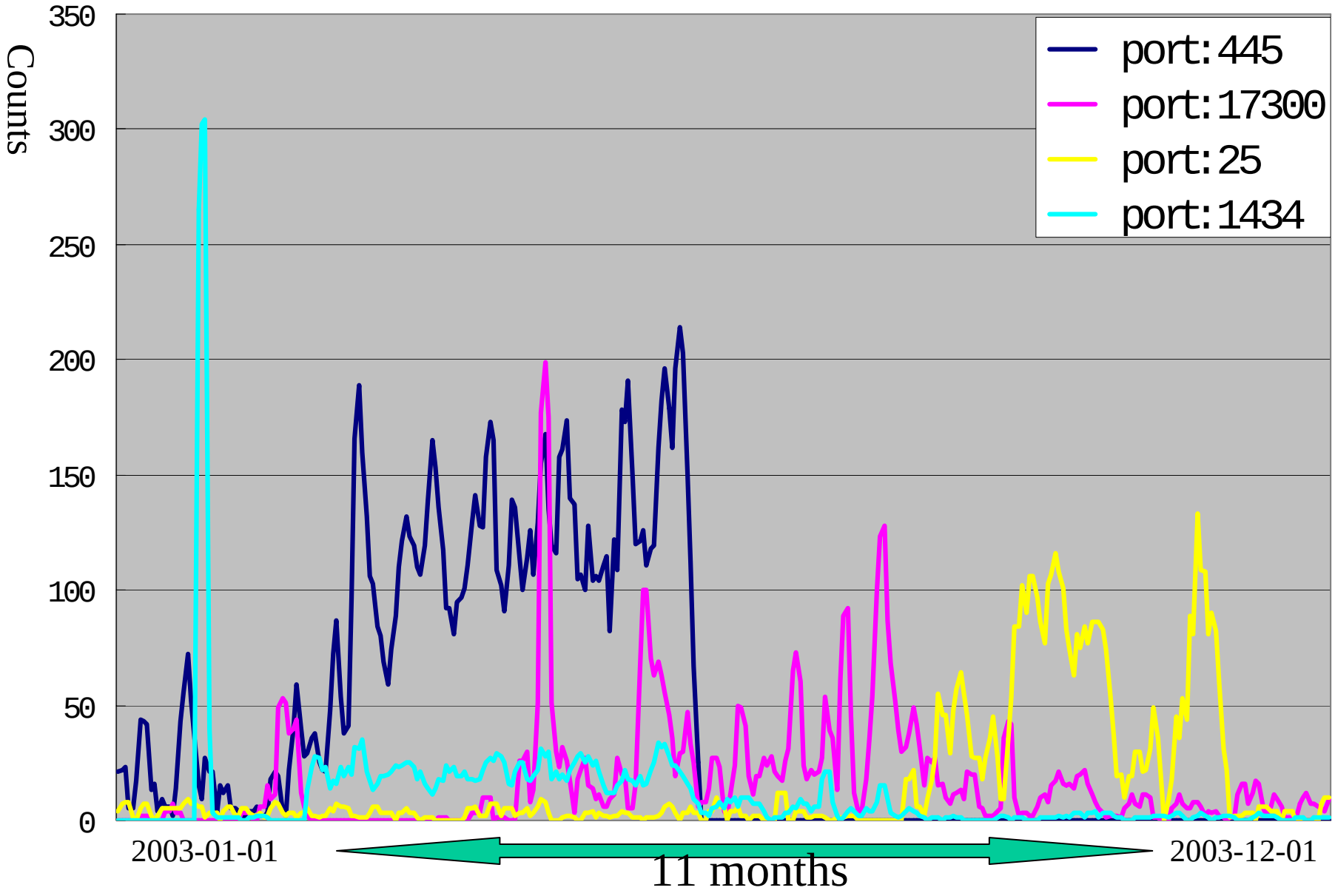
# *Evaluation by ROC Analysis*

- Receiver Operating Characteristic Analysis
- We apply ROC analysis which is a well-known evaluation method for signal detection
- We evaluate both false-positive and true-positive performance of our threat detection system

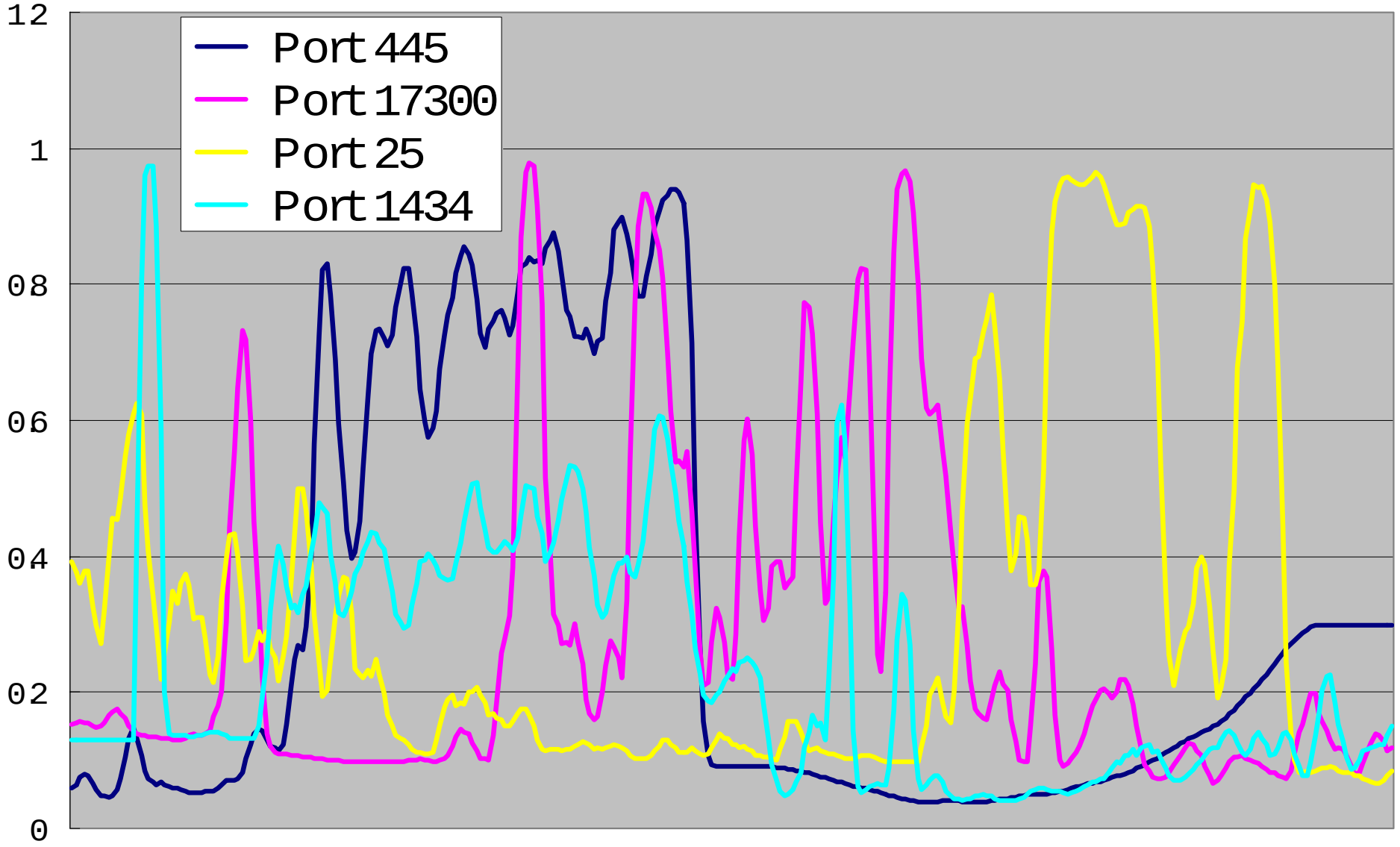
# *Evaluation by ROC Analysis*

- Target Data: *2003-01-01 , 2003-12-01*
- Relevant alerts during this period (JPCERT):
  - 2003-01-27, port1434(sql), MS SQL server 2000 scans (JPCERT-AT-2003-01-27)
  - 2003-03-18, Port80(http), MS IIS 5.0 vulnerability(JPCERT-AT-2003-0003)
  - 2003-03-31, port25(smtp), sendmail vulnerability (JPCERT-AT-2003-0004)
  - 2003-08-15, port135(rpc), Windows RPC scans (JPCERT-AT-2003-0006)

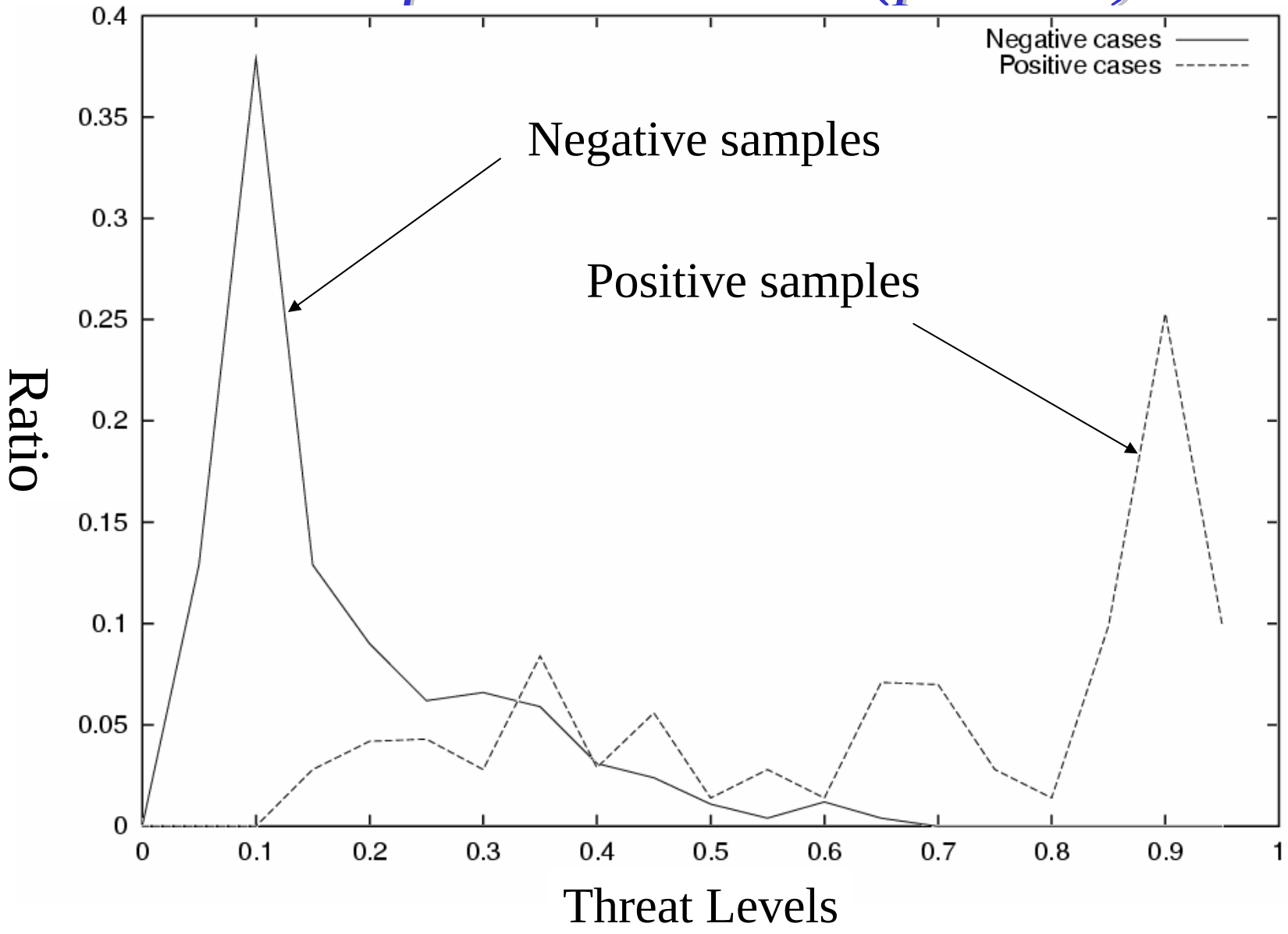
# *Time-Series Frequency Graph*



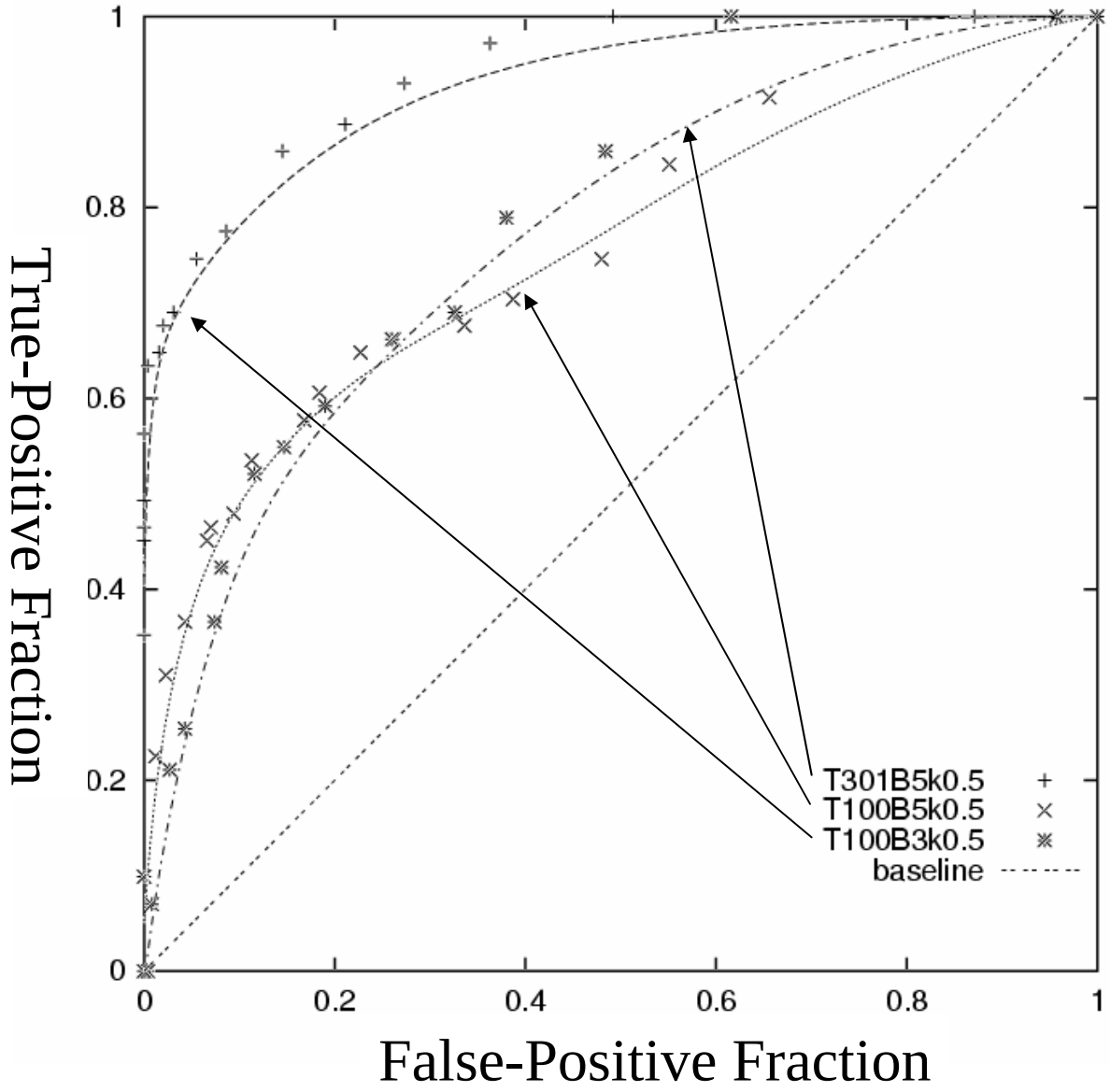
# *Time-Series Threat Level Graph*



# *Distribution of Threat Levels (port 25)*



# *ROC (receiver operating characteristics) Curve*




Port 25

Performace is very good!

Parameters:

| ID | Coeff. Bayesian Update | Bayesian Update Period | Trend Interval | Az Value |
|---|---|---|---|---|
| T301B5k05 | 05 | 5 | 301 | 095 |
| T100B5k05 | 05 | 5 | 100 | 079 |
| T100B3k05 | 05 | 3 | 100 | 08 |

WCLSCAN

# *Our Real Action using IWR aka WCLSCAN*

- Case Study 1
  - Doomjuice case
    - Type of Zero-day attack
- Case Study 2
  - SSL BOMB
    - Type of announcement effect attack

# *Case Study 1: Doomjuice*

2004-02-07 1pm: *We found port 3127, 1080 and 3128*

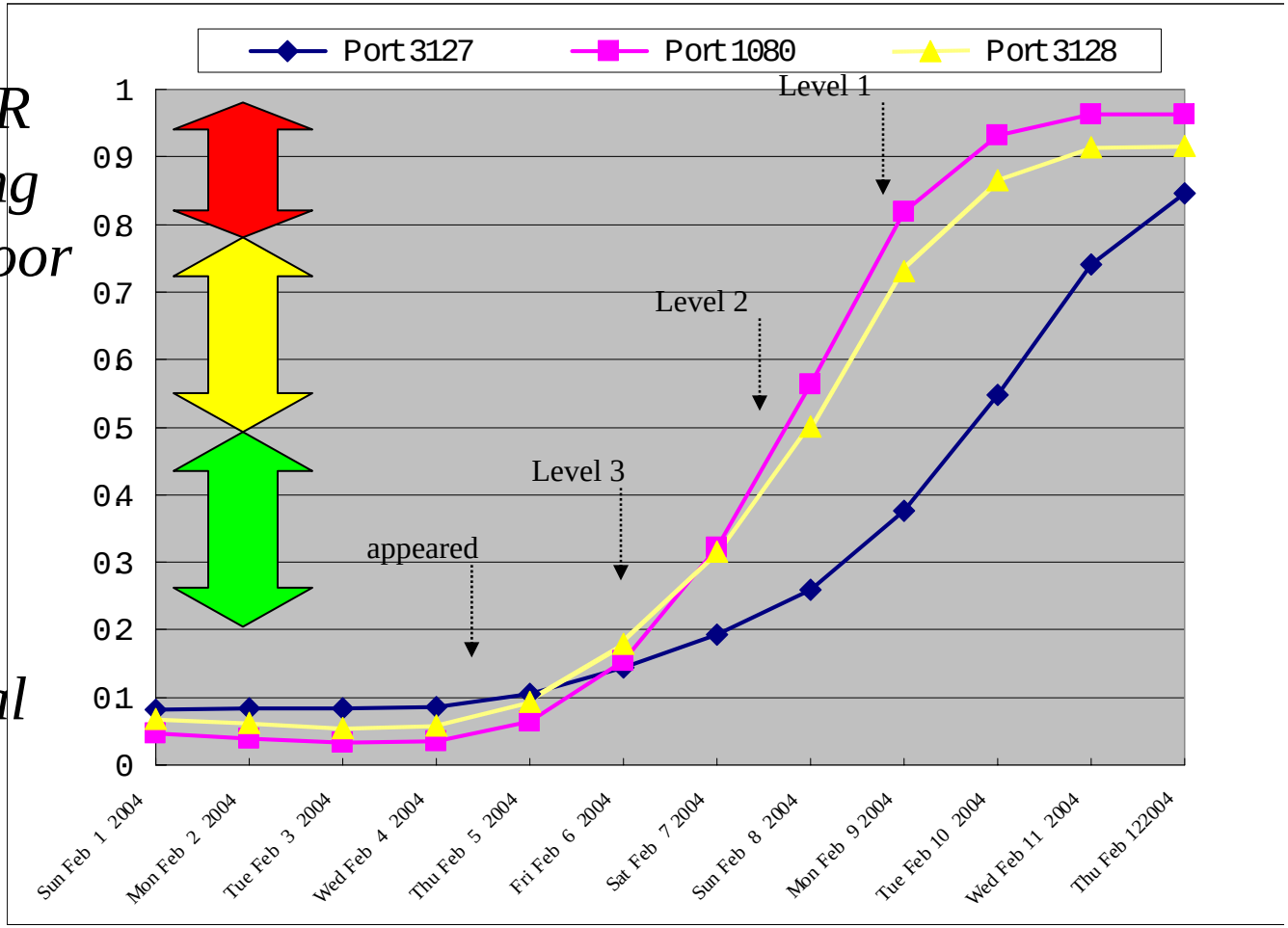
2004-02-07 4pm: *IWR mailing-list "Scanning for Mydoom's backdoor is increasing".*

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

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

Case of Zero-day attack

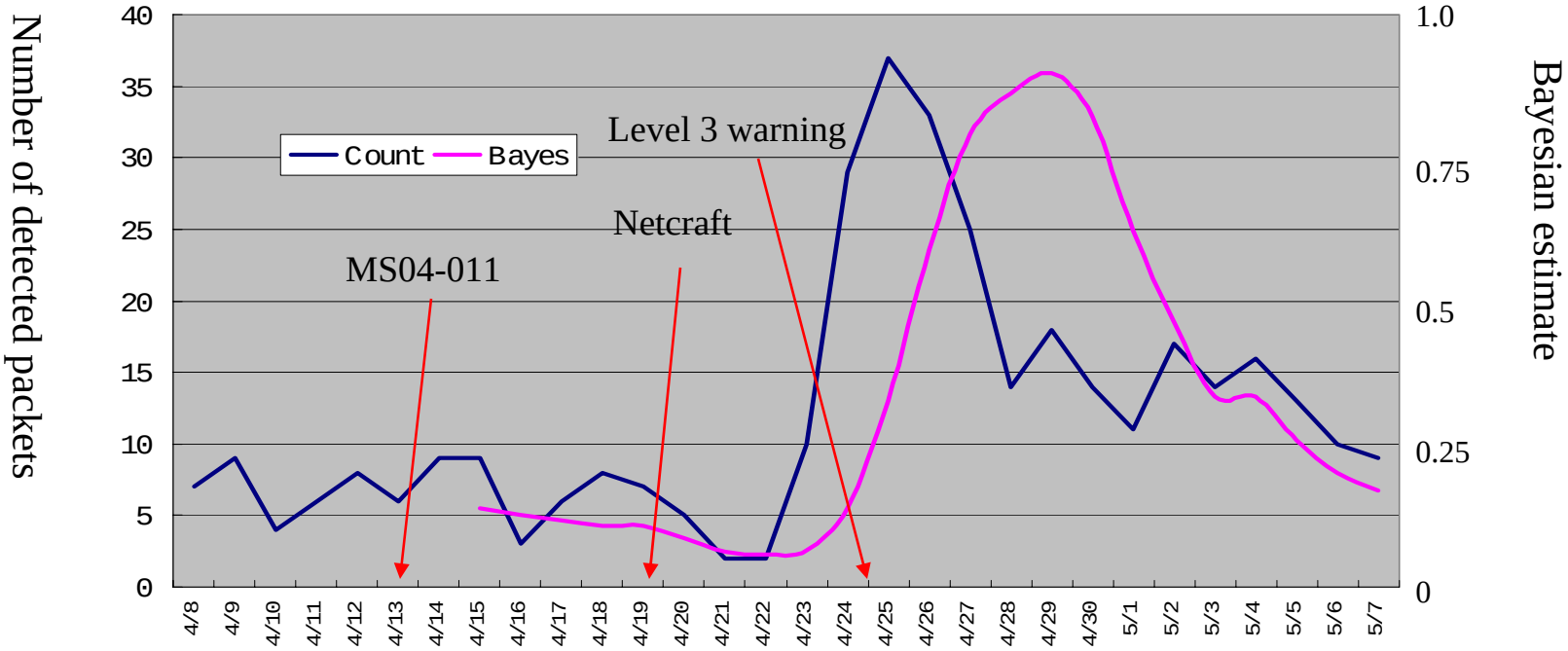
*Bayesian Estimation Curve*




*Time Zone is JST*

# *Case Study 2: SSL BOMB*

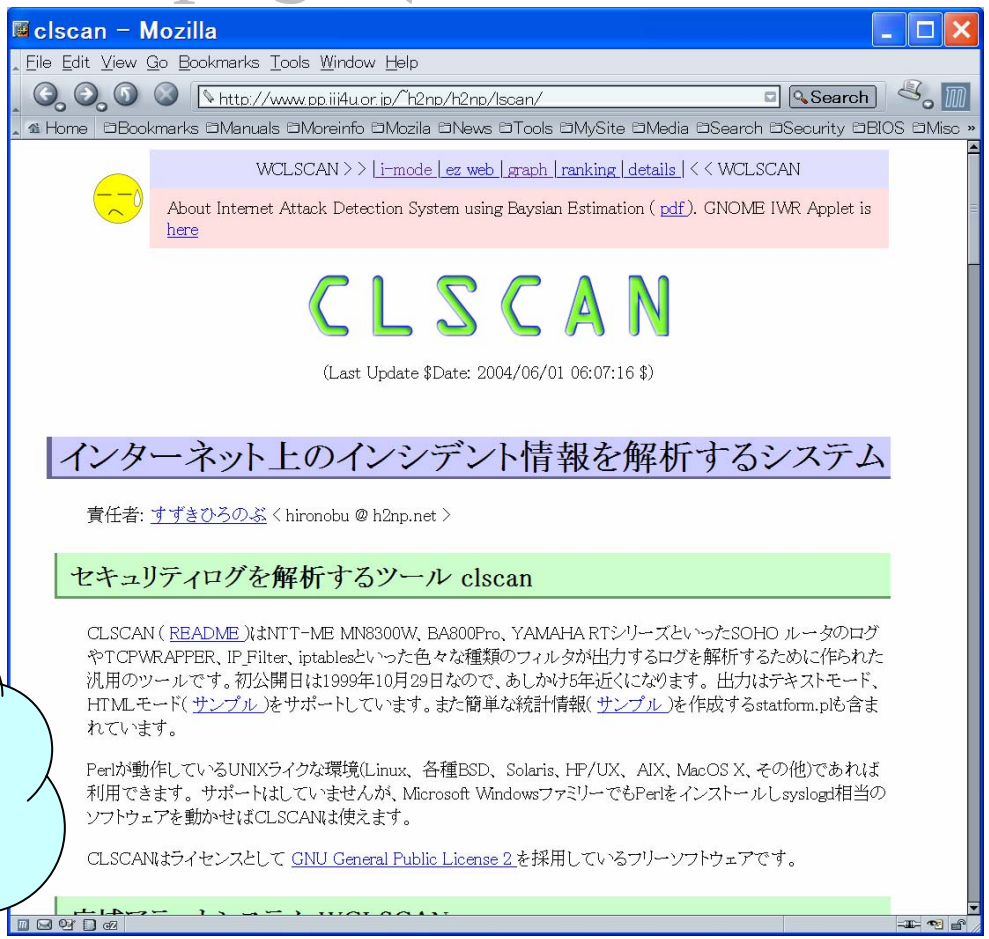
Case of announcement's effect




- 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

# *How to access WCLSCAN page (but in Japanese)*

- 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




```
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
```

*Over 68 millions "Keitai Denwa (mobile phones)" can access this page.*

**www.clscan.org**

• L: Alert level, P : port number, B : Bayesian estimation, C : packets count

WCLSCAN

# *Conclusion*

- We developed Internet threats detection system using Bayesian estimation, IWR aka WCLSCAN
- IWR automatically detects Internet threats and reports them
- IWR service is available 24hours/7days
- IWR performance is good
- IWR provides information for KEITAI-DENWA (smart phone) browser

WCLSCAN

# *On going project*

- Release source codes as Free Software
  - But all messages and documents are written in Japanese
- Visual analysis
  - 3D animation
- More sensor boxes
- Improve estimation method
- Etc. etc…

ご静聴有りがたう御座ゐました