vigilantplant®

The clear path to operational excellence

Network Packet Visualization Technology in Process Control Systems

Tatsuaki Takebe

Dr Kazuya Suzuki

Yokogawa Electric Corporation

YOKOGAWA

Agenda

vigilantplant®

1. Background
   - Security Framework
   - Threats situation in the Internet
   - Intrusion Detection
2. Our approach to the solution
3. Network Packet Visualization System
   - Three types of technique
4. Demonstration
5. Conclusion

Background 1 Security Framework

vigilantplant®

Basic Security Framework

- The Protection Framework is (Prevent, Deter, Detect, Respond) in Plan Do Check Act cycle.
- But things are not perfect.
- If they are not perfect, “detect” is the key.

Background 2 Threats situation

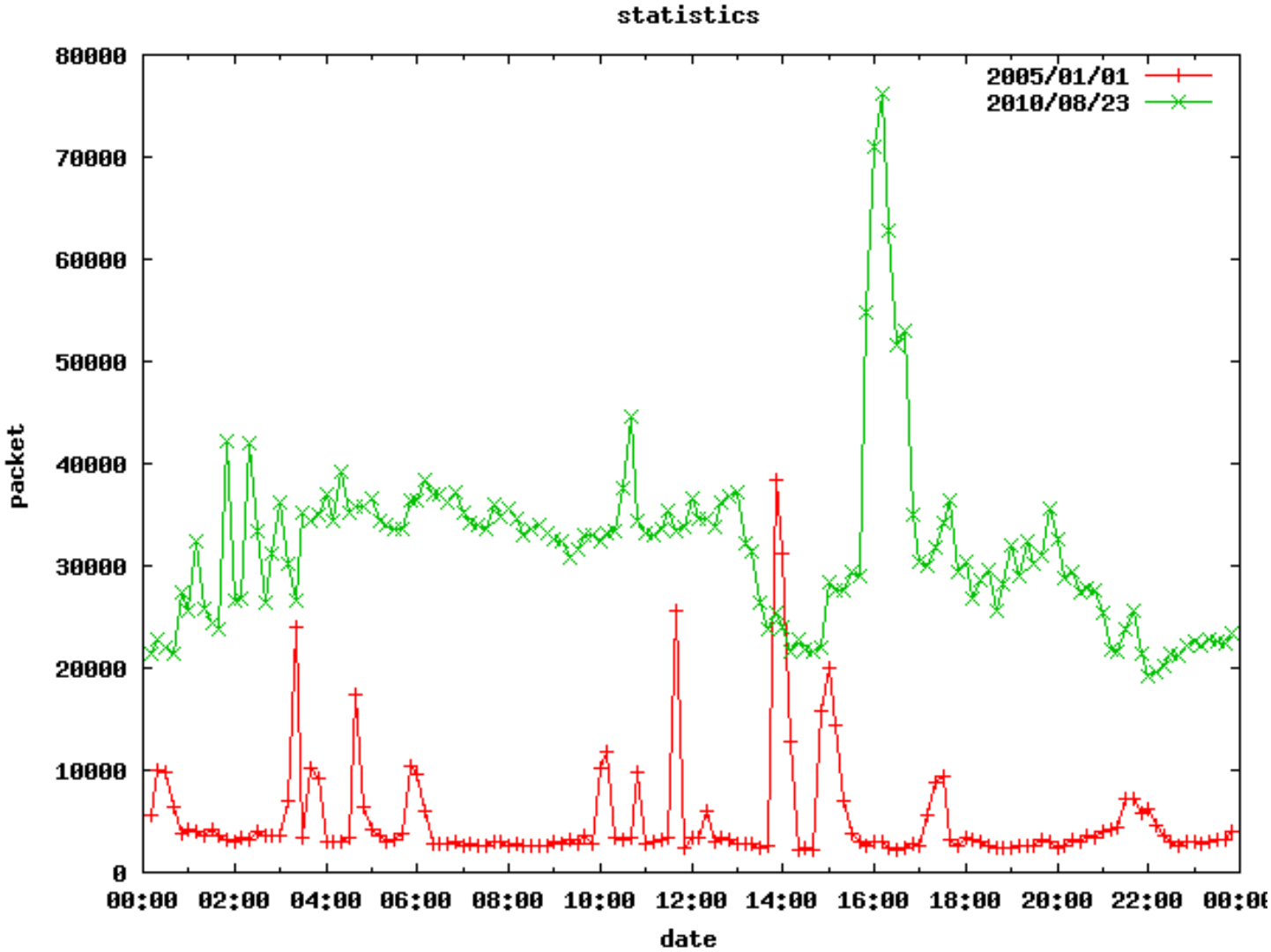
vigilantplant®

- Malicious Software (Malware)
  - Worm/Virus/Trojan horse
- Attacks
  - Network/USB stick/E-mail/Web/PDF/Flash file
  - Attacks have been increasing
- Malware in the Process Control Systems
  - Becoming Real
  - E.g. Stuxnet

Threats situation in the Internet (BG 2)

vigilantplant®

- One day Traffic Volume into a darknet (Attacks via NW)



Background 3 Intrusion Detection

vigilantplant®

Conventional detection techniques

- IDS/IPS depends on pre-defined signatures
  - Crackers twist malware to bypass IDS/IPS signature detection
  - Hard to maintain the signatures with the current malware production rate
- This type of single technique is not enough to detect all the network attacks.
- Multiple detection techniques running together for analysis is necessary to reveal what's really happening.
- The administrators are required to judge whether the network is intact or not.

Our strategic approach to the solution

vigilantplant®

- The network monitoring system should provide correct and straightforward information to administrators.
  - Multifaceted perspective assists network administrators to make the right decision.
- With this capability, Network Packet Visualization system becomes indispensable for the right judgment.

Related Visualization Techniques in the past

vigilantplant®

- Some researches have studied along this line
- Issues of those approaches
  - Their analyses are too complex and heavy to produce the data for visualization swiftly.
  - The analyses are not perfect to hold all of the attacks.

- Visualization needs
  - faster processing
  - independence from the analyses

Objectives of Network Packet Visualization System

vigilantplant®

- To provide the visualized information helping the network administrators grasp the network healthiness
  - Security non-professionals/NW non-professionals understand the situation by instinct.
- To provide performance and to avoid deletion of the potential attack symptoms by minimizing processing on the raw data.

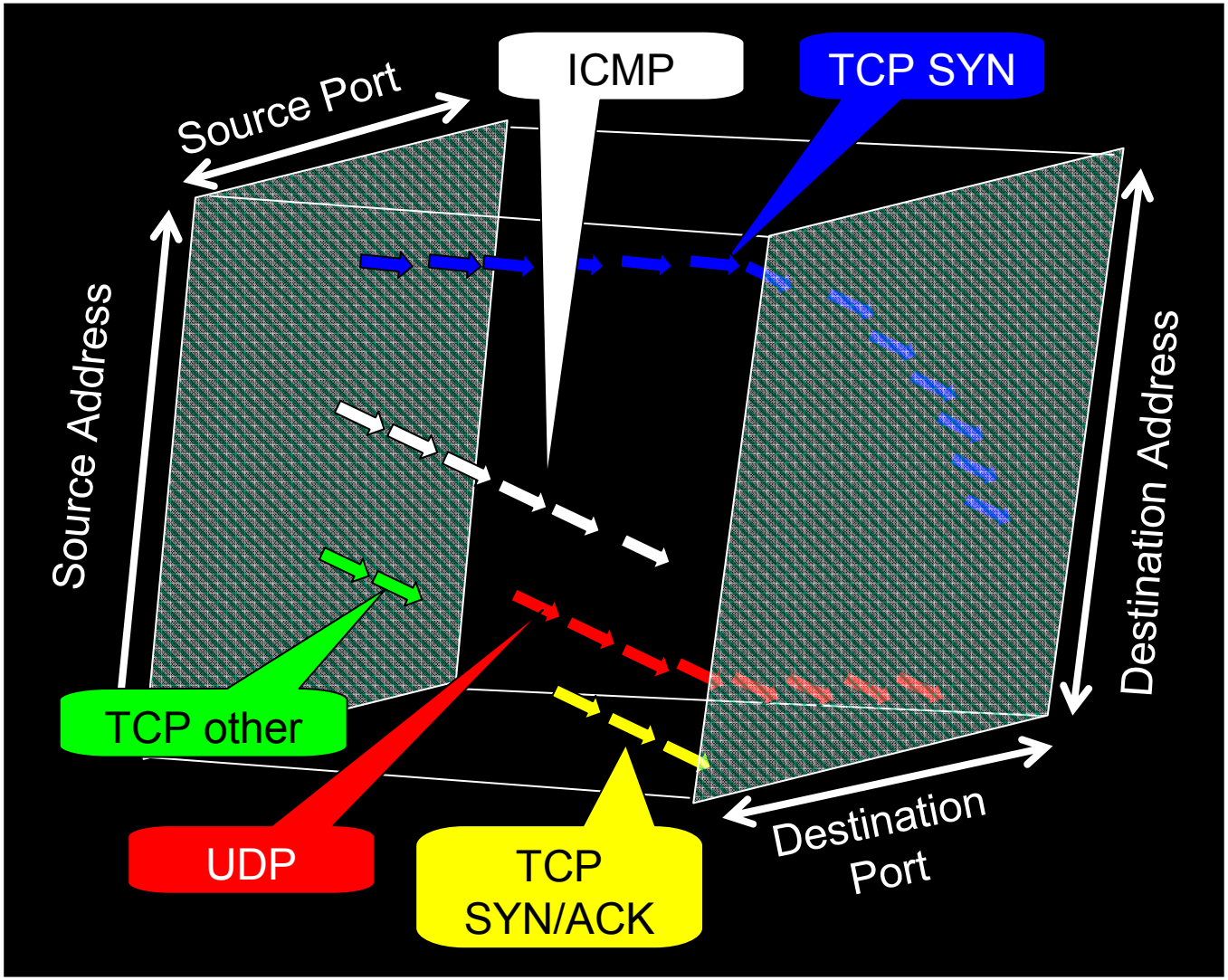
NW Packet Visualization System

vigilantplant®

- Cube
- World Map
- Purdue Plant Map

vigilantplant®

Three Dimensional Visualization



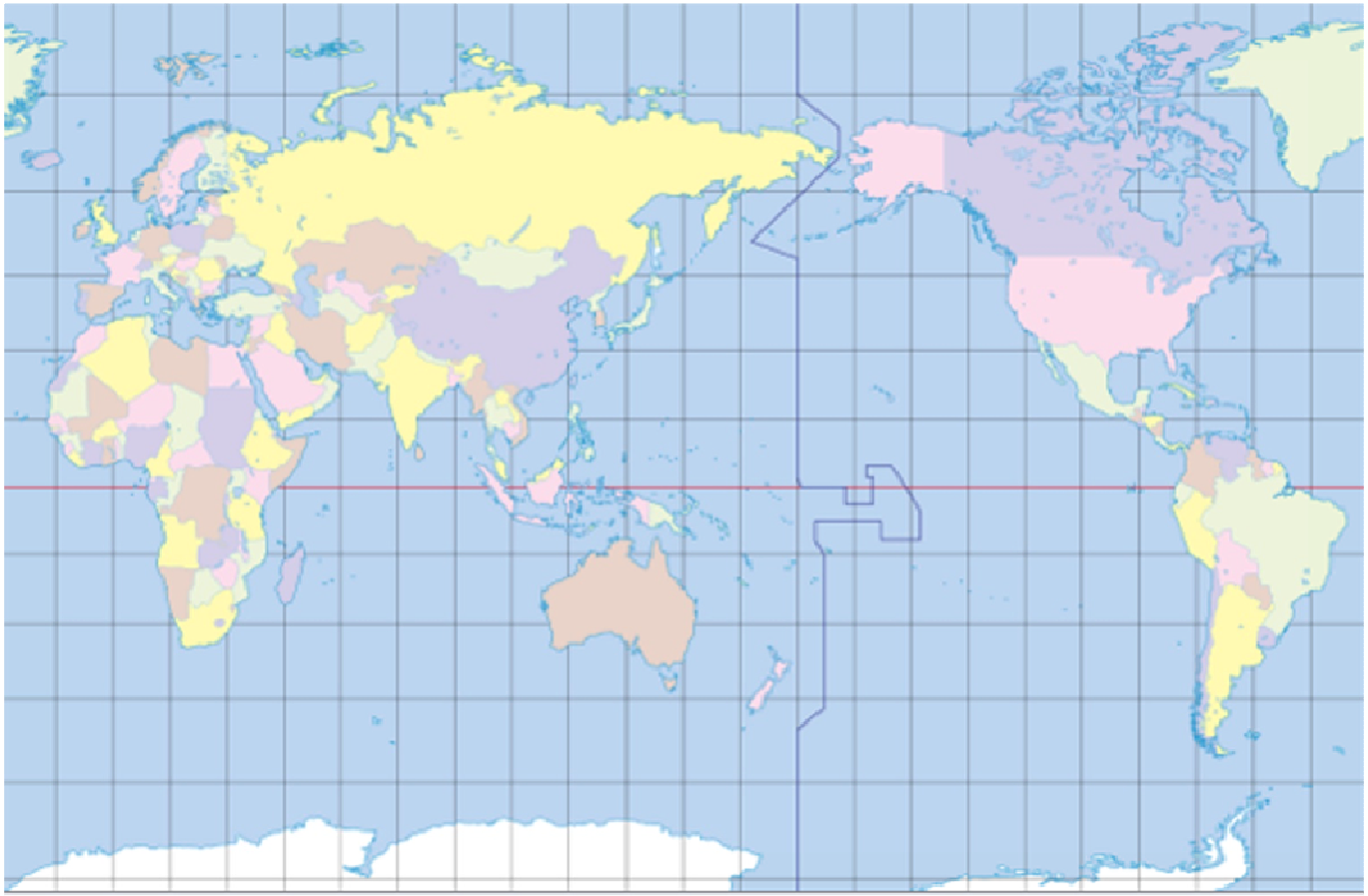
Only
- Source Address
- Target Address
- Port Number
- Protocol Type

are used.

This shows the variation.

World Map

vigilantplant®

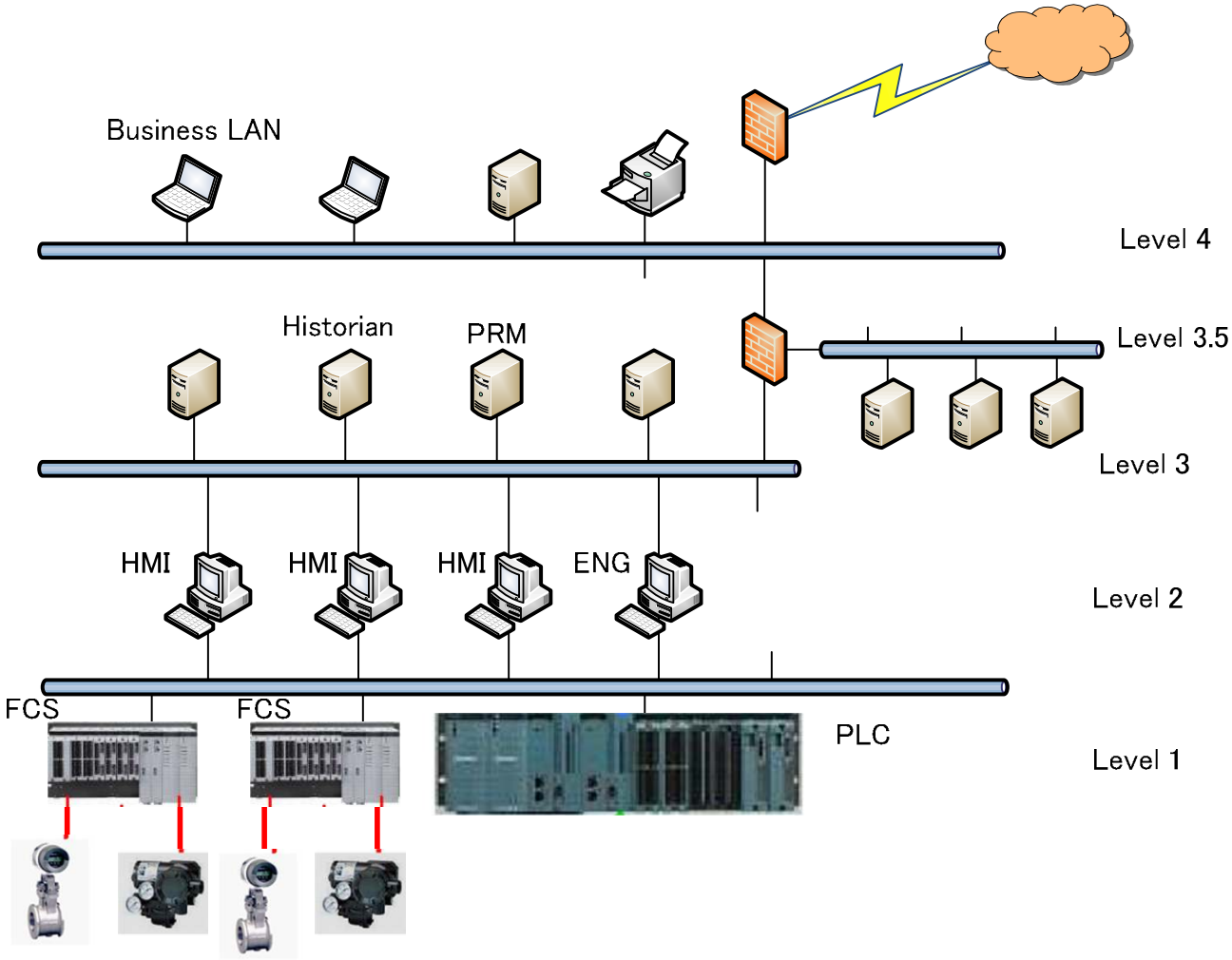


Only
•Source area
•Target area
are used.

- This shows the locality.
- Malware has locality.

Purdue Plant Map

vigilantplant®



Only
- Source address
- Target address

are used.

- Communication might reveal anomaly.

Demonstration

vigilantplant®

- Internet
  - Cube
  - World Map

- Plant network
  - Purdue Plant Map
  - Cube

vigilantplant®

- Visualization of the traffic to the darknet
  - Attack 0: No fancy attacks
  - Attack 1: Network Scan (TCP/SYN)
  - Attack 2: Network Scan (ICMP)
  - Attack 3: Network Scan (dasher worm)
  - Attack 4: Bots (series op UDP)
  - Attack 5: Atlas

Plant network

vigilantplant®

- Visualization of the traffic on the plant floor.
  - Purdue Plant Map
  - Cube
  - Sasser Worm Cube

NICTER

vigilantplant®

- NICTER stands for Network Incident analysis Center for Tactical Emergency Response.
- It is a network monitoring research project in Japan.
- NICTER system consists of three major systems.
- Macro Analysis System
  - Analyzes network traffics and helps detect attacks
- Micro Analysis System
  - Analyzes malwares
    - Static Analysis：Disassembles a malware and analyzes APIs used by the malware
    - Dynamic Analysis: Executes a malware in the sandbox
- Macro-Micro Correlation System
  - Synthesizes the results of Macro/Micro Analysis System
    - This identifies the cause of the behavior from Macro Analysis System

- Network Packet Visualization system is Macro Analysis System above in the NICTER project

Conclusion

vigilantplant®

- Network packets visualization system is proposed.
- Administrators/Operators watch the healthy network packets, they create healthy baseline image of the network traffics.
- If a visualization image changes, Administrators/Operators notice something happened easily.
- Non-security professionals/Non-NW professionals find network anomalies/attacks without lengthy education or training.

Thank you for your attention!

***) Product names in the slide are trademarks or registered trademarks of their owners.**