

Technology and Standards for CSIRT

Prof. Dr. Suguru Yamaguchi
JPCERT Coordination Center

Overview

- Elements required for CSIRT operations
- Who provide them and how?
- More considerations required for the realistic operations of CSIRT.

CSIRT



Information center
for their constituents

Active component for
handling computer
security incidents

CSIRT functions, today?

- Computer Security Incident Response Teams.
 - **Coordination body** for response activities linked with multiple organizations and entities.
 - **One-stop resource repository** for anyone who has to handle computer security incidents.
 - International point of contact (**PoC**) for further communication to handle computer security incidents.
 - **Technical assistance and support** functions provided by their specific customers defined as “constituency”
 - Not limited to public services, some CSIRT provides their services to the specific customers.
 - e.g CSIRT in large enterprises / NTT-CERT
 - **“Observatory”** for attack trend analysis of cyberspace.
 - Providing **educations and training** for human resource development (HRD) in related entities.

Technology for incident responses

- **Modern Incident Response**

- Computerized management system of incident responses, that enables us to trace down the status of each responses: e.g. Ticket tracking system.

- **Communication confidentiality and validation**

- **Modern cryptographic system** to protect communication between CSIRT and entities involved to computer security incidents. PGP is very popular for CSIRT community, but X.509 PKI based systems are getting popular.

- **Several databases** for actual response works

- Point of contact, technical database about malwares, pathological analysis of computer security incidents, social activities, news, ...

Technology for incident responses

- **Forensic** Tools for seeking out what made this incident and developments.
 - Analyzers on computer system, communication, application programs, OS and other basic elements.
- Excellent resource: NIST, “*Computer Security Incident Handling Guide*”, SP800-61 rev1, March 2008, DOC, USG.

Technology for assistance

- **Malware analysis capability**

- Malware today is developed not for pandemic.
- Customized development for specific organizations.
 - not detected by generic Anti-Virus software
 - Immediate feedback to field engineers who are working against the malware infections and activations
 - Use commercial services?
- Public CSIRT also can get benefits from this capability.
 - Categorization of malwares
 - Toward Polymorphic code analysis
- Good trend analysis to know what's going on in cyberspace.

Technology for assistance

- **Vulnerability analysis** capability
 - Only its developer can evaluate and confirm vulnerabilities in software products.
 - “Testbed” can help much that developers for vulnerability analysis.
 - Normally, the “testbed” can be shared.
 - The “testbed” can provide human resource development for evaluators and testers of software products.
 - E.g. Inter-Operability Labo., University of New Hampshire

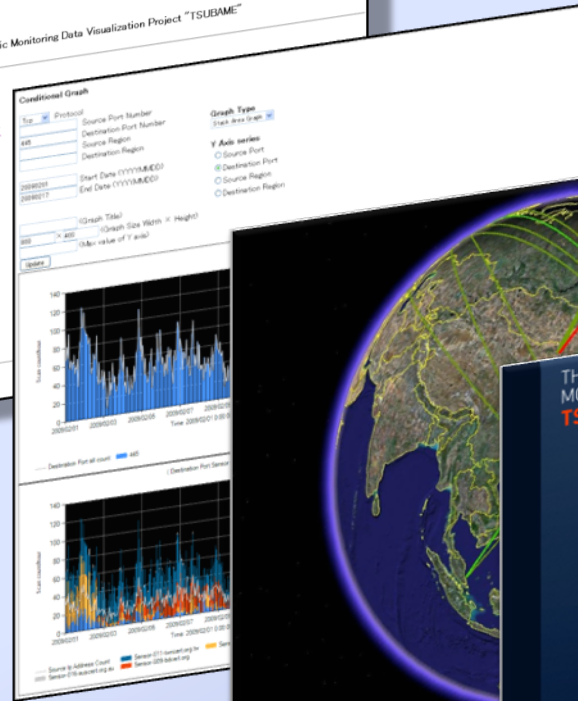
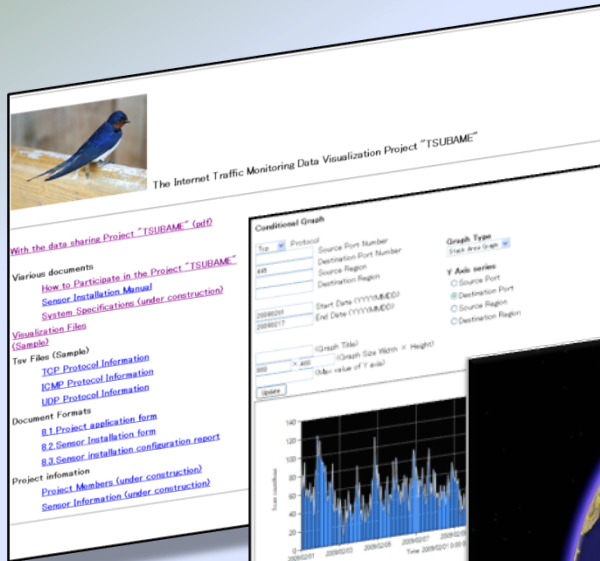
Technology for “Observatory”

- Good model: **Hurricane Center**
 - Observations of the Internet in 24/7 basis.
 - Monitoring of attacks
 - Trend analysis
 - Actual impact analysis and development of mitigation
 - Advices for response & recovery process
 - “Honey pot” & “Darknet”
 - From IP to Application servers.
- Providing this functions as a part of CSIRT
 - Einstein sensor / USCERT
 - Tsubame / APCERT.org
 - Darknet Project / TERENA’s cymru project.

TSUBAME Visualization Tools

..... Portal Site

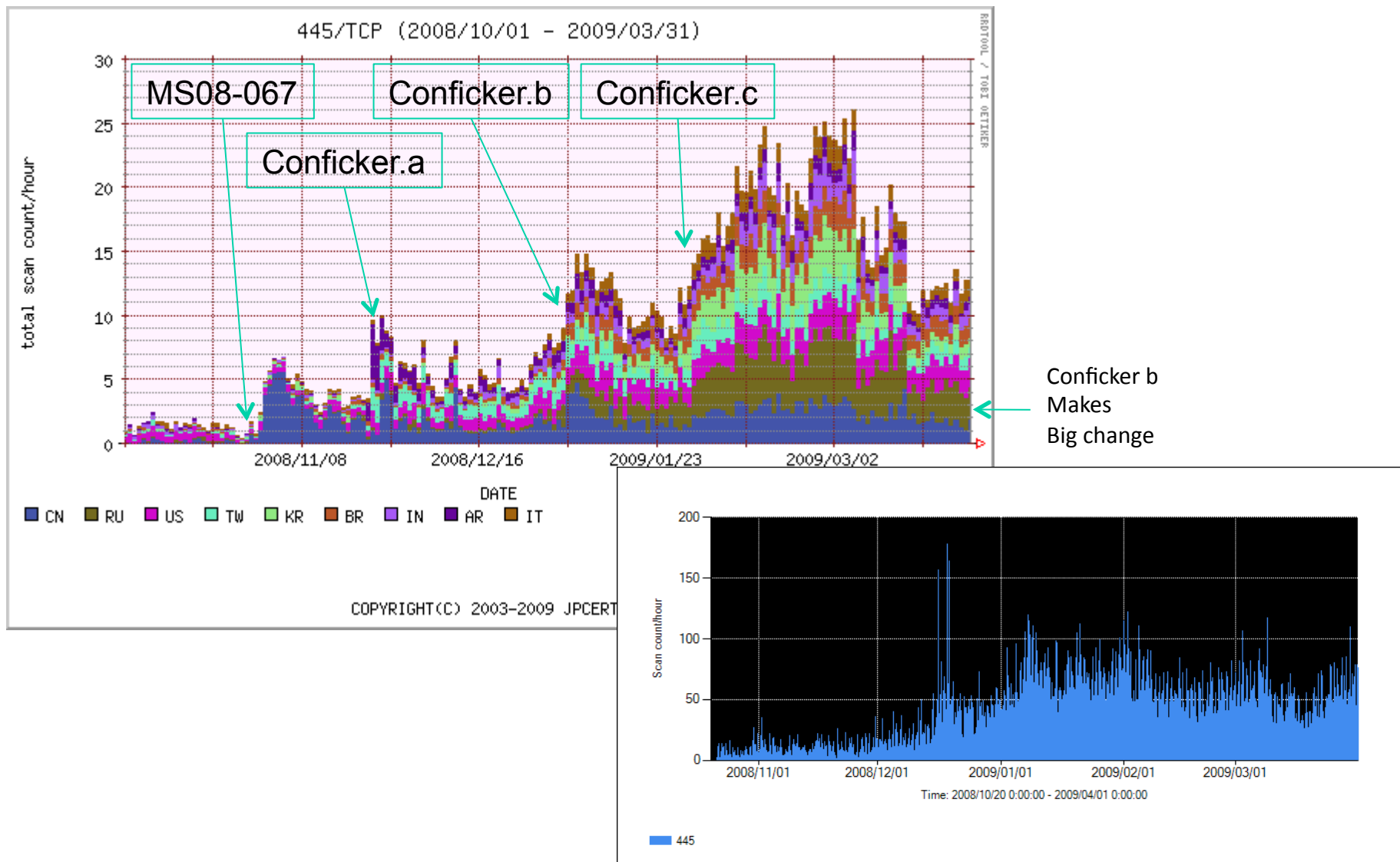
..... 2D Graph



3D Visualization Map

Analysis Portal

Conficker Activity on ISDAS (Monitored in Japan)



Standards

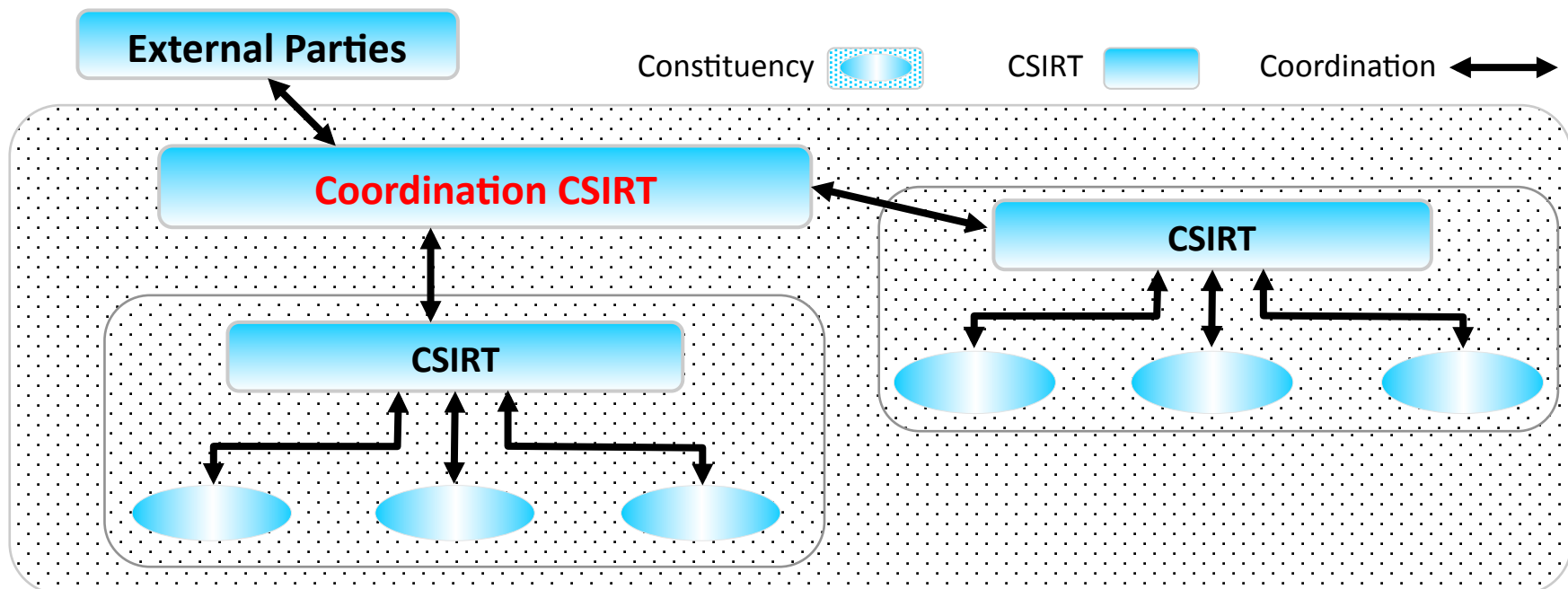
- ISO27001 ISMS
- ISO27035 Security Incident Handling
- ISO SC27, WG1 ISMS, WG2 Cryptographic systems and their management, WG3 CC (15408)
- IODEF, IETF for standard data exchange format for computer security incidents
- ITU-T SG17 Communication Security, X.509,

Technology for their business domain

- Several technology is required for their specific business domain.
 - Especially for CSIRT for specific enterprises.
 - E.g. Mobile / Cellular phone network operators.
 - Working together with other teams.
 - No separation with trouble shooting team
 - No separation with disaster recovery planning team
 - No separation with business continuity management team
 - No separation with risk management team

Coordinating CSIRT

- Coordinates and facilitates the handling of incidents across a variety of external or internal organization including other CSIRT
- Coordinating entity for individual subsidiaries of a corporation
- Having a broader scope and a more diverse constituency
- Sometimes, No authority over the members of their constituency
- Main function is to provide incident and vulnerability analysis, support, and coordination service, and guidelines, advice, warnings, and recommended mitigation and recovery solutions.



Business Design of CSIRT

- Stakeholders
- Organizational Structure
- Finance and sustainability
- Constituency
- Mission Statement
- Benefits and risks
- Services and coverage
- Resources
- Communication plan with other entities
- Evaluation and improvements.

Then, implement, but it's an endless game

- Planning multi-year “evolution”
 - Human resources
 - Information repository helping incident handlings.
 - Education for people who should understand CSIRT's benefit and outcomes.
- Once developed, then eventually split its functions to multiple entities.
 - No monopoly.
 - Collaborations amongst CSIRTS.