

Engineering for Improving the Performance of Incident handling process

Suguru Yamaguchi
Nara Institute of Science and Technology
Japan

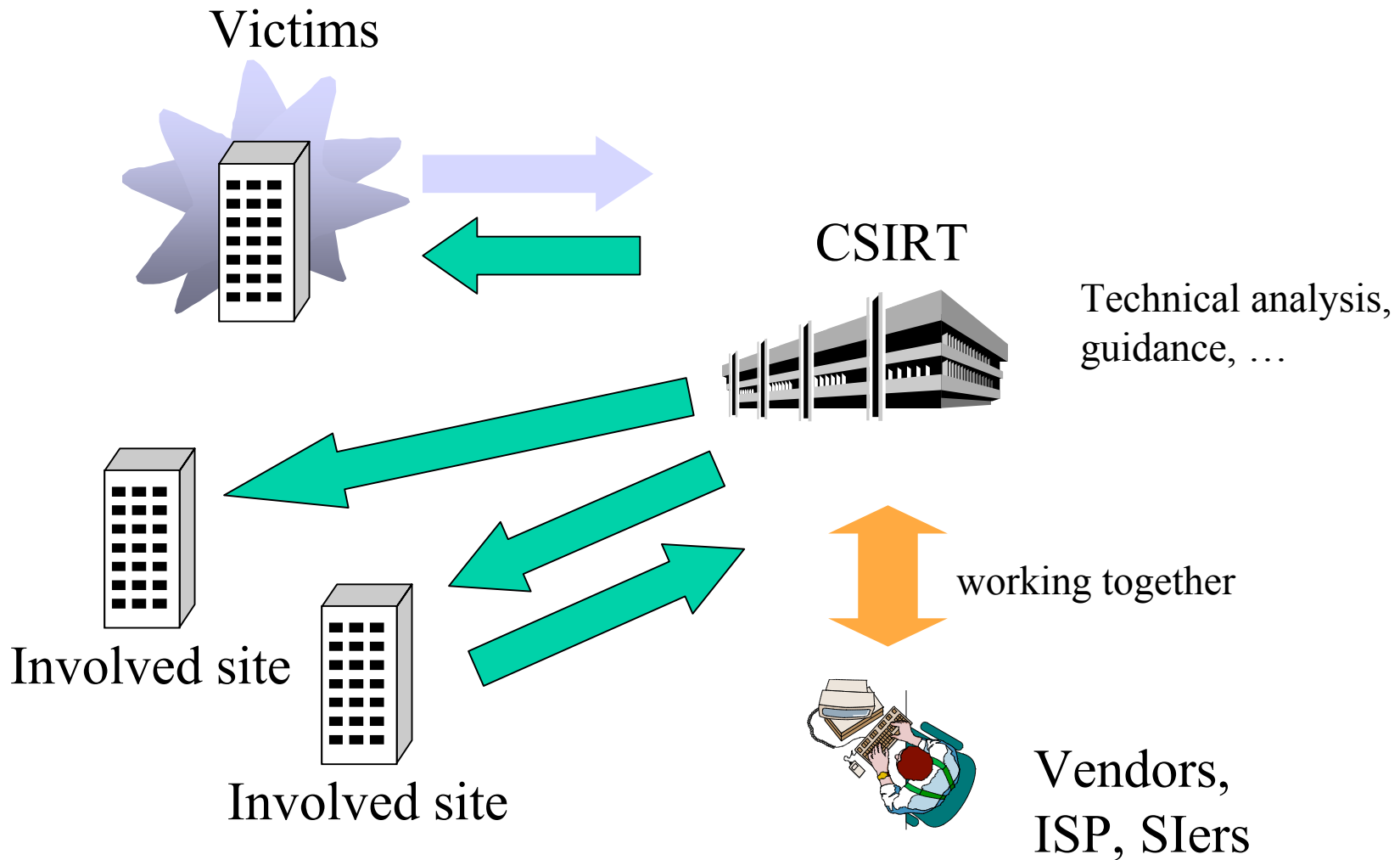
Overview

- Incident Handling by CSIRT
 - IODEF and its development & deployment
 - IODEF was originally developed as classic inter-CSIRT information exchanges.
 - Variety of information exchanged among CSIRT has been drastically changed: incident report, information about vulnerabilities in products, forecasts and analysis report, direct exchange of machine generated information,
 - Now phase II.
 - Our efforts
 - NAIST & JPCERT/CC in Japan
 - Supported by research grant from MEXT/JST (FY2002 - FY2004)
 - Working with US-CERT/CERTCC (US) and NISCC (UK)
 - Working with APCERT teams
 - IETF INCH WG
-

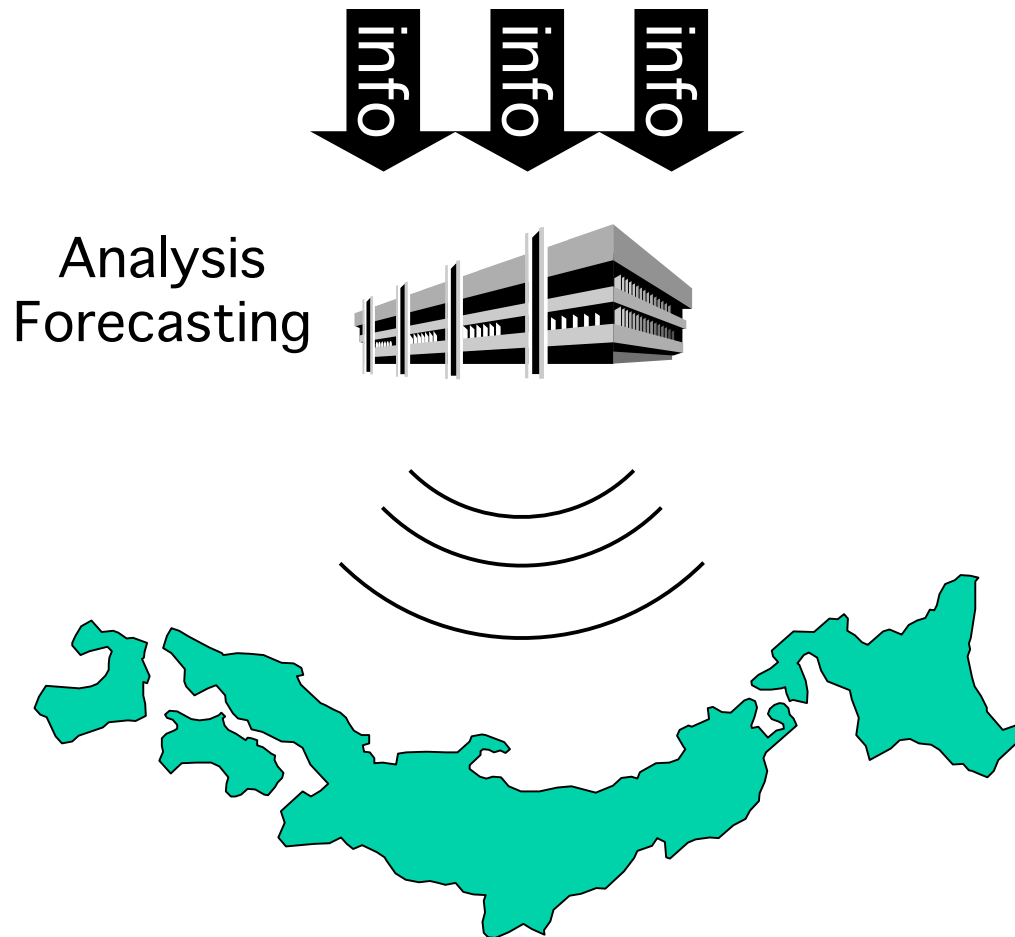
Overview of Incident Handling by CSIRT

- CSIRT: Computer Security Incident Response Team
 - CERT/CC, US-CERT, JPCERT/CC, Telecom-ISAC, NIRT, NISCC, ...
 - Functions
 - Provide response to incidents for its constituency
 - Provide warnings and alerts for its customers
 - Act as information clearing house, especially on information about vulnerabilities in commercial products
 - Act as information exchange among CSIRTS
 - Move from “response” to “preparation” and “prevention”
-

CSIRT: Coordination



CSIRT: warnings & alerts



- Technical source for fixing security holes
 - Vendor notes
 - CERT/CC advisory
 -
- Warnings & Alerts
 - Quick fix on systems in its constituency

Issues

- Too many forms of communication
 - Reports from victims (e-mail)
 - Reports from vendors (e-mail)
 - Reports from other CSIRT's (e-mail)
 - Automatic generated reports from IDS/IDP boxes. (SNMP, but normally private MIB, not colorful)

 - Acceleration required, but how?
 - Semi-automatic information exchange among CSIRT
 - Automatic information exchange, (challenge!)
 - Human readable form → machine readable form
-

Efforts, so far

- IETF INCH WG
 - INCident Handling WG
 - Define “IODEF” format, XML based, for information exchange among CSIRTs
 - Since 2002

 - Efforts
 - Initial version of IODEF, described in XML, by CERT/CC
 - “The Incident Object Description Exchange Format (IODEF) Implementation Guide,” draft-ietf-inch-implement-00.txt
 - Language extension, mainly by NAIST & JPCERT/CC
 - Extensions for real time, inter-network defense, (RID), by MIT group
 - Inter-AS data exchange
 - Traceback for DDoS
-

Activity for IODEF in our group

- Efforts on standardization in IETF INCH WG.
 - Tools developed for incident response handling procedures in CSIRT, using IODEF
 - Development of framework for APCERT (Asian Pacific CERT), as its deployment process
-

Standardization Activity

- IODEF: huge and complex description in XML
 - Exchange “incident report” among CSIRT’s
 - Still improved in progress
 - i18n (Internationalization) and l10n(Localization)
 - Some improvements
 - Simplification of “EventData” element tree which is responsible for representing actual incident events
 - Specification for treatment of “RecordData” and “AdditionalData” for automatic handling IODEF documents
-

Standardization of VEDEF

- New steps taken.
 - NISCC proposed VEDEF (Vulnerability and Exploit Description and Exchange Format) at INCH WG in previous IETF60 (June 2004)
 - JPCERT/CC had developed similar format called VuIDEF, based on IODEF
 - CERT/CC, JPCERT/CC and NICSS are collaborating for vulnerability handling
-

Tools Development by our group

- IODEF Verifier
 - Tool to create IODEF documents
 - Beta stage
 - Web System for receiving “Incident Reports” in IODEF format
 - Beta stage

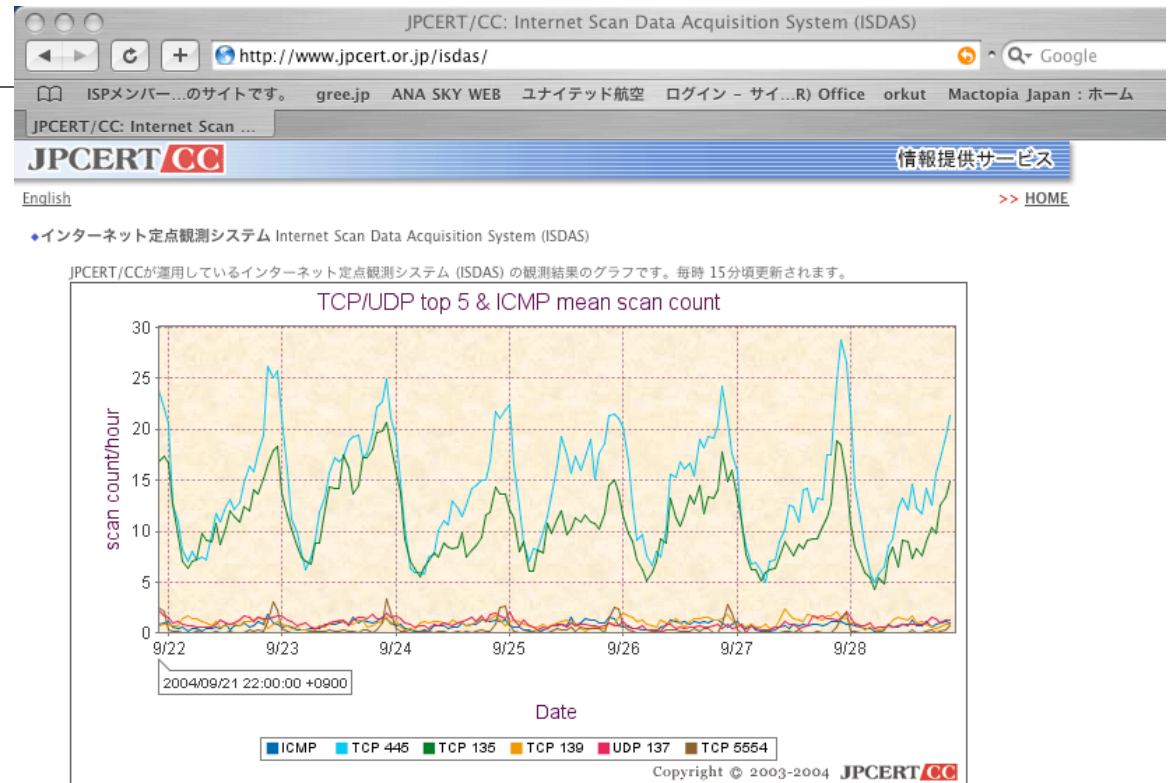
 - ISDAS (Internet Scan Data Acquisition System) traffic data sending system
 - RC stage, in operation @ JPCERT/CC
 - DBMS for ISDAS traffic data
 - Alpha stage
-

IODEF Verifier

- To verify XML format
 - the validity of syntax along IODEF XML Schema (or DTD)
 - To verify the semantic validity of the following
 - Time and date format
 - Timezone format as an UTC time zone format
 - IncidentID (provides a function but blank for now)
 - Omit following verification
 - Filename,e-mail address,URL,Postal code,TEL,FAX
 - To set and extract items (elements and attributes) from and to IODEF documents
-

ISDAS

- Traffic data analysis system
 - Mainly scan activities, from multiple distributed-installed sensors
 - More sophisticated data analysis we are aiming.
 - Data exchanged among CSIRT's internationally.
 - Using IODEF.



上のグラフが示す数値は、宛先ポート別にカウントしたスキャンログの総計をセンサー 1 台あたりの平均にした数です。

<説明資料>

- [インターネット定点観測システムの説明](#)
- [グラフの説明](#)

<参考資料>

- [インターネット定点観測システム稼働開始 \(プレス発表資料\)](#)
- [インターネット定点観測システムサービス提供開始 \(プレス発表資料\)](#)
- [Welchia/Nachi ワームの感染活動の減少を観測 \(プレス発表資料\)](#)
 - [2004年1月7日\(水\) 公開のグラフ](#)
- [Microsoft ASN.1 Library の脆弱性に関する注意喚起](#)
 - [2004年2月16日\(月\) 公開のグラフ](#)
- [Sasser ワームの感染活動に関連するポートスキャン状況について](#)

Handling tools for ISDAS Data

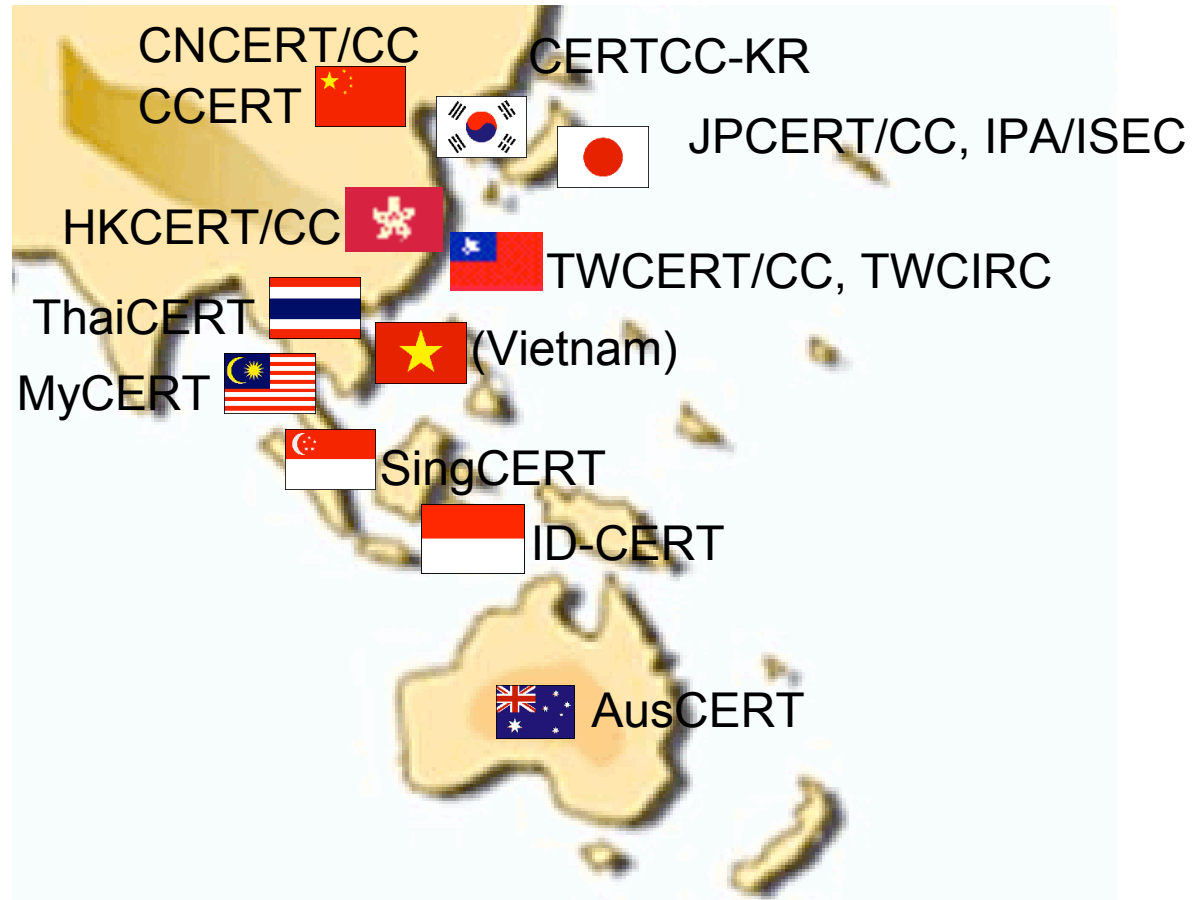
- ISDAS is Scan Monitoring System in JPCERT/CC
 - <http://www.jpccert.or.jp/isdas/>
 - JPCERT/CC sends ISDAS data in IODEF form every hour corresponding each AP countries
 - DBMS for ISDAS traffic data (Prototype)
 - With Cyber Solutions Inc.
 - Distributed IDS network developer/provider
 - Joint research activities.
-

APCERT

- Asia Pacific Computer Emergency Response Teams
 - Regional forum of CSIRT in AP
 - 1st AGM was held on Feb. 25th 2003 in APSIRC2003
 - AusCERT (steering committee chair)
 - SC: AusCERT, JPCERT/CC, HKCERT, SingCERT, MyCERT, CERTCC-KR, CNCERT/CC
 - Secretariat: JPCERT/CC and CERTCC-KR

 - APSIRC (AP Security Incident Response Conference) is our annual conference.
-

APCERT funding members



APCERT Cooperation Framework

- Making common profile (IODEF subset) in APCERT for exchanging incident data and traffic data among CSIRTs in Asia-Pacific Area
 - In progress
 - CNCERT (China), JPCERT/CC (Japan) and KRCERT (South Korea) are currently discussing for developing framework
 - Aiming direct exchange of machine generated data from sensors.
 - Distribution of tools for handling IODEF documents to CSIRTs, mainly for APCERT teams
 - Mainly EFT purposes.
 - I18N are highly required for Asian countries.
-

Profile for exchanging Traffic Data among APCERT

Reporter	Name
Å@	Organization
Å@	Tel
Å@	E-mail
Å@	Fax
∞	country
Å@	local area
Å@	time
Å@	Timezone
Destination	IP
Å@	Port
∞	country
∞	local area
Å@	time
∞	timezone
Source	IP
Å@	port
Å@	Protocol
Å@	attack type
∞	country
etc	purpose
Å@	restriction
Å@	ID
Å@	description
Å@	contact role

Future Development in our group

- Automatic Sending and Receiving Scan Incident Data with other CSIRTs in APCERT
 - To the actual field....
 - Apply to traditional IRH
 - Integration our system into “Web Form”
 - R&D for developing DBMS for general Incident Reports
-

RID: Real-time Inter-network Defense

- Information exchange among AS, mainly for traceback purpose.
 - Traceback of DoS traffic, with spoofed IP source address
 - Inter-AS information exchange required
 - “in time” manner is highly required.
 - Automatic response.
 - MIT group are working on this issue, so far.
 - RID
 - Various opinions and visions, still in discussion...
-

Summary: more engineering required

- Still human resource is not enough in this area.
 - Computer Security, Network Security, Incident response, ...
 - Internet and computer networks have turned to be a dependable infrastructure
 - We need more reality on security management
 - In every phase of cyber security components
 - CSIRT is one of vital components
 - More performance, more cost-effective ways in CSIRT
 - IODEF is one of the good example.
 - More engineering needed.
-