International Cooperation within Asia Pacific

Regional Initiative within Asia Pacific

Yurie Ito
JPCERT/CC
Topics

1. International Collaboration amongst CSIRT in Asia Pacific

2. About APCERT

3. The need to raise security awareness from other communities
International Collaboration among CSIRTs in Asia Pacific
Alliance among CSIRT (1)

Significant direct communication between CSIRTs in AP

• Incident Handling
  – Contact victims and involved sites via POC CSIRT
  – Sharing observations and statistics data

• Wide-spooling Incident Handling
  – Reporting network traffic flow, updating local activities
  – Sharing technical information and vendor’s notes
Case Study: Blaster worm

- 2003, August 12th --

- Constant overviews of network traffic levels in other countries.
- Reports of damage severity.
- Contact staff available through the night with the object of sharing data.
- Real time sharing of technical information.
- Identifying each of the effective DDoS counter measures within the member countries.
- Need to share Japan’s local situation: National summer holiday last week; the expectation of increased naïve internet access this week.
And what happened?

- 14th August: Coordinate the information exchange scenario with CSIRT at AP
- 15th August
  Afternoon: discussion with security vendors and ISPs (SECOND)
  17:00pm: Press Release to advice filter the packet to windowsupdate.com
  20:00pm: reverse engineering result released: Blaster starts DDoS attack only after
  system is rebooted after 00am.
  22:00pm: windowsupdate.com is missing from A record
  22:00pm - ISPs, security vendors start worrying DNS server would down because of
  the huge query packet sent by Blaster to look for the missing site.
  22:30pm: Information shared at SECOND the Blaster is programmed to try once –
  send 2 queries – and stops.
  22:45pm: Shared the information with CSIRT at AP and confirmed we have about
  same view – get back to SECOND – for specially ISPs
  22:45pm: Assumed the big DDoS threat was gone – and DNS server would be safe
  23:00pm: 00:00am at Australia time
  23:15pm: 00:15am at Australia time: Telephone call with AusCERT to see if they are
  Okay.
  23:45pm: 00:45am at Australia time: Telephone call with the AusCERT to share
  their traffic monitoring data. There was no high increase of traffic on DNS Server.
  Pretty confidence that there would be no too crazy things happening.
  00:00am(16th): traffic been same, watch the traffic with ISPs
  01:00am: Share the information with APCERT
Alliance among CSIRT (2)

- Development of regional forum
  - Internet is a dependable infrastructure for regional economic activities.
  - More demand to work together with the other CSIRT in the region.
  - Demand to raise security awareness, and CERT activity level.
  - Asia Pacific region’s unique demand.
About APCERT

Asia & Pacific Computer Emergency Response Team
History

- APNG formed WG in 1997
  - APNG Security and Incident Response Coordination, APSIRC
  - Jointly kicked off by CERTCC-KR, SingCERT and JPCERT/CC
  - Providing communication switchboard for established CSIRT
    - POC list
  - Encourage economies to build its own CSIRT
    - Jump start kit for CSIRT
    - Its conference
      - [http://apng.net.edu.cn/archive/wg&bof/apng-apsirc/](http://apng.net.edu.cn/archive/wg&bof/apng-apsirc/)

- APSIRC 2002
  - Organized by JPCERT/CC
  - Held in March 2002
  - Invited CSIRTs in AP, CERT/CC, FIRST representative, ...
  - Agreement on developing a regional forum of CSIRT
    - APCERT

- APSIRC 2003
  - APCERT was officially established
  - Held in February 2003 at Taipei
Objectives

- Security information-sharing among APCERT members
- To handle security issues on a regional basis
- Support establishment of CSIRT’s in other countries
- Collaborate with the other regional frameworks
Definition of Asia Pacific

APNIC’s Geographic boundaries
# APCERT Full Members

<table>
<thead>
<tr>
<th>APCERT</th>
<th>Description</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>AusCERT</td>
<td>Australian Computer Emergency Response Team</td>
<td>Australia</td>
</tr>
<tr>
<td>BKIS</td>
<td>Bach Khoa Internetwork Security Center</td>
<td>Vietnam</td>
</tr>
<tr>
<td>CCERT</td>
<td>CERNET Computer Emergency Response Team</td>
<td>Republic of China</td>
</tr>
<tr>
<td>CERTCC-KR</td>
<td>Computer Emergency Response Team Coordination Center-Korea</td>
<td>Korea</td>
</tr>
<tr>
<td>CNCERT/CC</td>
<td>China Computer Emergency Response Team Coordination Center</td>
<td>Republic of China</td>
</tr>
<tr>
<td>HKCERT/CC</td>
<td>Hong Kong Computer Emergency Response Team Coordination Center</td>
<td>Hong Kong, China</td>
</tr>
<tr>
<td>IDCERT</td>
<td>Indonesia Computer Emergency Response Team</td>
<td>Indonesia</td>
</tr>
<tr>
<td>JPCERT/CC</td>
<td>Japan Computer Emergency Response Team / Coordination Center</td>
<td>Japan</td>
</tr>
<tr>
<td>MYCERT</td>
<td>Malaysian Computer Emergency Response Team</td>
<td>Malaysia</td>
</tr>
<tr>
<td>PH-CERT</td>
<td>Philippine Computer Emergency Response Teams</td>
<td>Philippine</td>
</tr>
<tr>
<td>SecurityMap.Net CERT</td>
<td>Securitymap Networks Computer Emergency Response Center</td>
<td>Korea</td>
</tr>
<tr>
<td>SingCERT</td>
<td>Singapore Computer Emergency Response Team</td>
<td>Singapore</td>
</tr>
<tr>
<td>ThaiCERT</td>
<td>Thai Computer Emergency Response Team</td>
<td>Thailand</td>
</tr>
<tr>
<td>TWCERT</td>
<td>Taiwan Computer Emergency Response Team / Coordination Center</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>TW-CIRC</td>
<td>Taiwan Computer Incident Response Coordination Center</td>
<td>Chinese Taipei</td>
</tr>
</tbody>
</table>
Secretariat, SC members

- SC members (7 teams elected from the Full members)
  - AusCERT, JPCERT/CC, CNCERT, CERTCC-KR, MyCERT, HKCERT, SingCERT

- Secretariat: JPCERT/CC (with the CERTCC-KR support)
  - Organize the conferences
  - Web site, ML management
Activities

- **APSIRC - APCERT’s Annual Conference (Annual General Meeting)**
  - APSIRC 2004, 21, Feb, 2004 at KL, Malaysia
  - Joint organize with APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies)

- **SC meeting**
  - Telephone conference once every 3 months, Meeting once a half year

- **Working Group Activities**
  - **Accreditation WG**
    - to develop the accreditation rule for the APCERT membership
    - JPCERT/CC(Chair), AusCERT, CERTCC-KR, MyCERT, and HKCERT
  - **Training & Communication WG**
    - to discuss a training mechanism within APCERT (information exchange, CSIRT training)
    - TWCERT(Chair), AusCERT, SingCERT, MyCERT, JPCERT/CC, and CERTCC-KR
  - **Finance WG**
    - to discuss the membership fee in the short run, also develop the concrete scheme in the long run.
    - JPCERT/CC(Chair), TWCERT, AusCERT, HKCERT, CERTCC-KR, and TWCIRC
Communication

Technology within APCERT

Jungu Kang /CERTCC-KR

Jgkang@certcc.or.kr
Contents

1. APCERT Encrypted Mailing List
2. Web Site with Authentication for Sharing of Contact Information
1. The List has a PGP key assigned to it

2. Each subscriber provides their own PGP public key to the list administrator

3. To send email to the list, each subscriber encrypts the email with the list’s PGP key and then sends the email to the list server.

4. The list server decrypts the email and then re-encrypts it with each person’s individual PGP key and re-sends it
1. This makes it easier than using a shared passphrase

2. The list server can also be configured to reject messages if they are not PGP signed or if they are not PGP encrypted

3. It can also be used to authenticate messages to the list

4. Everyone should sign all their email to the list with PGP, which is a little more effort
1. APCERT is planning to provide https web page with authentication for sharing of contact information

2. This technology is very standard and basic
Cooperation with the other regional framework

• Existing regional framework
  – FIRST, TF-CERT, EGC
  – Will be launched soon?: North America, Latin

• Why Regional framework?
  – Time difference
  – IP address block

• How do we efficiently communicate?
  – Encrypted ML system
  – Contribution to IODEF standardization
Demand from other communities
Regional WG in intergovernmental coordination framework

- ASEAN’s e-security WG
- APEC/TEL e-security WG
- E-government initiatives in each economy
- ….
Work Together

- Harmonization
- Players are different in each segment.
  - Government, CSIRT, Law Enforcement, …
- Encourage them to have conversations and cooperation
  - Mutual trust, information-sharing
Contact

- Reference web site
  - APCERT   http://www.apcert.org
  - JPCERT/CC  http://www.jpcert.or.jp

- Contact to:
  - APCERT Secretariat   (apcert-sec@apcert.org)
  - Yurie Ito  (office@jpcert.or.jp)
    - Tel  +81-3-3518-4600