APCERT Activities

Asia Pacific Computer Emergency Response Team

Jinhyun Cho
KrCERT/CC

Deputy Chair/ SC member of APCERT

AP* Retreat Busan Meeting
2nd September 2011

Copyright © 2011 APCERT

About APCERT

- **A**sia **P**acific **C**omputer **E**mergency **R**esponse **T**eam
  http://www.apcert.org

  - Forum of CSIRTs in the Asia Pacific region
  - Established in February 2003
  - Annual Events
    1. APCERT AGM & Conference
       - Exchange security trends & challenges
       - Local outreach and awareness raising for government & critical entities
    2. APCERT Drill (Simulation exercise of cyber attacks)
       - Communication checks based on given scenario
       - In conjunction with local exercise(s)
  - APCERT Annual Report
    http://www.apcert.org/documents/index.html
    - Released every spring
    - Includes APCERT team reports on incident trends, statistics, new projects, and more

Copyright © 2011 APCERT

APCERT New Vision Statement

-What can we do more for global commons? -

APCERT will work to help create a Safe, Clean and Reliable cyber space in the Asia Pacific Region through global collaboration.

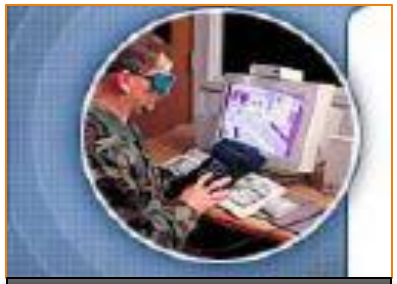
Copyright © 2011 APCERT

Objectives

- Encourage and support **regional and international cooperation** on information security in the Asia Pacific region;
- Jointly develop measures to deal with **large-scale or regional network security incidents;**
- Facilitate **info sharing and technology exchange,** including info security, computer virus and malicious code, among its members;
- Promote **collaborative research and development** on subjects of interest to its members;

Network Security Cooperation

- **Assist other CSIRTs in the region** to conduct efficient and effective computer security emergency response capability;
- **Provide inputs and/or recommendations** to help address legal issues related to info security and emergency response capabilities across regional boundaries;



Emergency Response

- Organize and conduct an **annual conference** to raise awareness on computer security incident responses and trends.

Computer Security Awareness

Copyright © 2011 APCERT

APCERT Member Teams

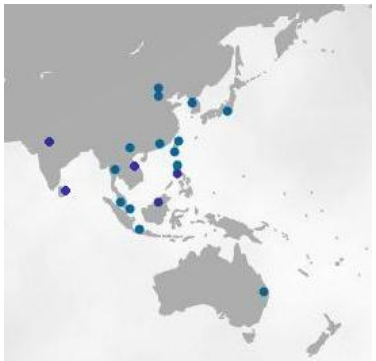
27 Teams/18 Economies, as of September 2011
(Started from 15 Teams/12 Economies)

Full Members (19)

- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **BruCERT** – *Negara Brunei Darussalam*
- **CCERT** – *People's Republic of China*
- **CERT-In** – *India*
- **CNCERT/CC** – *People's Republic of China*
- **HKCERT/CC** – *Hong Kong, China*
- **IDCERT** – *Indonesia*
- **ID-SIRTII** – *Indonesia*
- **JPCERT/CC** – *Japan* -> Chair / Secretariat
- **KrCERT/CC** – *Korea* -> Deputy Chair
- **MyCERT** – *Malaysia*
- **PHCERT** – *Philippine*
- **SingCERT** – *Singapore*
- **SLCERT** – *Sri Lanka*
- **ThaiCERT** – *Thailand*
- **TWCERT/CC** –*Chinese Taipei*
- **TWNCERT** – *Chinese Taipei*
- **VNCERT** – *Vietnam*

General Members (8)

- **BDCERT –** *Bangladesh*
- **BP DSIRT –** *Singapore*
- **CERT Australia –** *Australia*
- **GCSIRT** – *Philippines*
- **MOCERT –** *Macau*
- **MonCIRT –** *Mongolia*
- **NUSCERT –** *Singapore*
- **TechCERT –** *Sri Lanka*



Copyright © 2011 APCERT

How does APCERT work?

- **CSIRT (Computer Security Incident Response Team)**
  - Independent from politics, industry, market
  - Do not focus on WHO (attribute) and WHY (motivation)
  - Focus on details of what is actually occurring, how to stop the incident, how to prevent it, from a technical coordination perspective

- **CSIRT Common Policy**
  - MY security depends on YOUR security and vice versa
  - Web of trust – CSIRT trust relationship is developed based on a long time operational collaborative relationship

- **Systematic Handling – with repeatable procedure, PoC agreement**
  - Timely manner
  - Each team has appropriate domestic contacts to handle / respond to incidents (ISPs, critical infrastructure, government…)
  - Reaching to disconnected areas using CSIRT network, wherever that may be CSIRT

Copyright © 2011 APCERT

Consistent efforts

- **Developed close collaborative relationship (Bridge the gap)**
  - Regular face to face meetings among teams (Develop trust)
  - Developing long time tactical strategies addressing cyber related incidents
    - Training / Education / Awareness program
  - Regular communication on not only incident information but also trends, projects, etc.
  - Site visiting from time to time, organizing gatherings
- **POC arrangement between members**
  - 24 hour / 7 days a week Hotline
  - Encrypted communication tool
- **Practice - Incident Handling Drill**
  - Drills have been organized by APCERT members since 2005
  - ASEAN CERT Incident Drill (ACID) since 2006

Copyright © 2011 APCERT

Outreach to regional communities

- One important role of APCERT is education and training to raise awareness and encourage best practice.
  - APCERT members provide CSIRT trainings and outreach programs to newcomer economies
- Cross regional collaboration
  - FIRST: International CSIRT community
  - TF-CSIRT (TERENA's Task Force of Computer Security Incident Response Teams): European Counterpart of APCERT

Copyright © 2011 APCERT

APCERT Annual Events (2011)

- **APCERT Drill 2011**
  Date: 22 February 2011
  Participating Teams: 20 teams from 15 economies

- **APCERT AGM& Conference 2011**
  23rd-24th March 2011 in Jeju Island, Korea
  Hosted by KrCERT/CC

23 March (AM)	APCERT Annual General Meeting (AGM) Annual activity reports, future plans, new members, election
23 March (PM)	APCERT Conference (Closed for APCERT members & invited guests only)
24 March (All day)	APCERT Conference (Open to public)

New Chair <Term: 1 year> : Ms. Yurie Ito (JPCERT/CC)
New Deputy Chair <Term: 1 year> : Mr. Jinhyun Cho (KrCERT/CC)

- **APCERT Workshop 2011 on TSUBAME Network Traffic Monitoring Project**

25 March (AM)	(Closed for TSUBAME project members only)

Copyright © 2011 APCERT

Copyright © 2011 APCERT

APCERT Annual Events (2012)

- **APCERT Drill**
  February 2012

- **APCERT AGM& Conference 2012**
  March 2012 in Bali, Indonesia
  Hosted by ID-SIRTII

Please find information on the APCERT website (http://www.apcert.org)

Copyright © 2011 APCERT

Thank you

APCERT General Contact:
apcert-sec@apcert.org

APCERT Website:
http://www.apcert.org

Copyright © 2011 APCERT