APCERT Activity Update

Yurie Ito
JPCERT/CC
(On behalf of the APCERT Secretariat)

Introduction

- **APCERT** *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CSIRTs *(Computer Security Incident Response Teams)*. The organization was established to encourage and support the activity of CSIRTs in the Asia Pacific region.

Membership

- The geographical boundary of APCERT activity is the same as that of APNIC. It comprises 62 economies in the Asia and Pacific region.
  http://www.apnic.net/info/reference/lookup_codes_text.html
- 2 levels of membership
  - Full membership
  - General membership
- Membership opens to all CSIRTs being existing in AP region
- Current members: 15 teams from 12 economies

2003’ Activities

- **Representation to other Regional and International Bodies**
  - TF-CSIRT
  - EGC
  - FIRST
  - APEC-TEL
  - APNIC

2003’ Events

- APSIRC 2003
  - Was held in conjunction with APRICOT conference, hosted by TWCERT/CC and TWSIRC in Taipei
- APSIRC 2004
  - Was held in conjunction with APRICOT conference, hosted by MyCERT in KL
- APCERT Information Day
  - Organized in conjunction with the FIRST Technical Colloquium (TC) and hosted by JPCERT/CC in Tokyo
- APSIRC 2005
  - Will be holding in conjunction with APRICOT conference, will be hosted by JPCERT/CC in Kyoto, Japan, February 2005.

Outcomes 2003

Accreditation Scheme

- Accreditation scheme was accepted by the APCERT members at APSIRC 2004 Malaysia meeting.
  - APCERT Member Requirements
  - APCERT Application Form
  - SC and Sponsor's Check List
- Team Mission Criteria
  - 1. Teams must do Incident Response or Security Research within Asia Pacific Area (APNIC boundary)
  - 2. Teams must make a contribution to security community in Asia Pacific region.

Application Process

(1) General member:

1. Submit an application form to secretariat
2. Secretariat send an application to SC
3. SC member review the application form for a week and if no objection - acceptance

(2) Full member:

1. Submit an application form to secretariat
2. Secretariat send an application to SC
3. SC votes for the general member
4. Candidate decide to upgrade the membership
5. Candidate submit an application form to secretariat
6. Candidate or SC assign a sponsor team from the full members for the candidate
7. Candidate goes though Sponsor Process to upgrade the membership
8. SC member vote for the Full member after the process – 2/3 majority

Uniqueness (Accreditation for the Full membership)

Check Items for a Sponsor and SC (for vote)

1. Relevance of organization's services to the security field

i.e. Services such as IRT, Security Consulting, Security Research
i.e. Staff skill-set requirements for each service
[ ] Check all the items of service and skill-set on the application form to insure the APCERT requirements.

2. Contribution to the APCERT community/Expectation of the applicant team

- What is the team's Focus, Mission, number of Resources.
- Expectation of ROI from joining APCERT

[ ] Check all the items of Mission statement of the application form to insure the APCERT requirements.
[ ] Check the team's track record
i.e. to see how many times does the team attends conferences?
i.e. How many times the teams give presentations?
[ ] What is their main contribution to the security committee?
( ) Writing papers
( ) documents
( ) developing security tools
( ) public announcements (alerts, advisories)
( ) holding a workshop if its own?
[ ] Get a list of the team's expectation of APCERT

Uniqueness Cont’
(Accreditation for the Full membership)

3. Trust

- APCERT should clarify its policy with regards to;

[ ] Check the security policy how to handle the sensitive information.

( ) How is incoming information tagged or classified?

( ) How is information handled, especially with regards to exclusively?

( ) What considerations are adopted for the disclosure of information, especially incident related information passed on to other teams or to sites?

( ) Are there legal considerations to take into account with regards to the information handling?

( ) Policy on use of cryptography to shield exclusivity & integrity in archives and/or in data communication, specially email.

[ ] Check track record of working relationship with other teams.

[ ] Is the response quick? How many days it take to get the reply from them?

( ) Quick ( ) Reasonable ( ) Slow

[ ] Check the applicant’s policies on:

( ) Type of incidents and level of support

( ) Co-operation, interaction and disclosure of information

( ) Communication and authentication

Future Plan:

- **Integrate/standardize CSIRT accreditation globally. (Trusted Introducer, FIRST Sponsorship scheme, APCERT accreditation, etc)**
- **Send liaison member to FIRST accreditation WG.**

Outreach to multiple sectors

- One important role of APCERT is education and training to raise awareness and encourage best practice.
  - APEC-TEL: APCERT provided the recommendation/ advice to AP region intergovernmental initiative as security experts group in AP
  - ASEAN: APCERT members provide CSIRT training and Outreach program to newcomer economies
  - Future Plan: Support standard CSIRT training material, add regional modules on top of the core material.
    - Transit program – from EU

Traffic Data Share Project in AP

- Traffic monitoring Workshop at APSIRC 2004 at KL.
  - For the accuracy of the internet traffic trend – sharing traffic monitoring data within wide region is useful.
  - For the accurate analysis of internet trend, sharing analysis methodology, techniques is useful.
- Kicked off Traffic monitoring data share WG – two projects will be planned to expand to APCERT members.
  - IODEF
  - Portal site
- Early warning scheme within the APCERT scheme

Thank you.

- apcert-sec@apcert.org
- http://www.apcert.org

- Yurie Ito (office@jpcert.or.jp)
- Tel: 81-3-3518-4600