Asia-Pacific
Economic Cooperation

# APEC Project TEL01/2006 – Strengthening Effective Response Capabilities among APEC Member Economies - Final Report

Security and Prosperity Steering Group
APEC Telecommunications and Information Working Group

May 2008

# APEC Project TEL01/2006 – Strengthening Effective Response Capabilities among APEC Member Economies - Final Report

Security and Prosperity Steering Group
APEC Telecommunications and Information Working Group

Published by KrCERT/CC
May 2008

Prepared by
KrCERT/CC
Korea Information Security Agency
West 4F, 135 Jungdaero, Songpa-gu, Seoul,
Korea 138-950
Tel: +82 2 405 5138, +82 2 405 5424
Fax: +82 2 405 5129
Email: cert@krcert.or.kr
Website: http://www.krcert.or.kr

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6891 9600 Fax: (65) 6891 9690
Email: info@apec.org
Website: www.apec.org

APEC publication number: APEC#208-TC-01.1

# Contents

## *Executive Summary*

While Internet environment is growing fast in our planet, the cyber attack threatening our daily life also has been growing in commercial and economical perspective. Those attacks are becoming more sophisticated and complicated as the trend of motivation evolves to financial gain, so that more organized criminal activities are discovered in those attacks. Hence, every single attack can be involved with multiple stakeholders and economies. No superb organization alone can resolve those flooding incidents.

This trend is consistently demanding the need of cooperation among the stakeholders and multiple economies. However, the difficulties lies in digital divide, gaps existed in incident response capability, and etc. We grant a thoughtful meaning to the solutions if one can develop a type of indicator that can be referenced to narrow down those difficulties.

Considering the characteristic of cyber attack and the environment of many Internet incident response systems, focusing on cross-border cooperation is inevitable. Also, whether bilateral or multilateral, the cooperation should begin with learning the activities from the counterparts.

As the deliverables of the project, we developed an "APEC COOPERATIVE RESPONSE GUIDELINES IN CROSS-BORDER ENVIRONMENT", and a "Best Practice for cooperative response based on public and private partnership", and hosted a training course mainly for Computer Security Incident Response Team (CSIRT) staff who are working on response for cyber attacks in their daily life. The deliverables are produced separately with this final report as they are complete documents for each one, the guideline and the best practice, except brief description of the result of the training course which is included in this report. The brief summary or background of each deliverables not attached here inline is as follows.

### *APEC COOPERATIVE RESPONSE GUIDELINES IN CROSS-BORDER ENVIRONMENT*

The guideline is developed to assist APEC economies to strengthen cooperative incident response capabilities. The recognition of incident response capabilities among APEC is common to safeguard the prosperity of knowledge based economies. Many APEC declarations, statements and strategies have emphasized APEC economies to establish organizational incident response capabilities such as CSIRT, and cybercrime unit.

The guideline covers key cooperation issues of computer emergency or security incident response in cross-border environment. APEC economies need to give higher priority or special attention to incident response capability building to make their own infrastructures as well as those of other APEC economies secure. Trans-border characteristics of cyber attacks in cyber space call for regional and global cooperative response framework. The gap in incident response capabilities should be narrowed to ensure cyber security among all APEC economies.

### ***Best Practice for cooperative response based on public and private partnership***

The best practice mainly focuses on the system models, herein introduced, that can possibly be adopted by CSIRTs, including the national level CSIRT who acts as an overall coordinator for nation-wide major incidents and/or the CSIRT that has a relatively large scale of constituency, to mitigate malicious network activities in Internet involving various malware such as a bot, which is commonly recognized by security experts as a challenge to mitigate or overcome, therefore the introduced models herein can provide efficient and proactive ways to take action and response against those malicious activities, within the perspective of public and private partnership. This best practice also introduces the recent trends of APEC member economies who participated in the training course for building up and operation of CSIRT, including their activities and efforts to mitigate the Internet threats they face and as part of a best practice initiative.

The purpose of the best practice is to contribute to the APEC member economies by providing system models that can bring ideas of what type of scheme could be better for their environment of Internet threat regarding the circumstances and issues that may reside at the moment.

# *Introduction*

## *Background*

The project "Strengthening Effective Response Capabilities among APEC Economies" is for each APEC economy, including the developing economy, to have its own response capabilities for the Internet incidents. After many member economies began recognizing the importance and needs of CERT[1]/CSIRT[2], some of APEC member economies, including the developing economies, are promoting the establishment of CERT/CSIRT. Many economies do not have the capabilities of helping other CERTs' establishment and management.

To assist the APEC economies building the response capabilities, the project will provide the training course and develop guideline and best practice. The short-term training course is offered for other CERTs in APEC economies to have the opportunity to learn the methods and issues which should be considered during the establishment and management of a new CERT. The objective of the short-term training course is for the participants to have the capabilities to train other Information Technology or Information Security staffs for the establishment and management of CERT from the business and technology perspectives. The cooperative response guidelines in cross-border environment will be the referential material for international incident handling for major cyber incidents. Although most of CERTs have the internal process for the local incident handling, most of CERTs may not have any standardized process or referential material for cross-border or international incident handling. The previous experience of international incident handling drill will be the basis of the guidelines and the guideline will be drafted and revised with the discussion with CERTs in Asia Pacific Region. The best practices for cooperative response based on public and private partnership will be another referential material for developing the local response system, including network operators.

The project is partially funded by the Operational Account of the APEC Central Fund. The short-term training course is being organized by KrCERT/CC[3], a division of KISA[4], with the cooperation from FIRST[5] and TERENA[6] which provides the certified trainers for courses and training materials. This best practice is developed by the KrCERT/CC with the help from the staff who can advise and review of the content in the technical and non-technical perspectives.

## *Purpose of Project*

The main objectives of this project are to enhance the APEC economies' response capabilities. From the local perspectives, promoting the establishment of CERT and the

[1] Computer Emergency Response Team, an organization dealing with Internet security
[2] Computer Security Incident Response Team, generic term of CERT
[3] Korea Computer Emergency Response Team / Coordination Center
[4] Korea Information Security Agency
[5] Forum of Incident Response and Security Teams
[6] Trans-European Research and Education Networking Association

cooperation among the stakeholders such as ISPs[7], MSSPs[8] and vendors is the key factor. As well from the international perspective, the cooperation among cross-border CERTs would be the key factor.

All these activities can be integrated into one of APEC-TEL efforts on information security to make knowledge-based economies prosper. This project will contribute to make APEC economies secure by promoting CERT building and the cross-border CERT cooperation.

## Project Delivery

### Project Methodology

The execution of the project was conducted with three sequential components.

*Stage 1 – Preparation of the training course*
Utilize updated TERENA's CSIRT training materials, existing materials from the experts in KISA in diverse areas, and the results from the questionnaire pre-distributed to the participants.

*Stage 2 – Delivery of the training course*
Provide a training course to participants from China, Thailand, Viet Nam, Malaysia, Myanmar, New Zealand, Singapore, Laos, Philippines, Hong Kong, Brunei, Japan, and Mexico. The training was conducted in Seoul, Korea, on 18-22 September 2006. Within 5-day course, 3-day class focused on CSIRT building and operation, 1-day for introducing diverse security applications applied by KISA, and 1-day for sharing up-to-date information from the participants about their economies' Internet and its threat trends.

*Stage 3 – Writing out the guideline and the best practice*
Write out the guideline and the best practice based on the experience of the KrCERT/CC and the information sharing among the participants of the fore-executed training course.

[7] Internet Service Provider
[8] Managed Security Service Provider

## Provision of Training

On 18-22 September 2006, five-day training course, developed by KrCERT/CC, KISA, was delivered for technical staff of computer security incident handling, and the management staff or the government officials who is charged of overseeing a CSIRT or establishing a CSIRT in their economies, those for developing countries or countries in the stage of establishing a national CSIRT.

The training course is composed of three-days of FIRST/TRANSITS training course, one-day introduction to information security activities of Korea, and one-day economy update session and a site visit to KrCERT/CC.

Trainers certified by the FIRST education committee were invited to guarantee the quality of the course, for delivering proper lecture and hands-on exercise. Most of the lecture has fulfilled the requirement of the TRANSITS course, as well as hands-on class was developed by the trainers to pursue the participants' need for their experience for establishing and operating a CSIRT.

The objective of this training course was to provide participants with basic skills required to establish and operate a CSIRT and experience of experts who are working in the field including the Korean case.

As below, "2006 APEC Security Training Course List", provides mandatory topics covered in the course with the TRANSITS material and exercises provided, additional presentations provided by the experts from Korea Information Security Agency on their activities with tutorial subject which is not described here in detail.

### 2006 APEC Security Training Course List

- Introduction of Korea Information Security Agency
- Common Criteria
- Personal Information Protection
- Public Key Infrastructure
- Site Visit to KrCERT/CC
- Economy Update & Discussion (all participants)
- Introduction of TRANSITS & Discussions
- TRANSITS - Organizational Module
- TRANSITS - Operational Module
- TRANSITS - Legal Module
- TRANSITS - Business Module Exercise - Role plays (Group Basis)
- TRANSITS - Technical Module
- TRANSITS - Operational Module
- TRANSITS - Technical Module
- TRANSITS - Vulnerability Module
- TRANSITS - Technical Module Exercise - Log Analysis

## *Survey Findings*

Each participant was advised to complete and return a questionnaire and an evaluation form. The questionnaire was made by KrCERT/CC, and distributed to all participant economies before the course begins, to help to understand their cyber security environments and trends, and to share among all participants in economy update and discussion session, as the subjects are as follows:

- ✓ Internet Usage Statistics
- ✓ National Policy and Law on Information Security
- ✓ CERT Services and Statistics on malicious activities
- ✓ Information on your constituency

Consolidated questionnaires were used to incorporate the international field report as the annex of the 'Best Practice for cooperative response based on public and private partnership', which has been produced as one of the deliverables of this project.

Besides, an evaluation form to assess the course was also completed by each participant after the course, as the questions included the following:

(a) How have you or your economy benefited from the project?
(b) What new skills, knowledge, or value have you gained?
(c) What, if any, changes do you plan to pursue in your home economy as a result of the project?
(d) What needs to be done next? How should the project be built upon?
(e) Is there any plan to link the project's outcomes to subsequent collective action by fora or individual actions by economies?
(f) What is your assessment of the overall effectiveness of the project?
(g) Please provide any additional comments. How to improve the project, if any.

The most of the results replied by the participants illustrated that the course was an appropriate level and correspondent with the need of participants in the content and the delivery by the instructors and presenters.

All participants, including instructors and trainees, agreed that the first two days session regarding Korean activities and economy update before getting into the 3 days session of TRANSITS was helpful to get familiar and understand each other. A good and fruitful discussion was on place regarding all aspects showed on the course.

However, some have language barriers that their native language is not English, but which was not the reason of discouraging for participation.

Participants were satisfied with the overall content. Operational module was the most preferred session by the trainees as it included a role playing program with a certain scenario that they could actively participated in and even they wanted more time for that and more hands-on class.

TEL01/2006

Prepared by
KrCERT/CC
Korea Information Security Agency
West 4F, 135 Jungdaero, Songpa-gu, Seoul,
Korea 138-950
Tel: +82 2 405 5138, +82 2 405 5424
Fax: +82 2 405 5129
Email: cert@krcert.or.kr
Website: http://www.krcert.or.kr

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6891 9600 Fax: (65) 6891 9690
Email: info@apec.org
Website: www.apec.org

APEC publication number: APEC#208-TC-01.1