Industry Connections Security Group (ICSG)
Industry Connections Activity Initiation Document (ICAID)
Version: 3.0, 31 May 2016
IC09-001-05 Approved by the IEEE-SASB 30 June 2016

Instructions

- Instructions on how to fill out this form are shown in red. It is recommended to leave the instructions in the final document and simply add the requested information where indicated.
- Shaded Text indicates a placeholder that should be replaced with information specific to this ICAID, and the shading removed.
- Completed forms, in Word format, or any questions should be sent to the IEEE Standards Association (IEEE-SA) Industry Connections Committee (ICCom) Administrator at the following address: industryconnections@ieee.org.
- The version number above, along with the date, may be used by the submitter to distinguish successive updates of this document. A separate, unique Industry Connections (IC) Activity Number will be assigned when the document is submitted to the ICCom Administrator.

1. Contact

Provide the name and contact information of the primary contact person for this IC activity. Affiliation is any entity that provides the person financial or other substantive support, for which the person may feel an obligation. If necessary, a second/alternate contact person's information may also be provided.

Name: Mark Kennedy
Email Address: mkennedy@symantec.com
Phone: 424-750-7661
Employer: Symantec
Affiliation: Symantec

2. Type of Activity

Specify whether this activity will be entity-based (participants are entities, which may have multiple representatives, one-entity-one-vote), or individual-based (participants represent themselves, one-person-one-vote).

Entity-Based

3. Purpose

3.1. Motivation and Goal

Briefly explain the context and motivation for starting this IC activity, and the overall purpose or goal to be accomplished.

Industry Connections Security Group (ICSG) is a global group of computer security entities that have come together to pool experience and resources in combating the systematic and rapid rise in computer security threats.

In the past few years, attackers have shifted away from mass distribution of a small number of threats to micro distribution of millions of distinct threats. ICSG was established, under the umbrella of the IEEE-SA Industry Connections program, out of the desire by many in the security industry to more efficiently address these growing threats in a coordinated fashion. While there has been some ad-hoc co-operation in the industry in areas such as malware and phish URL sharing, this co-operation has not been standardized or documented in a format that lends itself to systematic improvement in operational efficiency, or visibility and review by people outside the vertical industries.

The charter of ICSG focuses its activities as follows:

- Providing a forum for discussions related to the sharing of computer security information and best practices.
- Developing, documenting and promoting proposals for computer security information sharing formats, best practices and computer security industry guides. The resulting documents may subsequently be submitted for broader formal review and dissemination as IEEE-SA publications, or submitted for formal standardization using the open processes of the IEEE-SA.
- Creating a roadmap of planned deliverables related to computer security, and reviewing the business reasons and implications behind them.

Accomplishments

Several subgroups were created to develop solutions for security threats, including the:

- Malware Working Group,
- Anti-Malware Support Service Management Committee (AMSS MC),
- Malware Metadata Exchange Format Working Group, and
- Privilege Management Protocols Working Group

The Malware Working Group's aim is to solve some of the malware related issues the industry faces today. The initial focus was to establish more intelligent ways of sharing malware samples and the information associated with them in a way that makes the computer security industry more effective. The Malware WG developed the Anti-Malware Support Service (AMSS) to enable security companies and the industry as a whole to respond more effectively and efficiently to the rapidly mutating universe of contemporary malware threats.

The AMSS MC oversees the launch and operation of the AMSS.

AMSS is comprised of two services each with its own sub-management committee:

1. Clean-file Metadata eXchange (CMX) System

   The CMX System provides a capability for software providers to communicate metadata (file names, hashes, file and product version information) to a host of security providers prior to the files being released to the public. This allows those security providers to take measures to assure that those files will not cause False Positives when they are released.

2. Taggant System

   The Taggant System consists of several parts: a PKI infrastructure for the creation of end-user licenses, a library to calculate and place a Taggant into a file, a library to extract and validate a Taggant, and a blacklist to identify known bad end-user licenses.

The Malware Metadata Exchange Format (MMDEF) Working Group expanded the breadth of information able to be captured and shared about malware in a standardized fashion. New capabilities were added to the MMDEF schema, which is currently in use by Anti-virus (AV) vendors for the purpose of augmenting shared malware samples with additional metadata. These capabilities include the following:

- Attributes and metadata specific to the characterization of clean (benign) files. More information can be found in the MMDEF v1.2 schema annotations as well as the example instance files.
- Blackbox behavioral metadata, such as the type of information captured by dynamic malware analysis tools. More information can be found in the MMDEF-B README file.

The Privilege Management Protocols (PMP) WG was formed to develop protocols for the efficient authentication and the secure determination of "who can do what". The "who" is defined as a framework that uses public key based identities that enable authentication and key establishment. The authorization of "what" a device can do is based on management of the identity that can be authenticated, formed by hashing the public key. This approach has considerable advantages over shared key based systems that must maintain strict protection of the information that can be authenticated. The PMP WG was disbanded upon agreement by the ICSG Executive Committee that the ICSG was not the appropriate home for this work.

Current Activity

The active subgroups are the Encrypted Traffic Inspection Working Group (ETI WG) and the AMSS MC. The Malware Working Group has been suspended until needed to enhance AMSS.

The ETI WG is working to devise a solution to allow security companies to *securely* monitor SSL communications. It is intended to work with other existing entities to refine the solution and develop a proposal for a new standard.

3.2. Related Work

Provide a brief comparison of this activity to existing, related efforts or standards of which you are aware (industry associations, consortia, standardization activities, etc.).

The work of the ICSG AMSS dovetails with some of the work of the Anti-Malware Testing Standards Organization (AMTSO). The purpose of both groups is to cooperate to help solve common problems across the anti-malware industry.

3.3. Previously Published Material

Provide a list of any known previously published material intended for inclusion in the proposed deliverables of this activity.

None currently known.

3.4. Potential Markets Served

Indicate the main beneficiaries of this work, and what the potential impact might be.

The AMSS is now expanding its scope from simply anti-malware companies to include CERT's, government agencies, and larger corporations. Additionally, CMX will allow an avenue for smaller software companies to interact with the larger group.

4. Estimated Timeframe

Indicate approximately how long you expect this activity to operate to achieve its proposed results (e.g., time to completion of all deliverables).

Expected Completion Date: None; the AMSS is an ongoing operational service overseen by the ICSG.

IC activities are chartered for two years at a time. Activities are eligible for extension upon request and review by ICCom and the IEEE-SA Standards Board. Should an extension be required, please notify the ICCom Administrator prior to the two-year mark.

5. Proposed Deliverables

Outline the anticipated deliverables and output from this IC activity, such as documents, proposals for standards, conferences and workshops, databases, computer code, etc., and indicate the expected timeframe for each.

- Encrypted Traffic Working Group:
  - Develop a solution to secure monitor encrypted traffic
- Malware Working Group:

    - Enhance the Anti-Malware Support Service as needed to meet the needs of existing and new users
- AMSS Management Committee:
    - Continue to oversee the operation of the Anti-Malware Support Service

6. Funding Requirements

Outline any contracted services or other expenses that are currently anticipated, beyond the basic support services provided to all IC activities. Indicate how those funds are expected to be obtained (e.g., through participant fees, sponsorships, government or other grants, etc.). Activities needing substantial funding may require additional reviews and approvals beyond ICCom.

Symantec has been contracted to provide the PKI Management System for the AMSS Taggant System for the amount of approximately $20,000 per year.

IEEE-SA provides support for AMSS administration and operations and also provides secretariat services to the ICSG Executive Committee.

Avira has agreed to provide programming and physical hardware support for the CMX system free of charge in exchange for an AMSS Subscriber License.

Enigma Protector developed the AMSS Taggant System and is contracted as needed to revise the code.

Funds to cover these expenses will be obtained from AMSS Subscriber License fees.

7. Management and Procedures

7.1. IEEE Sponsoring Committee

Indicate whether an IEEE sponsoring committee of some form (e.g., an IEEE Standards Sponsor) has agreed to oversee this activity and its procedures.

Has an IEEE sponsoring committee agreed to oversee this activity?: No

If yes, indicate the sponsoring committee's name and its chair's contact information, and skip the remaining parts of this section (skip 7.2 and 7.3, below).

Sponsoring Committee Name: Committee Name
Chair's Name: Full Name
Chair's Email Address: who@where
Chair's Phone: Number, including country code

Additional sponsoring committee information, if any.

7.2. Activity Management

If no IEEE sponsoring committee has been identified in 7.1 above, indicate how this activity will manage itself on a day-to-day basis (e.g., executive committee, officers, etc).

ICSG is managed by an Executive Committee (EC) consisting of a minimum of 5 and a maximum of 15 of the ICSG members. The EC provides the strategic direction for the activity, manages the growth of participation, directs the development of all deliverables, and performs whatever additional functions are required to fulfill the purpose specified in the ICAID. Among the responsibilities of the EC are the following:

- Creating a roadmap of planned deliverables that specifies what is to be developed, when, and what will then be done with the results.
- Establishing Working Groups (WGs), as and when needed, to develop the planned deliverables.
- Recruiting additional ICSG members to participate in the WGs.
- Creating and revising as necessary the ICSG policies and procedures, for approval by the ICCom.
- Overseeing the activities of all WGs to ensure the agreed processes are followed.
- Reviewing and approving all draft documents and other deliverables produced by the WGs.

7.3. Procedures

Indicate what documented procedures will be used to guide the operations of this activity; either a) modified baseline *Industry Connections Activity Policies and Procedures,* or b) Sponsor or Working Group policies and procedures accepted by the IEEE-SA Standards Board. The chosen policies and procedures must be reviewed by ICCom

Computer Security Group (ICSG)
Industry Connections Activity Policies and Procedures
Version: 2.0, 15 December 2015

8. Participants

8.1. Stakeholder Communities

Indicate the stakeholder communities (the types of companies or other entities, or the different groups of individuals) that are expected to be interested in this IC activity, and will be invited to participate.

The membership of ICSG includes broad industry representation from companies that specialize or have a substantive portion of their business in computer security. As the activity grows, ICSG membership will be open to a wide variety of entities that have an active involvement and interest in computer security, including security vendors, industry content contributors (e.g. Banks, ISPs, etc.), educational institutions and governmental organizations.

8.2. Expected Number of Participants

Indicate the approximate number of entities (if entity-based) or individuals (if individual-based) expected to be actively involved in this activity.

Number of entities = approximately 25.

8.3. Initial Participants

Provide a list of the entities or individuals that will be participating from the outset. It is recommended there be at least three initial participants for an entity-based activity, or five initial participants (each with a different affiliation) for an individual-based activity.

Use the following table for an entity-based activity:

The 2016 Executive Committee Members are:

Entity	Primary Contact	Additional Representatives
ESET	Righard Zwienenberg righard.zwienenberg@eset.com +31-6-51303768	
Kaspersky	Alexander Liskin Alexander.Liskin@kaspersky.com +7 495 797 87 00 x1340	
Intel	Igor Muttik Igor.Muttik@Intel.com +441296617756	
Microsoft	Enrique Gonzalez enriqg@microsoft.com +35317063593	
Netfountain	Tony Lee tonydlee@live.com	
Symantec	Mark Kennedy mkennedy@symantec.com 424 750 7661	
Trend Micro	Jamz Yaneza Jamz_Yaneza@trendmicro.com 626 437 5340	