IEEE STANDARDS ASSOCIATION

IEEE

Clean File Metadata Exchange Overview

19 October 2015

IEEE | 3 Park Avenue | New York, NY 10016-5997 | USA

CLEAN FILE METADATA EXCHANGE: OVERVIEW

Thomas Wegele
Avira Operations GmbH & Co.

and

Mark Kennedy
Symantec

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

To order IEEE Press Publications, call 1-800-678-IEEE.
Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Notice and Disclaimer of Liability
Concerning the Use of IEEE-SA Industry Connections Documents

This IEEE Standards Association ("IEEE-SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE-SA Industry Connections activity that produced this Work. IEEE and the IEEE-SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE-SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE-SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE-SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE-SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the IEEE-SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

CONTENTS

1. INTRODUCTION 1

2. OVERVIEW 1

3. COMMITTEES 2

   3.1 Operations Committee 2
   3.2 Executive Committee 2

4. PROCESSES 2

   4.1 Joining the CMX system—Registration process 2
   4.2 Using the CMX system 3
   4.3 Access to the IEEE-CMX system 4
   4.4 Expulsion from the IEEE-CMX system 4

5. ADMINISTRATIVE SUPPORT BY IEEE 4

   5.1 Costs 4

6. REFERENCES 5

CLEAN FILE METADATA EXCHANGE: OVERVIEW

1. INTRODUCTION

This document provides an overview of the Clean File Metadata Exchange (CMX) system developed by the Avira Operations GmbH & Co. KG under the umbrella of IEEE. It also describes the processes related **to the operation and participation of the CMX.**

The CMX system is now offered as part of the IEEE Anti-Malware Support Services (AMSS): http://standards.ieee.org/develop/indconn/icsg/amss.html.

2. OVERVIEW

2.1 Background

The IEEE Malware Working Group works to solve some of the malware-related issues facing the industry today. The initial focus has been 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. This has resulted in the development of IEEE Malware Metadata XML Data Exchange Format (MMDEF). For details, see Clause 6.

CMX aims to provide timely information about clean files in the form of metadata. Initially, the metadata should be provided for three types of Windows files: executable files (PE), CAB files, and MSI files. The metadata extraction should be performed after the final version of the product is created and all digital signing is complete. This should be the procedure for all software that is released to the public.

Nightly builds and limited betas are not the best candidates because they will not reside on many machines. Public beta versions shall be included.

2.2 Purpose

This document describes the operation of the CMX collaboratively created under the umbrella of IEEE ICSG – the bodies, the processes, and the legal requirements related to participation, operation, and the usage of the system and its background.

3. COMMITTEES

3.1 Operations Committee

Operation of the IEEE CMX system is overseen by the Management Committee. This committee will handle issues of revocation of access (in the case of violation of the license agreement), approval of new subscribers, and any other type of dispute that may arise from the use of this system. The Management Committee is comprised of a chair, a vice chair, and several other members.

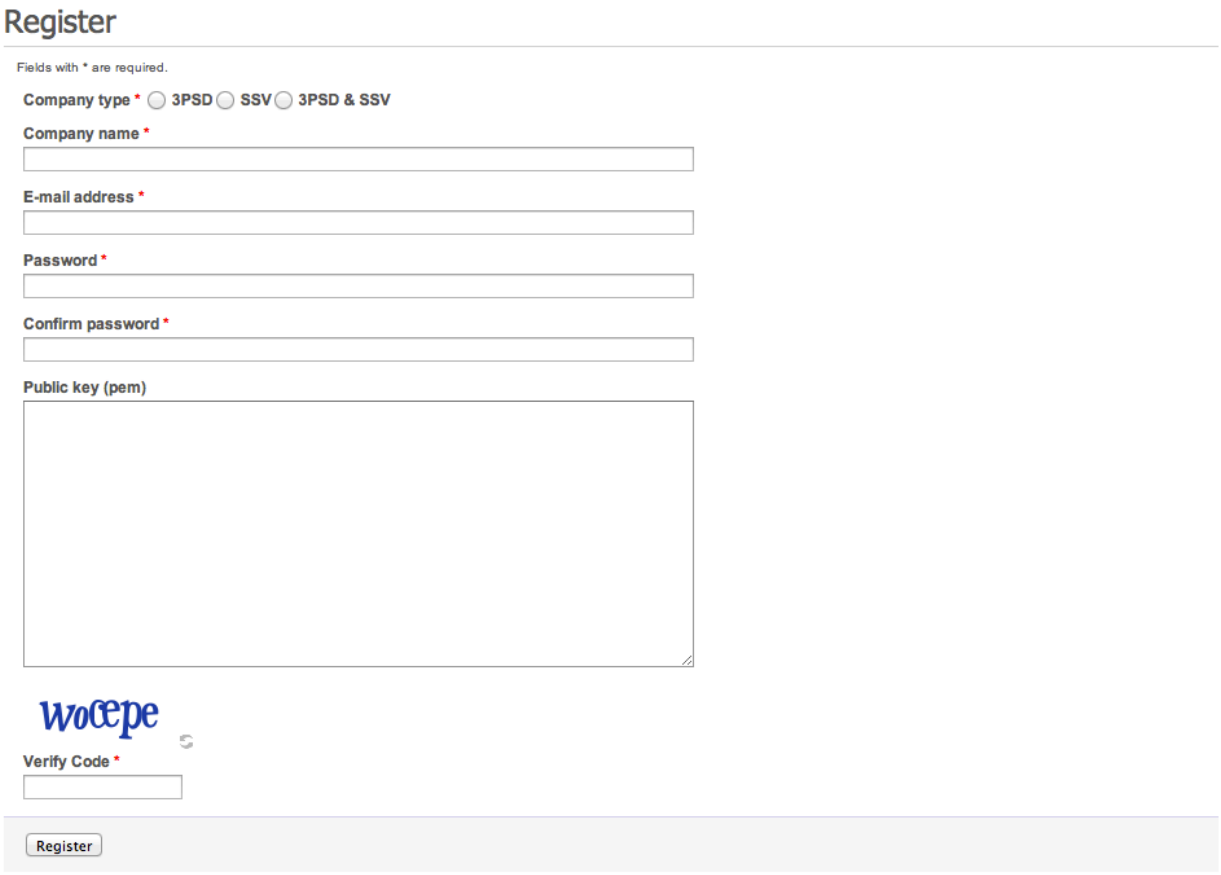
3.2 Executive Committee

The Executive Committee will review all appeals. The decision of the Executive Committee is final.

4. PROCESSES

4.1 Joining the CMX system—Registration process

All companies that are interested in participating in the IEEE CMX system can register an account at https://ieee-cmx.avira.com/site/register. During the registration process, the following page is displayed:



All fields are required in order to finish the registration process.

Company type	3PSD – 3rd party software developers SSV – Security Software Vendors 3PSD & SSV – Combination of 3rd party software developers and security software vendors
Company name	The name of the company
E-mail address	The Email address for the administrative account of the company
Password	The password for the administrative account of the company
Public key (pem)	The public key used for code signing
Verification code	The verification code in order to finish the registration process

After the registration is finished, an email to confirm the request will be sent and the account will be approved by the IEEE CMX Management Committee.

4.2 Using the CMX system

The CMX system hosts a 'Download' section that contains a user manual, a manual for the API, and a Python client. The Python client is based on MMDEF [6] and can create the metadata and submit it automatically. Vendor-specific implementations of the API are possible using all programming languages that support HTTPS.

4.3 Access to the IEEE CMX system

Access to the IEEE CMX system is as follows:

- The Management Committee will oversee requests from parties to join the program and will perform vetting (validating that the public key meets the requirements).
- The Management Committee will also handle removal. Should circumstances arise where the legitimacy of a user is called into question, this committee will make the decision to revoke that participation.
- The Executive Committee will handle all appeals. The Executive Committee's decision is final.

4.4 Expulsion from the IEEE CMX system

The expulsion procedure is as follows:

- The process can be initiated by any two members of the group (so any member must enlist support from at least one other to launch the inquiry) as a request to expel an existing member. Specific reasons (e.g., violating the license agreements, leaking confidential IEEE information) must be documented and supported by adequate evidence.
- The Management Committee will produce a decision in a reasonable timeframe.
- The Management Committee should notify the concerned party of the move to expel with reasons, including but not limited to, the supporting evidence.
- The Executive Committee will handle all appeals. The Executive Committee's decision is final.

NOTE—Not paying the license fee (beyond the grace period) will result in automatic loss of legal right to use the system and won't require an expulsion process to be initiated and completed.

5. ADMINISTRATIVE SUPPORT BY IEEE

5.1 Costs

IEEE CMX is a not-for-profit operation, however, the IEEE CMX system is not free to use as there are maintenance costs. Therefore, all users must adhere to the IEEE CMX license agreement.

Costs for use of the system are outlined on the AMSS Subscriber License.

6. REFERENCES

[1] IEEE ICSG Malware Metadata Exchange Format
http://standards.ieee.org/develop/indconn/icsg/mmdef.html

[2] Muttik 'Connecting the AV industry' Proc. Virus Bulletin International Conference, 2009, http://www.virusbtn.com/pdf/conference_slides/2009/Muttik-VB2009.pdf

[3] V. Weafer, I.Muttik 'Sample Meta-Data Exchange XML Format by IEEE'. Microsoft MSRA Summit, 2009 (http://standards.ieee.org/develop/indconn/icsg/icsgpres.pdf)