Cybersecurity in Agile Cloud Computing

Industry Connections Activity Initiation Document (ICAID)

Version: 1.0, 18 January 2021

IC21-001-01 Approved by IESS SMDC 22 March 2021

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: David Tayouri
Email Address: dtayouri@elta.co.il
Employer: ELTA Systems Ltd.
Affiliation: Cyber Division

IEEE collects personal data on this form, which is made publicly available, to allow communication by materially interested parties and with Activity Oversight Committee and Activity officers who are responsible for IEEE work items.

2. Participation and Voting Model

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.

In the era of agile computing, more organizations move their data centers and development resources to the cloud, in order to be able to use resources (networks, infrastructure and software) as and when required, and not have to pay for them when not being used. During 2020, especially because of COVID-19, more organizations transitioned to the cloud, enabling their employees to work from home. Therefore, secured remote access, in particular in a zero trust environment like the cloud, is now challenging more than ever.

The goals of this activity are to raise awareness of cloud remote access security risks (e.g. by workshops and conferences), recommend best practices and guidelines for cloud remote access and propose standards and certificates for cloud service providers regarding (context-aware) secured remote access.

In order to achieve these goals, we will start by framing the problems, identifying the existing approaches and technologies and examining solutions. In addition, we will perform a gap analysis of the existing cloud standards and certifications and evaluate the need for extending them for secured remote access. Emphasis will be put on defense organizations, which have more restricted security requirements, and may require more restricted security on remote access to their data.

Possible subjects of interest that will be examined by this activity:

- Provide a standard framework for authorization decisions based on projected cyber risk and authentication-based trust factors
- Leverage highly-correlated data points as real-time authentication factors for a given authorization scenario
- Define security guardrails around identity, platform, and application-level security in remote access scenarios
- Dynamically alter security and auditing controls based on importance of data, the environment context and level of risk in authorized activities

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 Cloud Security Alliance (CSA) is a not-for-profit organization with the mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing. CSA operates a cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring.

The Object Management Group (OMG) is an international, open membership, not-for-profit technology standards consortium. The OMG Cloud Working Group publishes vendor-neutral guidance on important considerations for cloud computing adoption, highlighting standards, opportunities for standardization, cloud customer requirements, and best practices to foster an ecosystem of open, standards-based cloud computing technologies.

The Cloud Signature Consortium (CSC) is a group of industry and academic organizations committed to building a new standard for cloud-based digital signatures that will support web and mobile applications and comply with the most demanding electronic signature regulations in the world.

None of the mentioned organizations/working groups deeply handles the secured remote access to cloud.

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

3.4 Potential Markets Served

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

The best practices and guidlines for secured remote access will be beneficial to the organizations whose employees access the cloud, since we intend to create a more secure solution for accessing the cloud. The standards and certificate we will propose will affect cloud service providers and enable more secured access to the cloud for anyone who uses cloud services.

3.5 How will the activity benefit the IEEE, society, or humanity?

One of the activity goals is proposing new standards to ensure secured remote access to the cloud, supporting IEEE's goal of advancing technology for humanity. This will assist IEEE in achieving its goals, and will enhance its reputation for addressing key emerging challenges. Users of cloud services will benefit from more secured access to the cloud.

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: 03/2023

IC activities are chartered for two years at a time. Activities are eligible for extension upon request and review by ICCom and the responsible committee of the IEEE SA Board of Governors. 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 (e.g., white papers, reports), proposals for standards, conferences and workshops, databases, computer code, etc., and indicate the expected timeframe for each.

- White Paper (framing the problems, current architectures, the need to address secure practices, technical approaches etc.) (4 months)
- Standards and certifications gap analysis (4 months)
- Recommendations for best practices & guidelines, for medium-large companies, in particular defense companies (4 months)
- Proposing IEEE standards/certifications (6 months)
- Workshops/conferences for awareness on Cloud Security and best practices (6 months)

5.1 Open Source Software Development

Indicate whether this IC Activity will develop or incorporate open source software in the deliverables. All contributions of open source software for use in Industry Connections activities shall be accompanied by an approved IEEE Contributor License Agreement (CLA) appropriate for the open source license under which the Work Product will be made available. CLAs, once accepted, are irrevocable. Industry Connections Activities shall comply with the IEEE SA open source policies and procedures and use the IEEE SA open source platform for development of open source software. Information on IEEE SA Open can be found at https://saopen.ieee.org/.

Will the activity develop or incorporate open source software (either normatively or informatively) in the deliverables?: No, there is no intention to deliver software

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.

No funding requests are anticipated beyond the basic IC support services provided by IEEE.

7. Management and Procedures

7.1 Activity Oversight Committee

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

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

If yes, indicate the IEEE committee’s name and its chair’s contact information.

IEEE Committee Name: Committee Name

Chair's Name: Full Name
Chair's Email Address: who@where

Additional IEEE committee information, if any. Please indicate if you are including a letter of support from the IEEE Committee that will oversee this activity.

IEEE collects personal data on this form, which is made publicly available, to allow communication by materially interested parties and with Activity Oversight Committee and Activity officers who are responsible for IEEE work items.

7.2 Activity Management

If no Activity Oversight 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).

An executive committee will be established from the members of the working group.

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,* (b) Standards Committee policies and procedures accepted by the IEEE SA Standards Board, or (c) Working Group policies and procedures accepted by the Working Group's Standards Committee. If option (a) is chosen, then ICCom review and approval of the P&P is required. If option (b) or (c) is chosen, then ICCom approval of the use of the P&P is required.

We will use the abridged Industry Connections Activity Policies and Procedures.

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.

Regulators, Industries, Cloud Service Providers, Cybersecurity Vendors, Academia.

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.

5-6

8.3 Initial Participants

Provide a number 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:

Entity	**Primary Contact**	**Additional Representatives**
ELTA Systems	David Tayouri	Eddie Kleinmintz
Microsoft Israel	Tomer Simon	
Check Point	Snir Hassidim	
Ben-Gurion University	Prof. Asaf Shabtai	

Use the following table for an individual-based activity:

Individual		**Employer**	**Affiliation**
Name			