Zero Trust Cybersecurity for Health Technology Tools, Services, and Devices

Industry Connections Activity Initiation Document (ICAID)

Version: 1.0, 24 February 2023

IC23-003-01 Approved by the CAG 22 March 2023

Instructions

- Instructions on how to fill out this form are shown in red. Please leave the instructions in the final document and simply add the requested information where indicated.
- Spell out each acronym the first time it is used. For example, "United Nations (UN)."
- 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: Habib Rehman
Email Address: muhammad_habib.rehman@kcl.ac.uk
Employer: King's College of London
Affiliation: Entity Name(s)

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.

The Motivation

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. **Zero Trust assumes that there is no traditional network edge**; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

The **zero trust security model**, also known as **zero trust architecture** (**ZTA**), **zero trust network architecture** or **zero trust network access** (**ZTNA**), and sometimes known as **perimeterless security**, describes an approach to the design and implementation of IT systems. The main concept behind the zero trust security model is "never trust, always verify," which means that devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified. ZTNA is implemented by establishing strong identity verification, validating device compliance prior to granting access, and ensuring least privilege access to only explicitly authorized resources.

The zero trust approach advocates mutual authentication, including checking the identity and integrity of devices without respect to location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication. The principles of zero trust can be applied to data access, and to the management of data. [Source: Wikipedia.org]

Microsoft's Zero Trust Adoption Report 2021 reports 96% of the decision-makers in charge of cybersecurity currently believe that zero trust is critical, with 76% of them in the process of implementation. Zero trust is viewed as a high priority and critical for both cybersecurity offense and defense.

An analysis of data breaches recorded on the Privacy Rights Clearinghouse database between 2015 and 2019 showed that 76.59% of all recorded data breaches were in the healthcare sector. Between 2009 and 2021, 4,419 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records.

The healthcare sector reported 337 breaches in the first half of 2022 according to Fortified Health Security's **mid-year report**. More than 19 million records were implicated in healthcare data breaches in the first six months of the year. IBM's annual "Cost of a Data Breach" report showed the **average cost of a healthcare data breach** is now $10.1 million per incident, signifying a 9.4 percent increase from 2021. The biggest healthcare data breaches reported in 2022 thus far report a rise in third-party vendor breaches.

The FDA, given the interconnected nature of the future of IoMT devices, augmented reality, robotics etc, advises healthcare organizations must shift to a Zero Trust model with a multipronged approach for the following:

a. device security
b. network security
c. data security
d. workload security
e. identity and access management
f. visibility tools and
g. orchestration platforms, focusing on data, workloads and identity

Major challenges:

1. In the US, the federal government has released a memorandum mandating a federal Zero Trust architecture strategy, which forces federal agencies to meet certain cyber security standards, by 2024.
2. Creating a secure, common federated identity management system
3. How to understand and implement a solution is befuddling with a multitude of approaches and levels
4. There are disconnects to identify and hurdles to implementation
5. Organizations must move their business functions to the cloud to support the work-from-anywhere workforce
6. Demand for endpoint security visibility and control is growing. An increasing number of organizations are improving their approach to identity access management; a core component of Zero Trust architecture. Additions such as multi-factor authentication and single sign-on are becoming more commonplace.
7. Zero Trust is becoming the foundation of an increasing number of hybrid cloud integrations, as it effectively addresses the security needs of the data-rich healthcare environment

A snapshot of the market:

- By 2026, the Zero Trust market is projected to reach $52 billion
- Zero Trust can reduce the cost of a data breach by roughly $1.76 million
- Seventy-two percent of organizations are either in the process of adopting Zero Trust or have already adopted it.
- Ninety percent of organizations state that advancing Zero Trust represents one of their top three IT and security priorities
- Zero Trust segmentation efficiencies translate into freeing up nearly 40 person-hours per week
- Organizations that leverage Zero Trust segmentation are 2X more likely to avoid critical outages due to attacks over the last 24 months.

The Goal

- The goal is to build conventional, general-purpose zero trust microsegmented IT infrastructure and guidelines in healthcare, that are aligned with IEEE standards, for remote patient monitoring tools, workforce, services, platforms, health systems, EHR (Electronic Health Record) , tokenomics (Token + Economics; the factors that impact a token's use and value, including but not limited to the token's creation and distribution, supply and demand, incentive mechanisms, and token burn schedules. A cryptocurrency that represents the value of health information can motivate individuals to make their health data shareable to those who are willing to pay for it. This contributes to growing sentiment of healthcare consumerism).
- Develop a roadmap to a suite of new zero-trust network access (ZTNA) standards that integrate commercial and open-source products to showcase robust security features of Zero Trust Architecture (ZTA) when applied to enterprise IT use cases. This will include authentication and authorization of subject and device discrete functions, remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary.
- Develop recommendations to validate and verify selected technologies to modernize standard cybersecurity approaches in healthcare to mitigate hacking, secure data and any interruption of work
- Identify frameworks for End to end security of authentication, privacy and security of data and users, ensuring interoperability and encryption enabling private transactions on a public blockchain for new healthcare products and services using tokenomics models
- Support other IEEE initiatives in common areas of internet, focus and applications through standards
- Engage a broader community in the domains of blockchain, trusted computing, federated learning, and decentralized identifier to increase universality of the standards collaborative output

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.).

Describe the related work.

- NIST SP 800-207, Zero Trust Architecture
- IEEE Global Initiative on Trust Technology Connections Program: https://standards.ieee.org/industry-connections/activities/the-ieee-global-initiative-on-trust-technology/.

3.3 Previously Published Material

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

List the previously published material, if any.

None

3.4 Potential Markets Served

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

- Zero trust, cyber security, and cloud companies
- Cyber security, and Identity as a Service (IDaaS) companies
- Think tank and NGOs
- Pharmaceutical and biopharmaceutical manufacturers, Laboratories, Contract Research Organizations
- Hospitals
- Regulatory organizations (i.e. FDA, EMA, European Commission, HHS, etc)
- Technology Companies, Medical Device manufacturers, App developers, RPM companies, Telehealth Platform and service Providers
- Artificial Intelligence, Machine Learning, Augmented Reality, Blockchain/DLT, IoMTs/Sensors
- Web3, NFT, DeSci, and DAO communities
- Universities, organizations, governments, corporations and individuals involved in the research, design and solutions around Trust technology

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

Describe how this activity will benefit the IEEE, society, or humanity.

- There are expected technical and data governance standards to be extracted and developed to braoden guidance and utilization from this activity
- Published white papers and industry recommendations to provide guidance
- Amplification of IEEE to audiences beyond current member base
- Development of workshops, worksteams and webinars to amplify the work-groups mission, objectives and membership

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: 03/2025

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.

Specify the deliverables for this IC activity, please be specific.

- Gap analysis of existing zero trust standards and best practices – publish by January 2024
- 2 F2F Workshops focused on zero trust frameworks closing the loop of trust in healthcare (Q1 2024; Q1 2025)
- Recommendations for standards about trust technology, including technical framework, technical and application requirements as it relates to connected health apps and devices
- Industry recommendation paper (i.e. industry behavior changes) for regulatory and industry behavioral adaptation to rapidly evolving changing technologies equally or more vulnerable to security breaches
- Develop roadmap of suite of needed zero-trust network access (ZTNA) standards that integrate commercial and open-source products to showcase robust security features of Zero Trust Architecture (ZTA) when applied to enterprise IT healthcare use cases – 03/25
- Create an open repository of Deployment models and healthcare use cases where zero trust could improve an enterprise's overall information technology security posture (start of repository June 2024 – but this will be ongoing data collection)

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?

Yes

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.

Specify funding requirements and sources, if any.

No additional funding requirement at this time.

7. Management and Procedures

7.1 Activity Oversight Committee

Indicate whether an IEEE Standards Committee or Standards Development Working Group has agreed to oversee this activity and its procedures.

Has an IEEE Standards Committee or Standards Development Working Group 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.).

Briefly outline activity management structure.

The Activity will be managed by an Executive Committee as described in the Activity's Policies and Procedures.

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* (entity, individual), (b) *Abridged Industry Connections Activity Policies and Procedures* (entity, individual), (c) Standards Committee policies and procedures accepted by the IEEE SA Standards Board, or (d) 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 (c) or (d) is chosen, then ICCom approval of the use of the P&P is required.

Specify the policies and procedures document to be used. Attach a copy of chosen policies and procedures.

(a) Modified Baseline Industry Connections Activity and 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.

Specify types of entities or groups of individuals.

- Zero trust, cyber security, and cloud companies
- Cyber security, and Identity as a Service (IDaaS) companies
- Think tank and NGOs
- New Technology Companies - (AI, Blockchain, VR/AR, Sensors/IoTs, etc)
- Existing Technology Systems
- Bio/Pharmaceutical companies, university research hospitals
- Hospitals
- Regulatory
- Academic researchers

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 or number of individuals.

125 entity participants

8.3 Initial Participants

Provide a few 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 Name	Primary Contact Name	Additional Representatives
Microsoft Federal	Jason Payne	
Auth0/Okta	Shiven Ramji	
Forcepoint	Sean Berg	
Illumio	Andrew Rubin	
CrowdStrike	Drex DeFord	
Apgate	Tony Zirnoon	
Akamai	Robert Blumofe	
Sentara Healthcare	Zishan Siddiqui	
Zscaler Cloud Protection	Gururaj Pandurangi	

8.4 Activity Supporter/Partner

Indicate whether an IEEE committee (including IEEE Societies and Technical Councils), other than the Oversight Committee, has agreed to participate or support this activity. Support may include, but is not limited to, financial support, marketing support and other ways to help the Activity complete its deliverables.

Has an IEEE Committee, other than the Oversight Committee, agreed to support this activity? Yes

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

IEEE Committee Name: IEEE EMBS Standards Committee
Chair's Name: Esteban Pino
Chair's Email Address: epino@ieee.org
Please indicate if you are including a letter of support from the IEEE Committee.