Security/Architecture Forums
Zero Trust Architecture Project Charter

Status: Draft
Revision level: v2.1
Date: 27 March 2020

A. Project Description

In recent times, there has been a lot said and written about a security concept known as 'zero trust architecture' (ZTA). Key drivers have been on the end user side and the supply side. Zero trust in the modern environment constitutes a holistic capability addressing components in the entire IT ecosystem. This project's approach is to assess the current state and to establish the direction for the industry, which could incorporate new approaches and models.

The consumer community has been driven by the rapid transition to a hybrid-cloud environment, with cloud-native and vendor-driven public and private clouds coupled with legacy platforms. The rapid rise of cloud-native or API environments has changed the enterprise IT landscape and thus driven the requirements for IT security. The rate of continuous change, both from a business and an IT perspective, is driving the creation of ecosystems of microservices and the enterprise as a set of service-oriented architectures (SOAs). Traditional perimeter-based models are becoming unable to support both the rate of change and the nature of the new IT ecosystem of SOAs.

As enterprises embark on their journey to cloud, they expose their IT infrastructure, applications, and data to a new set of actors. In traditional on-premises, enterprises were dealing with mostly internal employees and pre-screen contractors and vendors. With cloud, enterprises have cloud service providers and their partners; applications or APIs accessible over internet could be accessible by virtually anyone anywhere in the world instead of being limited to people on the intranet. The new Agile, DevOps, and microservices paradigms are increasing the complexity of the application stack from a traditional 3-tier, requiring a handful of software products be manually built and installed, to one where each microservice may have its own stack and loads of software in the CI/CD pipeline to automate build, test, and deploy. These changes are resulting in many threat actors and threat surfaces. Threats are not necessarily network-based attacks but cover the entire stack and are not limited only to the network. The people, processes, and technologies are interwoven in a proper security capability.

Existing vendor network models are no longer providing levels of security that meet modern requirements. Separately, the vendor community in the network technology sector has shown particular interest because (a) they see an opportunity to develop, market, and sell new products, and (b) some interpretations of the concept threaten to disrupt the network security industry, leaving some vendors without a meaningful offering in network security. The situation is a classic case of 'digital disruption,' leading to opportunities for digital evolution to meet the perpetual state of business and technology disruption.

The theoretical basis for this project is described by The Jericho Forum Commandments published in 2007. Industry analysts have published papers on Zero Trust (Forester) and Lean Trust (Gartner) that build upon this earlier thinking. Google has also published a series of BeyondCorp papers that describe their thoughts on implementing zero trust ideas in their business. What is new is the way in which vendors have picked up the ideas and are now using them to expand their product portfolios. Not all of those 'new' products are well conceived. Without standards, best practices guidance, and

(potentially) reference code implementations, the industry will struggle to achieve smooth interoperability.

Prior to initiating the standards activity, there is a need to build a willing ecosystem of end-user organizations and vendors. Experience at The Open Group in initiating and building industry transformational standards in areas as diverse as military avionics (FACE Consortium), process control systems standards (Open Process Automation Forum), sensors (SOSA Consortium), and data frameworks enabling cloud migration for oil & gas (Open Subsurface Data Universe Forum) have shown that it is critical to obtain broad buy-in and industry support in order to ensure uptake and adoption. Experience in starting these other initiatives also indicates that it is critical to place them in a vendor-neutral standards organization with the legal framework to allow collaboration between competitors without creating anti-trust concerns (and this has proven to be a concern both for vendors as well as for end user organizations).

Finally, this project envisions that the resulting standards will need to utilize a "standard of standards" approach, requiring liaisons with other standards organizations (as is being used in each of OPAF, OSDU, FACE and SOSA), for some foundational standards already exist that provide needed building blocks for ZTA (such as XACML, crypto, and key management standards). There is, therefore, a part to be played by The Open Group in developing such interoperable standards.

There is also a part to be played by The SABSA Institute C.I.C. in providing thought leadership in security architecture. This project is an excellent example of how The Open Group and The SABSA Institute can collaborate under the terms of their joint MOU to create standards and guidance for adoption across the cyber security industry. It is in the interests of both organizations to create product-agnostic standards and guidance.

B. Goals of this Project

The ultimate goals are to create an ecosystem of interested end-user and vendor organizations, publish technical standards, create business guidance for industry participants, establish a shared industry understanding and definition of zero trust, implement guidelines for zero trust architecture, potentially create open source projects leading to reference code implementations for aspects of zero trust architectures, and importantly, to drive adoption of the work products of the forum into the industry.

While this standard will take a standard of standards approach, one of the guiding principles is to provide simple, clear direction which applies to the ecosystem of digital architectures. In other words, the standard should be as simple as possible and have broad applicability, such as the Jericho Commandments were able to do.

C. Project Deliverables

<u>Group 1</u>

1. Zero Trust Landscapes *White Paper*
   Goal: Identify current landscape of key stakeholders, highlight differences in positions and gaps, and briefly describe where project will go
   a. Surveys to understand current Zero Trust awareness and understanding, organizational readiness, key drivers, and success factors and implementation (people, process, technology). All surveys will share a set of core questions to allow answer comparisons and analysis.

   i. Chief Information Security Officers (CISOs) & Chief Security Architects (CSAs)
   ii. Vendors (Product owners)
   iii. Academia
b. Reviews/Analyses of existing work/publications/products/services around Zero Trust
   i. Vendor offerings and positions, broken down by vendor category (e.g., network and network segmentation, authentication and authorization)
   ii. Academic work done around zero trust (e.g., IEEE, ACM)
   iii. Standards organizations publications
   iv. Identification of gaps within current ZTA practices to identify where they are heading in the wrong direction
   v. Additional issues that emerge during the course of the research gathering

2. Zero Trust Core Principles *White Paper*
   Goal: Provide current state definition of Zero Trust to be updated later upon completion of reference architecture and model
   a. Explain what Zero Trust is to stakeholders
   b. Describe Zero Trust and go beyond principles
   c. Input from draft white paper from John Sherwood and The SABSA Institute ("Redefining Security Architecture in the Cloud") → current state of Zero Trust
      i. Defining vision, core principles

3. "Zero Trust Manifesto" *White Paper*
   Goal: Provide similar set of core principles that are easily understood and take similar approach to Jericho Commandments
   a. Simple to allow to follow and approach zero trust problem
   b. Easy for all organizations to adopt
   c. Will include a focus on data themselves being secure
   d. Ensure useful for appealing to executives
   e. Identify attributes initially deemed important to consider
   f. Input assets
      i. "Axioms for the Practice of Security Architecture"
      ii. Jericho Commandments

4. A reference architecture and model (*Standard*) for implementing ZTA
   Goal: Provide template solution for Zero Trust Architecture utilizing common vocabulary
   a. Will contain what Zero Trust means in context of different use cases
   b. Will include presentation layer and define other layers within the architecture
   c. Will define capabilities
   d. Will consider different use cases and design patterns
      i. For things like web access, PII access, VDI access, the security, privacy, and trust requirements will be necessarily different.
   e. Will offer guidance on cloud native and microservice architectures (prescriptive and normative)
      i. To be informed by the TOGAF Series Guide on this content being developed by the SOA and Microservices teams.
   f. Will establish a reference metadata model for zero trust
   g. Will define identity classification model and consideration of compliance controls
   h. Will include guidance on implementing Data Lake

i. To be updated based on learning for AI

Group 2

5. Zero Trust Algorithm
   Goal: Create trust algorithm to complement Zero Trust reference architecture and model for implementing ZTA
   a. Able to be slotted into any zero trust architecture or used deliberately by the one designed by the ZTA Project Work Group
      i. It will include well-described and measurable attributes.
         1. O-ISM3 Security Objectives
         2. SABSA Business Attributes
      ii. It will incorporate multiple logical constructs.
         1. If, then, else
         2. Case
         3. Except
      iii. It will be capable of granting/denying access on a dynamic basis based on current context.
      iv. It will be based on domains from either/both NIST SP800-207 or/and NASA SEWP.
      v. The sources of attribute values will be the output from security services, such as Identity Service, Registration Service, Authentication Service, Authorization Service, etc.

6. Zero Trust Practitioners *Guide*
   Goal: Provide a process framework for implementing Zero Trust, leveraging the Reference Architecture and Zero Trust Manifesto deliverables
   a. Will include updated definition of zero trust architecture
   b. Will use the landscape review to articulate concepts which are prevalent today (a current state analysis - hypothesis is this will be network-centric)
   c. Will review the Jericho Forum principles and team insights/experience to derive gaps with current concepts (a future state analysis)
   d. Will associate the concepts explained above with each other (an ontology) to help create clear, opinionated definitions and show the fundamental semantic differences between network- and data-centric thinking in the ZTA domain
   e. Will create actionable steps that practitioners should take to move from a network-centric model toward a data-centric model
   f. Will focus on set of primary controls, leveraging content of Zero Trust Manifesto deliverable
   g. To be updated based on learning for AI

7. Zero Trust Threat Modelling *White Paper*
   Goal: identify threats within Zero Trust
   a. Exact contents TBD
   b. As existing threat models break down, there is a need for an updated industry standard threat model against zero trust architecture.
   c. Identify threats specific to implementing/using a Zero Trust Architecture
   d. Develop a threat modelling approach that complements reference architecture
   e. Input assets

i. Excerpts from textbooks of The SABSA Institute on threat modelling and threat scenario analysis
ii. Work done by the Security Forum and/or Architecture Forum on threat modelling

f. Potential collaboration with the ArchiMate® Forum for this deliverable
g. To be updated based on learning for AI

Group 3

8. A Business *Guide*
Goal: Provide a simple guide to Senior and C-level Executives and Enterprise Architects that explains what Zero Trust is, what impact it has on business, and the reasons for implementing Zero Trust in a business context.
    a. Define Zero Trust in a nutshell, providing a quick introduction covering drivers, state of the art and how it applies
    b. Describe the Zero Trust ecosystem, both before and after standards work is done
        i. Use examples from OPAF, FACE, SOSA
    c. Explain Zero Trust in the life of the executive
        i. Offer quick overview of use cases for zero trust.
        ii. Explain using a hypothetical example for Acme corp.
    d. Describe drivers in more detail
        i. Align with the SOA4BT taxonomy
    e. Describe a day in the life of an organization
        i. Zero Trust in the life of the C-Level executive who is not an IT-executive
            1. Making Zero Trust decisions and their impact on the life of the C-Level executive who is not IT
        ii. Zero Trust in the life of the C-Level IT executive who is not a CISO or CISA
        iii. Zero Trust in the life of the CISO and CISA
        iv. Zero Trust in the life of the Enterprise Architect
    f. Conclusions and where next

D. Future Directions

Upon completing publication of the planned deliverables detailed above, the project will work to create a development plan and road map for a second phase for the production of detailed standards and guidelines**.** Part of this may include considering open source projects for ZTA components.

The second phase of this ZTA Project will include a consideration of Artificial Intelligence (AI) and the tainting—whether accidental or deliberate—of data and applications it relies upon to reach conclusions or reason and how this relates to Zero Trust. The second phase will also consider the Internet of Things (IoT) and embedded systems in relation to sustainability and emerging technologies; it may consider critical infrastructure as a use case for IoT and embedded systems.

E. Project Value Proposition

A. This project will provide thought leadership for members of The Open Group.
B. This project will further consolidate the relationship between The Open Group and The SABSA Institute.
C. This project will establish industry standards for interoperability in ZTA.

D. This project will establish a shared industry understanding and definition of Zero Trust and its implications, covering people, processes and technology.
E. This project will develop standards and best practices to assist in jump-starting the development of interoperable products and true microservices based upon industry standards.

F. Project Personnel

A. Stakeholders
    a. The governing stakeholders of the project are:
        i. The Open Group
        ii. The SABSA Institute CIC
B. Team
    a. The project team will be drawn from members of The Open Group Security Forum (including representatives of The SABSA Institute) and the Open Group Architecture Forum.
        i. The Open Group Business Development team will take the task to recruit from the large customer and vendor member organizations (some of whom already have membership entitlements, and some of whom are not Security Forum members as yet). The target organizations are listed as an additional appendix to this charter.
    b. The Project Facilitators will be Nikhil Kumar from the Architecture Forum and Altaz Valani from the Security Forum.
    c. At the appropriate points in the project, open community contributions will be encouraged.

G. Project Methodology

This final section describes the project methodology, which includes:

A. Approach
    a. The philosophical approach that will guide how the work is done
    b. As a part of the approach, an early focus be on recruiting customer-side organizations to this effort, as the vision and pain points need to come from them first, and then in a second phase, focus on involving key vendors. We've used this approach successfully in all of the four standards initiatives described above, and it works.
    c. Outreach should include to CISO Forums to try and elicit views from non-member organization CISO's and chief security architects.
    d. There will be a need to involve industry groups from key verticals (finance, defense, and healthcare). We will seek to leverage existing liaisons from The Open Group to BIAN, as well as healthcare contacts.
B. Governance and Entitlements
    a. Governance of the initiative will be the Open Group standard policy and procedures.
    b. Membership entitlements are provided to members of both of the Open Group Security and Architecture Forums, as inside of The Open Group this is a joint Security & Architecture activity, and via liaison to the SABSA Institute.
    c. There will be a need in this project to allow for contributions from non-members. In the ecosystem building stage, we'll limit this to broadly circulating a survey. Following the model from the OSDU Forum and the DPWG, when we get to creating

standards, best practices, and possibly code, we will facilitate open contributions from non-members via GitLab, with governance of changes and submissions remaining with members, per the Open Group standards process.

C. Approval
    a. Project deliverables will be approved by The Open Group and The SABSA Institute.
    b. The project charter will be approved through the normal mechanism of The Open Group and The SABSA Institute under the terms of the MOU.

D. IPR Ownership
    a. The IPR of the outputs will be jointly owned by both the Open Group and The SABSA Institute.

Appendix A

For current Open Group members with entitlements, active outreach is needed to find security architects with interest in ZTA. For current members without entitlements in the Security Forum or Architecture Forum, outreach is needed to find security architects with interest in ZTA, and an additional membership agreement discussion is also needed.

Current Members, End User Organization target participants:

Philips	Boeing	Exxon Mobil	Shell
UK MoD	NASA	Nationwide	Noble Energy
Petrobras	Raytheon	Moody's	State Bank India
Australian Post	Air China	MITRE	Sykehus Partner
Kerala State (India)	Government of Andhra Pradesh (India)	Banco de Mexico	Alaska Airlines
Chevron	China Eastern Airlines	Dubai Customs	HSBC
Nissan	Societe General	South Africa Reserve Bank	Swiss Federal Administration
TaiPei City Government	Texas Dept. Motor Vehicles	ESRI (South Africa)	IAG
Anadarko Petroleum**	Honeywell**	BASF**	Dow**
BP**	Baker Huges**	BHP Biliton**	ConocoPhillips
Emerson**	Equinoir**	Halliburton**	BAE**
Schlumberger**	Hess Corp.**	Hitachi**	Aramco Services**
LockheedMartin**	US Army PEO Aviation**	US Navy NAVAIR**	US Airforce**
Merck**	Marathon Oil**	Reliance Industries**	Rockwell Automation**
Schneider Electric**	ABB**	Siemens**	Total**
Woodside Energy**	GE Aviation**	Northrup Grumman**	General Dynamics**
Collins Aerospace**	Harris Corp.**	UTC**	Northrop Grumman**
Thales**			

Note: ** = current members, but no entitlements at present.

Current Members, Vendor target participants (from among Open Group membership):

IBM	Oracle	KPMG	Fujitsu
Microsoft	Deloitte	Accenture	DXC
Micro Focus	HCL	Cap Gemini	EY
PriceWaterhouseCoopers	SAP	Software AG	WIPRO
HPE	Amazon**	Google**	Dell**
Apple**	Cisco**	Infosys**	ServiceNow**
Seagate**	Wind River**	Intel**	Applied Technology Solutions, Inc. (ApTSi)

Target participants (from non-members):

Vendors: TBD. Most large security vendors and many small ones will find their products affected, and as such will be membership targets.

End user organizations: TBD. Focus will need to be on very large enterprises, and on those industries and organizations that are generally early adopters.