Document #: MCS-PWG 2022-009

NIST Multi-Cloud Security Public Working Group (MCSPWG)

DRAFT Meeting Minutes

Meeting #6, April 11, 2022

1. Michaela Iorga started the meeting at 3:01 PM ET, April 11, 2022.
   - Attendance: 26 attendees – see Annex B for the list captured on screen during the meeting. See Annex C on a screen shot of the meeting chat.
   - No presentation used for the meeting or recording made of the meeting.
   - No meeting minutes for meeting #5, March 28, 2022, was posted for comments.
   - The first Draft meeting agenda (see Annex A) includes teleconference <bluejeans> information was sent to MCSPWG mailing list on the Friday (April 8, 2022) prior to the meeting, and an updated draft agenda was on the morning of April 11, 2022.

2. Michaela introduced Nida Davis as the new co-Chair of MCSPWG.

3 Agenda #3 Organizational issues
   - Each group should have a central folder for references that is accessible to every member of each group.
   - In response to a question was raised on whether it is acceptable to use other meeting platforms than Bluejeans such as Zoom, US federal participants may not be able to use Zoom. Michaela Iorga is able to set up separate Bluejeans meetings per Group Leads' requests.
   - Meeting time: Group Leads are encouraged to establish a mutually agreed meeting time, and thereby, are to consistently use this meeting time and meeting platform.

4. Teams' charters /mission statement
   - Greg Thomas, Deb Mukherjee, and Abdul Rahman Sattar presented on each group's status including developing group's mission statement. A discussion ensued on definition on credential, identity and authorization, and entities and non-entities, e.g., owners, devices, etc.
   - Suggested that to set up a glossary to harmonize terms and definition used globally and in the US. For example, Sources and Resources – NIST Computer Security Resource Center Glossary https://csrc.nist.gov/glossary, ISO Online Browsing Platform (OBP) https://www.iso.org/obp/ui/#search, ISO Publicly Available Standards https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.
   - Discussion also considered the scope for multi-cloud such as layers and architecture in understanding the complexities and challenges for implementation. Michaela maintained not to be prescriptive to allow ample flexibility for each group's discussion.
   - MCSPWG does cover IaaS, PaaS, and SaaS focusing on multi-cloud and not hybrid cloud.

Groups	Members on Slack	Proposed Mission statement
Zero Trust solutions in a multi-cloud ecosystem - ICAM	Gregory Thomas Katy Craig Total 22 listed	Identify Global Identity and Credential Challenges for Secure Multi-Cloud systems and recommend best practices to solve for these challenges in a multi-cloud world.
Zero Trust solutions in a multi-cloud ecosystem – Access Control	Aradhna Chetal Sergio Pozo Nathanael Coffing Total 28 listed	<Had two meetings as of April 11>
Authorization/Certification of multi-cloud solutions - Risk Management	Angela Phaneuf Debjyoti Mukherjee Total 23 listed	<Had two meetings as of April 11>
Authorization/Certification of multi-cloud solutions – Continuous Monitoring	Abdul Rahman Sattar Saeed Akhter Total 22 listed	The purpose of this group is: 1. Identify challenges with continuous monitoring in the MCS context 2. Identify various use cases that continuous monitoring will support for MCS (threat detection, risk monitoring, monitoring for security controls and compliance use cases) 3. Provide high level architecture guidelines for continuous monitoring design for MCS (system level architecture, automation, data governance, metadata management etc.) 4. Provide guidelines on where continuous monitoring fits into the overall ZTA paradigm for MCS.
TIC 3.0	Galeal Zino Total 12 listed	Pending set-up
Data Exchange Security for Interconnected CSPs	Galeal Zino	Pending set-up

** see links for meeting minutes for each group on Annex A below.
Note: Individual folders for each group are set up within the MCSPWG Public Document https://drive.google.com/drive/u/0/folders/1c9OV10sAQGFRMplsQALSrKNMtjqKx1CQ

We were not able to accommodate discussion on the groups and any in-depth discussion on Agenda item #6.

5. Action items for next meeting:

   a) Deb Mukherjee proposed to have this meeting every week instead of the current arrangement of every two-week. The proposal was accepted and effective immediately, MCSPWG will meet weekly. Michaela Iorga will send out calendar invite to the mailing list for every Monday, 3:00 PM ET.

6. The next meeting will be next week, April 18, 2022, at 3:00 PM ET.

7. Meeting adjourned at 4:21 PM ET.

Annex A

Meeting #6 Agenda

Document #: MCS-PWG 2022-009A

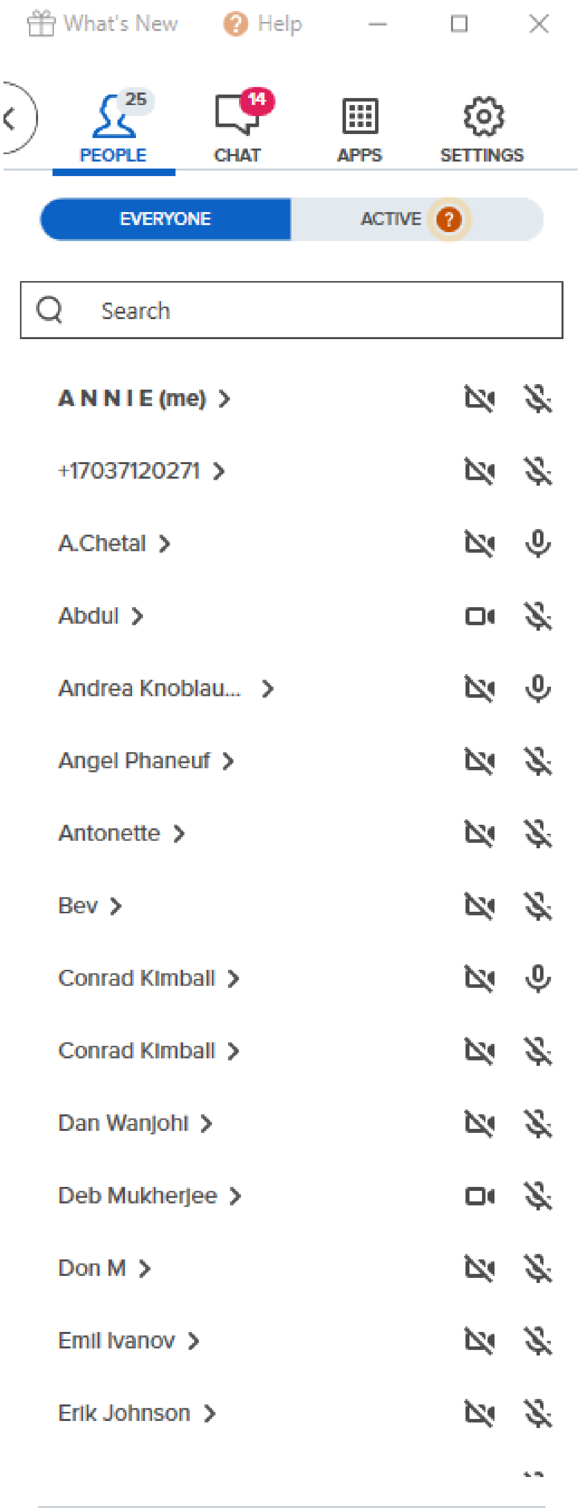
NIST
MULTICLOUD SECURITY PUBLIC WORKING GROUP (MCSPWG)
DRAFT MEETING AGENDA
April 11, 2022, 3:00 PM ET

1. Welcome
2. Review of meeting agenda
3. **Organizational issues (Default directories: Charter, Meeting Minutes/Notes, References)**
4. **Teams' charters /mission statement**
5. **Group Leads research updates. Issues and concerns**
    I. Team 1: ZTA-ICAM, Gregory Thomas and Katy Craig [https://drive.google.com/drive/folders/1mZ8358M_dOJ1HGZwdhleYQ6DxTrqKkUL]
    II. Team 2: ZTA-AC, Aradhna Chetal and Swapnil Kulkarni [https://drive.google.com/drive/folders/1F3sABpsiEjOQFK-WFMxpAcicw0Ji1-ad – currently empty]
    III. Team 3: RM-ATO, Angel Phaneuf & Deb Mukherjee [meeting minutes https://drive.google.com/drive/folders/1kllR8u0aYTBMyXRWps3GY4R1Lx69-EqA]
    IV. Team4: Continuous Monitoring, Abdul Rahman Sattar [https://drive.google.com/drive/folders/1Nau9A3Qtgq-s1NVYteiEFjK3C8Hur5rx]
6. **Open Floor (technical discussion) –** suggested topic Greg's blog: **Cloudy with a Chance of Zero Trust** (a must read)
7. Meeting adjournment

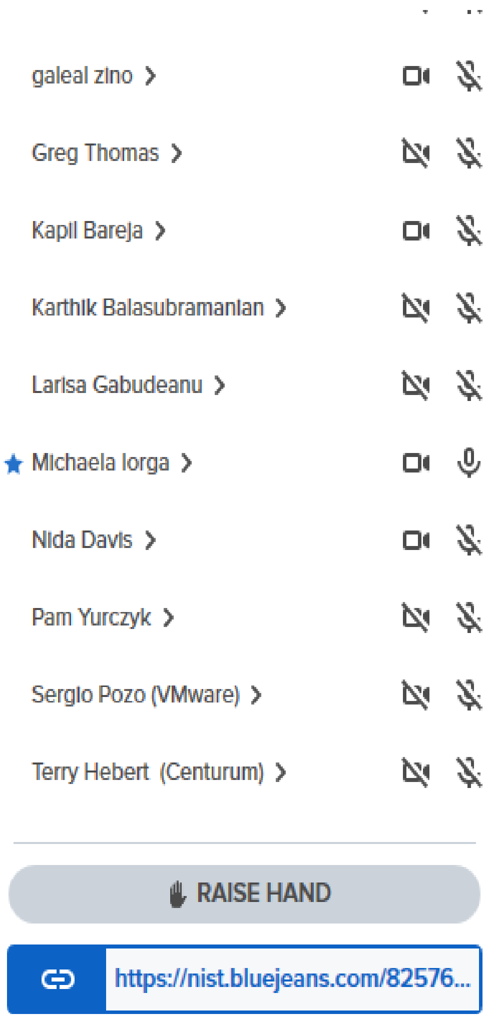
Meeting logistics
Date/Time: February 28, 3:00PM – 4:00 PM EST
Web conferencing tool: https://bluejeans.com/825766225/2335
Meeting ID: 825 766 225
Participant Passcode: 2335
Phone Dial-in:
+1.202.795.9254 (US (Washington DC))
+1.408.317.9254 (US (San Jose))
To test your video connection: https://bluejeans.com/111

Annex B

Meeting #3 Attendees



ANNIE (me)
+17037120271
A.Chetal
Abdul
Andrea Knoblau...
Angel Phaneuf
Antonette
Bev
Conrad Klmball
Conrad Klmball
Dan Wanjohl
Deb Mukherjee
Don M
Emll Ivanov
Erlk Johnson



galeal zlno
Greg Thomas
Kapll Bareja
Karthlk Balasubramanlan
Larlsa Gabudeanu
Mlchaela lorga
Nlda Davls
Pam Yurczyk
Serglo Pozo (VMware)
Terry Hebert (Centurum)

Annex C

Meeting Chat

MCSPWG

April 11, 2022

(3:01 PM) Bev: Hello!

(3:04 PM) Greg Thomas: ICAM-ZTA Proposed Mission Statement = Identify Global Identity Challenges for Secure Multi-Cloud systems and recommend best practices to solve for these challenges in a multi-cloud world.

(3:06 PM) Greg Thomas: Welcome Nida!

(3:06 PM) Deb Mukherjee: Welcome Nida

(3:06 PM) Greg Thomas: Excited to have a 1:1 get to know and work with you! greg.thomas@hashicorp.com

(3:06 PM) Abdul: Welcome Nida!

(3:06 PM) Bev: Welcome Nida!

(3:10 PM) Greg Thomas: We are fine with Zoom for now. Good to know it is an option!

(3:12 PM) A.Chetal: We r fine with Zoom

(3:12 PM) Erik Johnson: Hi NIda. It's been a while. Congrats on the new role with Microsoft!

(3:13 PM) Nida Davis: Hi Erik ... thank you

(3:13 PM) Abdul: ConMon is fine with zoom too. Haven't heard any concerns

(3:13 PM) Nida Davis: and thank you all

(3:13 PM) Nida Davis: Monday is good

(3:14 PM) Kapil Bareja: Hello All!

(3:16 PM) A.Chetal: Greg: are you addressing Credential management ? I presume so

(3:18 PM) A.Chetal: Kapil Lets connect offline

(3:18 PM) Kapil Bareja: Sure Aradhna!

(3:19 PM) A.Chetal: Access controls is a separate working group

(3:20 PM) Larisa Gabudeanu: acces control

(3:23 PM) A.Chetal: so we really need to break it down by use cases

(3:23 PM) A.Chetal: and tease out the concepts

(3:24 PM) Greg Thomas: Yes I like the use cases. It really does depend 😀

(3:24 PM) Erik Johnson: agree that credentials should be included with identities

(3:24 PM) A.Chetal: Also cloud services, container services , service mesh all can be use cases

(3:25 PM) Greg Thomas: Yes, I specialize in service mesh so would be happy to assist there. The multi-cloud, multi-runtime based on identity that is cryptographically protected is something to consider.

(3:26 PM) A.Chetal: yes and I specialize in NGAC and service mesh integration so AC work there I can define

(3:26 PM) Greg Thomas: 👍

(3:26 PM) A.Chetal: NISt 800-204b

(3:27 PM) Kapil Bareja: 👍

(3:27 PM) A.Chetal: Application identity

(3:27 PM) Greg Thomas: Yes, NIST 800-204b is primarily what I think we should write updates for based on multi-cloud, multi-runtime. It is singularly based on K8 and maybe a single cloud...

(3:28 PM) Nida Davis: PAM Accounts / Non-Human Service Accounts

(3:28 PM) Greg Thomas: Also, does not document global identity in respect to the Universal Principles of Zero Trust.

(3:29 PM) Greg Thomas: NIST defines identity as "the set of physical and behavioral characteristics by which an individual is uniquely recognizable."

(3:31 PM) Nida Davis: Bots too

(3:31 PM) Greg Thomas: NPE is for bots

(3:31 PM) Greg Thomas: Identity was defined more than a decade ago and may need to be reviewed.

(3:32 PM) A.Chetal: NSIt definitions are the best

(3:32 PM) A.Chetal: More authoritative

(3:32 PM) Nida Davis: not in the financial sector Chetal

(3:32 PM) A.Chetal: I m in the financial sector too Nida

(3:33 PM) A.Chetal: We use NIST as standard

(3:33 PM) Nida Davis: Not globally

(3:33 PM) Erik Johnson: Can we expand the scope of the ICAM and AC teams to include non-human identities in scope? Seems like that would make sense.

(3:33 PM) A.Chetal: Focussing on US

(3:33 PM) Nida Davis: Not good to just focus on the US ...

(3:33 PM) A.Chetal: Erik already expanded to user, Device apps

(3:34 PM) A.Chetal: yes but ISO is pretty much mapped to NIST all standards have cross references

(3:35 PM) Nida Davis: Not really, I spent two years working on cyber terms and evaluating ISO and NIST usage in terms of harmonization. Check the FSB Cyber Taxonomy ... we found deviations that caused issues for the financial sector.

(3:35 PM) Greg Thomas: Hi Erik, yes agree happy to include NPE with Identity and credentials in our portion.

(3:35 PM) Greg Thomas: w/ use case identity based service mesh for multi-cloud/multi-runtime

(3:36 PM) A.Chetal: Nina please share deviations if you can

(3:38 PM) Nida Davis: Chetal, we provided NIST the analysis two years ago

(3:38 PM) Nida Davis: I can connect you with the NIST person

(3:38 PM) Nida Davis: who has the details

(3:39 PM) A.Chetal: sounds good, please do

(3:39 PM) Greg Thomas: Agree that architecture diagram being consistent or provided to each group will help.

(3:40 PM) Erik Johnson: General scope question for the overall workgroup regarding applicable cloud service models: are we addressing all types of cloud service models (IaaS/PaaS and SaaS) in various combinations, or some subset of use cases?

(3:40 PM) Nida Davis: https://www.nist.gov/people/nadya-bartol

(3:40 PM) A.Chetal: I really think we need to have step by step approach....Requirements, use cases then focus on architecture...

(3:40 PM) Greg Thomas: I like that approach.

(3:40 PM) A.Chetal: Erik : SaaS is out of scope

(3:41 PM) Angel Phaneuf: Slack does the same to me

(3:45 PM) Abdul: https://docs.google.com/document/d/10X4sOnaydwPr09jzOmOM2VotGQ28K7FrCLSQWFBllVA

(3:46 PM) Greg Thomas: Good job on CON MON Abdul!

(3:46 PM) Erik Johnson: A.Chetal - where in the workgropu charter does it say that SaaS is out of scope? The only reference to service models that I found mentions all 3.

(3:47 PM) Erik Johnson: https://csrc.nist.gov/projects/mcspwg/mcspw-charter

(3:49 PM) A.Chetal: Erik that was discussed in first meeting Michaela had on this subject

(3:49 PM) A.Chetal: not sure where it is documented

(3:50 PM) A.Chetal: SaaS and zero trust will be very complex is what was quoted as a challenge

(3:50 PM) Erik Johnson: Maybe we should confirm that with her and suggest a charter update to make sure everyone is on the same page?

(3:51 PM) Bev: Michaela, Isn't there also a "relying party"?

(3:51 PM) A.Chetal: yes, for sure

(3:53 PM) A.Chetal: Blue Jeans connectivity is choppy today

(3:55 PM) Kapil Bareja: Draft NISTIR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight - We can get info from here

(3:55 PM) Kapil Bareja: Abdul take a note we can go through

(3:55 PM) Nida Davis: secure vs. non-secure network layer

(3:55 PM) Deb Mukherjee: https://docs.google.com/document/d/175-lOo6En3WEf2udDcTjRACKRj1zpKu9nyhTkCE1UpQ/edit

(3:56 PM) A.Chetal: First meeting we discussed this

(3:57 PM) Abdul: Thanks Greg :)

(3:58 PM) A.Chetal: I have to drop , Thank you for the conversation today !!

(3:58 PM) Conrad Kimball: Distinguishing multicloud from hybrid cloud is splitting hairs a bit. In both cases you are using more than one cloud provider.

(4:00 PM) Erik Johnson: So all 3 service models are in scope: IaaS, PaaS & SaaS

(4:02 PM) Nida Davis: ATO for Interconnectivity as an added module

(4:06 PM) Angel Phaneuf: We use CRFM

(4:06 PM) galeal zino: I am being pinged for my next meet and will drop. Our group charters to be shared for input this week.

(4:06 PM) Angel Phaneuf: Yes, If your AO approves

(4:07 PM) Angel Phaneuf: Depends on your AO

(4:07 PM) Angel Phaneuf: The army software factory uses a playbook and it allows us to push on demand.

(4:07 PM) Erik Johnson: IN the RM-ATO group are we focusing on NIST RM frameworks, or a larger set?

(4:08 PM) Nida Davis: weekly

(4:08 PM) Larisa Gabudeanu: yes

(4:08 PM) Erik Johnson: agreed

(4:08 PM) Larisa Gabudeanu: weekly calls would be great

(4:14 PM) Don M: Good discussion, have a fantastic day everyone

(4:14 PM) Nida Davis: Thank You!

(4:14 PM) Bev: Thank you!