2023-04-27 AIM TF Meeting Notes

Meeting Date & Time

- 27 Apr 2023
  - **09:00-10:00 PT / 16:00-17:00 UTC**

Zoom Meeting Links / Recordings

Meeting: https://zoom.us/j/98931559152?pwd=d0ZwM1JHQ3d5cXRqVTh4NlRHeVJvQT09

Recording: https://zoom.us/rec/share/N2v2FLqGxGk5itIcO7FSfSQSKkwC8JTLdzrvohD487Rq0UgqGWHYeiIniFoeD1Ur.P0RJQHTOYi4D-kio

Attendees

- Wenjing Chu
- Sandy Aggarwal
- Neil Thomson
- Daniel Bachenheimer
- Sumabala Nair
- @chang Lu

Main Goal of this Meeting

This is the AIM TF's #21 meeting.

One of our main goals is to have individual member presentations on what problems/challenges they see in AI & Metaverse related to trust.

Starting in the new year (2023), we plan to start drafting white papers or other types of deliverables of the task force.

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
2 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review	Chairs	• **Antitrust Policy Notice:** *Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws.* • ***ToIP Policy**: Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.* • ***ToIP TSWG IPR Policy:** see TF wiki page. AI & Metaverse Technology Task Force*

3 mins	• Introduction of new members • Any general announcement, news, that could be of interest to the TF	All	

30 mins	• IIW update
	• DeepFake attacks
	• Wallet + Biometrics + Liveness + OTP
		Daniel Bachenheimer
		Wenjing Chu
			• IIW presentation Wenjing Chu and attendee responses
			• Following up from last meeting's discussion -dive into the scenario of DeepFake attacks armed with a GAI agent and how we may protect against them.
			  ◦ We went through the recap email Mathieu wrote (to be published as a blog soon)
			  ◦ We then discussed two types of 'content' based attacks to authentication: Presentation and Injection. Presentation is easier to detect because it's hard to produce 3D synthetic models (and harder to scale). Injection attacks combined with an AI-enabled agent behind it may be the hardest challenge today.
			  ◦ Protection of injection attacks can be strengthened with an strong identity - EUDI, mDoc, KERI - common methods like biometrics or liveness tests can be emulated with sufficient publicly disclosed data, but these methods combined with a signature by a key in the wallet can be much harder. Dan mentioned sealing the camera inside a strong package. Wenjing mentioned C2PA allows camera's to sign photo at inception. Neal stated that not disclosing the private information is the the flip side of the same coin - confidentiality (or a form of 'zero knowledge' proof) would enable us to use more PII for authentication. Dan mentioned the current EU methods's PID and photo (or other content) be signed by an authority (like an issued credential). We also discussed the alternative way of issuing through mDoc e.g. different credentials for selective disclosure - i.e. another credential that stating a person is older than 21, rather than relying on new cryptographic algorithms/protocols.

10 mins	• Vivik Nair paper on unique identification of users by motion data in metaverses	Wenjing Chu	• We had Vivik Nair present their previous work in this area a few month ago. This is a follow-up and even more relevant research from the team https://medium.com/predict/privacy-in-the-metaverse-might-be-impossible-new-research-study-64935481c6de
	• Daniel Kang paper on zk-SNARK to DNN (inc. GPT etc)	@Matteo Midena	• This paper suggests it's practical to scale zk-SNARK to some DNN models: https://www.youtube.com/watch?v=S5RrlYjCjOQ

15 mins	White paper status updates	• Phil Wolff • Sandy Aggarwal • Wenjing Chu	Sandy Aggarwal reported the status of the gaming white paper and work in the LF mentorship program. Question on game engines, e.g. unreal, on emulating characters (non-playable character) - which is commonly programmed today. Wenjing mentioned this can be then enhanced to use GPT-like models for more intelligent behavior. The result can be a human-emulator which is the injection attack scenario we discussed in the agenda item above (DeepFake attacks).
	• Review decisions /action items • Planning for next meeting • AOB	Chairs	We ran out of time and will push the Vivik Nair paper and Daniel Kang paper to next time.