2024-02-29 AIM TF Meeting Notes

Meeting Date & Time

- 29 Feb 2024
  - **09:00-10:00 PT / 16:00-17:00 UTC**

Zoom Meeting Links / Recordings

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

Recording:

Transcript:

Attendees:

Neil Thomson

Eric Drury

Steven Milstein

Main Goal of this Meeting

Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
5 min	• Start recording • Welcome & antitrust notice • Introduction of new members • Agenda review • Assigning minutes taker	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. Please remember that TSWG2 has transitioned to a new IPR policy using OWF license.*
5 mins	• Introduction of new members • Any general announcements, news, that could be of interest to the TF • Last week's action items	All	• Last week's action items: update will be postponed to the next meeting. Both chairs are out of town traveling. • Except this action item is DONE. ◦ Present to the ALL Members Meeting on Feb 21. Watch its recording here: 2024-02-21 All Members Meeting Notes • Samuel Smith's dire warning during this week's 2024-02-27 KERI/ACDC Meeting Note ◦ We appear to have reached an inflection point of the success of cyber attacks. ◦ The arms race has tilted in the favor of the attackers ◦ Expertise in edge attacks... they have become much more sophisticated. ◦ The web is an excellent discovery mechanism but a horrible security mechanism. **ChatGPT4 Prompt: Please elaborate on Sam's concerns based on the following transcript:** 38 00:03:22.730 --> 00:03:29.470 Samuel Smith: Well, well, I'm gonna I'm gonna make an announcement. It's not really announcement. Sort of announcement. 39 00:03:29.690 --> 00:03:37.940 Samuel Smith: I've been monitoring more closely over the last few months the 40 00:03:38.410 --> 00:03:45.990 Samuel Smith: the ability of of hackers to attack infrastructure. and just 41 00:03:46.070 --> 00:03:48.339 Samuel Smith: anecdotally based on 42 00:03:49.360 --> 00:03:55.439 Samuel Smith: various new sources in the rate at which they're happening, and

43
00:03:55.700 --> 00:04:01.899
Samuel Smith: types of attacks and the the scope and scale of the attacks

44
00:04:02.150 --> 00:04:08.649
Samuel Smith: it it it it appears that we are in a inflection point

45
00:04:09.000 --> 00:04:15.580
Samuel Smith: where we're in the knee of a curve or just above the knee, where we've got

46
00:04:15.650 --> 00:04:19.860
Samuel Smith: an exponential increase in in successful attacks.

47
00:04:20.060 --> 00:04:21.940
Samuel Smith: And

48
00:04:22.010 --> 00:04:29.900
Samuel Smith: so we're I think we're in a new regime. The last 10 or 20 years. Last 10 years

49
00:04:30.490 --> 00:04:34.129
Samuel Smith: there's been a sort of a battle where.

50
00:04:34.530 --> 00:04:48.479
Samuel Smith: you know, there's sort of even, you know, people would protect their infrastructure. They'd there'd be little exploits. People would would patch them up. It's sort of an arms race just a gradual, steady arms race, but it looks like

51
00:04:48.610 --> 00:04:53.999
Samuel Smith: the the. It looks like the the attackers are now decisively winning the battle.

52
00:04:54.100 --> 00:04:58.999
Samuel Smith: So that's just my, that's just my announce. That's just my announcement

53
00:04:59.010 --> 00:05:01.160
Samuel Smith: that we're in a different regime now.

54
00:05:01.360 --> 00:05:04.519
Samuel Smith: And like likely to see

55
00:05:05.190 --> 00:05:08.330
Samuel Smith: even even even more serious stuff happening.

56
00:05:10.360 --> 00:05:11.900
Henk van Cann: we got a more

57
00:05:12.000 --> 00:05:14.559
Henk van Cann: may be a more positive announcement to.

58
00:05:20.660 --> 00:05:28.349
Rodolfo Miranda: I say, is it a specific reason why you think is is happening or method to attack?

59
00:05:28.810 --> 00:05:40.269
Samuel Smith: Yes, edge attacks now. So so the expertise in edge attacks. So if you look back about 5 years ago

60
00:05:40.720 --> 00:05:54.200
Samuel Smith: might be a little more most of the articles on security said that the the the front. The front line for security was the edge. That's where the vulnerabilities were is in the edge.

61
00:05:54.270 --> 00:06:06.799
Samuel Smith: The the the stupid things like SQL. Injection and tax, and and all of those stupid things that that people were able to exploit for for years. For the most part we're we're patched up anybody with

62
00:06:06.810 --> 00:06:16.420
Samuel Smith: any kind of a sense in it, knew how to knew how to protect their infrastructure from from those sorts of things, but but because of the way authentication is done.

63
00:06:16.710 --> 00:06:25.449
Samuel Smith: If you can attack the edge you can. You can. You can get in to the wall right? The authentication will let you in the wall.

64
00:06:25.530 --> 00:06:41.700
Samuel Smith: Lets you through the gate lets you through the perimeter. It that starts at the edge. Yeah. So so now we've got much more sophistication. It's taken a few years. But when you've got tens of thousands of people working for

65
00:06:41.740 --> 00:07:07.579
Samuel Smith: in the in many cases governments, that their job is just to figure out how to do edge attacks, and you and th that they've now figured out how to do edge attacks really, really well. And and the thing is is that the protection against edge attacks hasn't substantially changed. We're using the same mechanisms we were 5 years ago, and being a little bit better in your it. Security doesn't protect you because Edge, because of the nature of edge attacks.

66
00:07:07.770 --> 00:07:22.499
Samuel Smith: And you know, phishing is just one of the types of edge that social engineering. But there's lots of lots of little little things people do like. For example, the one I just posted in the link that that Phil found from Akron is is attacking domain names

67
00:07:22.750 --> 00:07:26.110
Samuel Smith: attacking

68
00:07:26.320 --> 00:07:45.620
Samuel Smith: see name records and stale domain names. Right? Just so. So. And Chat Gbt has now made edge attacks much easier, because now people who don't speak English as a first language can now write phishing emails that look

69
00:07:46.020 --> 00:08:10.870
Samuel Smith: and sound and feel not like some person who couldn't really speak English well, wrote them, but like it came from from the actual source. And so things like this domain attack. Now make phishing emails much, much easier, because now you can send an email that passes your Dkim, your Spf, whatever email protections you have that email looks like it came from the bank.

70
00:08:10.870 --> 00:08:30.620
Samuel Smith: Looks like it came from Semantic the names of the the hackers. There you got semantic, Macafe vmware, you know. You're going, hey? You know my security provider, the one that is securing my infrastructure sent me an email, and that when I look it up it is their email address. And so it must have come from them. I didn't come from a hacker, right? So

71
00:08:30.630 --> 00:08:43.780
Philip Feairheller: so so you know, just just just those sorts of things. Yeah. And you know, this might be a really good II just added it to future topics. We we could fill a whole discussion 25 min with it. That'd be a really good, I think, a really good time.

72
00:08:44.210 --> 00:08:47.550
Philip Feairheller: Yeah. So so here's here's my little soapbox.

73
00:08:48.190 --> 00:08:55.620
Samuel Smith: The web is a fantastic discovery mechanism. It's a horrible security mechanism. And I mean, Dns.

74
00:08:55.750 --> 00:08:59.810
Samuel Smith: so any identity system

75
00:09:00.150 --> 00:09:06.290
Samuel Smith: that doesn't have a root of trust stronger than the web to just use the web

76
00:09:08.150 --> 00:09:09.550
Samuel Smith: and

77
00:09:10.320 --> 00:09:11.980
Philip Feairheller: because

78
00:09:12.480 --> 00:09:15.210
Samuel Smith: this what's the point? Right?

79
00:09:15.430 --> 00:09:32.590
Samuel Smith: And and and I'm I'm pointing this at the at at at any did method out there that is web based is what? Why, the web's already better discover mechanism that did ever will be. So just use. Just use the web if you're not going to be more secure than the web. Just use the web.

80
00:09:33.610 --> 00:09:36.799
Samuel Smith: If, anyway, that's my soapbox.

81
00:09:37.490 --> 00:10:01.519
Philip Feairheller: Alright when you said Web, you you meant web for discovery and security. But yeah, like, did Webex uses the web, which is great, but only for discover, only for discovery. That's right. But but if you have an identity system where your root of trust is the web that then you're using the web for security and discovery, because that's your route of trust. Right? That's what I meant by when I said, root of trust.

			82
			00:10:03.090 --> 00:10:04.000
			Samuel Smith: Yep.
			
			83
			00:10:04.900 --> 00:10:15.770
			Samuel Smith: so don't use the web for security. You can use it for discovery. And if all you're doing is using, if you're using the web. For if you're using something else for security.
			
			ChatGPT 4 Response:
			
			Sam Smith expresses several key concerns regarding the current state of cybersecurity:
			
			1. **Inflection Point in Cyberattacks:** Sam observes that we are at an inflection point, experiencing an exponential increase in successful cyberattacks. This indicates a significant shift in the cybersecurity landscape, where attackers are becoming more effective in breaching defenses.
			
			2. **Edge Attacks**: He specifically highlights the growing sophistication of edge attacks, where attackers target the perimeter of networks (the "edge") to gain access. These attacks exploit vulnerabilities in the authentication process, allowing attackers to bypass security measures and infiltrate networks.
			
			3. **Outdated Security Measures**: Sam points out that the mechanisms to protect against edge attacks haven't substantially changed in recent years. He argues that being slightly better in IT security is not enough to protect against these advanced threats, as the nature of edge attacks requires more innovative defense strategies.
			
			4. **Phishing and Social Engineering:** The use of AI tools like ChatGPT has made phishing emails more convincing, as attackers can now craft messages that appear legitimate and are difficult to distinguish from genuine communications. This increases the risk of individuals falling victim to these scams, further compromising security.
			
			5. **Domain Name Attacks:** Sam also mentions attacks targeting domain names, such as exploiting stale domain names and CNAME records. These tactics can make phishing emails appear even more authentic, as they can pass through email protections like DKIM and SPF, making it seem as though the emails are coming from trusted sources.
			
			6. **Trust in the Web for Security:** Finally, Sam criticizes the reliance on the web as a root of trust for security. He argues that any identity system that depends on the web for security is inherently flawed, as the web is better suited for discovery rather than providing a secure foundation for identity verification.
			
			Overall, Sam's concerns highlight the evolving nature of cyber threats and the need for more robust and innovative security measures to protect against these increasingly sophisticated attacks.
			
			Related:
			
			▪ Also discussed at 2024-02-27 KERI/ACDC Meeting Note
			  ▪ 8,000+ Domains of Trusted Brands Hijacked for Massive Spam Operation
			▪ Eric Drury on Slack
			  ▪ Alibaba just published a new paper showing AI generated expressive talking head portrait videos using a single image and a soundtrack. They go directly from audio to video synthesis, bypassing the need for intermediate 3D models. Check out the videos in the link below. https://humanaigc.github.io/emote-portrait-alive/

45 mins	What is RAG? Introduction and discussion.	Steven Milstein	• Steven Milstein will give an introduction and lead a discussion around RAG (Retrieval augmented generation). • Savita Farooqui can't join this time and offered to share her thoughts in a future meeting.

5 mins	• Review decisions /action items
	• Planning for next meeting
	• AOB
		Chairs	NEW ACTIONS from the previous meeting postponed to the next meeting.
			
			• Update draft Authentic GAI Proposal:
			  ◦ Update the proposal : https://docs.google.com/document/d/1Snga-dkUG0XaLaXx1q9FKojaFy42CTZhvyFJbo9KgLU/edit document with updated screenshot and use it to communicate with other groups in ToIP, DIF, CA, C2PA
			  ◦ Revised - need to expand to a short white paper.
			• Potential to present to All Members Meeting 21 Feb
			  ◦ Reached out to Eric Scouten
			  ◦ DONE.
			• Wenjing Chu to present to Steering Committee Meeting next week
			    ▪ Postponed to next week
			• Each of us thinks of a few use cases for the above proposal. This will give us guardrails on the scope.
			  ◦ We will discuss these use cases starting at the next meeting.
			  ◦ As part of the use cases, we can discuss more about what is not in scope.

Screenshots