IoT Security Foundation Executive Steering Board
Follow-Up Notes and Actions From
Thursday 12th Sept 2024, Physical Meeting

***"Success breeds complacency. Complacency breeds failure. Only the paranoid survive"* Andy Grove, Intel**

0 Agenda

1. Roundtable perspectives on relevant/contemporary matters
2. Strategy workshop
3. Conference key messages and panel session
4. AOB
5. Next Meeting

0.1 Attendees

Stephen Pattison (SP), John Moor (JWM), Sarb Sembhi (SS), Nick Allott (NA), Tim Snape (TS), Carsten Maple (CM), Peter Davies (PD), Anna Maria Mandalari(AMM), Richard Marshall (RM), Chris Bennison (CB)

0.2 Non-attendance for ESB meeting

Darron Antill (DA), Haydn Povey (HP), Ben Azvine (BA), Ken Munro (KM)

Note: apologies in advance from DA 'on holiday', HP 'late health appointment'– provided written input.

These notes to be read in conjunction with slides '50 ESB Strategy Sept 2024.pdf' and 'IOTSF Strategy Paper for ESB.pdf' – available on basecamp: IoTSF ESB Communications > Docs & Files

0.3 Thank You AMM and UCL

A special thank you to Anna for hosting us in London at UCL and providing a buffet lunch and refreshments.

1 Roundtable perspectives on relevant/contemporary matters

Due to time constraints, we did not do an activity update as usual but focused on the strategy discussion. See '4 AOB' for actions update carried over from last meeting.

Perspectives were shared amongst those attendants which fed directly into the strategy session.

On-going challenges with regulation – especially PSTI, CRA and RED – NIST CF2 also relevant. Further underlining the relevance of the IoT Security Assurance Framework as a practical tool for satisfying/demonstrating compliance. The need for simplicity, lower costs and automation was echoed in numerous comments to help OEM's.

A view was expressed that it is impossible to comply with CRA and pragmatism is a trend over cyber regulation. It was stated – from experience - that the EU is looking for the spirit of the law – 'unlikely to get a fine but expected to improve' but also that 'lies will get punished'.

Further, 'money is all' and companies need to be 'secure with perspective' – best practice is contractual yet harms such as threats to life or physical safety is a different paradigm and 'you can't use common criteria in criminal cases'. Business continuity and insurance are of greater interest. Costs for compliance must be brought down.

Once again, it was noted that "IoT" is losing its shine for some – but not all - and the 'next practice' work that IoTSF is engaged in remains contemporary (AI, PQT, zero trust environments etc).

2 Strategy Workshop

SP reiterated the need for IoTSF to maintain its relevance and "digital security is not going away" however, "only the paranoid ~~survive~~ thrive" (JWM's modification).

SP posited that we should look at 'three words":

1. Resilience
2. Transparency &;
3. Supply Chain

Q: Would IoTSF only survive because of the threat of litigation?
A: The consensus was that regulation is only one area that IoTSF supports – indeed, there are more important/valuable areas for our members/stakeholders beyond regulation.

In the round-table discussion, it was also expressed that 'legislation is for bottom feeders' w.r.t to what we might focus on in the future. The Assurance Framework (AF) has proven its worth, but more value could be derived – especially if it can be linked to procurement. If we could achieve this link, it would create a strong membership proposition.

NA will produce a strawman strategy for how we might proceed on this front.

Q: Should we lobby Government?
A: A qualified 'yes'; if members want it and their views are represented.

We may reappraise how we position ourselves with respect to Brussels and the UK Government – we have good links to US NIST, CISA and forging links into FCC (re: labelling). We should consider publishing policy papers with the intent of (a) influencing policy and (b) being seen as an expert group that understands the business implications beyond first-order effects (i.e. nuanced).

In summary

- Develop the Assurance Framework and use to (a) engage more stakeholders (b) be central to procurement
- Develop plans to engage EU/UK at the policy level

What was not discussed, yet worth including/retaining here as it has been discussed prior

- How IoTSF can help members with publicly funded projects (and be a partner).
- This was an item carried over from 25th January meeting.
- This is being worked on with colleagues across TechWorks – activity is happening, nothing significant to report just yet however 'watch this space'.

3 Conference key messages and panel session

JWM asked for volunteers to join a panel at the IoTSF Conference discussing IoT Security.

SP/AMM/PD/RM & HP will join a panel to discuss the work of IoTSF – where we have come from, where we are now and what we see ahead.

4 AOB

None for this meeting.

Action updates carried over from last meeting:

2.1 10th Annual Conference
ACTION: JWM to follow up as necessary.
In progress / complete

3.1.2 SEMI Collaboration/Partnership
ACTION: JWM to continue the discussions and report back as necessary.
We are changing the way we publish the Assurance Framework hence are changing our approach to partnering with SEMI.
JWM has been invited to speak at Semicon Europa (Munich) on Nov 12th and will give a talk raising awareness and promoting the Framework

3.1.3 CSA Collaboration/Partnership
ACTION: JWM to determine how best to proceed and determine the legitimate basis for any liaison and joint working with help from ESB as necessary.

JWM presented to the CSA's Product Steering Committee on July 19th with an intro to IoTSF. We have positioned IoTSF as a leader, as a pre-standards body, a forward-thinking organisation and a natural partner to CSA. No immediate/further action is necessary at this stage.

4 Projects: Does the UK Government understand the strategic significance of SBoMs to the domestic industry?

ACTION: SP, TS, NA and JWM to form a project team to determine the issues, messages and identify who to reach out to in UK Government.

Several conversations have happened in the interim – SP has spoken to NCSC CTO Ollie Whitehouse and several other conversations with NCSC, DSbD and DSIT have highlighted SBoM's potential. An event at Kellog College Oxford, as part of our TAIBOM project is intended to take this further: see https://www.techworks.org.uk/event/taibom-workshop-assuring-systems-integrity-for-ai-and-software

JWM comment: Perhaps we should publish a policy paper on this subject?

5 Next Meeting

JWM posited meeting dates as either:
Dec 4th London – pre-TechWorks annual dinner OR 21/22/23 January.
It was suggested/agreed that we should first have a virtual meeting shortly after the IoTSF conference to review opportunities that arise.

ACTION: JWM to send calendar invites for virtual meetings.

- Nov 6th 2 pm
- Jan 23rd 2 pm

5.1 RETAINED WORDING AS AIDE_MEMOIRE

There have been some issues with some members of ESB not receiving calendar invites
ACTION: All ESB members to manually put a note in their diaries as a precautionary measure.

Please note that the Basecamp calendar is kept up-to-date as a fallback option.