SIRTFI Exercise Working Group End of 2023 Report

Repository ID: TI.173.1
Persistent URL: http://doi.org/10.26869/TI.173.1
Publication Date: November 28, 2023
Author: Kyle Lewis, SIRTFI Exercise Working Group (SEPWG) Chair
Sponsor: InCommon Community Trust and Assurance Board

Summary

In 2023, the SEPWG planned and conducted InCommon's second annual community Cybersecurity Cooperation Exercise, focusing on the Sirtfi framework. Fourteen organizations from the InCommon Federation volunteered to participate, in addition to the Australian Access Federation and the Research and Education Advanced Network New Zealand (REANNZ). In November, the SEPWG conducted the exercise with the participating organizations. Post-exercise feedback was positive, with a consistent desire to do more of this again. The bottom line recommendation is to re-charter the SEPWG for 2024 to evolve the learning activities and continue to give member organizations the chance to practice using the Sirtfi framework.

Details

The SEPWG was formed to provide federation member organizations' security teams opportunities to practice using the Sirtfi framework to facilitate communication and coordination during cybersecurity incidents.

The SEPWG adopted a three-phased approach, plus a "Phase 0" preparatory step for the working group.

During Phase 0, the SEPWG walked through a basic script to practice how to run an exercise and get an understanding of how participants would play in the exercise. Upon completion of Phase 0, SEPWG requested InCommon send a call for participation.

Sixteen organizations volunteered interest, remained engaged, and successfully participated in Phases 1 through 3 (detailed below):

- Australian Access Federation
- Cal Poly San Luis Obispo
- National Institute of Allergy and Infectious Diseases (NIAID)
- National Institutes of Health (NIH)
- NDSU North Dakota State University
- Nevada State University
- Nevada System of Higher Education - SCS
- Research and Education Advanced Network New Zealand
- Rice University
- UNC-Chapel Hill
- University of California, Irvine
- University of Illinois at Urbana-Champaign
- University of Missouri
- University of Nevada, Reno
- University System of New Hampshire
- West Virginia University

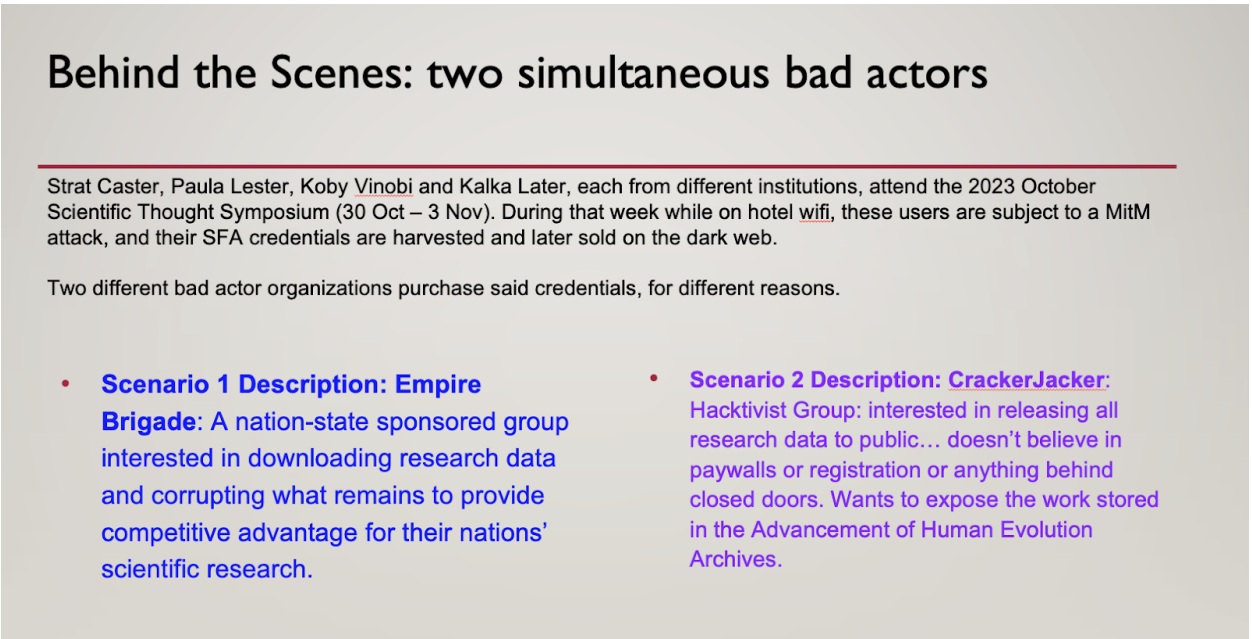
For **Phase 1**, the SEPWG conducted a communications test. The SEPWG used the POC's submitted entity IDs to look up each organization's Security Contact. Phase 1 consisted of the SEPWG sending emails to each Security Contact requesting acknowledgment. For those

that did not respond, the SEPWG followed up with the respective organization's POC. Most organizations responded within a few hours.

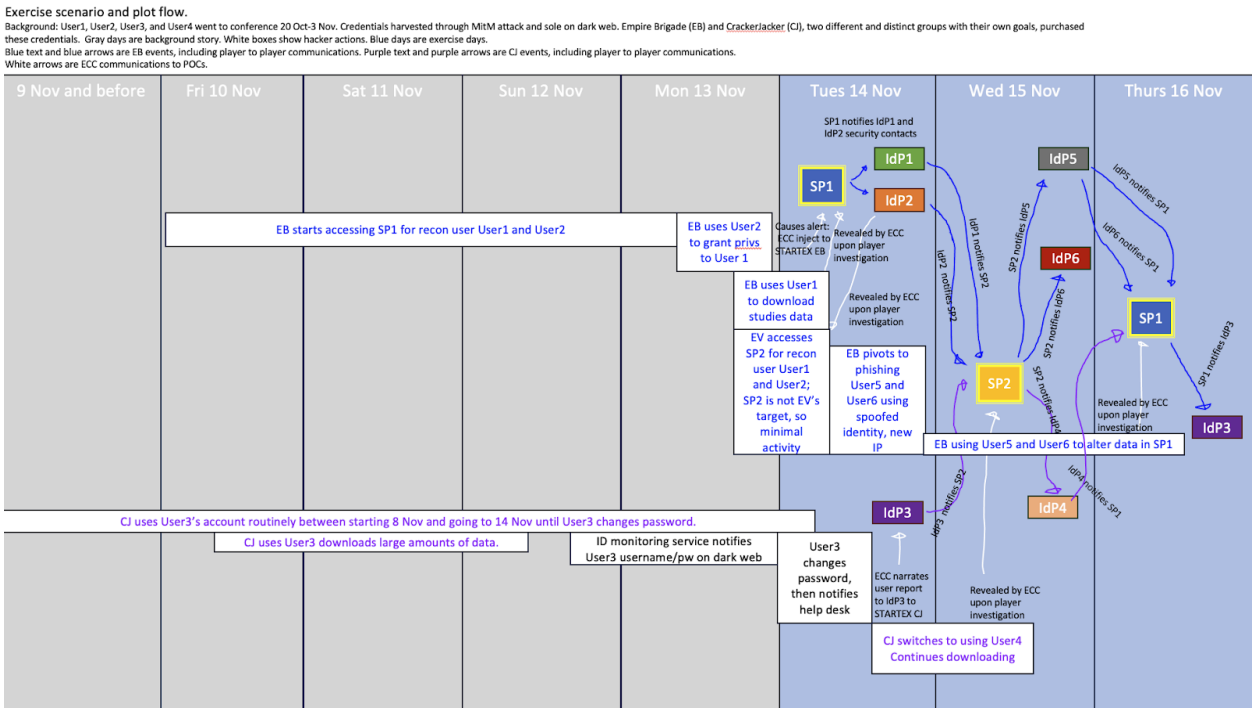
Phase 2 consisted of training all the organization's exercise POCs on how the exercise would be orchestrated, and their respective roles.

Phase 3 consisted of the actual exercise, 13-17 Nov 2023. It was a 3-day scripted event starting on Tuesday and ending on Thursday. It was book-ended by a kickoff session the Monday before the script started, and a wrapup session on Friday.

Phase 3 improvements this year included a more narratively rich 'backstory' and a more complex exercise flow. Instead of a serial SP to IdP to SP to IdP chain of events, we had multiple IdPs handling parts of the scenario in parallel, two different simulated bad actors acting simultaneously, and SPs handling multiple inputs from different IdPs as the same time, forcing them to stretch their Event Response Controller skills.



The narrative flow and backstory "storyboards" that guided script development are illustrated here, which were shared with the participants at the wrapup:



The sixteen organizations were divided into two groups of 8. The SEPWG ran two concurrent tabletop exercises, with 2 Exercise Controllers overseeing each. Three of the four had never done this before, providing exercise design and exercise conducting experience to SEPWG members that they can now take back to their respective organizations.

This year, about 50% of the participants remembered to notify InCommon security of the (simulated) security breaches. This year saw participation from the InCommon security lead in both the SEPWG and during the exercise.

All files, to include the exercise scripts, training, kickoff and wrapup presentations, out-brief at TechEX, and documentation on the phased methodology is recorded in the SEPWG online folder, and available for future planning teams.

Specific feedback from the SEPWG ECC and exercise participants was recorded in the wrapup session slides, and attached in Attachments 1 and 2. There was a consistent desire to participate again next year.

Takeaways

Feedback this time included feedback from security teams stating “This was valuable; I was not aware of the IAM world, and this has exposed our team to this aspect.” This reflects InCommon’s goal of increasing federation-mindedness in those security teams who participated and increasing security-mindedness in the IAM teams involved. Finding security contacts is not always straightforward; if given an entity ID it’s easy if you know the tool; some players looked up security contacts by organization names and got the wrong security team (some Universities and govt organizations have multiple IdPs and SPs registered, with different security contacts). Some feedback mentioned they operate an “SP Proxy” with multiple SPs behind it.. might be worth discussing more.

(Full feedback is detailed below in Attachments 1 and 2).

Recommendation

Recommend CTAB send out another call for volunteers for an SEPWG kickoff in Jan 2024, and re-charter the group. Call for volunteers would also be forwarded directly to last year’s exercise POCs from the volunteering organizations to get the word to this year’s players who expressed interest in helping next year.

Attachment 1: ECC feedback from SEPWG perspective

Overall:

- Well done! All completed the objective actions
- Many were responsive and did not require prompting
- Many teams took full 3-4 hours to do internal reviews of security procedures/teachable moments including investigating techniques before reaching out to ECC for answers

- Some IdPs/SPs have chosen to use “external” email addresses/aliases in their metadata, e.g. cloud IdPaaS security contact. Some use an internal mailing list/contact that is not shared between IAM and security teams.
- Discoverability of contact info is challenging. MET tool doesn’t always give useful search results (e.g. search for “New Hampshire” and you get 0 results), and security contacts display as “other” contact. Searching for entities via InCommon’s website doesn’t always surface multiple IdPs that are registered under a single organization

- Next year instruct players to only use security contacts found with in-game provided entity IDs (ref: Cirrus Identity being contacted
- Keeping track of who is where in the narrative can be challenging with so many players. Fewer players could make for simpler coordination, but could also diminish the value of the federated exercise.
- next time we need to formalize timestamps for injects to be UTC so there's no confusion between UTC and EST and local time for the participants
- scenario. The author needs more help next year making sure injects at the end scenario are as richly detailed (e.g., timezones) as they are in the beginning: seeking script reviewers to please look out for timestamps etc..
- add intel updates to script (about hacker organizations)... provide clues that if they remember to notify InCommon federation, the federation operator can put the story together and provide such information to the affected parties
- injects that are timed where one player sends to another, and that's supposed to trigger a simultaneous ECC inject (like when going from SP2 to IdPs 5 and 6 on day 2) are too variable as written; about half the players didn't put the two inputs together and acted on the ECC inject. This resulted in some IP addresses not getting passed from player group to player group

Attachment 2: Participant feedback during wrapup session

- NIAID IBRSP: thanks to all participants; your participation made our infosec processes better; improvement points: being more specific in info being passed along; request for ISO format/UTC based to keep us all straight; for next year, we want to include other groups internal to our organization that this time we simulated as NPCs; fantastic community learning experience
- Rice University: echoing what NIAID said; the narrative was useful; we activated our full incident response team; new team members got training on our response plan; next year we're going to expand internally to a larger IT drill with other departments, such as legal, public affairs, etc; last year was good but less informative; this year was better
    - Each day, possibly have end of day summary for those who have 'already gone' so they can see the story progression
    - Send out injects regardless of whether people have come across that information or not...

- NSHE: our construct is that our office manages multiple communities/IdPs; we'll be using this to prompt us to look at how we figure out our own internal communications lines; very helpful exercise
- UNC-Chapel Hill: fun to be an edge case; thanks for putting this together; helped get our arms around the federation piece of this; The scenario allowed for interesting things to happen; for those on IAM became more aware of our security incident response processes; achieved InCommon's goal to have security and IAM be more integrated and aware of each other;
- Cal Poly: we identified when one of our primary participants was out of the office, we had to fill in and we misread one of the injects; internally we learned to focus on the inject and the details
- AAF: incredible experience; thanks to InCommon for organizing it; helped our new members get exposure to federation security cooperation; helped all members deep dive into our internal response plan
- REANNZ: Wasn't sure what to expect; learning how to do an exercise; gave us a view into our processes; got our security team to play and discuss the scenario; for the federated side, emphasized the importance of having security contacts to publish to metadata!
- U of CA Irvine - We went to the POC training, but once I got into the game my mind simplified it and once we got the inject, we did our investigation and sent emails to both users' contacts we were investigating; brought in SECOPs team to go over the scenario with us; reviewed checklists; got an email from another group that was confusing at first... treated it as a notification vs investigation... overall, good experiment to through; I work on security team so this was good exposure to IAM, and created conversations between security and IAM teams