Mutual Monitoring Update

Progress Report 3

A.J. Stein

astein38@gatech.edu

Problem

- Cloud service providers are everywhere, but their security is complex.
- Continuous monitoring is complex, tedious multi-party process.
  - FedRAMP is a very public example.
- Everything is manual.
- Information flows in one direction, not to everyone who needs it.
- Is there a better way?

Solution

- Examine FedRAMP as a representative example.
- Re-imagine a new system with:
  - a new technological approach; and
  - change the process and how people interact.
- Estimate improved cost and performance.

Solution Deliverables

🎁 1️⃣ Critical analysis of FedRAMP

🎁 2️⃣ Architecture specification

🎁 3️⃣ 🤷 Prototype code for mutual monitoring transparency service 🤷‍♀️

🎁 4️⃣ A quantitative cloud security measurement framework

💥 🔍 Evaluation results

4

Status

- 🎁 1️⃣ I completed more desk research and fleshed out my deliverables' outline.
- 🎁 2️⃣ I completed a full draft of architecture specification.
- 🎁 3️⃣ I had to quickly write scripts to dump all data from the FedRAMP modernization forum.
- 🎁 3️⃣ I worked on the critical analysis of FedRAMP to complete in the next day or so.
- 💥 🔍 Publish survey to request interviews with stakeholders for final evaluation.

Status

- After less than 24 hours, nine legitimate (and one fake) volunteers.
- Current sample of volunteer has even distribution of relevant stakeholder backgrounds.
- Hopefully more to follow!

When it comes to FedRAMP, I have experience working
10 responses

Copy chart

Category	Count
in the FedRAMP Program Management Office (PMO).	5 (50%)
in a FedRAMP-authorized cloud service provider (CSP).	6 (60%)
in a Third Party Assessor (3PAO) advising or assessing FedRAM...	5 (50%)
in a government agency, a CSP customer who sponsored or ap...	5 (50%)
somewhere else, but I think it is relevant to FedRAMP.	3 (30%)
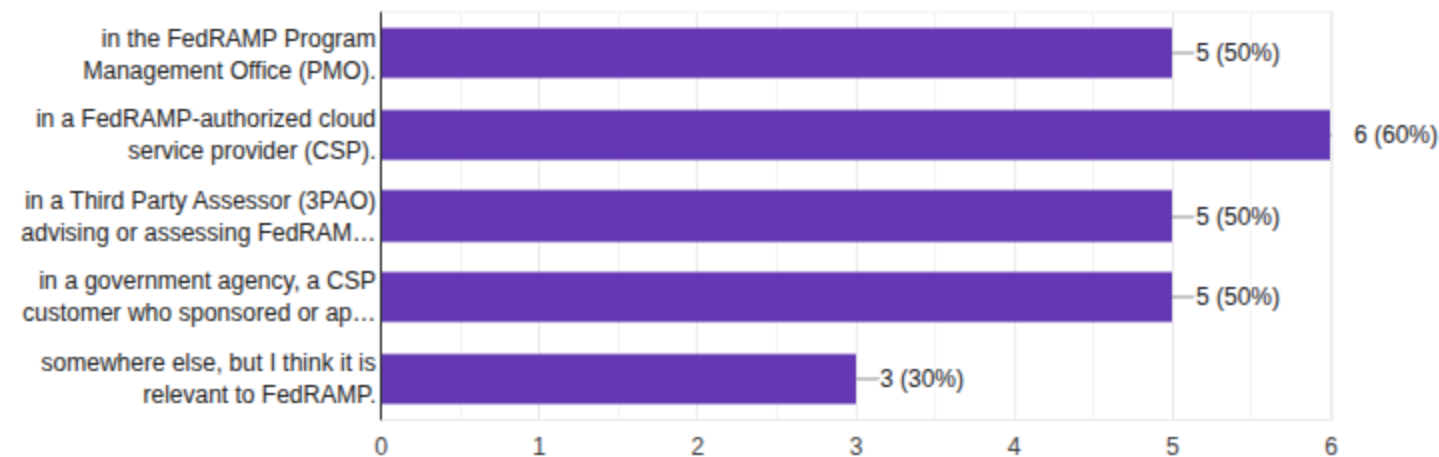
Challenges

- Interpreting specs from other use cases for mutual monitoring
- Finding transparency service data
    - model resource requirements
    - compare model of transparency service for mutual monitoring use case
- Fake volunteers with profane names registering for evaluation interviews

Questions

1. Can I deprioritize 🎁 3️⃣ the prototype & focus on 🎁 1️⃣ the specification?

2. I will interview stakeholders, what **must** I publish with the final paper?
   - interview methodology?
   - interview questions?
   - detailed (but properly redacted) interview notes?

3. How do I cite conversations in private Slack channels with developers that make transparency services, but for different use cases than mine?

Next Weeks' Focus

1. 🎁 1️⃣ Finish FedRAMP critical analysis, get advisor feedback, polish.
2. 🎁 2️⃣ Update the architecture specification, pending advisor feedback
3. 🎁 3️⃣ 🤷 Reduce scope or stop prototype development. 🤷
4. 🎁 4️⃣ 🤷 Create the quantitative cloud security measurement framework.
5. 🎁 🎯 Finish outline of final paper, get ready for the end.

Feedback

- You can provide feedback in multiple ways.

- Post in the class discussion board in Canvas.

- Open issues in my GitHub repo at github.com/aj-stein/practicum/issues.

Conclusion

Et fin.

(See you all again in two weeks.)