FAA ERAM Outage Case Study

Bastian Tenbergen

April 2021

FAA ERAM Outage

Background

Air traffic control in the United states is a major undertaking, comprising over 600,000 licensed pilots, more than 2,500 flights at any given moment, which may merely enter US air space or arrive and depart from one of the US' 19,000 active airports. Nearly 600 air traffic control centers supervise regular air traffic procedures using what is known as the National Airspace System (NAS).

To optimize NAS functionality, a paper-based legacy system was replaced in a tiered process between 2006 and 2009 with ERAM – En Route Automation Modernization, a system developed by Lockheed Martin to provide "fast processing of route requests and flight route changes."

Case Study Overview

In 2014, a military surveillance aircraft filed a flight plan that exceeded the complexity of typical flight plans of passenger and hobby aircraft and did not contain a cruise altitude. After an air traffic controller manually entered an altitude of 60,000 – the typical altitude of surveillance aircraft – ERAM began to search for possible routes across all possible flight levels that do not conflict with other filed flight plans. Albeit details on the search algorithm remain unavailable to the public, the search soon exceeded available computer memory, causing ERAM to continually restart and retry the search.

While this issue is primarily related to Software Testing, this case example brought up immediate concerns about security vulnerabilities, as evidently manually entering a single value could cause the system to fail repeatedly.

Student Instructions

This case study investigates the relationship between Software Testing and Cybersecurity Governance.

1. Explain the relationship of Software Testing and the failure experienced during the ERAM outage. You may want to research "equivalence class testing" or "specification based testing techniques". Explain the purpose of equivalence class testing, the procedure, and demonstrate how it could have prevented this particular failure.
2. Investigate official DoT, FAA, and GOA reports and determine failures in cybersecurity governance. Describe the security vulnerabilities found in the ERAM case example, organizational structures that led to them, and recommended actions to mitigate them.

Instructor notes

This case study may be assigned as an individual or team exercise, either in synchronous or asynchronous educational settings. A proven strategy is "Think-Pair-Share": use a similar CyBOK case study (Wilson et al. 2018) to discuss CyBOK KAs in class, then group learners into small teams of 2-3 and ask them to solve this assignment. Then, in a following class meeting, have teams present results and discuss implications.

Since this case study represents a concrete example of mismanaged software acquisition, it is a rich resource that allows investigating supple chain risk management and cybersecurity in a broad manner. For this purpose, the above tasks are kept rather specific to give students a narrow scope in which to apply theoretical knowledge in supply chain risk management and cybersecurity that should be introduced to them in a structured fashion before assigning this case study.

Students should be encouraged to learn as much as they can about this case example to absorb the perils of improper supply chain risk management and cybersecurity incident response by means of a real-world project. The formative task of related Software Testing aspects is intended to apply knowledge students may have from Software Verification knowledge areas of other curriculums, such as ACM CC 2020.

Example solution

1. Explain the relationship of Software Testing and the failure experienced during the ERAM outage.
    a. Specification based testing means testing a software based on required inputs and guaranteed outputs specified in some type of reference document (e.g., documentation, requirements)
    b. Equivalence class-based testing is an example of a specification-based testing technique, where rather than executing every possible combination of input parameters, representatives are picked from intervals possible input ranges, allowed by the specification.
    c. Units are executed with these representatives as example inputs and the unit outputs are compared to what the specification prescribes.
    d. In this case, the "altitude" parameter during manual entry should have been tested against typical, extreme, and impossible values (e.g., "18,576", "95,001", and "-500,000", respectively) in a manner compatible with boundary value analysis to ascertain proper behavior.
2. Investigate official DoT, FAA, and GOA reports and determine failures in cybersecurity governance.
    a. The GOA report lists quite clearly the key issue was unclear roles in incident response, lack of roles and responsibilities wrt. security incidents, and unclear incident response procedures along with lack of role-appropriate training for the involved officers.

References

Wikipedia: “ERAM”, online resource available at: https://en.wikipedia.org/wiki/ERAM, accessed 30 Mar 2021.

Scott, A.; Menn, J.: “Exclusive: Air traffic system failure caused by computer memory shortage,” online resource available at: https://www.reuters.com/article/us-airtraffic-bug-exclusive/exclusive-air-traffic-system-failure-caused-by-computer-memory-shortage-idUSBREA4B02320140512, 2014. Accessed 14 Mar 2021.

Storm, D.: “$2 billion air traffic control system failed by running out of computer memory,” online resource available at: https://www.computerworld.com/article/2476246/-2-billion-air-traffic-control-system-failed-by-running-out-of-computer-memo.html#:~:text=It%20was%20a%20shortage%20of,be%20delayed%20on%20April%2030, 2014. Accessed 14 Mar 2021.

Hampton, M: “FAA Has Taken Steps to Address ERAM Outages, but Some Vulnerabilities Remain.” US Department of Transportation Report Number AV2019004. Available at: https://www.oig.dot.gov/sites/default/files/FAA%20Actions%20to%20Address%20ERAM%20Outages%20Final%20Report%5E11-07-18.pdf, 2018. Accessed 14 Mar 2021.

Wilshusen, G.; Barkakati, N.; Dillingham, G.: “FAA Needs to Address Weaknesses in Ait Traffic Control Systems.” US Government Accountability Office Report Number GAO-15-221. Available at: https://www.gao.gov/assets/gao-15-221.pdf, 2015. Accessed 14 Mar 2021.

Jones, T: “Fact Sheet – En Route Automation Modernization (ERAM).” Federal Aviation Administration resource available at: https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=7714, 2020. Accessed 14 Mar 2021.

Guru 99: “Boundary Value Analysis and Equivalence Partitioning Testing”, online tutorial available at: https://www.guru99.com/equivalence-partitioning-boundary-value-analysis.html, accessed 30 Mar 2021

Wilson, K.; Brickman, P; Brame, C: Group Work. Life Sciences Education 17(1), 2018.