Software Challenge Case Study Proposal – Team-G

Note: This is an imaginary case study proposal. Hence some imaginary timelines and organisation names have been referred.

1. Background

In recent years, Smart Metering and Smart Grids became one of the hottest subjects in Engineering. Many reasons, including increasing productivity, increasing reliability, reducing emissions and using sustainable energy sources can be named as incentives for Smart Metering.

Smart Grid is a combination of electrical grids, communication networks, hardware, and software for measuring, monitoring, controlling, and managing the generation, transmission, distribution, storage, and consumption of energy. A smart meter serves as the heart of Smart Grid, processing the end results, and sharing the information related to usage patterns with the concerned parties. But, designing and maintaining such a system was of a great challenge. In our Case study, we would like to highlight one of what key decisions were taken to overcome the hurdles.

2. Design Challenge

Unlike a dumb meter that doesn't communicate, a smart meter is always connected and possesses a risk of numerous vulnerabilities. In the year 2000 at California labs, while drafting the smart metering grid design architecture for the Unites States, a single layer security design was proposed between each party for the exchange of messages. The business process was to exchange public and private keys which served as an identifier for incoming messages. However, very soon in 2002 during the trial runs in a mocked environment, it became evident that there are several loopholes and the overall design is prone to cyber threats. Recognizing and eliminating such loopholes before any security breach happens was very essential.

Although the design was functionally capable, during the Penetration testing, it was identified that using brute force attack, the testing team was able to pull hourly usage patterns from the smart meter. This possess a threat as sensitive information is being leaked. This is dangerous because the attacker can process this data and obtain usage patterns, an easy way to attack a house for theft and robbery. This issue halted the implementation until there is a discussion and agreement of a clear way forward. Particularly this was more challenging considering the fact that it was being implemented for the first time and the industry lacked experts.

3. Decision Points

An immediate meeting was called between the System Architecture Engineer, Security Architecture Engineer, Security Team developers, Security Test team, Project Manager, Programme Manager, Infrastructure support team and Release Manager. The situation was clearly discussed and understood. It was agreed to have additional layer of security implemented on top of existing security certificate authentication to prevent the hacking attacks. However, it was unclear as to how this could be achieved as business was very adamant on Go-live date. Both System Architecture Engineer and Security Architecture Engineer have agreed to work in pair for the next 3 weeks to agree on best suitable methods which will add the additional security without overriding the current Architecture (as that could lead to a lot of rework and end up delaying the project timelines significantly). In meantime, both Project Manager and Programme manager have agreed to have a separate discussion to have a discussion with Project driving group to bring in additional budget to have the agreed changes implemented.

After 3 weeks, based on several discussions with various teams there were three key decisions made regarding the additional security implementation. Those were Implementing:

- Secure on-chip memories
- Cyberattack-detection mechanism
- Embedded Firewalls

The same group have gathered again where the proposals were put forward. The agenda of this meeting was to finalise the next steps. As, Programme Manager has already requested the Security Architecture Engineer and his team to come up with effort estimate, they have proposed the following:

Design Implementation Decision	Man Day Effort	Description
Secure on-chip memories	100 Man-days	These can be locked and encrypted making it difficult for the attacker to read or reverse engineer the software.
Cyberattack-detection mechanism	120 Man-days	Implementation of this to smart meters will detect when it gets compromised
Embedded Firewalls	600 Man-days	Embedded firewalls can limit communication only to known trusted sources and before even initiating an attack.

The Man-day efforts were proposed after the fair negotiation within the team and hence were very realistic. Security Architecture Engineer (SAE) further explained that based on his teams' investigations, there is no single solution to the problem as a security threat can be of any nature and hence, they believed that all three security designs have to be implemented. However, Programme Manager was not ready for this as he has got budget approval only for 220 Man-days (220 x $500 = 110K). It became a debatable situation as SAE was not ready to compromise on dropping any of the implementation. Further SAE raised that with his current teams' capacity, he will not be able to achieve all three and suggested either hiring additional resources or outsourcing.

Project Manager was silent during this debate situation as he was constructing a plan within his mind. Finally when discussions were going in cross paths without a conclusion, he started.

He explained that in summary, we have the following problems:

- SAE suggests implementing all 3 security requirements which is a combined 820 Man-days effort
- Current Go-live date is unchanged; The whole release is expected to go to production in 2 Months
- Security Team has only 50 Man-days as spare capacity.

Based on the situation, he suggested the following decisions:

- Let's not compromise on Security, if an expert in the area is suggesting something based on his findings, we need do it.
- As we do not have a spare capacity, we need to look for alternatives. This will be outsourcing as we won't be able to hire developers now and get their clearances sorted in this short span.
- For the previous release, we have worked with Tampa Bay Consulting, which did a great job. They charge us Fixed Price which will be far less (Based on previous collaboration experience)
- Hence, Let Embedded Firewalls be outsourced to Tampa Bay Consulting. And that would be around $50k
- For the "Secure on-chip memories" implantation, we are left with budget but are lack of spare capacity. Let's have an additional working day as OT. Even if we account for 6 resources each week, we should be able to absorb the impact. (SAE and his team agree on having a rotational shift)

The only point Project Manager wouldn't be able to address is how "Cyberattack-detection mechanism" could be implemented with only $10K budget and no resourcing. He was sure that Tampa Bay Consulting wasn't experienced in this area and no other Consulting firms would agree to do it in such low budget, meeting the timelines. Everyone started re-thinking.

Suddenly, a guy from the Security test team suggested on on-boarding Cybersecurity Graduates from USF. He explained his previous working experience with USF cybersecurity graduates on various releases.

Project Manager Immediately praised him for his thoughtful remarks. He announced that, lets hire Graduates from USF to implement "Cyberattack-detection mechanism" and I'm sure we will be able to do it well within the remaining 10K. The meeting concluded with all the key decisions made.

4. Conclusion

At the end, the Smart Metering Implementation went live on the original date. Business were very pleased on the way project team has shown utmost flexibility and have adapted to the changes. The Project Manager was awarded a “Delivery Excellence” Award. Today, the Solution stands strong defending all the cyberattacks thanks to SAE’s future proof design.