Secure Acquisition Case Study 1: Project Initiation

Dan Shoemaker, University of Detroit Mercy

April 2021

Risk Management Case 1: Secure Acquisition/SCRM Project Initiation

Background

Systems are built out of components that are integrated from the lowest level of a supply chain up to a finished product. This creates a serious weakness in that malicious code, or counterfeit parts can be inserted at the bottom of the process without scrutiny and then integrated up into the end-product, as was demonstrated by the recent SolarWinds hack.

The possibility of such a thing occurring is so obvious that you would think that there have been practical efforts to address it. However, even though we've expended much time and effort to ensure robust, efficient and defect free code, we have done very little to ensure against compromises that could occur during the integration process. Thus, the aim of this project is to help the student understand the stages involved in establishing supply chain capability, as well as present a sample solution.

Case Study Overview

The purpose of secure SCRM is to identify and mitigate any risks in the software supply chain. For this exercise you will define the potential functions required in the product as well as who will supply them. This is the essential first step as it establishes all of the links in the supply chain.

Student Instructions

Please prepare a response to the following items. You will take the following steps:

1. *Identify a process in the case that you intend to support by a software application – this should include a scope, business case and assurance case statement.*
2. *Define top-level functions required to carry out the desired process – these must be coherent (e.g., logically related, and complete)*
3. *Decompose the top-level functions into a second level of component functions.*
4. *Decompose the second level functions into a third level of component functions (e.g., formulate a component tree)*
5. *Assign a (imaginary) supplier for each component at all tiers – these will be assumed to be subcontracted relationships (e.g., the work will be done by a subcontractor directly employed by the higher-level entity)*

Instructor notes

This is an individual assignment done during a live-lab session. The process steps are taken a step at a time as guided by the instructor. This is done in-class as a first of four lab projects done over the semester to illustrate an explicit process for functional identification and classification of potential supply chain organizations.

Example solution

Step 1. Identify a process in the case that you intend to support by a software application – this should include a scope, business case and assurance case statement.

As IoT starts to play a role in our everyday life, the demand for smart home devices is increasing. Our company will be developing a product that will be affordable, secure, and reliable. A product that will position our company for profitable years to come. This product is a smart camera. This version of the camera will be targeted towards residential customers who need to access their camera feed while away from home.

Step 2. Define top-level functions required to carry out the desired process – these must be coherent (e.g., logically related, and complete.)

In order to ensure that we have a camera system that allows the user to connect to remotely access the camera feed via a mobile app, the product will be broken down into the five components below:

1) *A physical camera and a base station for local recording*
2) *A firmware - Integrates the software with the hardware. Allows for the ability to perform over the air updates.*
3) *A mobile application – develop and document the necessary applications to run on the most popular mobile platforms (Android & iOS)*
4) *Cloud Storage – allows the users to purchase a subscription to give them access to 14 days' worth of recording.*

Step 3. Decompose the top-level functions into a second level of component functions.

For this case, the second level of component functions are as follows.

1) *A physical camera and a base station for local recording*
    a. *Determine hardware requirements to ensure that the camera passes the following:*
        i. *An IP65 weather resistance certification*
        ii. *Hardware specification to handle strong encryption and account for any future software upgrades that will require higher processing power.*
        iii. *Base station must have the ability to communicate with the camera and pull video feed securely for local storage.*
        iv. *Camera must have infrared sensors for night vision capability.*

2) *A firmware - Integrates the software with the hardware. Allows for the ability to perform over the air updates.*
    a. *Develop a firmware for the camera and the base station and allow users to perform over the air updates. The firmware acts as the operating system of the units and provides the company the ability to continue to enhance the camera functionality in future updates. Firmware development process must be performed in-house using a well-defined process. The code of the firmware must undergo a code review and regression testing prior to being approved. The principle of separation of duties must be present. The team that develops the firmware must be different than the team that performs QA and approval for production release.*

3) *A mobile application – develop and document the necessary applications to run on the most popular mobile platforms (Android & iOS)*
        i. *The development of the mobile applications will be outsourced to a software development company. Below are the key security requirements:*
            a. *The vendor must perform security testing of the mobile applications to ensure that they are secure and not vulnerable to compromise.*
                i. *Static testing*
                ii. *Dynamic testing*
                iii. *Interactive testing*
                iv. *Mobile testing*
            b. *The vendor must perform a threat modeling exercise on the application during the design phase to ensure any architectural security flaws are addressed early in the project.*

        ii. *The mobile apps must have the following security features:*
        i. *Two-factor authentication – this will prevent unauthorized access to user accounts.*
        ii. *Strong authentication of credentials – In the case the credentials are compromised, they will be in an encrypted format.*
        iii. *The communication between the app and the cloud storage is done via TLS 1.2 or above.*

4) *Cloud Storage – allows the users to purchase a subscription to give them access to 14 days' worth of recording:*
    Storage of recorded video will leverage Cloud Storage in Amazon AWS. The cloud storage is configured to have the following features:

        i. *Storage buckets with no public access – Storage will be configured to only be accessed when the user is logged into the app and authenticated.*

ii. *Users have the ability to turn on a sharing feature, which moves the video to a publicly accessible bucket and made available for everyone to view.*

Step 4: Decompose the second level functions into a third level of component functions (e.g., formulate a component tree)

1) *A physical camera and a base station for local recording*
    a. *Determine hardware requirements to ensure that the camera passes the following:*
        i. *An IP65 weather resistance certification*
        Build camera with housing that can withstand harsh weather.
        ii. *Hardware specification to handle strong encryption and account for any future software upgrades that will require higher processing power.*
        iii. *Base station must have the ability to communicate with the camera and pull video feed securely for local storage.*
            - *Communication between base station and camera must be encrypted.*
            - *Video stored in the base-station is accessed via the same app and only visible when the user is logged in.*
        iv. *Camera must have infrared sensors for night vision capability.*
        Integrate 5 infrared sensors to allow for night vision up to 30 feet.

2) *A firmware - Integrates the software with the hardware. Allows for the ability to perform over the air updates.*

    a. *Develop a firmware for the camera and the base station and allow users to perform over the air updates. The firmware acts as the operating system of the units and provides the company the ability to continue to enhance the camera functionality in future updates. Firmware development process must be performed in-house using a well-defined process. The code of the firmware must undergo a code review and regression testing prior to being approved. The principle of separation of duties must be present. The team that develops the firmware must be different than the team that performs QA and approval for production release.*
        i. *Develop the necessary firmware code for the interface apps with the understand that the firmware cannot be replaced or modified by the user.*
        ii. *Ensure that all the code that is developed is documented and inspected for security vulnerabilities.*

3) *A mobile application – develop and document the necessary applications to run on the most popular mobile platforms (Android & iOS)*
    iii. *The development of the mobile applications will be outsourced to a software development company. Below are the key security requirements:*
        a. *The vendor must perform security testing of the mobile applications to ensure that they are secure and not vulnerable to compromise.*
            i. *Static testing: A static code analysis tool such as Coverity or Checkmarks must be used to scan the source code and any libraries used to ensure all vulnerabilities are identified and resolved before every release.*
            ii. *Dynamic testing: Dynamic testing is done after the application goes into production. This ensures continuous monitoring.*
            iii. *Interactive testing: This includes fuzz testing.*

        b. *The vendor must perform a threat modeling exercise on the application during the design phase to ensure any architectural security flaws are addressed early in the project.*
            i. *Create an architectural diagram with all the entry points in order to perform a threat model on the mobile apps to identify any risks.*

Step 5. Assign a (imaginary) supplier for each component at all tiers – these will be assumed to be subcontracted relationships (e.g., the work will be done by a subcontractor directly employed by the higher-level entity).

For the development of the hardware (Camera and Base), we plan to utilize the following vendors and suppliers:

- *Foxconn will be responsible to for the overall manufacturing of the camera and the base.*
    - *A subcontractor will be responsible to supply Foxconn with the housing and IR sensors.*
- *Samsung will be responsible for creating the chipset of both the camera & base station.*
- *Sony will be responsible for manufacturing the camera lens.*
- *Amazon will be responsible for providing the cloud environment for app development and storage via their AWS infrastructure.*
- *Gorilla Logic company will be responsible to develop the mobile apps.*

References

Sigler, Ken, Dan Shoemaker and, Anne Kohnke, *Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product*. Auerbach Publications; (Internal Audit and IT Audit) 1st Edition, November 3, 2017

Shoemaker, Dan, and Kenneth Sigler, "Cybersecurity: Engineering a More Secure IT Organization", Cengage Learning, 2014, Chapters 5 and 7

ISO 27001 and ISO 27002 (provided as BS7799)

IEEE 1028-1997 Standard for Software Reviews

ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)

IEEE 610 - Standard Glossary of Software Engineering Terminology

The Common Weakness Enumeration http://cwe.mitre.org/

Foreign Ownership, Influence or Control Investigations (FOCI)
http://www.dss.mil/isp/foci/foci_info.html