Sebastian Canales Burke

2025-03-26

IT Security W2025

Assignment 2 – Home Security, Security Analysis

Casa Jetson - Smart Home Security Analysis: Devices, Activities, and Sensitive Data





Table of Contents

1. Introduction
2. Presentation of Use Case
3. Asset List
4. Risk Register Concept
5. Risk Register
6. Action Plan
7. Defense in Depth
8. Security Design Principles
9. Conclusion

1. Introduction

**Purpose**: This report aims to identify, analyze, and propose solutions for cybersecurity risks within a modern smart home environment, called Casa Jetson. The goal is to protect the residents, Jorge and Jane, along with their sensitive information, personal privacy, and digital assets from cybersecurity threats.

**Target Audience**: The target audience of this report is non-technical readers and individuals without prior formal training in IT security.

2. Presentation of Use Case

Casa Jetson is a modern home filled with smart devices that make life easier for Jorge and Jane. These devices include security cameras, smart locks that allow them to open doors without physical keys, and voice-controlled assistants like Alexa that answer questions and perform tasks. They also use a smart thermostat that automatically keeps their home temperature.

Jorge and Jane rely on these devices every day. Jorge often uses apps on his smartphone to manage devices like cameras, locks, and even garage doors. He enjoys shopping online and banking through apps. Jane uses social media to run her business selling custom-made outfits for dogs. She also shares pictures of her dog and uses apps to share her jogging routes in real-time.

Both Jorge and Jane work from home, so they use their computers connected to the home Wi-Fi network to store important business information, customer details, and financial records. With all these devices connected to the internet, their home becomes vulnerable to various cyber threats. This situation puts their personal privacy, safety, and sensitive data at risk.

This report will identify potential dangers and suggest practical steps to protect their smart home environment.

3. Asset List

1. Physical Assets

|  |  |  |
| --- | --- | --- |
| **Device** | **Function** | **Location** |
| Security Cameras | Streams 24/7 to cloud, motion-sensing, local 48h storage | Garage, backyard, living room |
| Doorbell Camera | Camera + 2-way audio | Front door |
| Smart Plugs | Turn lights on/off | Bedrooms, living room |
| Nest Thermostat | Controls house temperature | Living room |
| D-Link DIR-627 Router | Wi-Fi access point | Living room |
| Amazon Alexa Speakers | Voice assistant, smart home hub, orders, reminders | Kitchen, bedroom, foyer |
| Smart Door Lock | Combo pad or app controlled | Front door |
| Garage Door Opener | App-controlled or combo pad | Garage |
| Fridge with Webcams | Inside webcam (food view), outside webcam (video calls) | Kitchen |
| Jorge’s Work PC | Work files, remote work, connected to Wi-Fi | Bedroom 2 |
| Jane’s Laptop | Business data, connected to Wi-Fi | Living room |
| Personal smartphones/tablets | App-based controls, connected to Wi-Fi | Throughout the entire home |

1. Privacy Assets

|  |  |
| --- | --- |
| **Category** | **Examples** |
| Personal Data | - Names, address, contact info  - Calendar reminders, events, birthdays  - Online shopping history  - Contact lists  - Social media accounts |
| Financial Info | - Banking credentials  - Online orders and saved payment info  - Transaction history |
| Work Data | - Jorge’s company data  - Jane’s customer lists, invoices |
| Behavioral Data | - Smart home usage patterns  - Alexa usage logs  - Strava jogging routes  - Dog walker's entry patterns |
| Home Security | - Camera feeds  - Smart locks & garage door access  - Remote control of home entry |
| Reputation | - Jane’s business profile  - Jorge’s online identity |
| Device Data | - IP addresses  - Login credentials  - Firmware/software versions of devices |

4. Risk Register Concept

Risks identified will be assessed based on:

* Likelihood (scale 1–5; 1 being rare and 5 very likely)
* Impact level + reference to the CIA Triad:
  + Confidentiality (Unauthorized disclosure)
  + Integrity (Unauthorized alteration)
  + Availability (Disruption of service)
* Cost, mapped to real dollar values (e.g., 1 = $50, 5 = $5000+).

5. Risk Register

**\* View attached Casa\_Jetson\_Risk\_Register.xlsx \***

6. Action Plan

Based on the risk assessment, the following actions are prioritized:

Must-do actions (High Priority):

1. Smart Cameras: Change default passwords; enable Multi-Factor Authentication (Cost: $100)
2. Wi-Fi Router: Conduct regular firmware updates and establish strong passwords (Cost: $100)
3. Work Computers (PC/Laptop): Install antivirus software, firewall, and encrypt sensitive data (Cost: $500)
4. IoT Devices (thermostat, plugs): Isolate devices and secure network configurations (Cost: $250)
5. Smart Locks: Regular app updates and ensure secure authentication (Cost: $200)
6. Alexa Devices: Configure privacy settings and review voice data (Cost: $100)

Nice-to-have actions (Lower Priority):

1. Strava Jogging App: Adjust privacy settings and limit data sharing (Cost: $50)
2. Fridge Webcam: Implement webcam covers or disable when unused (Cost: $20)

**Total estimated cost for all proposed measures:** $1,320

7. Defense in Depth

Defense in Depth refers to implementing multiple layers of security controls to protect systems and data. At Casa Jetson, the Wi-Fi router is a major risk because its software is old and easy for hackers to attack. To better protect it, several layers of security should be used:

1. **Physical Security**:
   * Put the router in a locked or hidden spot so unauthorized people can't easily reach it.
2. **Perimeter Security**:
   * Set up firewalls to control what internet traffic can enter or leave the network.
3. **Network Security**:
   * Regularly update the router's software to fix any security weaknesses.
   * Use strong Wi-Fi encryption, such as WPA3, to make it hard for hackers to access.
   * Choose strong passwords that are hard to guess.
4. **Endpoint Security**:
   * Make sure all devices connected to the Wi-Fi have updated antivirus software.
   * Ensure devices also have their own firewalls active.
5. **Application Security**:
   * Control which devices can connect to the network by using secure apps that require authentication.
   * Monitor network connections regularly to quickly notice any suspicious activity.

By following these steps, Casa Jetson can greatly reduce the chance of cyberattacks and keep their network safer.

8. Security Design Principles

* **Least Privilege**: This principle ensures that users and devices are granted the minimum levels of access necessary to perform their functions. In Casa Jetson, each IoT device and user account should have limited permissions strictly required for their operations, reducing potential damage from compromised accounts or devices.
* **Fail-safe Defaults**: The principle of fail-safe defaults means that access decisions should default to denial. Access is granted only when explicitly permitted. For Casa Jetson, devices and network settings should deny any connections or actions unless explicitly allowed by the homeowners, ensuring unauthorized access attempts are blocked by default.

9. Conclusion

Casa Jetson is a great example of how smart home technology can make life easier but also bring new risks. Several serious security problems that could put the household at risk came up during the analysis. This shows how important it is to have strong cybersecurity in place.

To make the Jetson home safer, it’s important to focus on key security steps. These include keeping all devices and systems updated, using strong and unique passwords (or other forms of secure login), and making sure all data is encrypted. It's also important to follow basic security rules like giving users the least amount of access they need (called Least Privilege) and making sure systems default to safe settings (called Fail-safe Defaults).

By putting these measures in place and using multiple layers of protection, the Jetsons can better protect their privacy, keep their personal information safe, and enjoy the benefits of smart technology without as much worry. Taking action early and staying alert is the best way to keep a smart home secure.

Diagram, engineering drawing

Description automatically generated