AVS

Cooper Redfern, Ian Russo, Jared Trenhaile, Uxoa Bertiz

Problem: Viruses More Prevalent than Ever

- As electronic devices continue to become more central to our world, our personal and professional lives are continually being put at a greater risk.

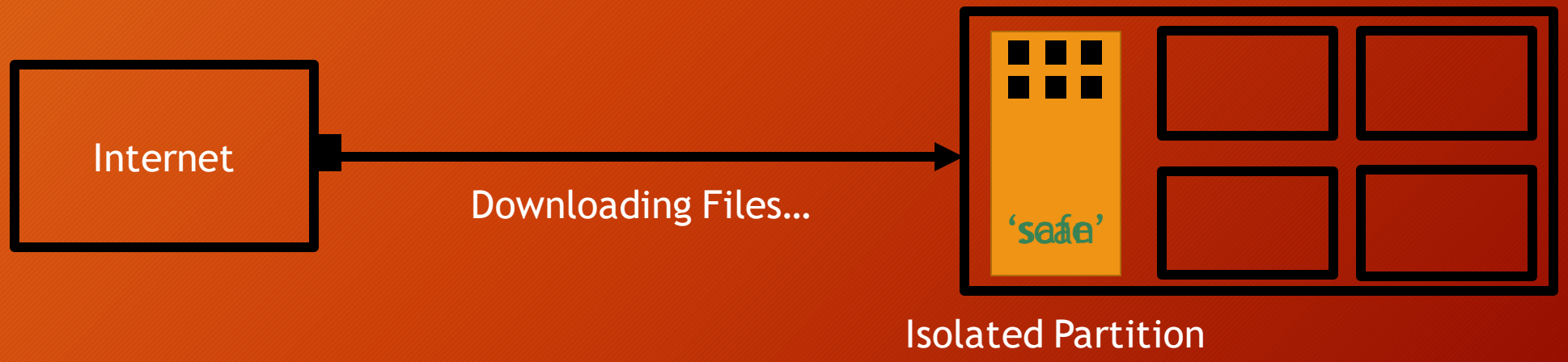
- Malicious programming seeks to steal your valuable information.

Problem: Most Common Method of Attack

- “Piggy-Backing” on downloaded files.
  - Trojans
    - Download looks legitimate, but is in-fact malware
    - Creates backdoors and collects user information
  - Keyloggers
    - Hackers track keystrokes to steal passwords
  - Remote Webcam Access
    - Hackers gain access to microphone/webcam
    - Spying
    - Biometric data theft

Problem Solutions

- Realtime Protection
  - Constantly monitor activity in memory to detect malicious software
  - Check downloaded files in an isolated partition for signs of malicious software before allowing it to spread to other partitions



Problem Solutions

- Single File Scan
  - Cross Checks signatures from the file with MD5 Hashes from virus list

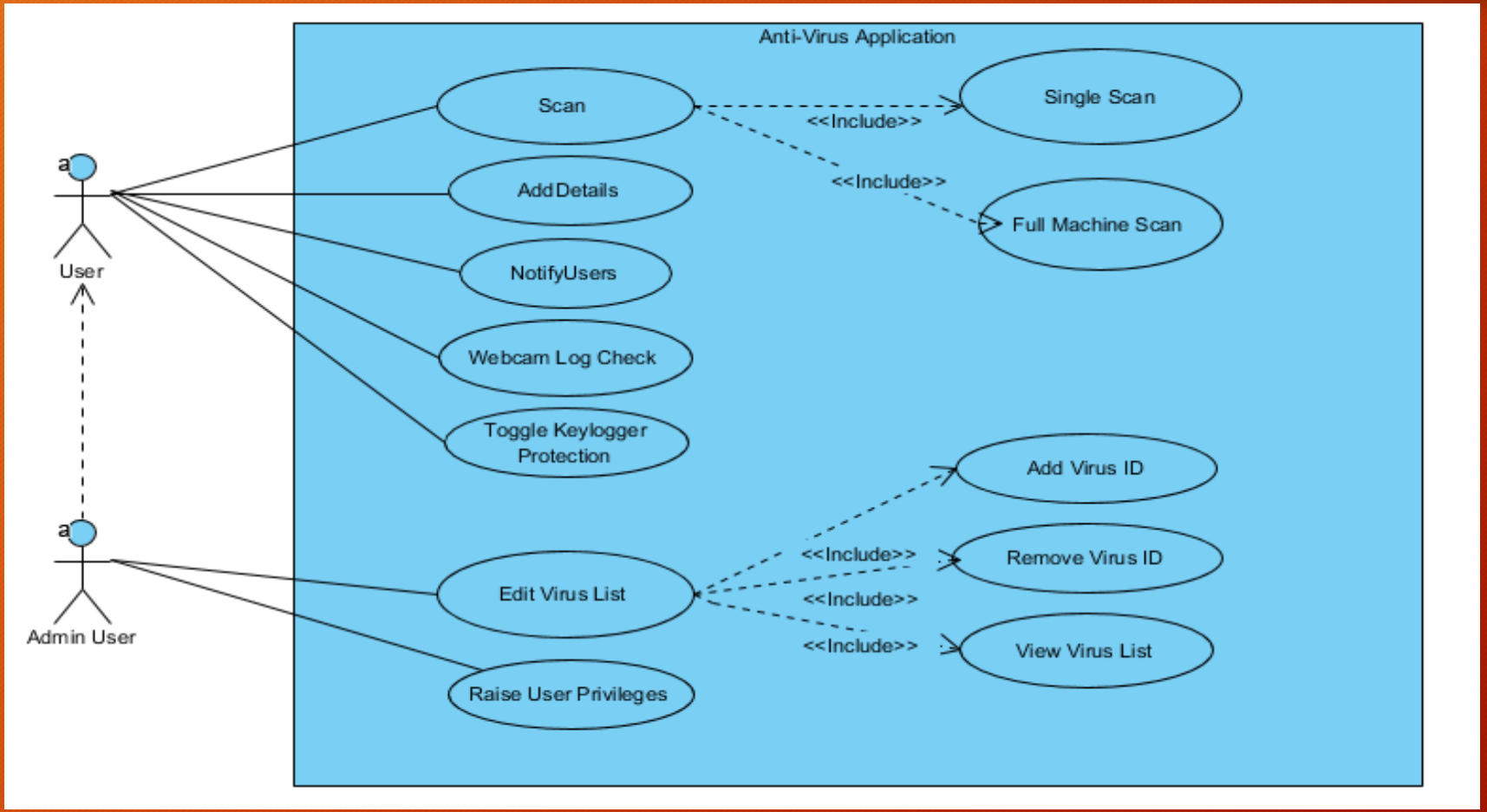
Problem Solutions

- Keylogger Protection
  - Software Keyloggers
    - Encrypt keystrokes and decrypt if current application is deemed safe.

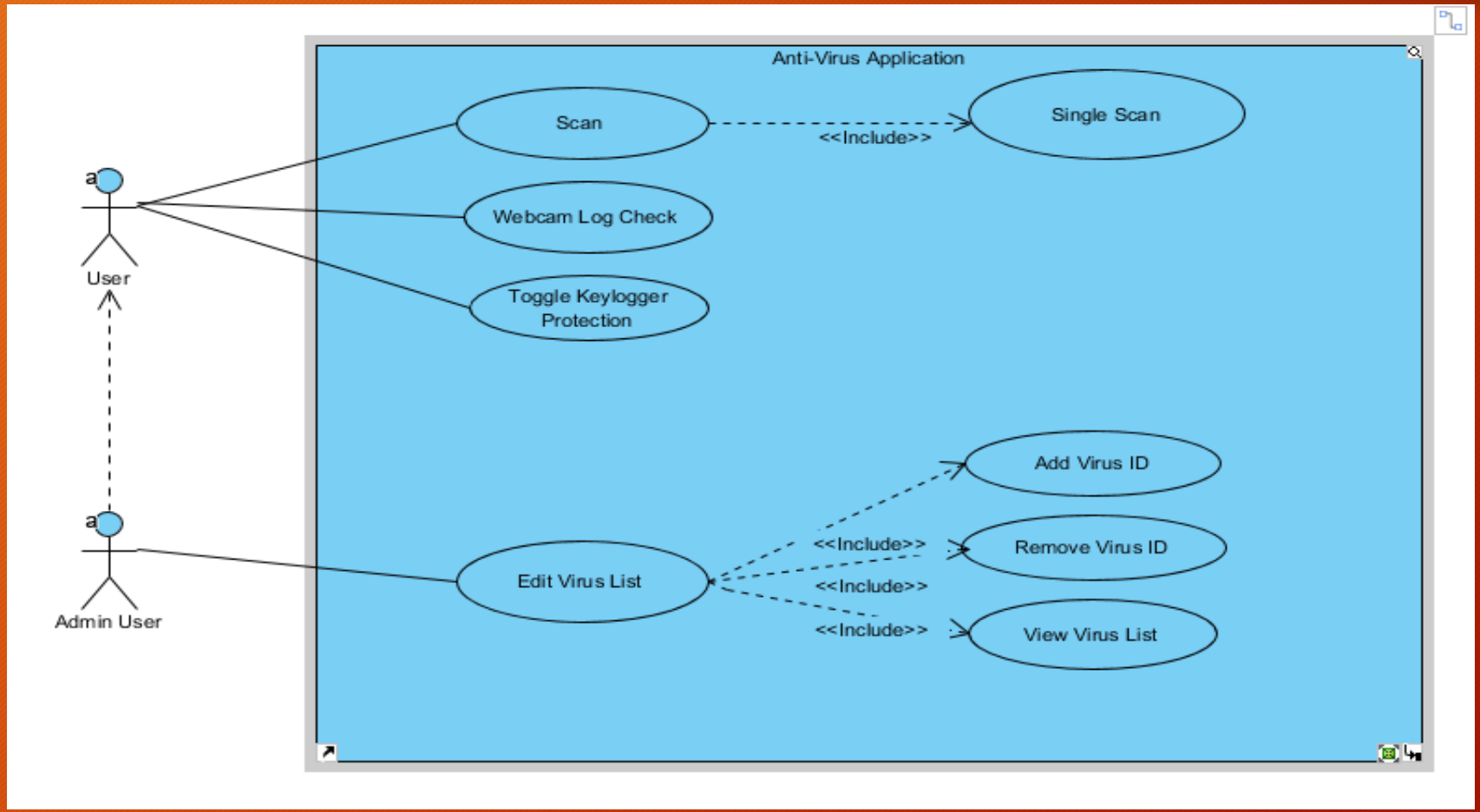
Problem Solutions

- Webcam Activity Monitor
  - Silently track when webcam is activated.
    - User can determine if webcam was activated unknowingly.

Updated System Use Cases



Sprint 1 Use Case Diagram



Sprint 1 Use Cases

- ***Users***
  - **Single File Scan** ---> A _user _can select a file from windows file explorer to scan for viruses
  - **Webcam Log Check** ---> A *user* can check the webcam log to view recent activity
  - **Toggle Keylogger Protection** ---> A *user* can toggle whether keyboard protection is enabled or disabled
- ***Admin Users***
  - **View Virus List** ---> An *admin user* can view the list of MD5 hashes and their associated virus

Tech Plan

- The primary code of our software will be written in C++.
  - This will require a considerable amount of research on our end, but the general consensus is that this is the best programming language for the task.

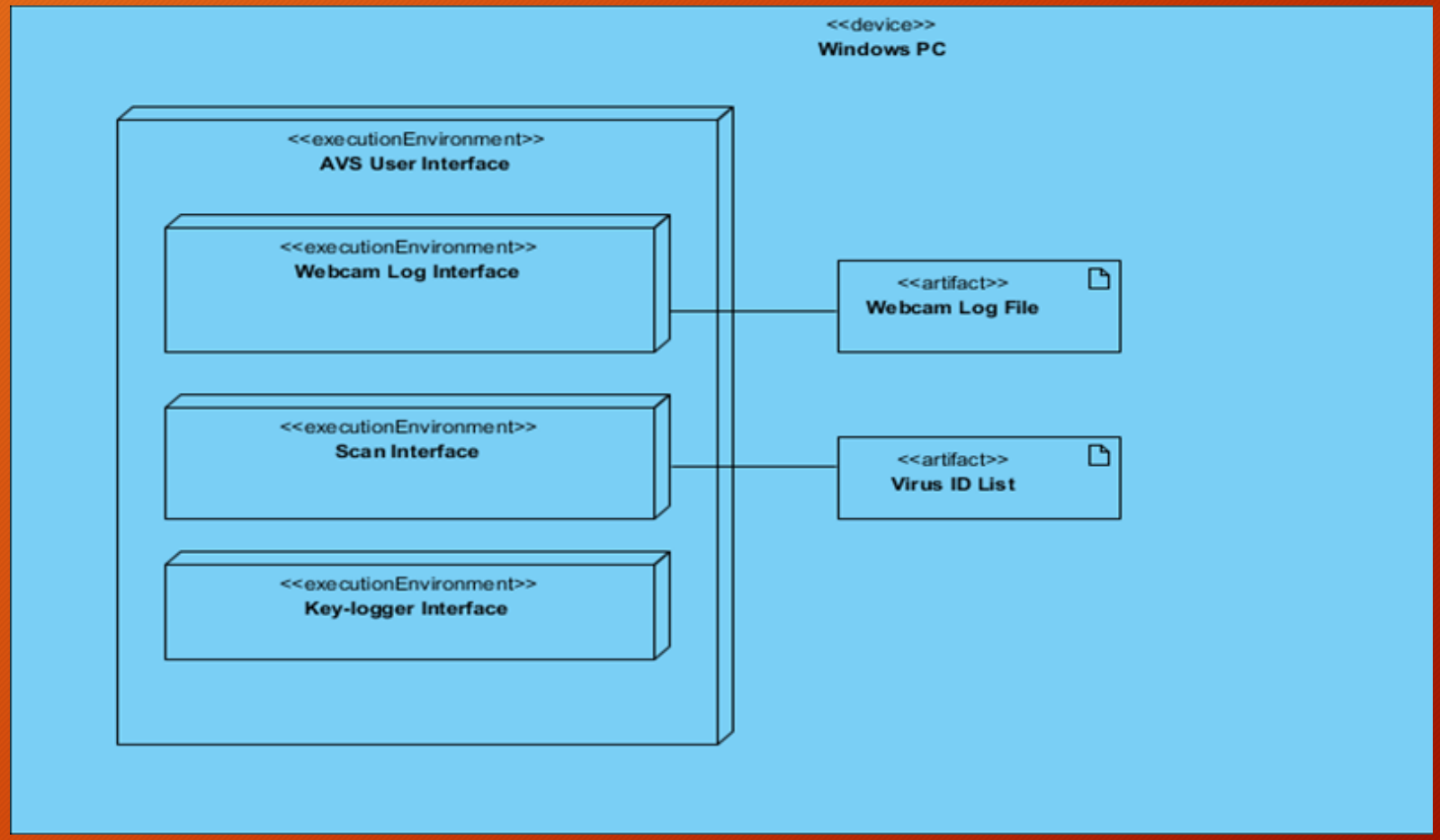
- The operating system for our software will be Windows.
  - By-far the operating system that we are most familiar with.

Technology	Experience Rating
Platforms	
Windows	Extensive
Anti-Virus Technologies	
Simple Scan	Tutorial
Webcam Logger	Tutorial
Keystroke Encryption	Tutorial
Application Development	
Python	Moderate
Java	Small Scale
C++	Tutorial

Tech Training Plan

- C++ Training
  - Udemy Course: Beginning C++ Programming
  - Udemy Course: Learning C++ By Creating
  - Study Documentation: http://devdocs.io/cpp/
- Scan Algorithm Research
  - JackkTutorials: How to Make a Basic Anti-Virus Scan
    - https://www.youtube.com/watch?v=OU0Ar2LeSgU
- Keylogger Research
  - Udemy Course: Build an Advanced Keylogger using C++ for Ethical Hacking

Sprint One Architecture



Non-Functional Requirements

- Users can navigate easily through a simple UI.
- Users can enable or disable certain features as they wish.
- Users will receive a notification if malicious behavior is encountered.

Security Requirements

- Only user admin has the ability to add/remove from list of known viruses. --- Single Scan.
- Keylogger protection will encrypt inputs and decrypt them for safe applications. --- Enable Keylogger Protection
- Webcam activity is silently logged. --- Webcam Log Check.

Effort Estimate

- **Screens**
- Keylogger Protection ---> Simple(1)
- Single File Scan ---> Simple(1) + Additional four screens: Type of scan, scan, results, and quarantine. 1 + 4 = 5
- Webcam Log Check ---> Simple(1)
- Add Known Viruses ---> Simple(1)
- Server Side (md5 Comparisons) – 2 Components --- > Difficult(10) * 2 = 20

- Effort Estimate:
- Effort = (32 x (1 – 0/100))/13 = **2.46 Person Months**
- Calendar Estimate:
- Assume we can each work 12hr/week.
- 12 hours x 4 weeks = 48 x 4 people = 192hr/month
- There are 140 hours in a standard person month.
- 192/140 = 0.57
- Months = 2.46 x 1/1.37 = **1.80 Months**

In Conclusion