Department of Computer Science & Engineering
The University of Texas at Arlington

System Requirements Specification
CSE 4316: Senior Design I
Fall 2023

Team Honeycomb
HoneyTrap

Jair Rea
Raed Ali
Hugo Mendoza
Praisy Daniel
Joshua Catalan

Revision History

Revision	Date	Author(s)	Description
0.1	10.01.2015	GH	document creation
0.2	10.05.2015	AT, GH	complete draft
0.3	10.12.2015	AT, GH	release candidate 1
1.0	10.20.2015	AT, GH, CB	official release
1.1	10.31.2015	AL	added customer change requests

Contents

1 Product Concept

This section outlines the product concept for the initiative designed to combat online scams, specifically those targeting vulnerable individuals such as the elderly. The project aims to create a comprehensive defense tool against scammers by employing advanced AI technology and strategic engagement techniques. Through the creation of a simulated online persona, the system will infiltrate scammers, engaging them in conversations while gathering valuable intelligence. The primary purpose of this initiative is to disrupt scammer operations, delay their fraudulent activities, and provide critical data to law enforcement agencies. Users of this system, including ethical hackers, cybersecurity experts, and individuals passionate about online security, will employ the tool to actively counteract scams. This product will be a useful tool by helping vulnerable families to not be swindled by online thieves.

1.1 Purpose and Use

The purpose of the outlined plan is to combat online scams targeting vulnerable individuals, specifically the elderly. The plan involves creating a fake persona to lure scammers, engaging with them, and reporting their activities to the authorities. The ultimate goal is to gather information about scammers, delaying their operations and potentially aiding law enforcement in apprehending them. The plan also aims to raise awareness about online scams and educate others about utilizing technology to counteract such threats.

1.2 Intended Audience

The intended audience for this plan includes individuals and organizations concerned about online scams, particularly those preying on vulnerable individuals. This could involve law enforcement agencies, cybersecurity experts, ethical hackers, or researchers interested in understanding and combating online fraud. Additionally, the plan targets individuals looking to make a difference in their communities by actively contributing to the fight against cybercrime.

2 Product Description

This section provides a comprehensive overview of our anti-scamming initiative, focusing on its core features and functions. The initiative employs AI technology to create a simulated persona used to engage online scammers, primarily those targeting vulnerable individuals. For this project, we will be using a Facebook account, however this technology could be applied to other social media network accounts. The core functionalities include the generation of realistic profile information and interactions to lure scammers, employing delaying tactics during conversations, and gathering valuable data on scammer activities. The system acts as a shield against online fraud, disrupting scammer operations and offering critical insights to law enforcement agencies. Users can access a user-friendly interface where they can track scammer interactions, view gathered intelligence, and contribute to the initiative's collaborative efforts. By employing a multidisciplinary approach and leveraging advanced AI, our initiative equips users with the tools and knowledge to actively combat cybercrime and create a safer digital environment for all users.

2.1 Features & Functions

The plan incorporates several key features and functions, including the creation of a fake online persona using AI-generated content. It involves engaging scammers in conversations, employing delaying tactics, and tracking their activities. Furthermore, the plan emphasizes the importance of emotional support for those involved and the necessity of collaborating with legal and technical experts to ensure the project remains within ethical and legal boundaries. Additionally, it highlights the significance of education and awareness campaigns to inform others about online scams and preventive measures.

2.2 External Inputs & Outputs

External inputs for this plan include information gathered from online sources, such as social media profiles and scammer interactions through posts, comments or messages. Outputs comprise the data collected on scammer tactics, trends, and potential leads for law enforcement.

2.3 Product Interfaces

The primary product interfaces for this plan involve online platforms and social media networks where scammers operate. These interfaces serve as entry points for engaging with scammers. Additionally, there is an interface with law enforcement agencies, facilitating the sharing of information and collaboration in filing reports. Collaboration interfaces also extend to experts in fields like AI, cybersecurity. Potential dducational interfaces involve blogs, articles, social media channels, and conference presentations, reaching a wider audience to spread awareness.

3 Customer Requirements

Bellow we have the major requirements for our chat bot. Most of these requirements were given to us by our sponsor, but we came up with a few others in this section.

3.1 Chatbot's behavior

3.1.1 Description

We will be creating a Facebook chatbot that acts like a vulnerable elderly widow. It should seem like they are speaking with a real person. The bot should also sound like someone who is technically illiterate in the conversations it will have. If the scammer is asking for money the bot is supposed to drag and delay out the payment process. Our sponsor also mentioned having the bot trick the scammers into calling a number that would track their location. We were thinking we could also have the bot trick the scammer into clicking a Grabify IP link to get the scammer's IP address.

3.1.2 Source

Our sponsor(Michael Magnus)

3.1.3 Constraints

- Any limitations there may be in the Large Language Model we may use. Oftentimes times we have seen chatbots that use large language models act out of character whenever you speak with them.

- The chat logs and data we have. If we don't have sufficient data on how a vulnerable widow may act to feed to our LLM then it will become obvious to whoever is talking to the bot that they are speaking with a bot.

3.1.4 Standards

- ISO 9241-210: Human-Centered Design for Interactive Systems. This standard is related to creating a user-friendly interface. Which will be needed in order to communicate with the chatbot.

- ISO 13407: Human-Centered Design Processes for Interactive Systems. This standard is related to having a design that is user-centered. Which will be needed to communicate with the scammer aka the user.

3.1.5 Priority

Critical

3.2 Chatbot's scammer recognition

3.2.1 Description

We will be creating a system to recognize scammers through direct messages. We will implement a machine-learning approach to analyze any trends in how the scammers talk.

3.2.2 Source

Our sponsor(Michael Magnus)

3.2.3 Constraints

- The chat logs and data we have. If we don't have sufficient data on how a scammer may act to feed to our LLM then it will become harder to properly identify a scammer.

3.2.4 Standards

- ISO 27701: Privacy Information Management System (PIMS). This standard is relevant for making sure we protect the privacy of the users. Since we are reading other people's private messages, we have to make sure we do so in a responsible manner.
- ISO 26000: Social Responsibility. This standard is relevant for making sure we respect ethical and social responsibilities. Our bot is reading the private messages of others, so it's important we do so ethically.

3.2.5 Priority

Critical

3.3 Scammer and vulnerable people recognition of Facebook pages

3.3.1 Description

We will be creating a system to identify potential scammer accounts on Facebook. But first, we must create an algorithm to find any vulnerable widows on Facebook, after we find these widows we will send them friend requests. If they accept our friend request we will then web scrape their friends list to look for any potential scammers. We will make an algorithm to determine by looking at their profiles if they are scammers or not. If they are identified as a scammer our bot will friend request them and we will wait for them to get in contact with our bot and confirm the suspensions by engaging in conversations with them.

3.3.2 Source

Our sponsor(Michael Magnus)

3.3.3 Constraints

- The scammer's behavior. This whole step is dependent on the scammer eventually messaging us and accepting our friend requests. If they never do this we can't move on to any of the other steps

3.3.4 Standards

- ISO 27701: Privacy Information Management System (PIMS). This standard is relevant for any of the data we web-scrapped with our bot. It provides guidelines for managing this data.
- ISO 19944: Privacy by Design for Consumer Goods and Services. Since we are scraping a lot of Facebook pages it's important we act responsibly with this data and respect any privacy standards when doing so.

3.3.5 Priority

Critical

3.4 Reporting scammers

3.4.1 Description

We will be Creating a system to report scammers. Once we have identified our code will automatically report their account on Facebook. We will also file a police report of that scammer with the appropriate instructions if they are to pursue this situation. We were also thinking of creating a website or another Facebook account that would have the names and accounts of the verified scammers to warn others not to interact with these accounts.

3.4.2 Source

Our sponsor(Michael Magnus) and for the scammer database suggestion(Raed Ali)

3.4.3 Constraints

- It may be a little difficult to test out the police report feature since we can't create a bunch of fake police reports just to test our product. Which would be an ethical concern. We don't want to waste the police's time.
- Another ethical concern is that the scammer's recognition from the previous steps was not flawed. If it is flawed we could potentially end up filing police reports when we don't need to.

3.4.4 Standards

- Police Report Standards, we must comply with any legal standards to make sure we file the police reports appropriately and submit meaningful information that can be used legally.

3.4.5 Priority

Moderate

4 Packaging Requirements

This section is dedicated to how the final product will look. Here we mostly visually discuss how the bot's Facebook profile will look and how direct messaging from the bot will look.

4.1 Believable and legal profile pictures

4.1.1 Description

Each of our bot accounts will have an AI-generated profile picture(using Midjourney) to represent that account. This profile picture will look realistic and not be a real elderly person's picture since that may violate privacy and not be legal.

4.1.2 Source

Our sponsor(Michael Magnus)

4.1.3 Constraints

- Any limitations there may be with the AI-generated images, for instance, many AI-generated images we can tell that they are not real. There are features that are kind of off from them. These images may exist in the uncanny valley.

4.1.4 Standards

- ISO 25010: System and Software Quality Models. This standard will help us have a framework of what the quality of the images we use will be like.

4.1.5 Priority

High

4.2 Accounts will have natural account growth

4.2.1 Description

Each fake account will grow and update its profile over time. The activity will seem natural. The Facebook threads created by our account will also seem like real threads created by real people. It won't look like a bot account that was just created. However, it is important later down the line our account will make posts talking about missing their husband and talking about being lonely to bait the scammers. It can't all just be that since it has to look real.

4.2.2 Source

Our sponsor(Michael Magnus)

4.2.3 Constraints

- Time is a big constraint for this. Implementing this will take some time. We can't implement this feature in just one day, this could take weeks to do, since we have to slowly grow the accounts. So we would have to work on this early on.

4.2.4 Standards

- Facebook's terms and service. It would be important that we don't violate any of Facebook's terms and service when making our posts. So we don't get our account banned.

4.2.5 Priority

High

4.3 Conversations with the bot will look natural

4.3.1 Description

Whenever someone tries to have a conversation with our bots with Facebook Messenger, the conversations will feel natural and not seem AI-generated.

4.3.2 Source

Our sponsor(Michael Magnus)

4.3.3 Constraints

- Just like how we discussed in the Customer Requirements the limitations of the LLM we use will factor into the constraints.

4.3.4 Standards

- ISO 9241-210: Human-Centered Design for Interactive Systems. If we follow this standard it will make sure we give the scammers a good user-friendly interface so they can communicate with our bot.
- ISO 13407: Human-Centered Design Processes for Interactive Systems. This is an important standard to make sure our bot will be user-centered. In this case, the user is the scammer.

4.3.5 Priority

Critical

5 Performance Requirements

In order to fulfill the goal of our product, and to ensure it operates effectively in protecting elderly individuals from financial scams and mitigating cybercrime, the following performance requirements have been established to guide the design and development of Honey Trap:

5.1 Response Time

5.1.1 Description

This requirement specifies how quickly the Honey Trap must react when it receives a message from a potential scammer. The bot is expected to respond within 5 minutes of receiving the initial message. This rapid response time is crucial to engage potential scammers effectively and maintain their interest in the conversation. A quick response can prevent scammers from becoming suspicious and ensure they divulge important information, aiding in the product's mission to track and trap scammers.

5.1.2 Source

Requirement specifications provided by the sponsor.

5.1.3 Constraints

- Software Limitation: The processing and memory capacity can impose constraints on response time. Inadequate software may limit the system's ability to respond quickly.
- Peak load and scalability: The need to handle peak loads during high traffic periods can be a constraint.
- Budget: Financial limitations may affect the system's inability to invest in infrastructure or technologies that optimize response time. Staying within budget can be a significant constraint.

5.1.4 Standards

- ISO 25010 - System and Software Quality Models: ISO 25010 provides a comprehensive framework for evaluating the quality characteristics of software systems, including performance attributes like response time
- ISO/IEC 9126 - Software Engineering - Product Quality: ISO/IEC 9126 outlines quality characteristics, including response time, and provides guidelines for measuring and evaluating software quality.

5.1.5 Priority

Response time is a critical performance requirement for our product, especially in the context of engaging with potential scammers in real-time. Failing to meet high response time standards could diminish the product's effectiveness and thus, this requirement reflects a high priority status.

5.2 Language Recognition

5.2.1 Description

This requirement is the fundamental aspect of the product because it is essential for it to have the ability to engage with a diverse pool of potential scammers effectively. This ensures that the product can understand and respond to the messages of scammers in a diverse way thus enhancing its capacity to engage with a wide range of scammers of all age groups.

5.2.2 Source

Requirement specifications provided by the sponsor.

5.2.3 Constraints

- Data Availability: Language recognition relies on extensive data sets for training and accuracy. Constraints on the availability of these data sets, especially for less commonly used language styles can be a limitation.

- Cultural Sensitivity: Language recognition should be culturally sensitive and avoid biases or misinterpretations based on cultural differences. Achieving cultural sensitivity can be a constraint.

- Continuous Model updates: Keeping language recognition models up to date with the latest linguistic changes and emerging languages can be a resource-intensive task, and constraints on updates may affect accuracy.

- ISO 25010 - System and Software Quality Models: ISO 25010 provides a comprehensive framework for evaluating the quality characteristics of software systems, including performance attributes like response time

- ISO/IEC 9126 - Software Engineering - Product Quality: ISO/IEC 9126 outlines quality characteristics, including response time, and provides guidelines for measuring and evaluating software quality.

5.2.4 Priority

Language recognition plays a vital role in our system and it reflects a status of medium to high priority.

5.3 Scammer Data Collection

5.3.1 Description

This requirement involves gathering information related to potential scammers' tactics, identities, and operations. It involves tracking their communication, digital traces, linguistic patterns, and information that could be used to report their profiles to combat scams.

5.3.2 Source

Requirement specifications provided by the sponsor.

5.3.3 Constraints

- Consistency and accuracy: Ensuring that data collected accurately represents the actions and identities of potential scammers is a constraint. Misinterpretation or misidentification can have legal and ethical consequences.

- Data Security and Protection: Storing and handling sensitive data related to scammers, their tactics, or their targets must adhere to strict security and privacy standards. Protecting this data from breaches or unauthorized access is a significant constraint, especially when it involves personally identifiable information (PII).

- Data Volume and Management: Managing a significant volume of data related to scammer interactions can be resource-intensive and require constraints on data handling, storage, and processing capabilities.

5.3.4 Standards

- ISO 27001: The ISO 27001 standard offers a framework for information security management systems. Adherence to this standard ensures data security during collection and storage.
- Evidence Handling Standards: If the collected data is intended for legal use or law enforcement, there may be specific standards or best practices for evidence handling in the relevant jurisdiction.

5.3.5 Priority

Scammer data collection is of utmost importance in our goal to combat fraudulent activities and protect vulnerable individuals from scams. Thus, this requirement reflects a high priority status.

6 Safety Requirements

The safety requirements for our product focus on mitigating potential risks and hazards. These requirements are designed to protect users and prevent harm such as privacy protection, no exposure to harmful content to users, data retention and deletion, etc. However, it's important to note that there are no physical safety requirements involved in our product, as it operates solely in the digital realm, focusing on the safety of user interactions and data.

6.1 Laboratory equipment lockout/tagout (LOTO) procedures

6.1.1 Description

Any fabrication equipment provided used in the development of the project shall be used in accordance with OSHA standard LOTO procedures. Locks and tags are installed on all equipment items that present use hazards, and ONLY the course instructor or designated teaching assistants may remove a lock. All locks will be immediately replaced once the equipment is no longer in use.

6.1.2 Source

CSE Senior Design laboratory policy

6.1.3 Constraints

Equipment usage, due to lock removal policies, will be limited to availability of the course instructor and designed teaching assistants.

6.1.4 Standards

Occupational Safety and Health Standards 1910.147 - The control of hazardous energy (lockout/tagout).

6.1.5 Priority

Critical

6.2 National Electric Code (NEC) wiring compliance

6.2.1 Description

Any electrical wiring shall be completed in compliance with all requirements specified in the National Electric Code. This includes wire runs, insulation, grounding, enclosures, over-current protection, and all other specifications.

6.2.2 Source

CSE Senior Design laboratory policy

6.2.3 Constraints

High voltage power sources, as defined in NFPA 70, will be avoided as much as possible in order to minimize potential hazards.

6.2.4 Standards

NFPA 70

6.2.5 Priority

Critical

6.3 RIA robotic manipulator safety standards

6.3.1 Description

Robotic manipulators, if used, will either housed in a compliant lockout cell with all required safety interlocks, or certified as a "collaborative" unit from the manufacturer.

6.3.2 Source

CSE Senior Design laboratory policy

6.3.3 Constraints

Collaborative robotic manipulators will be preferred over non-collaborative units in order to minimize potential hazards. Sourcing and use of any required safety interlock mechanisms shall be the responsibility of the engineering team.

6.3.4 Standards

ANSI/RIA R15.06-2012 American National Standard for Industrial Robots and Robot Systems, RIA TR15.606-2016 Collaborative Robots

6.3.5 Priority

Critical

7 Maintenance & Support Requirements

Ensuring the long-term reliability and effectiveness of our integrated anti-scam solution is crucial. To keep everything running smoothly and provide excellent support for customers and end-users, we need specific maintenance and support requirements.

7.1 Requirement Name

Maintenance and Support for the Chatbot Component

7.1.1 Description

Our chatbot, driven by advanced AI technology, must receive regular care to function optimally. This includes:

a. Software Updates: We need to keep the chatbot's AI model up to date with the latest information and scammer tactics.

b. Database Management: The database of scammer information that the chatbot uses needs regular updates and maintenance.

c. Monitoring and Evaluation: We'll constantly assess how well the chatbot interacts with scammers and its ability to gather their contact details and prevent scams.

d. Bug Fixing: Any issues or bugs that crop up during interactions need to be identified and fixed quickly.

7.1.2 Source

These maintenance and support tasks will come from the teams responsible for developing and operating the system.

7.1.3 Constraints

We must always ensure that the data collected during interactions is kept secure and complies with privacy laws. Ethical considerations are also essential to make sure the chatbot's actions remain ethical and legal.

7.1.4 Standards

We'll adhere to industry standards for data security, privacy, and ethics, and follow best practices for quality assurance and testing.

7.1.5 Priority

Keeping the chatbot component well-maintained and supported is a top priority. This ensures the system continues to protect elderly individuals from scams effectively and without interruption.

8 Other Requirements

In addition to our primary anti-scam measures, our system has some other important requirements to make sure it stays effective, reliable, and adaptable.

8.1 Requirement Name

System Flexibility and Future-Proofing

8.1.1 Description

We need the system's architecture and design to be adaptable and ready for future improvements. This means it should be built in a way that makes it easy to add new features and adjust to changing technologies and programming languages. It's crucial that this design is well-documented, making it straightforward for our development team to integrate new functionalities when needed.

8.1.2 Source

These requirements come from our product development and architecture teams. Their goal is to ensure the system remains relevant and sustainable over the long term.

8.1.3 Constraints

While creating this adaptable system, we must still adhere to industry standards for flexibility and maintain data security and privacy standards. Any future enhancements we make must not compromise the ethical and legal aspects of the system's actions.

8.1.4 Standards

We will strictly adhere to industry standards when it comes to making our system adaptable and modular. This includes using well-documented APIs and maintaining clear coding practices. These guidelines are vital for ensuring that our system can grow without causing major disruptions or requiring extensive rewriting.

8.1.5 Priority

This requirement holds a high priority because having a system that can adapt and evolve will help us stay ahead of ever-changing scammer tactics and new threats. This is essential for ensuring the continued effectiveness of our system in protecting elderly individuals from scams.

9 Future Items

9.1 Requirement Name

- Customization for Specific Industry Verticals
- Advanced Anomaly Detection Techniques
- Support for Multilingual and Globalization

9.1.1 Description

- The ability to customize the fraud detection software for specific industry verticals, such as healthcare or e-commerce, will not be included in the prototype version. This feature requires additional development and fine-tuning to address unique industry requirements.
- While considered, advanced anomaly detection techniques beyond the core algorithms will not be implemented in the prototype due to the constraints of time and feasibility analysis. These may include more sophisticated statistical models and deep learning approaches.
- Extensive support for multilingual and globalization features will not be included in the prototype. Adapting the software for diverse languages and regions is a resource-intensive task that is deferred to future phases.

9.1.2 Source

Our source is from our own understanding. A.K.A Team HoneyComb.

9.1.3 Constraints

- Time Constraints
- Risk Constraints
- Human Constraints

9.1.4 Standards

- ISO/IEC 27001 - Information Security Management: This international standard provides a framework for information security management systems, which is essential for safeguarding sensitive data in a fraud detection software.
- ISO 9001 - Quality Management: This standard is relevant for maintaining a high level of quality in the software development process and ensuring that the fraud detection software meets industry standards.
- SANS Institute's Critical Security Controls: These are a prioritized set of actions to help organizations protect against the most common and damaging cyberattacks.

9.1.5 Priority

The following are not a high priority as we plan to face practical functionality that will fit within a two semester time date. Anything we deem time extensive, will be held to a lower degree and placed into an idea box where they will not be entirely cut from the project, rather if the idea fits and is able to be implemented, it will be placed and fixed into the final product.

References