Technische Universität Braunschweig

IAS | INSTITUTE FOR APPLICATION SECURITY

Software-Entwicklungspraktiktum (SEP)

ARID - Augmented Reality in Disguise

Software-Entwicklungspraktikum (SEP)
Sommersemester 2024

Angebot

Auftraggeber:
Technische Universität Braunschweig
Institut für Anwendungssicherheit (IAS)
Prof. Dr. Martin Johns
Mühlenpfordstraße 23
38106 Braunschweig

Betreuerin: Alexandra Dirksen

Auftragnehmer:

Name	E-Mail-Adresse
Amir Fakhim Hashemi	a.fakhim-hashemi@tu-braunschweig.de
Ibrahim Abdullah	i.abdullah@tu-braunschweig.de
Jadon-Kim Fischer	jadon-kim.fischer@tu-braunschweig.de
Mohamed Ali Mrabti	m.mrabti@tu-braunschweig.de
Tim Kütemeyer	t.kuetemeyer@tu-braunschweig.de
Vyvy Nguyen	Vyvy.nguyen@tu-braunschweig.de

Braunschweig, 16. April 2024

Bearbeiterübersicht

Kapitel	Autoren	Kommentare
1	Amir, Mohamed Ali	—
1.1	Amir, Mohamed Ali	—
1.2	Amir, Mohamed Ali	—
2	Amir, Mohamed Ali	—
3	Vyvy	—
3.1	Vyvy	—
3.2	Vyvy	—
4	Tim	—
4.1	Tim	—
4.2	Tim	—
4.3	Tim	—
5	Jadon	—
5.1	Jadon	—
5.2	Jadon	—
5.3	Jadon	—
6	Ibrahim	—
6.1	Ibrahim	—
6.2	Ibrahim	—
6.3	Ibrahim	—
7	Sämtliche	Fortlaufend ergänzt

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Steganographie ist eine Wissenschaft die es ermöglicht, Informationen verborgen in einem Trägermedium zu speichern, sodass sie vor der Einsicht dritter geschützt ist. In diesem Projekt nutzen wir diese Methode, um verschlüsselte Nachrichten innerhalb eines Bildes zu verbergen. Diese verschlüsselten Nachrichten können dann ausschließlich von autorisierten Personen gelesen werden, die im Besitz eines Augmented-Reality Geräts namens Monocle sind. So lässt es sich kommunizieren, ohne das unbefugte Personen verdacht schöpfen können.

1.1 Ziel

In einer Welt, in der Informationen und deren Sicherheit von zentraler Bedeutung sind, ist es unser Ziel, Botschaften öffentlich und doch unsichtbar, für Unbefugte zu verbergen. Bereits durch die Kryptographie können Informationen vor der Einsicht dritter geschützt werden, jedoch wird hier die Information vorher verschlüsselt und versendet. Hierbei ist immer bekannt das zwischen Parteien kommuniziert wird. Auf diese Weise, kann die Nachricht abgefangen und dessen Verschlüsselung geknackt werden, wodurch es zu diversen gefahren kommen kann. Durch die Kombination der beiden Wissenschaften, wollen wir in unserem Projekt ein Verfahren entwickeln, mit dem die Kommunikation verschleiert wird und die Informationen verschlüsselt sind, um so eine Möglichkeit zu bieten, verdeckt und sicher kommunizieren zu können. Für dieses Ziel generiere wir uns mithilfe von Künstlicher Intelligenz ein Bild welches unser Steganogramm darstellen soll. In dem Bild verstecken wir anhand von Steganographie einen QR-Code welcher eine Nachricht enthält. Diese Nachricht wird vorher mit dem AES verschlüsselt und daraus der QR-Code generiert. Um nun aus dem Steganogramm den QR-Code lesen und die Nachricht entschlüsseln zu können, verwenden eine Augmented-Reality Hardware namens Monocle. Dies ist ein Brillenglas ausgestattet mit einer eingebauten Kamera, wofür wir Software entwickeln, um diese Funktionen bereitzustellen. Nachrichten können mit diesem Verfahren sicher ausgetauscht werden, indem nur autorisierte Nutzer, die im Besitz des Monocle sind, die versteckten Nachrichten lesen können, während sie für den Rest nicht erkennbar sind.

1.2 Motivation

Im Rahmen unseres Softwareentwicklungspraktikums (SEP) sind wir bestrebt, nicht nur theoretisches Wissen anzuwenden, sondern auch praktische Lösungen zu entwickeln. Dieses Projekt, die Entwicklung von Software, das Arbeiten mit Künstlicher Intelligenz, sowie das Verwenden kryptografischer Verfahren, reflektiert diesen Ansatz. Es zielt darauf ab, die Übertragung von verschlüsselten Informationen sicherer zu gestalten, da Informationen teils von sehr großem Wert sein können. Ein weiterer Punkt der uns reizt, ist der Unterschied zur Kryptografie, bei dem die Existenz der verschlüsselten Nachricht die Aufmerksamkeit von Angreifern wecken kann. Mithilfe unseres Ansatzes, fügen wir eine weitere Sicherheitslayer hinzu, indem die Existenz der verschlüsselten Nachricht komplett verschleiert wird. Zudem bietet das Projekt eine Plattform, um die Technologien der Bildverarbeitung und Kryptographie zu kombinieren. Es bietet uns die Möglichkeit, praktische Erfahrungen in den Bereichen Bildverarbeitung, Kryptographie, eingebettete Systeme und Steganographie zu sammeln, während wir gleichzeitig unsere Fähigkeiten und unser Verständnis in diesen technisch anspruchsvollen Bereichen erweitern. Darüber hinaus ermöglicht das SEP, dass wir als Team in einem strukturierten Umfeld arbeiten können, wo wir nicht nur technische Fähigkeiten entwickeln, sondern auch lernen, wie man komplexe Probleme in einem kooperativen Kontext löst. Diese Erfahrungen sind für unsere akademische und berufliche Laufbahn von unschätzbarem Wert. Die Motivation hinter dem Projekt ist daher tief verwurzelt in unserem Bestreben, durch das SEP sowohl einen technologischen Beitrag zu leisten als auch persönliches Wachstum und berufliche Entwicklung zu fördern.

2 Formale Grundlagen

In diesem Kapitel wird die formale Grundlage für die Entwicklung der Software für das Monokel-Projekt dargelegt. Unsere Software wird für die Anwendung auf dem Monocle entwickelt. Das Gerät dient als Haupthardwareplattform, auf der unsere Software läuft. Darüber hinaus verfügen wir über einen Workflow zur Integration von QR-Codes, die steganographisch in KI-erstellte Bilder eingebettet wurden. Die verschlüsselte Nachricht wird dann mithilfe der Augmented-Reality-Hardware des Monocle angezeigt und bietet dem Benutzer ein interaktives Erlebnis.

Das Hauptziel der Software besteht darin, eine Lösung zu bieten, die es Nutzern ermöglicht, verschlüsselte Informationen und diskret zu entschlüsseln, zu lesen und zu zeigen. Dabei werden Informationen schnell und sicher zugänglich gemacht, unter Verwendung bereits vorhandener Methoden.

Wir haben uns für das Monocle von BrilliantLabs als AR-Gerät entschieden, weil es uns eine klare Richtlinie für die Entwicklung, wo wir MicroPython nutzen werden. Mit der Nutzung von MicroPython können wir sicherstellen, dass unsere Software optimal auf dem Monocle funktionieren wird , wo die Entwicklungszeit kurz wird und und es wird nicht zu komplex sein. Außerdem ermöglicht uns die Verwendung verschiedener Python-Bibliotheken und des AI-Modells StableDiffusion von StabilityAi eine effiziente Implementierung von Bildverarbeitung und Steganographie. Diese Kombination aus spezifizierter Hardware und flexiblen Softwaretools gibt uns die Grundlage, eine leistungsstarke und dennoch gute Anwendung für das Monocle zu entwickeln.

3 Projektablauf

In diesem Abschnitt wird der Projektablauf des ARID-Projektes beschrieben. Diesem sind die wichtigsten Termine und Meilensteine zu entnehmen und zudem ist eine visualisierte Darstellung anhand eines Gantt-Diagramm vorhanden.

3.1 Meilensteine

Aus der Tabelle sind die wichtigsten Termine zu ersehen, diese sind dabei festgelegte Termine des IBR und gruppeninterne Termine.

Nummer	**Meilenstein**	**Dokumente**	**Abgabetermin**
1	Projektstart - Kickoff	-	04.04.2024
2	Angebot Vorabgabe (Gruppenintern)	Angebot	17.04.2024
3	Angebot Abgabe	Angebot	17.04.2024
4	Pflichtenheft	Pflichtenheft	08.05.2024
5	Abnahmetestspezifikation	Abnahmetestspezifikation	08.05.2024
6	Vorabgabe Präsentation (Gruppenintern)	Präsentation	13.05.2024
7	Ziwschenpräsentation Präsentation der Building Blocks	Präsentation	17.05.204
8	Fachentwurf	Fachentwurf	29.05.2024
9	Technischer Entwurf	Technischer Entwurf	16.06.2024
10	Testdokumentation	Testprotokoll	03.07.2024
11	Fertigstellung Präsentation (Gruppenintern)	Präsentation	08.07.2024
12	TDSE - Vernissage	Poster	11.07.2024

3.2 Geplanter Ablauf

Der in dem Kapitel *Meilensteine* vorgestellte Projektablaufplan ist in der Abbildung 3.1 graphisch zusehen. Es wurden neben den festgelegten Meilensteine noch die Bearbeitungszeiten der Building Blocks abgebildet.

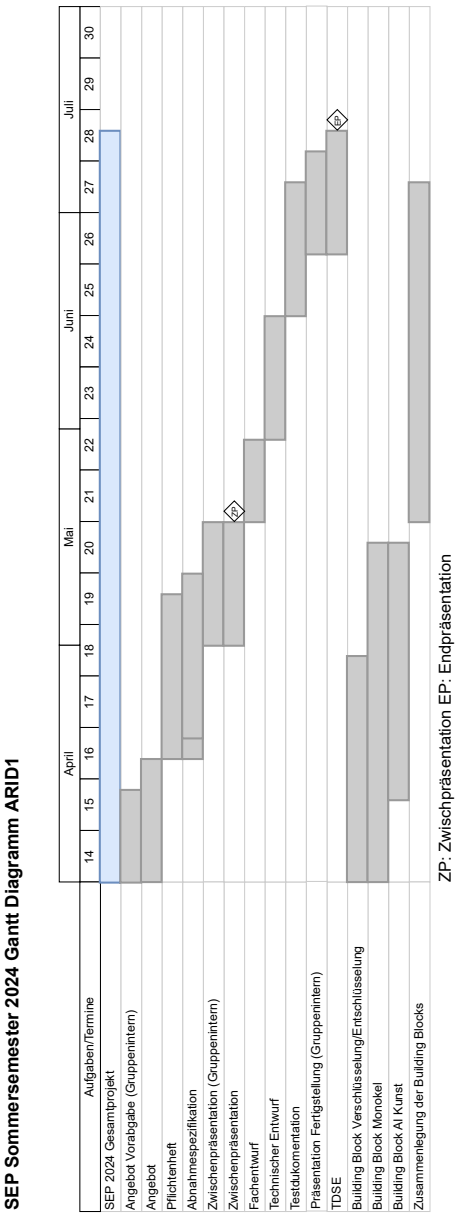

Abbildung 3.1: Gantt-Diagramm der Gruppe ARID1

4 Projektumfang

Dieses Kapitel definiert den Umfang des Projekts ARID - Augmented Reality in Disguise:

4.1 Lieferumfang

Der Lieferumfang umfasst folgende Komponenten und Aktivitäten:

1. **Building Blocks:**
   - Entwicklung einer MicroPython Software die das Erkennen, Dekodieren und darstellen des Klartexts von Barcodes auf dem Monokel ermöglicht.
   - Software zum erstellen von Barcodes mit verschlüsselten Nachrichten.
   - Ein Workflow zur Integration von Barcodes in KI generierte Bilder.
2. **Integration der Bausteine:** Zusammenführung der entwickelten Komponenten zu einem funktionalen Gesamtsystem.
3. **Vorbereitung der Vernissage für TDSE:**
   - Organisation von Druckmaterial und Präsentationsständen.
   - Entwicklung einer Halterungen für das Monokel.
   - Erstellung eines Projektposters.
4. **Dokumentation für das SEP:** Erstellung aller erforderlichen SEP-Dokumentationen, inklusive Angebotsdokumentation, Pflichtenheft, Abnahmetestspezifikation, Zwischenpräsentation, Fachentwurf, technischer Entwurf und Testdokumentation.

4.2 Kostenplan

Posten	**Teilkosten netto [€]**	**Teilkosten brutto [€]**
Sachkosten (Druckkosten, Lizenzkosten, etc.)	405,00	500,00
Geräte	234,90	290,00
Personalkosten	60750,00	75000,00
Gesamtkosten	**61339,90**	**75790,00**

4.3 Funktionaler Umfang

Der funktionale Umfang beinhaltet:

1. **Verschlüsselung von Nachrichten:** Verschlüsselung von Nachrichten und Generierung von Barcodes.
2. **Erstellung QR-Code AI Kunst:** Entwicklung einer Methode zur versteckten Integration von Barcodes in visuell ansprechende Kunstwerke.
3. **Barcode-Erkennung, Entschlüsselung und Darstellen des Klartexts:** Effiziente Erkennung und Entschlüsselung der versteckten Nachrichten in den Kunstwerken.
4. **Interaktive Präsentation während der Vernissage:** Präsentation der Technologie auf der TDSE, die es den Besuchern ermöglicht, die Kunst-Barcodes zu scannen und die verborgenen Nachrichten zu entschlüsseln.

5 Entwicklungsrichtlinien

Im Folgenden finden sich die technischen Eckdaten zu der Entwicklung der Monokel-Anwendung bezogen auf den Prozess der Erarbeitung.

Allem voran soll das Vorgehen des Projekts dem Modell SCRUM folgen. Die Sprints erfolgen wöchentlich und die Protokolle der Sprints und Reviews werden im Git abgelegt. Die Kommunikation mit dem Kunden erfolgt in Absprache alle zwei Wochen.

5.1 Konfigurationsmanagement

Für die Aufbewahrung und Versionierung der Anwendung stellt das IBR eine Instanz des Cloud-basierten Tools Gitlab zur Verfügung. Jede Änderung an der Anwendung wird mit einem Kommentar versehen und es wird ausschließlich ausführbarer Code für die anderen Teilnehmer über Gitlab zugänglich zu machen. Außerdem wird jede Änderung von dem Teilnehmer für die anderen zugänglich gemacht, der die Änderung selber durchgeführt hat. Für Dateien die bereit für die Übergabe sind, soll ein dafür ausgewiesener Ordner verwendet werden.

5.2 Design- und Programmierrichtlinien

Die Teilnehmer einigen sich darauf den Programmcode je nach Aufgabenteil (etwa Verschlüsselung-Eingabe) in dafür separate Dateien auszulagern. Zusätzlich sollen Kommentare in den Programmcode eingebettet werden, um den anderen Teilnehmern sowie dem Kunden die eigenständige Einsicht zu erleichtern. Codeabschnitte sollen so weit wie möglich in logisch geschlossene Funktionen zerlegt werden.

5.3 Verwendete Software

Für das Schreiben des Programmcodes wird die Entwicklungsumgebung Microsoft Visual Studio Code verwendet. Die Bearbeitung der Dokumententation erfolgt über Miktex und dessen Cloud-basierte Alternative Overleaf. In den Dokumenten erhaltene Diagramme werden mit dem als

Web-Anwendung verfügbaren Tool draw.io angefertigt. Sämtliche Dokumente basieren auf der dafür vorgesehenen Formatisierungssprache LateX.

Die KI Bilder werden unter Verwendung von StableDiffusion von StabilityAI generiert.

6 Projektorganisation

In diesem Kapitel wird die Kommunikation innerhalb des Teams und mit der Auftraggeberin festgehalten.

6.1 Schnittstelle zum Auftraggeber

Die Betreuerin kann über die universitäts-interne Matrix*-App erreicht werden, dabei wurde ein privater Chatraum für das ARID-Projekt eingerichtet. Hier können Fragen an die Auftraggeberin gestellt werden und mögliche Probleme, die auftreten können diskutiert werden. Zusätzlich steht eine E-Mail-Adresse zur Verfügung. Außerdem kann die Auftraggeberin im Büro des IAS aufgesucht werden. Es finden auch alle zwei Wochen persönliche Treffen zwischen des Teams und der Betreuerin statt. Diese dualen Kommunikationswege ermöglicht eine Zusammenarbeit mit dem Auftraggeber.

6.2 Schnittstelle zu anderen Projekten

Aktuell gibt es keine direkten Schnittstellen zwischen unserem Projekt und anderen Projekten innerhalb unseres Instituts oder externen Anwendungen.

6.3 Interne Kommunikation

Die interne Kommunikation des Teams findet über die Plattform Discord* statt. Für jede Projektphase wie Dokumentation, QR-Code-Verschlüsselung und Monocle-Programming wurden Räume eingerichtet. Die Treffen über Discord finden in Gruppenanrufen statt, an denen alle Teammitglieder teilnehmen können. Das ermöglicht die Ideen auszutauschen, weiteres Vorgehen, Probleme gemeinsam zu lösen und das Einholen von Feedback.

7 Glossar

(Alphabetisch und absteigend sortiert)

AES - Steht für Advanced Encryption Standard, welches eine Blockchiffre ist, die zum Ver- und Entschlüsseln von Informationen verwendet wird.

ControlNet - Ein Hochgeschwindigkeits-Kommunikationsprotokoll für industrielle Automatisierungs- und Steuerungssysteme, das den Datenaustausch zwischen Geräten wie SPS, Sensoren und Aktuatoren innerhalb eines Netzwerks ermöglicht.

Discord- Eine beliebte Plattform für Instant Messaging, Sprach- und Videoanrufe sowie soziale Interaktionen, die von verschiedenen Gruppen, einschließlich Gaming-Communities, für die Zusammenarbeit und Kommunikation genutzt wird.

Draw.io - Ist ein Online-Diagrammwerkzeug, das im Projekt verwendet wird, um verschiedene Arten von Diagrammen zu erstellen und zu bearbeiten.

Matrix - Ein offenes Kommunikationsprotokoll App für Echtzeitkommunikation.

Monocle - Hardware-Gerät der Firma Brilliant Labs in Form eines Monokels, das die Anwendung von AR-Technologie ermöglicht.

Git - Programm zur Versionsverwaltung von Code-Projekten. Änderungen werden in Paketen, so genannten "Commits", hinterlegt und über eine zentrale Schnittstelle zugänglich gemacht.

Overleaf- Ist eine Online-Plattform für die kollaborative Erstellung und Bearbeitung von LaTeX-Dokumenten.

Stable Diffusion - Eine gleichmäßige und stetige Ausbreitung von Partikeln, Substanzen oder Informationen innerhalb eines Mediums, wobei im Laufe der Zeit eine konstante Diffusionsrate beibehalten wird.

TDSE - Ist ein spezieller Tag, der der Anerkennung und Feier der Arbeit von Softwareentwicklern gewidmet ist.

Python- Ist eine weit verbreitete und vielseitige Programmiersprache, die für ihre Einfachheit, Lesbarkeit und Flexibilität bekannt ist.

MicroPython - Ist eine Variante der Programmiersprache Python, die für Mikrocontroller und eingebettete Systeme optimiert ist.

QR-Code - Kurz für Quick Response, ist ein zweidimensionaler Strichcode, welcher Informationen in Form von Zeichen und Ziffern speichert.

Steganographie - Wissenschaft der verborgenen Speicherung von Informationen in einem Trägermedium.

Steganogramm - Trägermedium, welches durch die Anwendung von Steganographie eine Nachricht enthält.

Kryptographie - Wissenschaft der Verschleierung von Informationen mittels Verschlüsselung mit dem Ziel den sicheren Austausch dieser zu ermöglichen.

IAS - Institut für Anwendungssicherheit an der TU Braunschweig.

IBR - Institut für Betriebssysteme und Rechnerverbund an der TU Braunschweig.

Visual Code Studio - ist eine integrierte Entwicklungsumgebung (IDE) von Microsoft, die eine Vielzahl von Tools und Funktionen für die Softwareentwicklung bietet.