

2. Mini-Projekt – Winner Linien

Tea Aliaj (12325250), Efe Bideci (12333450)

Januar 21, 2025

1. Einleitung

“Menschen sind oft das schwächste Glied in der Sicherheitskette und verantwortlich für das Scheitern von Sicherheitssystemen.” Mit diesem Gedanken im Hinterkopf analysieren wir im Rahmen unseres Projekts Schwachstellen im Wiener U-Bahn-Ticketsystem, die nicht auf Technik, sondern auf menschlichem Verhalten basieren. Unsere Beobachtungen zeigen, dass Kontrolleure oft visuelle Hinweise wie die Uhrzeit priorisieren und technische Prüfungen wie das Scannen von QR-Codes vernachlässigen, was dazu führen kann, dass sie unabsichtlich zu Listigkeiten und Täuschungen einladen. Also untersuchen wir, wie kognitive Verzerrungen gezielt eingesetzt werden können, ganz nach dem Motto “Amateure greifen Maschinen an, Profis Menschen”.

1.5. Ideenfindung

Bevor wir unser aktuelles Projektthema auswählten, haben wir fünf weitere Ideen gesammelt und eliminiert,

❖ **Kognitive Verzerrungen und deren Auswirkungen**

Untersuchen wir kognitive Verzerrungen und finden heraus, wie diese Entscheidungen beeinflussen können.

❖ **Hacker und ihre Vorgehensweise**

Analysen wir Methoden und Denkweisen von Hackern, um besser zu verstehen, wie sie Angriffe planen und durchführen.

❖ **Warum ist TUWEL die sicherste und beste Plattform auf der ganzen Welt**

Erklären wir anhand Tuwel(als ein Laborrat) populäre Hackerangriffe wie DDoS, Phishing, SQL-Injection und wie man sich dagegen schützen kann

❖ **Wie kann man kognitive Biases vermeiden**

Wir finden einige Techniken, um kognitive Verzerrungen zu vermeiden und uns gegenüber ihnen widerstandsfähiger zu machen.

❖ **Verbindung zwischen Critical und Criminal Denken**

Wir untersuchen die Auswirkungen von critical Denken oder nicht critical Denken in kriminellen Kontexten. Und die Grenze, an der intensives kritisches Denken zu Illegalität und ethischer Fragwürdigkeit führt.

2. State of Art

Wir haben recherchiert, welche Schwachstellen es in der Vergangenheit bei nicht-physischen Ticketsystemen gab, und interessante Beispiele gefunden. Einige davon, Boston's "CharlieCard", London's "Oyster Card" und die "Dutch OV-Chipkaart", basieren auf dem Mifare-Classic-Chipsatz. Bei diesen "Mifare Classic RFID" based Systemen wurde die Verschlüsselung geknackt, was es möglich machte, Kartenwerte zu verändern oder die Karten zu kopieren. [1][2][3][4]

Ein weiteres Beispiel ist die "Izmirim-Kart" aus der Türkei. Hier nutzte eine Person die Tatsache aus, dass die QR-Codes nicht vollständig verschlüsselt waren. So konnte sie ohne Bezahlung durch die Drehkreuze gehen, indem sie manipulierte Codes verwendete. [5]

Dagegen sieht in Wien die Situation anders aus. Wiener Linien verwendet keine NFC oder RFID Technologie. Außerdem sind die QR-Codes in den E-Tickets stark verschlüsselt. Sie können nur vom Anbieter korrekt gelesen werden. Diese Schwachstellen sind also hier nicht relevant.

Was macht Wien so besonders?

Anders als in vielen anderen Städten gibt es hier keine Drehkreuze, die den Zugang zu U-Bahn oder Straßenbahn kontrollieren. Stattdessen basiert das System auf Vertrauen. Die Kontrolle erfolgt durch zufällige Ticketprüfungen. Menschen, die kein Ticket haben, riskieren eine Strafe, was viele davon abhält, schwarz zu fahren. Für ehrliche Fahrgäste, die sowieso ein Ticket kaufen, macht das keinen großen Unterschied.

Aber wie passt unsere Idee dazu? Da das technische System sicher wirkt, haben wir uns entschieden, eine andere Schwachstelle zu nutzen die "kognitiven Verzerrungen der Menschen".

Auf den ersten Blick scheint die Idee, ein gefälschtes Ticket zu erstellen, wenig Erfolgchancen zu haben. Schließlich kann man leicht erkennen, wenn ein physisches Ticket oder Geldschein gefälscht ist. Solche Dinge folgen immer bestimmten Standards, und selbst kleine Abweichungen können Verdacht erregen.

Bei E-Tickets ist die Situation aber anders. Diese werden auf Smartphones angezeigt, und jedes Smartphone hat unterschiedliche Bildschirmgrößen und Auflösungen. Dadurch sehen die Tickets je nach Gerät anders aus. Trotzdem sollte der QR-Code der wichtigste Prüfpunkt sein, richtig?

In der Praxis scheint dies jedoch häufig nicht der Fall zu sein. Unsere persönlichen Beobachtungen zeigen, dass Ticketkontrolleure bei der U-Bahn den QR-Code oft außer Acht lassen. Stattdessen achten sie verstärkt darauf, ob die Uhr auf dem Ticket sich bewegt oder korrekt ist – und hier setzen wir an.

Unsere Idee basiert darauf, ein E-Ticket zu erstellen, das täuschend echt aussieht und eine realistisch animierte Uhrzeit anzeigt. Indem wir uns auf diese Beobachtung stützen, nutzen wir eine Schwachstelle, die nicht im System, sondern im Verhalten der Kontrolleure liegt.

2.1 Normstorming

Hier haben wir die Normen hinter Ticketkontrollsystemen analysiert. Normalerweise basiert solche Systeme auf der Annahme, dass QR-Codes und NFC-Technologien zuverlässig sind und als Basis für die Kontrolle dienen. Kontrolleure sollen also diese Technologien nutzen, um die Echtheit von Tickets zu prüfen.

Allerdings zeigt sich in der Praxis, dass die Sicherheit des Wiener Ticketsystems stark von der menschlichen Komponente abhängt. Unsere persönlichen Beobachtungen legen nahe, dass Kontrolleure bei U-bahn den QR-Code oft ignorieren. Stattdessen fokussieren sie sich vermehrt auf visuelle Merkmale wie die Uhrzeitanzeige. Dies könnte daran liegen, dass diese Merkmale schneller überprüfbar sind und intuitiv als ausreichend wahrgenommen werden.

Diese Abweichung von der Norm schafft eine Schwachstelle, die wir in unserem Projekt adressieren. Das System selbst ist technisch sicher, aber die menschliche Komponente also die Kontrolleure und deren Verhalten zeigt eine deutliche Schwäche. Das hat uns inspiriert, eine Schwachstelle beim Mensch und nicht in der Technik zu nutzen

2.2 Fame vs Shame

Hier hatten wir die Möglichkeit, die Stärken und Schwächen unserer Idee besser zu verstehen. Hier ist, was wir dabei erkannt haben:

➤ Fame

- ✓ Unser Projekt zeigt auf humorvolle Weise die kognitiven Schwächen der Kontrolleure und stellt diese ins Zentrum.
- ✓ Es ist kreativ und bringt eine originelle Perspektive auf ein alltägliches System.
- ✓ Durch unsere Beobachtungen ist das Projekt eng mit der Realität verknüpft und dadurch authentisch.

➤ Shame

- Wenn Kontrolleure die QR-Codes tatsächlich scannen würden, würde das Projekt sofort scheitern.
- Es gibt ethische Fragen: Wir zeigen zwar keine böse Absicht, aber das Projekt ist trotzdem illegal, auch wenn nur als Experiment. Unser Ziel ist es nicht, das Wiener Ticketsystem zu schwächen oder aktiv zu täuschen. Vielmehr wollen wir durch dieses Experiment die Bedeutung menschlicher Faktoren in der Sicherheit hervorheben und darauf hinweisen, wie kognitive Verzerrungen ausgenutzt werden können. Diese Erkenntnisse könnten genutzt werden, um zukünftige Sicherheitssysteme robuster zu gestalten.

3. Creative-Lotus Blossom

Unsere Idee basiert auf der gezielten Nutzung kognitiver Verzerrungen, die das Verhalten der Kontrolleure beeinflussen, deshalb starteten wir mit der zentralen Frage: "Welche kognitive Verzerrungen ausgenutzt werden und wie?".

Ausgehend von dieser Kernidee haben wir sechs Hauptbiases identifiziert, die unsere Projektentwicklung beeinflussen können:

- **Confirmation Bias:** Kontrolleure vertrauen eher auf das, was sie sehen will, und übersehen mögliche Hinweise auf Fälschung. Unser Ticketdesign enthält alle grobe Elemente, die ein echtes Ticket ausmachen, wie z. B. die typische Anzeige eines QR-Codes und ein übliches Layout. Es entspricht den Erwartungen, sodass es wird selten hinterfragt.
- **Anchoring Bias:** Kontrolleure verlassen sich auf das erste sichtbare Merkmal und vernachlässigen andere wichtige Details. In unserem Fall vermittelt die Uhranzeige auf dem Ticket das Gefühl von Aktualität und Authentizität. Kontrolleure konzentrieren sich oft auf die Uhrzeit, was das Ticket auf den ersten Blick glaubwürdiger macht.
- **Normalcy Bias:** Kontrolleure gehen davon aus, dass ein Ticket "normalerweise" echt ist, und übersehen mögliche Abweichungen. Es gibt nichts am Ticket, das ungewöhnlich aussieht. Kontrolleure gehen deshalb automatisch davon aus, dass es sich um ein echtes Ticket handelt.
- **Overconfidence Bias:** Die Annahme von der Kontrolleure, dass sie Täuschungen aufgrund von Erfahrung immer erkennen können, führt zu Nachlässigkeit.
- **Decision Fatigue/ Ego Depletion:** Nach mehreren Kontrollvorgängen werden ihren Entscheidungen hastig und oberflächlich getroffen. Denn Kontrollprozesse sind oft monoton, und mit der Zeit nimmt die Aufmerksamkeit ab, was führt dazu, dass Sicherheitsprotokolle vernachlässigt werden.

Diese Biases haben wir nicht nur identifiziert, sondern auch als Ansatzpunkte für unser Artefakt verwendet. Zum Beispiel dient die Uhranzeige im Ticket dazu, den Anchoring Bias auszunutzen. Gleichzeitig zeigt der Confirmation Bias, dass es ausreicht, wenn unser Ticket überzeugend aussieht, ohne perfekt zu sein. [6]

4. Project

Zu Beginn haben wir uns ein wenig mit der Wien Mobil App beschäftigt. Nachdem wir alle Fotos heruntergeladen und alle Daten abgerufen hatten, begannen wir mit Snack Expo zu arbeiten. Technisch haben wir mit js gearbeitet. Wir fügten einfach die Infos hinzu und bearbeiteten sie so, dass sie so identisch wie möglich mit der echten App waren. Das war gar nicht so schwer, da unsere Coding-Spezialistin Tea schon vorher damit gearbeitet hatte und es viele Informationen im Internet gibt. Mit Hilfe der Tutorials haben wir dann die funktionierende Uhr erstellt und voila. Alles fertig!

5. Reflexion und Feedback

Wie wurde Ihr Verständnis der gewählten Denkweisen durch diese Übungsarbeit verändert?

Unsere Arbeit hat uns gezeigt, wie eng Criminal Thinking und Critical Thinking miteinander verbunden sind und entscheidend ist, um Schwachstellen in scheinbar sicheren Systemen zu identifizieren und zu verstehen.

Am Ende haben wir durch diese Übung ein viel tieferes Verständnis darüber gewonnen, wie menschliche Schwächen gezielt in Cyberattacks und auch in vielen anderen Lebensbereichen ausgenutzt werden können. Wir haben auch erkannt, dass ein rein technischer Fokus oft nicht ausreicht, um ein System wirklich sicher zu machen, und dass die menschliche Komponente immer berücksichtigt werden muss.

Inwiefern kann ein nachhaltiges Verständnis der gewählten Denkweisen Ihnen im Studium oder danach im Beruf helfen?

Wir denken, dass diese neuen Verständnisse nicht nur theoretischer Natur, sondern für die Praxis hochrelevant sind. Criminal Thinking half uns, aus der Perspektive eines potenziellen Angreifers zu denken und menschliche Schwächen wie kognitive Verzerrungen zu unserem Vorteil zu nutzen. Gleichzeitig erforderte Critical Thinking, diese Erkenntnisse zu hinterfragen, objektiv zu bewerten und in ein praktikables Konzept umzuwandeln. Dieses Verständnis kann im Studium und später im Beruf besonders nützlich sein, beispielsweise bei der Entwicklung von Sicherheitsmechanismen, die sowohl technische als auch menschliche Faktoren berücksichtigen.

Welche Teile dieser Arbeit fanden Sie besonders schwer, welche zu einfach?

Der schwierigste Teil war, die kognitiven Verzerrungen so in unser Artefakt zu integrieren, dass sie wirklich überzeugend wirken. Unsere Beobachtungen waren zwar klar, aber daraus ein realistisches und funktionales Konzept zu entwickeln, hat Zeit gekostet. Es war eine Herausforderung, die Theorie so umzusetzen, dass sie praktisch Sinn ergibt. Dagegen die Codierungs Teil war sehr einfach, da Tea bereits viel Erfahrungen damit hatte (ein Lob an Code for Albania), und es war definitiv eine Herausforderung, den Hintergrund zu gestalten.

Welche Aspekte dieser Arbeit haben Ihnen gut gefallen, welche würden Sie wie ändern?

Besonders interessant war die Erkenntnis, dass unser Artefakt nicht nur eine theoretische Schwachstelle aufzeigt, sondern etwas sein könnte, das Menschen tatsächlich nutzen würden. Einige Kollegen_innen gaben in ihrem Feedback sogar an, dass sie sich vorstellen könnten, unser Artefakt selbst zu verwenden. Das zeigt, wie attraktiv und effektiv es auf den ersten Blick erscheint, auch wenn es rechtlich sussy ist.

Allerdings haben wir unser Artefakt nie in der Praxis getestet, da der Einsatz nicht legal ist. Eine mögliche Weiterentwicklung wäre, mit den zuständigen Behörden ein kontrolliertes Experiment durchzuführen. Mit weiterführenden Experimenten oder einer größeren Stichprobe könnten unsere Ergebnisse noch präziser und allgemeingültiger werden. Trotzdem glauben wir, dass unsere Arbeit ein gutes Beispiel dafür ist, wie wichtig es ist, menschliches Verhalten in Sicherheitskonzepten einzubeziehen.

Sind Sie mit Ihrer Arbeit zufrieden?

Ja, insgesamt sind wir sehr zufrieden. Wir haben gezeigt, dass Sicherheitslücken nicht nur durch Technik, sondern auch durch menschliche Schwächen entstehen können. Unser Artefakt nutzt Biases gezielt aus, was uns eine realistische und kreative Lösung ermöglicht hat. Natürlich gibt es immer Raum für Verbesserung, aber zu der Zeit, als es fertig war, war es ziemlich faszinierend!

References

- [1] <https://medium.com/@bobbyrsec/operation-charlie-hacking-the-mbta-charliecard-from-2008-to-present-24ea9f0aaa38>
- [2] <https://www.zdnet.com/article/security-researchers-hack-the-london-underground-train-for-free-ride/>
- [3] <https://en.wikipedia.org/wiki/OV-chipkaart#Security>
- [4] <https://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf>
- [5] <https://www.gazetemizmir.com/izmirim-karti-hackledi-ucretsiz-kullanimlarini-sosyal-medyada-anlatti/114492/>
- [6] <https://thesecuritycompany.com/the-insider/20-cognitive-biases-that-hackers-target-and-strategies-to-train-them-out/>