Contact Tracing *ohne* Überwachung?

von Mareen Przybylla, Beat Döbeli Honegger, Michel Hauswirth und Michael Hielscher

Um Infektionsketten zu unterbrechen, wurden während der Covid-19-Pandemie in vielen Ländern Contact-Tracing-Apps entwickelt. In diesem Beitrag wird die Entwicklung und Erprobung einer Unterrichtseinheit für die Sekundarstufe I vorgestellt, mit der die Funktionsweise von dezentralen Contact-Tracing-Apps und die dahinterstehenden Informatikkonzepte erklärt werden.

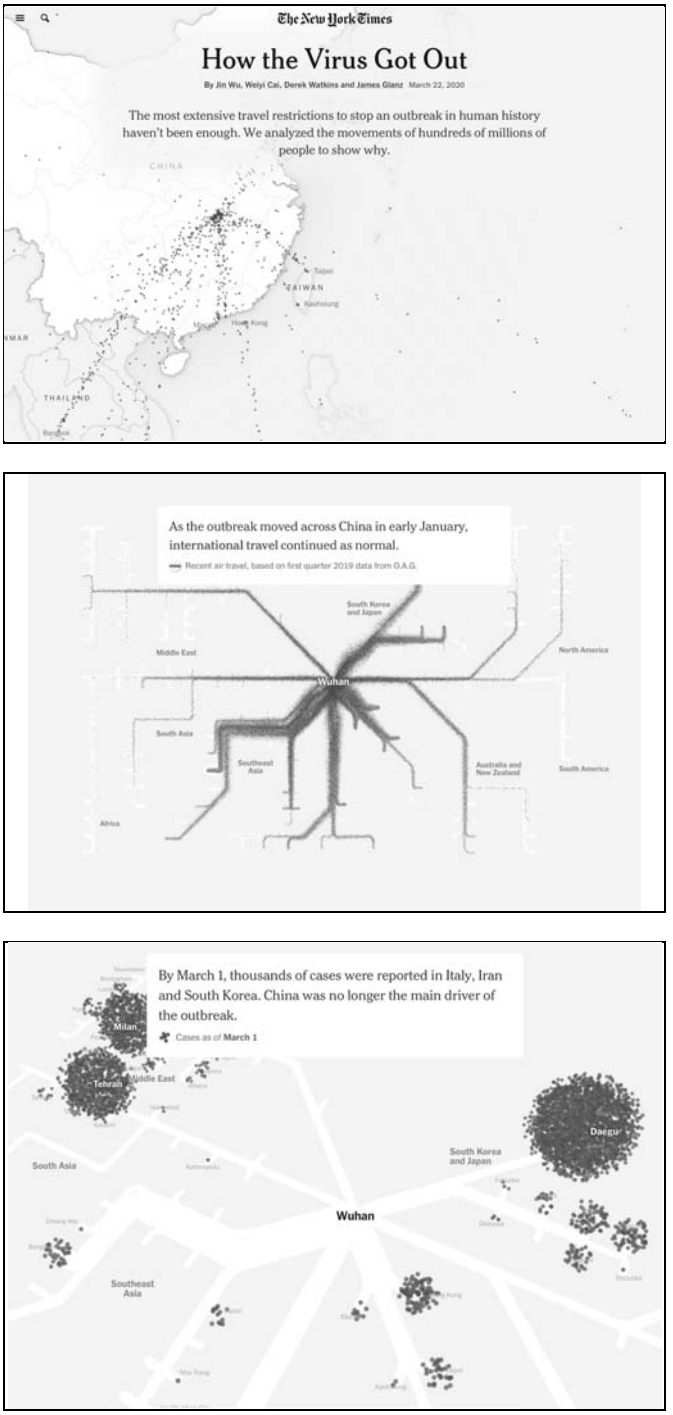
Worum geht es?

Die etwa seit den 1960er-Jahren immer stärker zunehmende Globalisierung ermöglicht heutzutage eine nahezu uneingeschränkte Mobilität von Personen weltweit. Dies bringt neben allen Vorteilen auch Risiken mit sich: Beispielsweise können sich Infektionskrankheiten heute mit rasanter Geschwindigkeit über den gesamten Globus verbreiten. Aktuellstes Beispiel dafür ist die COVID-19-Pandemie, deren erste Fälle in der chinesischen Großstadt Wuhan bekannt wurden. Von dort aus verbreitete sich das Virus binnen weniger Wochen über alle Kontinente. Auf einer Webseite der *New York Times* wird dies besonders anschaulich erklärt (vgl. Wu u. a., 2020; siehe auch Bild 1, nächste Seite).

Die Weltgesundheitsorganisation (WHO) hat im Jahr 1999 ihre ersten Empfehlungen zu Planung nationaler Maßnahmen im Falle von (globalen) Pandemien herausgegeben (vgl. WHO, 2017); viele Länder haben seitdem nationale Pandemiepläne erarbeitet. Die Schweiz bereitet sich beispielsweise sogar bereits seit 1995 systematisch auf Pandemien vor und hat im Jahr 2004 ihren ersten Influenza-Pandemieplan veröffentlicht (vgl. BAG, 2018); in Deutschland wurde 2005 erstmals ein nationaler Pandemieplan vom Robert-Koch-Institut herausgegeben (vgl. RKI, 2017). Das Hauptziel von Maßnahmen zur Bekämpfung von Pandemien ist die Unterbrechung der Übertragungsketten, um weitere Infektionen zu verhindern und die unkontrollierte Weiterverbreitung einzudämmen. Dabei spielt neben Einschränkungen von Reisetätigkeiten und allgemein der Reduktion von Kontakten zu anderen Menschen („Social Distancing“) unter anderem das sogenannte „Contact Tracing“ eine große Rolle, also die Rückverfolgung von engen Kontakten infizierter Personen, um alle Betroffenen zu informieren und bis zur Klärung einer potenziellen Infektion von ihren Mitmenschen zu isolieren. Manuelles Contact Tracing ist aufwendig: Geschultes Personal muss mit jeder infizierten Person über einen längeren Zeitraum (z. B. 14 Tage) eruieren, wann und wo Kontakte stattgefunden haben, die zu einem erhöhten Ansteckungsrisiko führen, also Personen identifizieren, die sich möglicherweise angesteckt haben. Je mehr Infizierte es gibt, desto schneller gerät das manuelle Contact Tracing an seine Grenzen. Daher wird viel Hoffnung in die Verwendung von Contact-Tracing-Apps gesetzt, die es ermöglichen sollen, ihre Nutzerinnen und Nutzer zu informieren, wenn diese über einen längeren Zeitraum Kontakt zu einer infizierten Person hatten, die ebenfalls diese App auf ihrem Handy installiert hat. Hierfür installieren idealerweise alle Personen, die ein Smartphone besitzen, eine entsprechende Anwendung auf ihrem Gerät. Wenn sich nun zwei Personen in kurzer Distanz zueinander aufhalten, tauschen die Geräte Daten aus, um sich diesen Kontakt zu „merken“, falls dieser über einen gewissen Zeitraum (z. B. 15 Minuten) bestehen bleibt. Sollte sich eine dieser Personen später infizieren, kann sie dies über die App ihren Kontaktpersonen mitteilen. Auf diese Weise soll das Contact Tracing auch dahingehend erweitert werden, dass unbekannte Kontaktpersonen schnell informiert werden können (beispielsweise, wenn der Kontakt bei einer längeren Fahrt mit öffentlichen Verkehrsmitteln zustande kam).

Als Anfang 2020 die Einführung solcher Apps in verschiedenen Ländern diskutiert wurde, waren die Positionen dazu vielfältig und reichten von euphorischer Hoffnung (“Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown”, vgl. University of Oxford, 2020) bis hin zu großer Skepsis und Vergleichen mit einem Überwachungsstaat: „Das Parlament bereitet derzeit die Schaffung der rechtlichen Grundlagen für die Einrichtung eines staatlichen Informationssystems vor, das Bewegungen, Orte, Aufenthaltsdauer und Begegnungen im gesellschaftlichen Leben aufzeichnen soll […] Das erinnert mich an George Orwell und ‚1984‘, und das macht mir ein wenig Angst“ (Thomas de Courten, Nationalrat der Schweizerischen Volkspartei (SVP), zitiert nach Mombelli, 2020).

Seit dem 25. Juni 2020 steht die schweizerische Contact-Tracing App für Android und iOS zur Verfügung und wurde bis zum 29. Oktober 2020 2,68 Millionen Mal heruntergeladen. Am 31. Oktober 2020 waren bei 8,6 Millionen Einwohnern der Schweiz und Liechtenstein 1,84 Millionen Apps aktiv und in der letzten Woche davor hatten 6384 Personen über die App eine Infektion gemeldet (vgl. BFS, 2020).



Quelle: Wu u.a., 2020

Bild 1: Ausschnitte aus der Webseite der *New York Times* zur Visualisierung der Virusverbreitung über den Globus.

Didaktische Ziele

An der Pädagogischen Hochschule Schwyz wurde im Frühsommer 2020 mit der Entwicklung einer Unterrichtseinheit für die Sekundarstufe I zur schweizerischen Covid-App begonnen, die auf der gleichen technologischen Grundlage basiert wie die Apps anderer Länder (z.B. Deutschland). Im Laufe des Sommers konnte die Unterrichtseinheit in mehreren Weiterbildungen mit Lehrpersonen sowie den Dozierenden der Pädagogischen Hochschule Schwyz erprobt und aufgrund dieser Erfahrungen überarbeitet werden. Hinter der Entwicklung standen folgende Ziele:

- ▷ *Gesundheitsförderung:* Förderung der Akzeptanz der App durch Erklärung der (datensparsamen) Funktionsweise der App und damit Beitrag zur Pandemieeindämmung durch die Informatikdidaktik.
- ▷ *Informatik im Kontext:* Erklärung langlebiger Informatikprinzipien anhand eines aktuellen, alltagsrelevanten Beispiels.
- ▷ *Fachliche Fundierung von gesellschaftlichen Fragen:* Versachlichung aktueller gesellschaftspolitischer Diskussionen durch Vermittlung informatischer Kompetenzen.

Zugrundeliegende Informatikkonzepte

In der entwickelten Unterrichtseinheit sollten folgende, in der Contact-Tracing-App steckende Informatikkonzepte exemplarisch gezeigt und erklärt werden:

Privacy by Design

Im europäischen Raum wird viel Wert auf den Schutz der Privatsphäre gelegt. Spätestens seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) bzw. General Data Protection Regulation (GDPR) der Europäischen Union, die zumindest teilweise auch die Schweiz betrifft, spielt „Privacy by Design" bei der Entwicklung von Software eine große Rolle. In Art. 25 Abs. 1 der DSGVO heißt es (EU, 2016, S.48):

> Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Ver-

arbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Konkret bedeutet dies für die Entwicklung von Software, dass bereits zu Beginn der Konzeption immer mitberücksichtigt wird, dass ausschließlich für den jeweiligen Zweck notwendige Daten erfasst, gespeichert und verarbeitet werden. Dementsprechend wurden in Bezug auf die Contact-Tracing-App unterschiedliche Ansätze diskutiert, analysiert und verfolgt, um das Ziel zu erreichen, mittels einer App das Contact Tracing zu ermöglichen und dabei die Privatsphäre der Nutzerinnen und Nutzer maximal zu schützen. Dabei ging es unter anderem um die Frage, welche Daten erfasst und wie diese verwaltet werden sollen.

Datensparsamkeit

Eine zentrale Strategie zur Umsetzung von „Privacy by Design" ist das Prinzip der *Datensparsamkeit* (auch *Datenminimierung* genannt). Dabei wird darauf geachtet, zur Lösung eines Problems möglichst wenig Daten überhaupt zu erfassen, zu speichern und zu übertragen, denn nicht vorhandene Daten können auch nicht missbraucht werden. Angewandt auf das Problem des Contact Tracings bedeutet dies, dass eine datensparsame App weder die Namen der Nutzenden noch ihre Aufenthaltsorte erfassen und speichern muss. Es reicht, wenn die App darüber informiert, zu welchem Zeitpunkt man näheren und längeren Kontakt mit jemandem hatte, der sich als positiv getestet bekannt hat. Der Zeitpunkt des Kontakts hilft, dass die benachrichtigte Person sich aus dem Gedächtnis erinnern kann, wo und eventuell mit wem der Kontakt stattgefunden hat und damit die effektive Gefährlichkeit einschätzen kann.

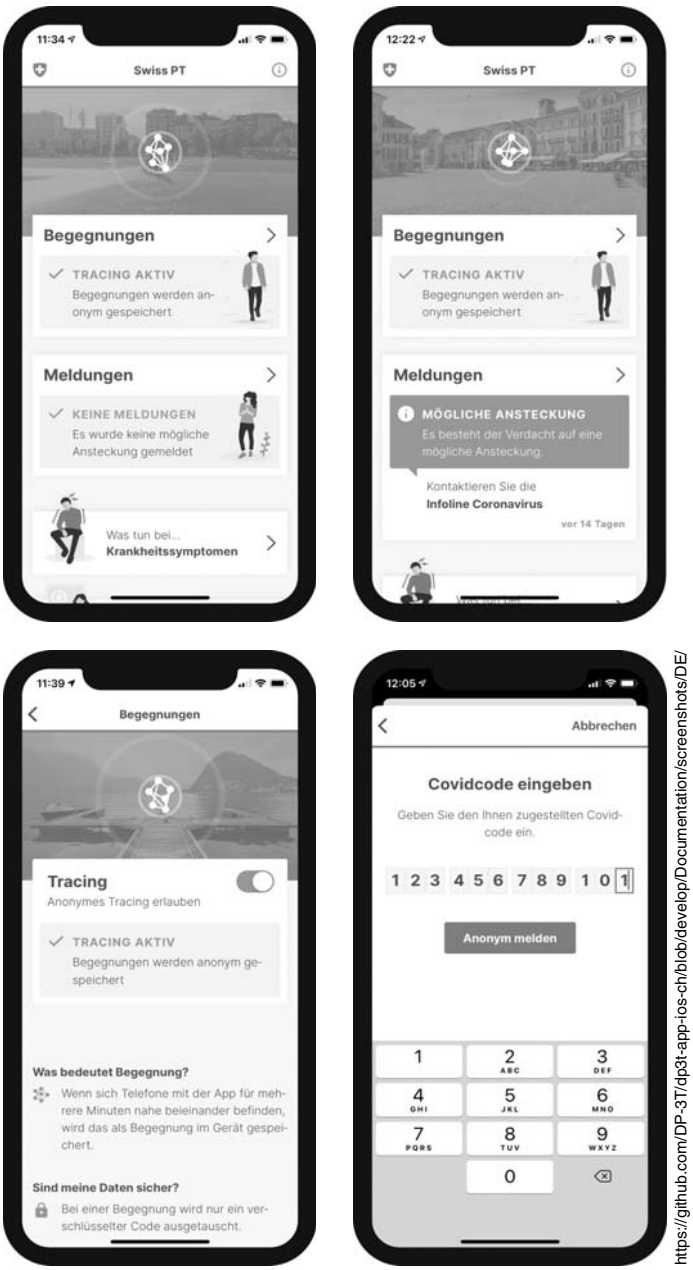
Zentrale vs. dezentrale Datenspeicherung

Eine grundlegende Entscheidung, die in Hinblick auf „Privacy by Design" in der Planung zur Entwicklung von Contact-Tracing-Apps getroffen wurde, war die Frage der Speicherung der Kontakte entweder zentral auf einem Server oder dezentral auf den jeweiligen Endgeräten. Der zentrale Ansatz sieht vor, dass per App alle IDs von Kontaktpersonen einer infizierten Person an einen zentralen Server gesendet werden, der dann diese Personen über eine Nachricht auf ihren Geräten informiert. Da hierbei alle Daten an einem zentralen Platz gespeichert sind, birgt dies das Risiko für Missbrauch: Sollte jemand unberechtigt Zugriff auf den Server bekommen, ist die De-Anonymisierung und Offenlegung privater Daten grundsätzlich möglich (vgl. Lehner, 2020). Der dezentrale Ansatz sieht vor, dass nur infizierte Personen ihre eigene ID an einen Server übermitteln und alle Geräte regelmäßig die Daten vom Server mit den gespeicherten Kontakten abgleichen. Auf diese Weise kann sichergestellt werden, dass nur die Kontaktpersonen selbst darüber Bescheid wissen, dass sie Kontakt zu einer infizierten Person hatten. Der zentrale Server kennt lediglich die IDs der Infizierten.

Die EU hat im April 2020 Leitlinien für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 verabschiedet (vgl. European Data Protection Board, 2020), in denen beide Varianten zugelassen werden, aber eine Empfehlung für die dezentrale Datenspeicherung ausgesprochen wird, da diese „im Allgemeinen eher dem Grundsatz der Datenminimierung" entspräche. In diesen Leitlinien wird unter anderem klargestellt, dass „Grundsätze der Datenminimierung sowie des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen eingehend berücksichtigt werden" sollen, indem

a. keine Standorte, sondern Begegnungsdaten erfasst und gespeichert werden,

Bild 2 (unten): Bildschirmkopien der Schweizer Contact-Tracing-App *SwissCovid*.



https://github.com/DP-3T/dp3t-app-ios-ch/blob/develop/Documentation/screenshots/DE/

b. geeignete Maßnahmen getroffen werden, um eine De-Anonymisierung zu verhindern,
c. erhobene Informationen im Endgerät des Nutzers verbleiben,
d. lediglich relevante Informationen, sofern absolut notwendig, erhoben werden.

Umsetzung als App mit DP3T

Die folgenden Erläuterungen beziehen sich auf die Funktionsweise der Schweizer Proximity-Tracing-App *SwissCovid* (siehe Bild 2, vorige Seite), die den dezentralen Ansatz verfolgt.

Die Benutzer installieren diese App auf ihrem Smartphone, schalten Bluetooth dauerhaft ein und tragen das Smartphone immer bei sich. Das Smartphone tauscht dann via Bluetooth verschlüsselte IDs (Prüfsummen) mit Geräten aus, die sich für einen definierten Zeitraum (15 Minuten innerhalb eines Tages) in einem definierten Abstand (<1,5 Meter) zum eigenen Gerät befinden. Die von den Geräten gespeicherten Prüfsummen werden nach einer bestimmten Zeit wieder gelöscht (14 Tage). Alle hier angegebenen Werte stammen von der Webseite des BAG (vgl. BAG, 2020) und werden mit zunehmender Erfahrung angepasst.

Wird ein Nutzer der App positiv auf das Coronavirus getestet, erhält er vom Arzt einen sogenannten *Covidcode*, mit dem er über die App seine Kontaktpersonen anonym informieren kann, dass sie sich möglicherweise angesteckt haben.

Die dabei genutzte Technologie ist unter dem Namen *Decentralised Privacy-Preserving Proximity Tracing* (deutsch: dezentralisierte Privatsphäre-schützende Nahbereichsverfolgung – kurz: DP-3T, auch DP3T) bekannt und wird auf Github dokumentiert (vgl. DP-3T, 2020; siehe auch Kasten „DP-3T – Das Konzept in acht Schritten", nächste Seite).

Dieses Verfahren eignet sich also gut, um Epidemiesoftware auf einem Smartphone zu nutzen, ohne sich dabei in einen Überwachungsstaat zu begeben. Es gilt aber natürlich zu bedenken, dass Menschen anhand der Zeitstempel und mithilfe ihrer Erinnerung durchaus in der Lage sein können, Rückschlüsse auf die Infektionsquelle zu ziehen.

Didaktische Überlegungen

Bei der Erarbeitung der Unterrichtseinheit für Schülerinnen und Schüler ab der Sekundarstufe I wurden folgende didaktische Überlegungen angestellt.

Umsetzung als Rollenspiel

Kern der Unterrichtseinheit ist ein Rollenspiel nach dem Ansatz *Computer Science Unplugged*. Dies soll die Verständlichkeit der abstrakten Datenstrukturen und Abläufe erhöhen, aber auch einen Gegensatz bilden zu den vorhandenen Ängsten vor den vermeintlich versteckt im Smartphone ablaufenden Überwachungsalgorithmen. Durch das Rollenspiel soll kein Aspekt der Funktionsweise der App im Verborgenen bleiben. Ein nicht unerwünschter Nebeneffekt des Verzichts auf Computer ist die einfachere Umsetzbarkeit und rasche Verbreitung der Unterrichtseinheit in verschiedenen Kontexten.

Betonung der Freiwilligkeit

In der Schweiz wurde gesetzlich verankert, dass sowohl die Installation und Nutzung der App als auch die bei positivem Covid19-Test erwünschte Meldung der Infektion durch Eingabe des Covidcodes in die App absolut freiwillig sein muss. Um die Akzeptanz des digitalen Contact-Tracings zu fördern und um auch bei der gesellschaftspolitischen Diskussion die relevanten Überlegungen bei der App-Entwicklung abzubilden, wird der Aspekt der Freiwilligkeit an verschiedenen Stellen des Rollenspiels betont.

Betonung der dezentralen Datenspeicherung

Die dezentrale Datenspeicherung soll den Schülerinnen und Schülern im Rollenspiel deutlich erfahrbar gemacht werden.

Didaktische Reduktion

Um die Verständlichkeit für alle Schülerinnen und Schüler ab der Sekundarstufe I zu erhöhen, wurden an verschiedenen Orten Vereinfachungen der tatsächlichen Abläufe vorgenommen. Insbesondere bei der Hashfunktion wurde zugunsten der Verständlichkeit und rascher Umsetzbarkeit im Unterricht sehr stark reduziert. Das Generieren der Schlüssel mittels Hashfunktion wird aufgrund der Komplexität nicht durchgeführt, sondern bei Interesse außerhalb des Rollenspiels im Unterricht besprochen. Stattdessen erhalten die Schülerinnen und Schüler einen Umschlag (repräsentiert die App auf dem Smartphone) mit Karten, auf denen eine Matrix an Emoticons abgebildet ist (siehe Bild 3, übernächste Seite).

Diese repräsentieren die Prüfsummen, die untereinander ausgetauscht werden (markiert mit den Ziffern 1 bis 5), und sind so aufgebaut, dass die Anzahl zweier Arten von Smileys (z.B. x Kusssmileys und y Sonnenbrillensmileys) pro Smartphone-Umschlag immer gleich sind; dies repräsentiert den geheimen Schlüssel des jeweiligen Nutzers. Eine weitere Karte enthält den zufällig generierten geheimen Schlüssel (markiert mit „behalten"). Auf diese Weise sind zentrale Elemente einer Einwegfunktion gewahrt: Es ist relativ einfach, die Matrix zu erstellen, aber unwahrscheinlich, aus einer beliebigen Matrix den geheimen Schlüssel zu erraten (sofern unbekannt ist, um welche Emoticons es geht). Auch beim Covidcode wurde reduziert: Dieser wird im Spiel durch die Ärzte in Form eines Klebezettels mit ei-

DP-3T – Das Konzept in acht Schritten

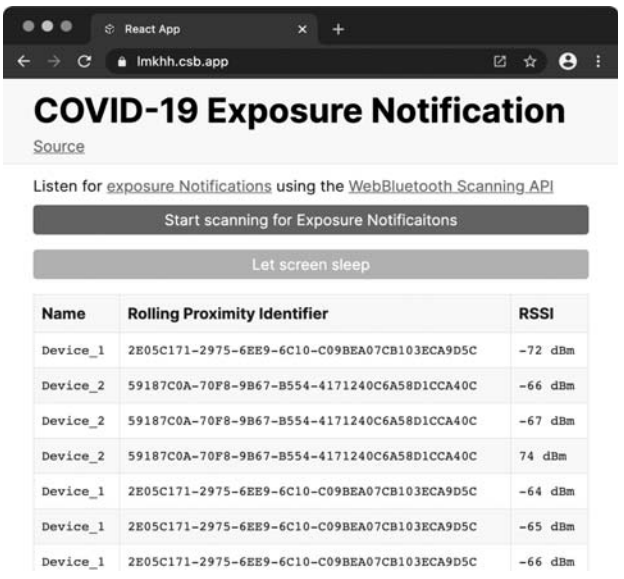
in Anlehnung an Recher/Traussnig, 2020

1. Schlüssel generieren
Jedes Gerät generiert beim ersten Start der App einen digitalen Schlüssel, der so lang ist, dass es sehr unwahrscheinlich ist, dass mehrere Geräte den selben Schlüssel generieren.
Beispiel einer solchen (pseudo-)zufälligen Zeichenkette: 4dae1ca7847ccc86e0ad488bf322d30cd45430b7d57cbba9f8ac210ed4e89443 (hier: 64 hexadezimale Zeichen (je 4 Bit) → 256 Bit → 2^256 = 1158×10^77 mögliche Schlüssel (!)).

2. Sich bemerkbar machen
Jedes Gerät sendet im laufenden Betrieb über Bluetooth LE (Reichweite etwa 10 Meter) in regelmäßigen Zeitabständen ein Datenpaket aus, um nahe Geräte über seine Präsenz zu informieren.

3. Austausch initiieren
Empfängt ein anderes Gerät dieses Signal, antwortet es und bittet um weitere Informationen, nämlich einen Zeitstempel und eine Prüfsumme, die es abspeichert.

4. Prüfsumme berechnen und übermitteln
Das angefragte Gerät generiert nun mittels eines kryptografischen Verfahrens (Hashfunktion: HMAC – Hash Message Authentication Code) aus seinem geheimen Schlüssel und dem aktuellen Zeitstempel eine Prüfsumme und sendet diesen zusammen mit dem Zeitstempel an das andere Gerät (siehe Bild):



https://lmkhh.csb.app

Auflistung der durch die *SwissCovid-App* veranlassten Aussendung der Identifier zweier Geräte.

HMAC(Schlüssel + Zeitstempel) = Prüfsumme
HMAC(4dae1ca7847ccc86e0ad488bf322d30cd45430b7d57cbba9f8ac210ed4e89443 + 2020-08-25T11:01:06) = 64e5db55ef3fe6ff55cbeb5e96a64734abe6f855ab98955ce85d85368c934fb9
Die Berechnung der Prüfsumme erfolgt mittels einer Einwegfunktion, das heißt aus dem Schlüssel und dem Zeitstempel kann zwar die Prüfsumme leicht berechnet werden, es ist jedoch nahezu unmöglich, aus der Prüfsumme und dem Zeitstempel umgekehrt den geheimen Schlüssel zu ermitteln (einzig bekanntes Verfahren: Schlüssel raten, Prüfsumme aus dem geratenen Schlüssel berechnen und mit tatsächlicher Prüfsumme vergleichen). Hashwerte haben, unabhängig von der Eingabelänge, immer dieselbe Länge, welche je nach verwendetem Verfahren variiert. Ein Tool zur Berechnung von HMACs findet sich beispielsweise bei *Codebeautify.org* (Code Beautify, 2020).

5. Angaben speichern
Jedes Gerät speichert die empfangenen Zeitstempel-Prüfsummen-Paare für 14 Tage (oder einen anderen definierten Zeitraum).

6. Infektion melden
Wird ein App-Nutzer positiv getestet, erhält er von zertifizierter Stelle einen sogenannten *Covidcode*, mit dem er über die App seine Infektion bekannt geben kann. Auf diese Weise soll Missbrauch durch Falschmeldungen verhindert werden. Die App schickt nun den geheimen Schlüssel, der zur Generierung der Prüfsummen verwendet wurde, an einen Server. Dies ist unter Berücksichtigung der Privatsphäre der Nutzer möglich, denn aus dem geheimen Schlüssel können keinerlei Rückschlüsse auf das dahinterstehende Gerät resp. die dazugehörige Person abgeleitet werden.

7. Schlüssel herunterladen
Alle Geräte synchronisieren sich regelmäßig (ca. alle 12 Stunden) mit dem Server und laden die veröffentlichten Schlüssel infizierter Personen herunter.

8. Schlüssel prüfen
Mit diesen Schlüsseln werden nun alle gespeicherten Zeitstempel-Prüfsummen-Paare getestet: kann aus einem Zeitstempel und einem der heruntergeladenen Schlüssel eine korrekte Prüfsumme berechnet werden, befanden sich also die Geräte der infizierten Person und des Nutzers in kurzer Distanz zueinander. Sind mehrere solcher Einträge vorhanden, steigt die Wahrscheinlichkeit einer Ansteckung. Anhand der Zeitstempel kann (zumindest grob) bestimmt werden, über welchen Zeitraum der Kontakt bestand und somit bei Überschreitung der 15 Minuten eine entsprechende Information erfolgen.

ner durch 7 teilbaren Zahl verteilt. Dies dient dazu, missbräuchlicher Verwendung vorzubeugen. Nur offiziell bestätigte Fälle sollen ihre Infektion über die App melden können. Im Rollenspiel können positiv „getestete“ Schülerinnen und Schüler entscheiden, ob sie ihre Emoticon-Karte, auf deren Rückseite „behalten“ stand, in eine Schachtel werfen möchten. Es kann dann durch den Server geprüft werden, ob der Covidcode echt ist (d.h. ob ein Klebezettel mit einer durch 7 teilbaren Zahl vorhanden ist). Natürlich ist Teilbarkeit durch 7 keine besonders starke Verifizierung, aber es reicht für den Zweck aus, sich der Überprüfbarkeit des Codes durch den Server bewusst zu werden.

Umsetzung als Rollenspiel

Das Rollenspiel besteht aus drei unterschiedlichen Rollen bzw. Posten und vier Phasen. Eine Lehrperson

kann das Rollenspiel ohne weitere Unterstützung durchführen (benötigt etwas mehr Zeit in der Durchführung) oder kann sich durch 1 bis 2 weitere Personen (z. B. Schülerinnen) helfen lassen (benötigt etwas mehr Vorbereitungszeit).

Rollen und Posten

Rolle	Aufgabe	Material	Bemerkungen
Spielleitung	teilt Rollen zu		Lehrperson
App-Nutzende	verwenden die App, tauschen Prüfsummen aus, gleichen mit Server ab	Umschläge mit je einem Kartenset (einige Umschläge sind unauffällig markiert, siehe Bild 4, nächste Seite)	alle verbleibenden Schülerinnen und Schüler
Arzt/Ärztin	führt Test durch und vergibt ggf. Covidcode	ca. 6 Klebezettel mit je einer durch 7 teilbaren Zahl (Rollenkarte)	Lehrperson oder 1–2 Schülerinnen/ Schüler
Server	prüft Korrektheit der Covidcodes und gibt entsprechende Schlüssel zum Download frei	Sammelbox Infowand (Rollenkarte)	Lehrperson oder 1–2 Schülerinnen/ Schüler

Vorbereitung

Als Vorbereitung muss das in der Tabelle erwähnte Material bereitgestellt werden. Dabei müssen die Umschläge mit den App-Bildschirmkopien bedruckt oder beklebt (Vorderseite: Home Screen der App, Rückseite: Anweisungen im Falle einer Infektion) und mit einem zusammengehörigen Kartenset bestückt werden. Einige Umschläge sollten mit einer unauffälligen Markierung versehen werden. Diese wird später als Hinweis auf Krankheitssymptome genutzt werden (siehe Bild 4, nächste Seite). Die Rollenkarten sind nur notwendig, wenn die Rolle nicht durch die Lehrperson übernommen wird.

Spielstart

Alle App-Nutzenden erhalten zu Spielbeginn einen Umschlag mit einem Set an Karten. Auf diesen Karten muss die Anzahl der Emoticons mit denen des geheimen Schlüssels („behalten"-Karte, z. B. 3 Kusssmileys, 2 Sonnenbrillensmileys) übereinstimmen. Der Umschlag symbolisiert das Smartphone, auf dem die SwissCovid-App installiert ist, die Karten enthalten jeweils eine Matrix mit unterschiedlichen Emoticons, die symbolisch für die Prüfsummen stehen, die mit anderen Geräten ausgetauscht werden (siehe Bild 3). Die Schülerinnen legen die Emoticon-Karte „behalten" auf ihr Pult. Diese Schlüsselkarte kann nach einem positiven Testresultat freiwillig auf den Server „geladen" werden. Die anderen Karten nehmen die Schülerinnen in die Hand. Sie dürfen nicht im Couvert bleiben, da dort die gesammelten Prüfsummen „gespeichert" werden.

Bild 3: Umschlag symbolisiert das Smartphone, Emoticon-Karten repräsentieren die auszusendenden Prüfsummen und befinden sich zu Beginn im Umschlag.

Phase 1: App im Alltag nutzen

Zu Beginn des Spiels laufen alle Schülerinnen und Schüler mit ihrem „Smartphone" beispielsweise auf dem Schulhof umher. Sobald zwei Personen sich nahe genug kommen (etwa <1,5 m), sprechen sie einander an und tauschen Emoticon-Karten untereinander aus. Die zu vergebenden Karten halten sie in ihrer Hand, empfangene Karten werden in den Umschlag gesteckt und dort „dezentral gespeichert". Es ist darauf zu achten, dass nicht versehentlich eigene und erhaltene Karten vertauscht werden. Wenn Schülerinnen und Schüler für die Rolle der Arztpraxis und des Servers eingesetzt werden, so machen sich diese währenddessen mit ihren Rollen vertraut.

Phase 2: Einzelne Personen erkranken

Einzelne Umschläge sind an einer zunächst nicht sichtbaren Stelle mit Stickern markiert. Dies bedeutet, dass diese Personen Krankheitssymptome haben und sich zur ärztlichen Untersuchung begeben sollten (siehe Bild 4, nächste Seite). Die Schülerinnen und Schüler werden darüber von der Spielleitung im Laufe des Spiels informiert.

Die potenziell Infizierten gehen zur Arztpraxis, werden dort getestet und erhalten bei positiver Testung einen Covidcode (notiert auf einem Klebezettel). Positiv „getestete" Schülerinnen und Schüler können entscheiden, ob sie ihre Infektion über die App melden möchten. Entscheiden sie sich dazu, senden sie ihren geheimen Schlüssel an den Server: Sie heften dafür auf die Rückseite der Karte mit der Markierung „behalten" den Klebezettel mit ihrem Covidcode und legen sie dann in eine Box am Posten Server. Der Server nimmt nur Karten mit korrektem Code an. Hierzu prüft er, ob

Bild 4:
Unter dem Smartphone-Aufdruck befindet sich bei einigen Umschlägen eine Markierung. Diese zeigt an, dass die Nutzer Krankheitssymptome entwickelt haben.

die notierte Zahl durch 7 teilbar ist oder nicht. Demnach korrekt gemeldete Schlüssel werden zum Download an alle Apps freigegeben (und beispielsweise symbolisch an eine Pinnwand gehängt). Wahlweise kann die Lehrperson Manipulationsversuche durch fälschliche Einsendung von Karten thematisieren und Schülerinnen und Schüler auch ohne Covidcode auffordern, ebenfalls ihre Karte abzugeben.

Phase 3: Schlüssel herunterladen und prüfen

Die Schülerinnen und Schüler vergleichen ihre gesammelten Karten mit den ausgehängten Schlüsseln: Passt ein Schlüssel auf eine oder auch mehrere ihrer Karten, hatten sie Kontakt zu einer infizierten Person und folgen den Anweisungen der App (Aufdruck auf der Umschlagrückseite).

Phase 4: Diskussion

Im Anschluss an das Rollenspiel wird das Erlebte gemeinsam besprochen und reflektiert. Dabei können unter anderem die folgenden Fragestellungen dienlich sein:

- ▷ Welche Argumente sprechen dafür bzw. dagegen, eine erkannte Infektion über die App zu melden?
- ▷ Welche Möglichkeiten gibt es, das System auszutricksen bzw. zu hacken?
- ▷ In welchen weiteren Anwendungen werden möglicherweise ähnliche Verfahren genutzt?
- ▷ Warum muss ich bei einer Meldung durch die App genau prüfen, wo und mit wem der Kontakt stattgefunden haben könnte?
- ▷ Ist die Abstandsmessung mittels Bluetooth verlässlich, auch wenn das Smartphone in der Hosentasche steckt?

Erfahrungen aus dem Unterricht

Erste Erfahrungen im Unterricht haben gezeigt, dass die Unterrichtseinheit in der hier präsentierten Form sich grundsätzlich mit Schülerinnen und Schülern der Zielstufe umsetzen lässt. Gleichzeitig wurde deutlich, dass sie umfangreiches Fachwissen der Lehrpersonen erfordert, um bei Rückfragen adäquate Antworten liefern zu können. So wurde beispielsweise in Weiterbildungsveranstaltungen öfter nachgefragt, wie gewisse Aspekte denn nun in der Realität im Detail aussähen. Gleichzeitig wird dadurch auch deutlich, dass sich das Rollenspiel gut eignet, um das Interesse am Thema und den dahinterstehenden informatischen Prinzipien zu wecken. Interessanterweise haben Durchführungen im Unterricht und in der Weiterbildung ebenfalls gezeigt, dass nicht alle Personen besonders großen Wert auf den Schutz ihrer Privatsphäre legen und das Design der App mit den vielen dahinterstehenden Überlegungen nur teilweise schätzen bzw. den damit verbundenen Aufwand als gerechtfertigt ansehen. Lehrpersonen in der Weiterbildung waren teilweise auch erstaunt über die vielen Überlegungen, die hinter der Entwicklung einer solchen App stecken (z. B. Privacy by Design) und auch darüber, welche Berechtigungen Apps wie *WhatsApp* oder *Facebook* im Vergleich dazu erfordern. Dies zeigt einmal mehr, dass diese Themen bisher nicht ausreichend im Informatikunterricht und der Ausbildung von Lehrpersonen verankert sind. Mit der hier vorgestellten Unterrichtseinheit kann dem entgegengewirkt werden.

Prof. Dr. Mareen Przybylla
Prof. Dr. Beat Döbeli Honegger
Dipl. Math. Michel Hauswirth
Dr. Michael Hielscher
Pädagogische Hochschule Schwyz
Zaystrasse 42
6410 Goldau
Schweiz

E-Mail: {mareen.przybylla | beat.doebeli | michel.hauswirth | michael.hielscher}@phsz.ch

Materialien
Alle Materialien für diese Unterrichtseinheit sowie weiterführende Internetquellen werden auf der Webseite

https://mia.phsz.ch/Informatikdidaktik/ContactTracingApp

zur Verfügung gestellt.

Literatur und Internetquellen

BAG – Bundesamt für Gesundheit: Influenza-Pandemieplan Schweiz – Strategien und Massnahmen zur Vorbereitung auf eine Influenza-Pandemie. Bern: Bundesamt für Gesundheit BAG, [5]2018.
https://t1p.de/qlhc

BAG – Bundesamt für Gesundheit: Neues Coronavirus – SwissCovid App und Contact Tracing. Bern: Bundesamt für Gesundheit BAG, 2020.
https://t1p.de/76un

BFS – Bundesamt für Statistik: SwissCovid-App-Monitoring. Neuchâtel: BFS, 2020 f.
https://t1p.de/w8m3

Code Beautify: HMAC Generator. 2020.
https://codebeautify.org/hmac-generator

DP-3T: DP-3T documents – Decentralized Privacy-Preserving Proximity Tracing. 2020.
https://github.com/DP-3T/documents

EDPB – European Data Protection Board: Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19. Brüssel: European Data Protection Board, 2020.
https://t1p.de/y4l7

EU – Europäische Union: Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). In: Amtsblatt der Europäischen Union, L 119/1, 2016. Luxembourg: Amt für Veröffentlichungen der Europäischen Union, 2016.
https://t1p.de/t6cs

Lehner, Chr.: Verschlüsselungssystem für sichere Contact-Tracing-App. München: Technische Universität München, 24. April 2020.
https://www.tum.de/die-tum/aktuelles/covid-19/artikel/article/35995/

Mombelli, A.: Parlament gibt grünes Licht für Covid-Tracing-App. Bern: SWI swissinfo.ch, 9. Juni 2020.
https://t1p.de/jxwq

Recher, P.; Traussnig, A.: So funktioniert eine Corona-Tracing-App, die Ihre Privatsphäre schützt. Zürich: Republik, 2020.
https://t1p.de/tm1z

RKI – Robert Koch Institut: Nationaler Pandemieplan Teil I – Strukturen und Maßnahmen. Berlin: Robert Koch Institut, 2017.
https://t1p.de/rrf7n

University of Oxford: Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. Oxford: University of Oxford, 16. April 2020.
https://t1p.de/mcsm

WHO – World Health Organization: Pandemic Influenza Risk Management – A WHO guide to inform & harmonize national & international pandemic preparedness and response. Genf: World Health Organization, 2017.
https://t1p.de/hirc

Wu, J.; Cai, W.; Watkins, D.; Glanz, J.: How the Virus Got Out. New York: The New York Times, 22.03.2020.
https://t1p.de/wakd

Alle Internetquellen wurden zuletzt am 18. Februar 2021 geprüft und können auch aus dem Service-Bereich des LOG IN Verlags (https://www.log-in-verlag.de/) heruntergeladen werden.