Fingerabdruck-Identifizierung im Seniorenwohnheim

Konstantin Knorr[1], Arne Schmidt[1], Tim Wambach[2]

[1]Hochschule Trier
{knorr, schmidta}@hochschule-trier.de

[2]Unversität Koblenz-Landau
wambach@uni-koblenz.de

Zusammenfassung

Die Identifizierung über biometrische Merkmale wie dem Fingerabdruck bietet speziell für Senioren deutliche Vorteile. Sie müssen sich bspw. kein Passwort merken oder sich an komplexe Passwortrichtlinien halten. Der Beitrag befasst sich mit IT-Sicherheits- und Datenschutz-Fragestellungen, die beim produktiven Einsatz einer fingerabdruckbasierten Identifizierung in einem Seniorenzentrum auftreten. Ein minutienbasiertes Verfahren mit zentraler Datenspeicherung stellt dabei besondere Anforderungen an den Schutz der Daten. Neben der Beschreibung des entwickelten Systems und seiner Absicherung geht der Artikel auch auf ein Schutzkonzept nach BSI-Grundschutz ein, erläutert relevante Aspekte des Datenschutzes und stellt das Vorgehen der durchgeführten Sicherheitsuntersuchung vor. Die Ausführungen orientieren sich an einem im Forschungsprojekt FIGURE entwickelten System, das in einem Seniorenzentrum produktiv eingesetzt wurde. Das Papier fokussiert auf die praktischen Erfahrungen und kann damit als Orientierungshilfe für vergleichbare Projekte dienen.

1 Einleitung

Das Projekt FIGURE[1] entwickelt aufbauend auf einem Sensor zur Fingerabdruckerkennung ein System zur Umgebungsregelung im Bereich der Heimautomation in einem Seniorenzentrum. Es handelt sich dabei um ein altersgerechtes Assistenzsystem (engl. AAL = Ambient Assisted Living). Innerhalb des Projekts sind sowohl der Datenschutz als auch die Datensicherheit von zentraler Bedeutung, da personenbezogene Daten wie z.B. die Minutien der Fingerabdrücke automatisiert verarbeitet werden. Das Bundesdatenschutzgesetz (BDSG) und die neue europäische Datenschutz-Grundverordnung (EU-DSGVO) fordern für solche Szenarien ein umfassendes Datenschutz- und Datensicherheitskonzept und die fortlaufende Prüfung auf Einhaltung.

Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) spricht im Kontext von AAL-Systemen von „industrialisierter Beobachtungen durch Maschinen“ und davon, dass „gerade im Bereich von AAL-Systemen die Machtasymmetrie zwischen Betreuten und Betreuenden ganz besonders ausgeprägt ist, wobei das Selbstverständnis der Betreuenden erfahrungsgemäß oftmals geradezu bedrohlich naiv ist.“, vgl. [ULD09]. Google stößt mit dem

[1] BMBF-Projekt FIGURE (Fingerabdruckgestützte, kontextsensitive Umgebungsregelung), https://vitaldaten.org, Laufzeit 2014-2017

P. Schartner · A. Baumann (Hrsg.) · DACH Security 2017, Seiten 398-408

Kauf der Firma NEST (https://nest.com/) in den AAL-Bereich vor, was die Forderung nach adäquatem Datenschutz verschärft.

1.1 Fingerabdruckbasierte Authentisierung

Beim Fingerabdruck handelt es sich um die älteste Form der Biometrie. Er wurde schon im alten China (ca. zehntes Jahrhundert) zur Identifizierung von Personen verwendet. Der Fingerabdruck ist vor allem deshalb geeignet, da doppelte Vorkommen (im Sinne von zwei Menschen mit identischem Fingerabdruck) aktuell nicht bekannt sind. Die Hautrillen sind für jeden Menschen und Finger einmalig und nicht veränderbar und werden deswegen für die Identifizierung mittels Fingerabdruckerkennung benutzt. Es existieren heute eine Vielzahl von unterschiedlichsten Verfahren, vgl. [MMJB09] für einen Überblick.

Im Kontext des Einsatzes in einem Seniorenwohnheim müssen die Vor- und Nachteile anders gewichtet werden als z.B. der Einsatz innerhalb eines Unternehmens. Insbesondere die direkte Verbindung von Handlung (Finger auflegen) zu einer speziellen Reaktion (Anpassung der Umgebung) ist für das Verständnis des Gesamtsystems von großem Vorteil. Die **hohe Benutzerfreundlichkeit**, dass für einfache Interaktionen mit dem System **kein Passwort** notwendig ist, ist insbesondere bei älteren Menschen von Vorteil. Ein Fingerabdruck kann **nicht weitergegeben** oder vergessen werden und unterliegt, abgesehen von der Qualität der Aufnahmen, auch **keiner Passwort-Richtlinie**, die immer wiederkehrende Aufwände für den Bewohner erzeugen würde.

Nachteilig ist, dass ein kompromittierter Fingerabdruck weltweit eindeutig ist und **nicht widerrufen** werden kann. Wie in den vergangenen Jahren häufig gezeigt wurde, sind Angriffe auf diese Systeme möglich [RuBran16]. Hersteller wie Google betrachten die Fingerabdruck-Authentisierung als **weniger sicher** als eine PIN, ein Muster oder ein Passwort [NHG17]. Ein Angriff wäre z.B. die Erstellung eines künstlichen Fingers aus den Fingerabdruckdaten („Artifical Fingerprint“). Ebenfalls müssen **rechtliche Einschränkungen** berücksichtigt werden: Laut EU-DSGVO dürfen biometrische Daten nur unter besonderen Bedingungen überhaupt erfasst werden.

Das Ziel des FIGURE-Projektes besteht darin, eine alltagstaugliche und für ältere/beeinträchtigte Menschen möglichst benutzerfreundliche und gleichzeitig adäquat abgesicherte Identifikationsmethode zu konstruieren.

1.2 Verwandte Arbeiten

Die automatisierte Verarbeitung von Fingerabdrücken ist, insbesondere im Bereich der Kriminalistik, seit den 70er Jahren etabliert [MaElec73]. Spätestens seit der Integration von Fingerabdrucksensoren in Smartphones, beginnend mit dem G500 bzw. G900 von Toshiba[2] im Jahr 2007, gewinnt die Art der Authentisierung auch im privaten Bereich zunehmend an Bedeutung.

Die Integration biometrischer Authentisierungsverfahren ins Internet of Things wird von Kantarci et al. [BKant15] diskutiert. So wird der Begriff „IoBT“ (Internet of Biometric Things) stellvertretend für Geräte eingeführt, die biometrische Merkmale erheben und ggf. zur weiteren Verarbeitung übermitteln. Durch zentrale Verarbeitung und die dort mögliche Verknüpfung mit

[2] Toshiba Portege G900 and G500: Finger-friendly smart phones: https://www.cnet.com/news/toshiba-portege-g900-and-g500-finger-friendly-smart-phones/, zuletzt abgerufen am 31.05.2017.

weiteren Informationen kann der Nutzungskontext für das verwendete Gerät spezifischer an die Bedürfnisse des jeweiligen Benutzers angepasst werden.

Ein potentielles IoBT-Gerät stellt das „FingerPhone“ von Oki et al. dar [MaOki15]. Dabei wurde ein Fingerabdrucksensor mit einer Türsprechanalage kombiniert, wodurch die Fingerabdruckinformationen des Besuchers während des Klingelvorgangs ausgelesen und dem Bewohner zur Verfügung gestellt werden. Neben der Bereitstellung der Besucherinformationen stellt die Verknüpfung unterschiedlicher Türklingelmelodien, abhängig vom Besucher, ein mögliches Anwendungsbeispiel dar.

Von Habib et al. wurde 2014 gezeigt, wie im medizinischen Umfeld die fingerabdruckbasierte Identifizierung eingesetzt werden kann, um die korrekte Verknüpfung der erhobenen medizinischen Daten mit der jeweiligen Person sicherzustellen [Habib14]. Auf diese Weise soll eine Verwechslung bzw. fehlerhafte Zuordnung zwischen aufgezeichneten Daten und dem Patienten technisch ausgeschlossen werden.

Die Vorteile dieser Authentisierungsform liegen u.a. in der leichten Handhabung, vgl. Kap. 1.1. Aus diesem Grund kommt ein Einsatz dieser Systeme im AAL-Bereich in Betracht. Dabei handelt es sich um Technologien, welche die Lebensqualität für Menschen, insb. in späteren Lebensphasen, erhöhen. Eine Übersicht aktueller AAL-Technologien und Projekte geben Rashidi und Mihailidis [RasMih13].

1.3 Struktur des Artikels

Der Artikel hat folgende Struktur. Kap 2 behandelt das zugrunde liegende Projektszenario, genauer die Systemarchitektur und die theoretischen und technischen Hintergründe der Identifizierung über Fingerabdruck. Ein Bedrohungsmodell für die besonders schützenswerten Fingerabdruckdaten wird in Kap. 3 beschrieben und darauf aufbauend ein Schutzkonzept basierend auf dem BSI-Grundschutz vorgestellt. Die Absicherung des Systems und anschließende Sicherheitsuntersuchung sind Gegenstand von Kap. 4. Kap. 5 geht auf die wichtigsten Erkenntnisse aus dem Praxiseinsatz ein. Kap. 6 beendet den Beitrag mit einem Ausblick auf zukünftige Arbeiten. Die Reihenfolge der Kapitel 3-6 entspricht dabei auch der zeitlichen Reihenfolge im Projekt, wobei das in Kap. 2 beschriebene System dem Zustand am Projektende entspricht.

2 Projektszenario

Das Forschungsprojekt FIGURE hat die Zielsetzung, eine fingerabdruckgestützte, kontextsensitive Umgebungsregelung in einem Seniorenwohnheim zu entwickeln und diese zu untersuchen. Die Sensoren zur Erfassung der Fingerabdrücke werden in Alltagsgegenstände wie Fernbedienung oder Lichtschalter integriert. Die Ermittlung der Daten erfolgt über ein optisches Bild eines Fingers, welches über einen speziellen Sensor aufgenommen wird. Diese Informationen lassen sich (1) zur Identifizierung der Nutzer über deren Fingerabdruck und (2) zur adaptiven Umgebungsregelung wie z.B. der individuellen Beleuchtungssteuerung nutzen. Ein zentraler Server speichert die Daten.

Neben diesen Zielen wurden im Projekt weitere Themen verfolgt, die aber in diesem Beitrag nicht weiter vertieft werden. Dies sind z.B. die Vitaldatenerfassung (Puls und Hautfeuchtigkeit), die Entwicklung des Sensors und der zugehörigen Algorithmen und Dienste, Akzeptanzanalysen, Nutzerintentionen, ethische, rechtliche und soziale Folgen der Nutzung des Systems sowie die Erstellung eines Betriebs- und Wartungskonzeptes.

2.1 Systemarchitektur

Die aus Sicht des Datenschutzes und der -sicherheit wichtigsten Komponenten im FIGURE-System sind Abb.1 dargestellt:

- Fingerabdruckleser (FAL): Diese Spezialhardware soll neben dem Fingerabdruck die Vitaldaten (Feuchtigkeitsgehalt der Haut, Puls und Sauerstoffgehalt des Blutes) ermitteln. Neben der Datenerfassung erlaubt der angeschlossene Rechner eine Speicherung, Verarbeitung und Übermittlung der Daten. Der Sensor basiert auf der NAOS-Technologie (Normal Absorption Optical Sensor). Das Herzstück ist eine patentierte Fiberglasplatte, welche aus 370 Millionen Glasfasersträngen besteht. Diese ermöglicht die Darstellung von Bedienobjekten und gleichzeitig die Aufnahme von Bildern.
- FIGURE-Server mit Datenbank und Web-Applikation: Es handelt sich um einen Linux-Server mit einer MySQL-Datenbank. Die für das Projekt entwickelte Web-Applikation wurde mit Java Enterprise Edition (Java EE) entwickelt und über einen Apache Web-Server bzw. Apache WildFly-Server zugänglich gemacht. Über eine Verbindung ins Internet werden externe Daten wie z.B. Wetterdaten über den Server an den FAL und weitere Clients verteilt.
- IT-Verbund des Seniorenwohnheims und Übertragungsnetze: Hier sind vor allem die Netzwerkkomponenten relevant, über die der FAL, weitere Clients und der Server in die bestehende Infrastruktur eingebettet sind und miteinander kommunizieren.

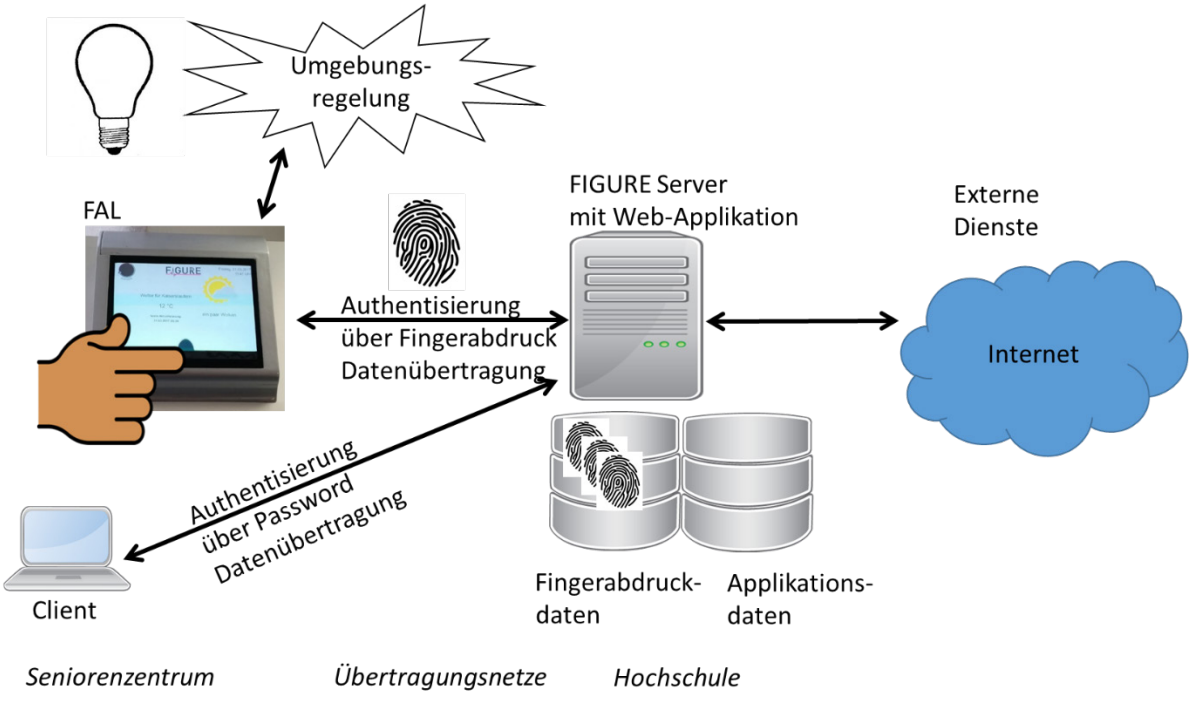

Abb. 1: FIGURE-Systemarchitektur

2.2 Identifizierung über Fingerabdruck

Das bekannteste und auch in FIGURE angewandte Verfahren zur Fingerabdrucküberprüfung basiert auf dem Abgleich von Minutien. Als Minutien werden Endungen und Verzweigungen

der Papillarlinien eines Fingerabdrucks bezeichnet. Statt die notwendige Software selbst zu entwickeln, nutzt das Projekt die bereits etablierte Implementierung NBIS (NIST Biometric Image Software) [NBIS].

NBIS enthält eine umfangreiche Software-Bibliothek inklusive Dokumentation für alle Aufgaben im Zusammenhang mit dem Erfassen, der Analyse und dem Vergleich von Fingerabdrücken. Die Minutien werden dabei über ein Vier-Tupel (x, y, θ, q) gespeichert. Die Koordinaten der Minutie sind x und y, θ gibt den Winkel der abgehenden Verzweigung oder Endung an. Über q wird die Qualität der Minutien gemessen. Minutien am Bildrand haben z.B. eine geringere Qualität als in der Mitte des Bildes.

Innerhalb des Projekts werden die Daten nach einer schriftlichen Einwilligung der Nutzer erfasst und zentral in der Datenbank des Servers gespeichert. Die Extraktion der Minutien erfolgt auf dem FAL über NBIS-FpMV (Fingerprint Minutiae Viewer). Auf dem FAL wird aus dem FpMV eine CSV-Liste mit den Minutien und deren Qualität extrahiert. FpMV nutzt den Minutien Detektions-Algorithmus MINDTCT von [NBIS]. Minutien mit schlechter Qualität werden ausgefiltert. Zusätzlich werden die Qualitätswerte normiert.

Die Minutien werden dann über einen HTTP POST an einen Web-Service auf dem Server übertragen und mittels SSL/TLS geschützt. Dort werden die Minutien entweder (1) für die Registrierung eines neuen Benutzers in der Datenbank hinterlegt oder (2) für die Identifikation gegen die in der Datenbank gespeicherten Werte gematcht. Als Matching-Algorithmus wird BOZORTH3 verwendet, der ebenfalls von NIST NBIS stammt. Serverseitig können gewisse Grenzwerte wie z.B. die minimal benötigte Minutien-Anzahl oder Anzahl der übereinstimmenden Minutien für eine geglückte Identifikation eingestellt werden.

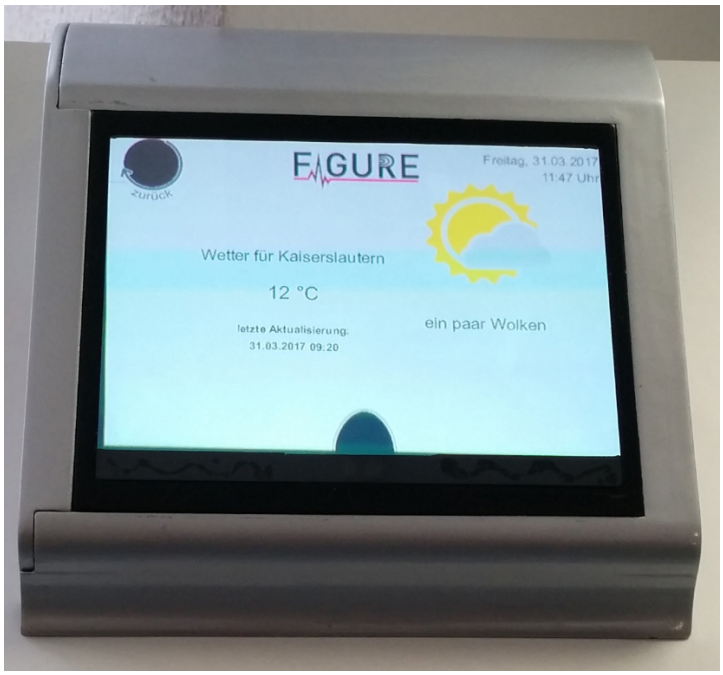

Abb. 2: FAL im Seniorenwohnheim. Das Feld zum Einlesen der Minutien befindet sich unten in der Mitte. Es werden Wetterdaten entsprechend dem Nutzerprofil dargestellt.

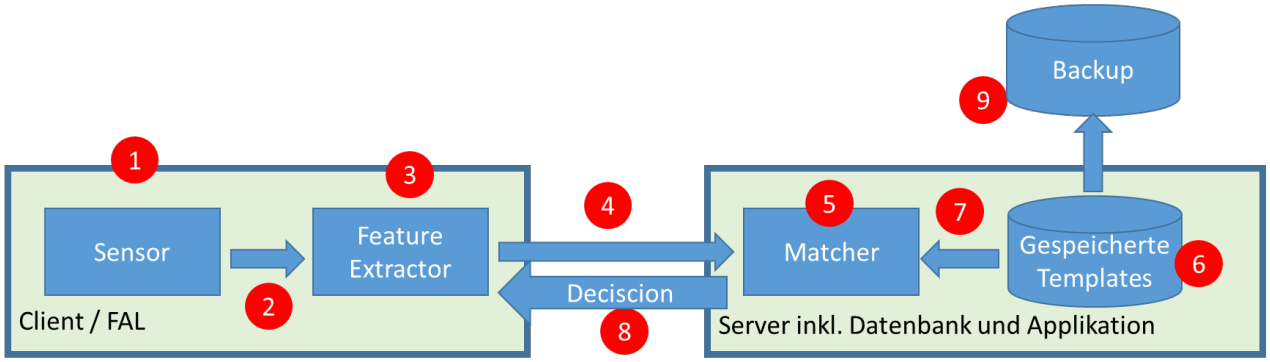

Abb. 3: Angriffspunkte auf die Fingerabdruck-Identifizierung, angelehnt an [RaCB01]

3 Bedrohungsmodell und Schutzkonzept

Das Einsatzszenario stellt besondere Anforderungen an Datenschutz und -sicherheit. Zunächst wurden daher mögliche Angreifer identifiziert und dann mögliche Bedrohungen für das Ausspähen und Manipulieren der Fingerabdrücke identifiziert. Mit diesen Erkenntnissen wurde dann ein Schutzkonzept basierend auf dem BSI-Grundschutz [BSI] erstellt. Spezifische Bedrohungen für Fingerabdruckdaten sind im BSI-Grundschutz nicht enthalten, während die meisten anderen Elemente des FIGURE-Systems wie z.B. Web-Applikation, Datenbank und Übertragungsnetz durch bestehende Bausteine abdeckt sind. Daher fokussiert die folgende Analyse auf Bedrohungen für die Minutien.

Folgende Akteure sind am geplanten Szenario in den Rollen Nutzer, Betreiber und Entwickler des Systems beteiligt und können daher auch als Angreifer agieren:

- Am Projekt teilnehmende Senioren
- Verwandte und Bekannte der Senioren
- Pflegedienst, IT-Abteilung und Leitung des Seniorenzentrums
- Hochschul-Team als Entwickler der Server-Applikation und als Server-Administratoren
- Entwickler des FALs
- Weitere Konsortialpartner
- Ärzte

Um die Einschätzung der betroffenen Senioren zu ermitteln, haben Schlauch, Schelisch und Spellerberg [AAA15] eine Befragung durchgeführt. Die meisten befragten Senioren vertrauen dem Arzt und Pflegedienst, äußerten allerdings teilweise Vorbehalte gegenüber den Verwandten und Angehörigen. Die Mehrheit der befragten Senioren gab an, keine Angst vor Datenmissbrauch der persönlichen Informationen zu haben. Auch auf Nachfrage äußerte nur eine Minderheit Bedenken. Damit decken sich die Ergebnisse mit denen des ULDs, vgl. [ULD09].

Die Betrachtung möglicher Angriffspunkte auf das Gesamtsystem erlaubt eine strukturiere Analyse möglicher Bedrohungen, vgl. Abb. 3. Die Angriffspunkte sind:

1. Verwendung falscher Minutien am Sensor, Auslesen der Minutien
2. Wiedereinspielung bestehender Minutien
3. Override des Outputs des Feature Extraktors
4. Manipulation, Auslesen, Replay der übertragenen Minutien
5. Override des Ergebnisses des Matchers

6. Manipulation oder Auslesen der gespeicherten Templates
7. Manipulation oder Auslesen der übertragenen Templates
8. Override der Decision
9. Manipulation oder Auslesen der gespeicherten Templates im Backup

Der FAL und der Server werden in einer geschützten bzw. überwachten Umgebung betrieben. Besonders kritisch sind daher die Angriffspunkte 1, 4, 8 und 9, da sie sich außerhalb dieser Umgebungen befinden.

Basierend auf dem Vorgehensmodell des BSI-Grundschutzes werden Gefährdungen und dazu passende Maßnahmen für das in Kapitel 2 und Abb. 1 beschriebene System identifiziert. Das System wurde mittels der Software „Vernice“ (vgl. https://verinice.com/) modelliert. Neben den aus dem Grundschutzvorgehen resultierenden mehreren hundert Gefährdungen und Maßnahmen wurden für das System spezifische Gefährdungen identifiziert, wie z.B.

- fehlende Akzeptanz des Systems durch zu lange Bearbeitungszeit
- Zwang zur Nutzung des AAL-Systems
- Fehldiagnose durch fehlerhafte Algorithmen zur Erfassung und Aufbereitung der Vitaldaten
- Umgehung der Fingerabdruck-Authentisierung durch Verwendung nachgebildeter Fingerabdrücke

Spezifische Maßnahmen sind z.B.:

- Verwendung spezieller seitenkanalresistenter Hardware und Software beim FAL
- Lebenserkennung der verwendeten Finger
- Einbau eines Ein- und Ausschalters in die AAL-Komponente (Lampe)
- Definition und Einhaltung eines Pseudonymisierungskonzepts für die Log-Dateien
- Trennung der Datensätze von Fingerabdrücken und sonstigen Applikationsdaten
- Verschlüsselung, Integritätsschutz und Replayschutz für alle Fingerabdruckdaten im Netzwerk mittels eines geeigneten kryptographischen Protokolls wie z.B. SSL/TLS
- Beidseitige Authentisierung von FAL und FIGURE-Server mittels eines geeigneten kryptographischen Protokolls wie z.B. SSL/TLS
- Fingerabdruckdaten verschlüsselt in Datenbank speichern
- Definition einer verantwortlichen Partei für die Vital- und Fingerabdruckdaten
- Erstellung, Unterzeichnung und Einhaltung eines Vertrags zur Auftragsdatenverarbeitung
- Erstellung einer detaillierten Einwilligungserklärung inkl. Angabe der Zweckbindung

4 Absicherung des Systems

Die in Kap. 3 ermittelten Maßnahmen wurden den relevanten Konsortialpartnern, üblicherweise den FAL- und Server-Entwicklern, weitergeleitet und bzgl. Aufwand und Umsetzbarkeit diskutiert. Die folgenden Abschnitte beschreiben ausgewählte, über den Grundschutz hinausgehenden Maßnahmen.

4.1 IT-Sicherheitsmaßnahmen

Die Web-Applikation beinhaltet ein umfangreiches Rechte- und Rollenkonzept für Bewohner, Pflegende, Ärzte, die Verwaltung und Administration des Seniorenzentrums. Neben Passwörtern ist für Probanden auch die Authentisierung über Fingerabdruck möglich. Die Minutien sind serverseitig von den anderen Applikationsdaten getrennt.

Der Apache Web-Server ist mit Zertifikaten und Schlüsselmaterial für die Kommunikation über SSL/TLS ausgestattet. Die Kommunikation mit dem FAL verwendet dabei beidseitige Authentisierung (vgl. Angriffspunkte 4 und 8 in Abb. 3).

Bei der Positionierung des FALs im Seniorenzentrum wurde auf eine zentrale Lage geachtet, so dass von der Rezeption eine Sichtkontrolle möglich war. Der Server wird im Rechenzentrum der Hochschule betrieben. Für das Backup der Daten (vgl. Angriffspunkt 9 in Abb. 3) wurden eine speziell abgesicherte Umgebung und ein passender Prozess etabliert.

4.2 Datenschutz

Das FIGURE-Datenschutzkonzept orientiert sich neben dem BSI-Baustein 1.5 „Datenschutz“ an den u.a. von Witt [Witt10] formulierten folgenden Datenschutz-Prinzipien:

- Einwilligung
- Zweckbindungsprinzip
- Rechtmäßigkeit: Relevante Gesetze sind u.a. BDSG und EU-DSGVO.
- Erforderlichkeit und Datensparsamkeit
- Transparenz und Betroffenenrechte
- Pseudonymisierung oder Anonymisierung

Laut Art. 9.1 EU-DSGVO ist es untersagt, biometrische Daten zur Identifizierung von Personen zu erfassen, wenn nicht die in Art. 9.2 genannten Fälle gelten. Im Projekt nahmen daher nur Freiwillige, die eine **schriftliche Einwilligung** (Art. 9.2a) erteilt hatten, an den Versuchen teil. Bei der Auswahl der Probanden wurde außerdem auf die **Testierfähigkeit** geachtet, da Senioren an Krankheiten wie Demenz oder Bewusstseinsstörung leiden können.
Der Einwilligung wurde ein Informationsschreiben mit einer detaillierten Erklärung des Projektziels und dem Zweck der Datenerhebung beigelegt und den Senioren vor Unterzeichnung ausführlich erklärt. Das Schreiben nennt auch die Rechte wie z.B. auf Widerruf der Einwilligung und auf Auskunft und gibt die dazu benötigte Kontaktdaten an.
Eine **Pseudonymisierung oder Anonymisierung** der Besitzer und deren Minutien war leider im Projektkontext nicht möglich, da die zusätzliche Erfassung von Vitaldaten und Alarmierung bei Überschreiten von Grenzwerten an Arzt oder Pfleger vorgesehen war. Die Minutien müssen außerdem **zentral gespeichert** werden, da mehrere FALs an einen Server angebunden werden können und die Identifizierung eines Bewohners von allen FALs aus möglich sein soll.
Als verantwortliche Partei wurde der Betreiber des Seniorenzentrums festgelegt. Da der Server von einer beteiligten Hochschule entwickelt und betrieben wurde, ergab sich nach §11 BDSG die Notwendigkeit, einen **Vertrag zur Auftragsdatenverarbeitung** zu schließen. Die Minutien und andere personenbezogene Daten des Systems wurden nach Projektende **gelöscht**.

4.3 Sicherheitsuntersuchung

Um die Datensicherheit zu gewährleisten, wurde vor Projektende eine Sicherheitsuntersuchung von bis dahin nicht am Projekt beteiligten Personen durchgeführt. Im Fokus der Analyse stand

der Server, der den Kern der FIGURE-Infrastruktur darstellt. Neben der Prüfung kritischer Systemkomponenten (Betriebssystem, Webserver, Datenbank) wurde die Web-Applikation als Schnittstelle zur Interaktion mit dem System untersucht.

Das Vorgehen der Analyse orientierte sich an bestehenden Best-Practices Guides für das Betriebssystem [Boelen16], den Web-Server Apache [Kumar15], die MySQL-Datenbank [Up15] und für die Web-Applikation [OWASP]. Die Analyse wurde im White-Box-Verfahren (Zugang zum Server und Quelltext) am Produktivsystem durchgeführt.

Die gefundenen Schwachstellen, ergänzt mit Empfehlungen für die Beseitigung, wurden den Entwicklern zur Verfügung gestellt und in kritischen Fällen unmittelbar behoben. Einzelne Schwachstellen wie z.B. der fehlende Schutz des FALs vor Seitenkanalangriffen wurden aufgrund des hohen Aufwands nicht beseitigt.

5 Erkenntnisse aus dem Praxiseinsatz

Es hat sich gezeigt, dass für das Design des FALs bzw. Zugriffsterminals die eingeschränkte Mobilität der Bewohner stärker berücksichtigt werden muss. Dies kann z.B. durch eine Höhenverstellbarkeit erreicht werden. Auch die Größe des Displays und die Schriftgröße der Anzeige müssen stark an die Sehfähigkeiten der Bewohner angepasst sein.

Als vorteilhaft erwies sich die Nutzung der Touchbedienung, bzw. der hier speziell genutzten Hardware, die den Fingerabdrucksensor mit einer Anzeigeeinheit verbindet (vgl. Abb. 2). Dies ermöglicht zusätzlich eine leichte Reinigung, da die Hygiene in diesem Umfeld von besonderer Bedeutung ist.

Höher als erwartet war der Anteil der Probanden, die z.B. aufgrund des Umgangs mit Reinigern bzw. Säuren in ihrem Arbeitsleben über keine oder schwer verwendbaren Minutien verfügten. Ähnliche Probleme sind von Maurern, Sekretärinnen und von Arbeitern mit Kalk bekannt. Die Elastizität der Haut nimmt mit zunehmenden Alter ab. Die Papillarleisten werden dicker, die Höhe der Leisten nimmt ab. Daher ist es schwerer von Senioren verwertbare Fingerabdrücke zu erfassen als bei jüngeren Personen.[3]

Die Absicherung des Systems über die Maßnahmen des BSI-Grundschutzes ist wegen der hohen Anzahl potentiell relevanter Maßnahmen sehr aufwändig und für gemeinnützige Organisationen als Betreiber von Seniorenwohnheimen schwer zu realisieren.

Die Verwendung von NBIS hat sich als praxistauglich erwiesen. Allerdings wird Personal benötigt, das ein tieferes Verständnis der eingesetzten Verfahren hat, um eine adäquat abgesicherte Konfiguration zu gewährleisten. Die Komplexität (1) der beidseitigen Authentisierung über SSL/TLS und (2) des Autorisierungskonzepts der Web-Applikation stellt eine große Herausforderung bei der sicheren Entwicklung und Konfiguration des Servers und Clients da. Auch hier muss das Personal ein Grundverständnis für diese Themen mitbringen.

Die begleitende Sicherheitsuntersuchung hat sich als vorteilhaft erwiesen, da entsprechende Lücken aufgezeigt und geschlossen werden konnten. Die Chronologie des Vorgehens zur Absicherung des Systems mit dem Schutzkonzept, der Umsetzung der Maßnahmen und der Sicherheitsüberprüfung hat sich im Projekt ebenfalls bewährt.

[3] https://www.scientificamerican.com/article/lose-your-fingerprints/

Technische und organisatorische Maßnahmen richten sich danach, wer die verantwortliche Stelle im Sinne des BDSG ist, was eine frühzeitige Klärung dieser Frage erforderlich macht. Aus der Verantwortung ergeben sich automatisch eine Reihe von Datenschutzpflichten wie bspw. Lösch- oder Auskunftspflicht. Im Projekt kam neben dem Seniorenwohnheim (als Erhebungsort) auch die im Projekt beteiligte Hochschule (als Verarbeitungsort) als verantwortliche Partei in Frage. So müssen alle weiteren verarbeitenden Stellen über einen Vertrag zur Auftragsdatenverarbeitung an Datenschutzauflagen gebunden werden.

In die Projektlaufzeit fiel die Einführung der EU-DSGVO. Die Einbeziehung eines Juristen ins Projekt war wichtig für die Klärung von Fragen beim Übergang vom BDSG zur EU-DSGVO, aber auch bei Fragen zum Medizinproduktegesetz.

6 Ausblick

Der Übergang von der prototypischen Umsetzung und Erprobung des Systems hin zu einem größeren produktiven Einsatz bietet eine Vielzahl an weiteren Arbeitsthemen. Ein standardisiertes Minutien-Format wie ISO/IEC 19794-2 würde z.B. die Erweiterung des Systems mit weiteren FALs erleichtern. Ebenso könnten FALs an Browser angebunden werden, um die passwortbasierte Authentisierung durch eine fingerabdruckgeschützte Authentisierung zu ersetzen, vgl. Abb. 1. Ebenso könnten die in Smartphones integrierten Fingerabdruckleser genutzt werden, um sich über das Smartphone gegenüber dem System zu authentisieren.

Einen weiteren interessanten Ansatz bietet die homomorphe Verschlüsselung biometrischer Daten, vgl. [Ba2010, Erki09]. Die Angriffe auf die zentral gespeicherten Minutien würden mit einem homomorphen Schutz der Daten ihre Kritikalität verlieren.

7 Danksagung

Die Autoren danken dem BMBF für die finanzielle Unterstützung des Projekts FIGURE im Rahmen des Programms „IKT 2020 - Forschung für Innovationen“. Die Arbeit von Tim Wambach wurde zusätzlich durch das interdisziplinäre Projekt „Strukturwandel des Privaten“ ermöglicht und durch die VolkswagenStiftung gefördert.

Literatur

[Ba2010] M. Barni und et al.: „Privacy-Preserving Fingercode“. In: Proc. of the 12th ACM Workshop on Multimedia and Security, NY, 2010, pp. 231-240.

[BKant15] B. Kantarci, M. Erol-Kantarci und S. Schuckers: "Towards secure cloud-centric Internet of Biometric Things". In: 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, 2015, pp. 81-83.

[Boelen16] M. Boelen: „Ubuntu Server Hardening Guide: Quick and Secure“. 26 09 2016. [Online]. Available: https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/

[BSI] Bundesamt für Sicherheit in der Informationstechnologie, Grundschutz-Vorgehen, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[Erki09] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk und T. Toft: “Privacy-preserving face recognition”. In: Proc. of the 9th International Symposium on Privacy Enhancing Technologies, 2009, pp. 235–253.

[Habib14] K. Habib, A. Torjusen und W. Leister: “A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth”, 2014.

[Kumar15] C. Kumar, „Apache Web Server Hardening & Security Guide“. 14 02 2015. [Online]. Available: https://geekflare.com/apache-web-server-hardening-security/

[MaElec73] M. Eleccion: “Automatic fingerprint identification”. In: IEEE Spectr. 10, 9, 1973, 36-45.

[MaOki15] M. Oki, K. Tsukada, K. Kimura und Satoshi Nakamatsu: „FingerPhone: smart interphone integrated with a fingerprint sensor“. In: Adjunct Proc. of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp/ISWC'15 Adjunct). ACM, New York, NY, USA, 277-280.

[MMJB09] D. Maltoni, D. Maio, A. Jain und S. Prabh: Handbook of Fingerprint Recognition, Springer, 2009.

[NBIS] https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis

[NHG17] Google Nexus Help: “Understand fingerprint security”, https://support.google.com/nexus/answer/6300638?hl=en

[OWASP] OWASP: “Testing Guide 4.0” 04/2016. [Online]. Available: https://www.owasp.org/images/1/19/OTGv4.pdf

[RaCB01] N. Ratha, J. Connell, R. Bolle: An Analysis of Minutiae Matching Strength. In: Proc. of International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA 2001, pp 223-228.

[RasMih13] P. Rashidi und A. Mihailidis: "A Survey on Ambient-Assisted Living Tools for Older Adults". In: *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 3, pp. 579-590, Mai 2013.

[RuBran16] Russel Brandom: Your phone’s biggest vulnerability is your fingerprint, http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

[SSS15] A. Schlauch, L. Schelisch und A. Spellerberg: „Ambiente Vitaldatenmessung: Akzeptanz und Vorbehalte im Seniorenzentrum“. In: 8. AAL-Kongress, Frankfurt a. M., 2015.

[ULD09] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: „Juristische Fragen im Bereich altersgerechter Assistenzsysteme“, VDI/VDE Innovation + Technik GmbH, Kiel, 2009.

[Up15] UpGuard: „Top 11 Ways To Improve MySQL Security“, 21 11 2015. [Online]. Available: https://www.upguard.com/articles/top-11-ways-to-improve-mysql-security

[Witt10] B. Witt: „Datenschutz Kompakt und Verständlich: Eine Praxisorientierte Einführung,“ kes, 2010.