Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 427

Privacy-Dashcam – Datenschutzfreundliche Dashcams durch Erzwingen externer Anonymisierung

Paul Georg Wagner[1] Pascal Birnstill[2] Erik Krempel[3] Sebastian Bretthauer[4] Jürgen Beyerer[5]

Abstract: Datenschützer sehen in Dashcams Videoüberwachungsanlagen, die von Privatpersonen im öffentlichen Raum betrieben werden und die durch das Aufzeichnen personenbezogener Daten in unverhältnismäßigem Ausmaß in das Recht auf informationelle Selbstbestimmung betroffener Bürger eingreifen. Eine Dashcam kann demnach nur dann datenschutzgerecht sein, wenn sie die Erhebung personenbezogener Daten vermeidet. Dies kann bspw. geschehen, indem mindestens die Gesichter von Passanten sowie KFZ-Kennzeichen automatisch erkannt und unkenntlich gemacht werden. Obwohl Anonymisierungsverfahren mit hinreichend hoher Genauigkeit existieren, kommen diese aufgrund ihres hohen Rechenaufwands nicht für den Einsatz in handelsüblichen Dashcams in Betracht. Dieser Beitrag stellt einen neuen Ansatz vor, der die Anonymisierung von verschlüsselt gespeicherten Dashcam-Videos auf einem separaten Rechner erzwingt, bevor der Benutzer darauf Zugriff erhält. Diese Videos werden auf ihrem Weg vom Speichermedium zu einer Anonymisierungskomponente mittels Methoden der Datenflusskontrolle überwacht, sodass beliebige Dashcams um Datenschutzmechanismen erweitert werden können.

Keywords: Dashcams, Datenschutz, Privacy, Nutzungskontrolle, Datenflusskontrolle

1 Einleitung

Dashcams, die aus einem Fahrzeug heraus das Verkehrsgeschehen aufzeichnen, sind in den letzten Jahren auch in Europa immer populärer geworden. Ihre Benutzer versprechen sich von den Aufzeichnungen eine vereinfachte Schadensregulierung bei Verkehrsunfällen, insbesondere zum Nachweis der eigenen Unschuld. Gleichzeitig ist die Verbreitung von Dashcams von einer datenschutzrechtlichen Kontroverse begleitet, da den Sicherheitsbedürfnissen der Betreiber gewichtige Nachteile gegenüber stehen. So können Dashcams als mobile Videoüberwachungsanlagen betrachtet werden, deren Betrieb durch Privatpersonen im öffentlichen Raum kaum zu legitimieren ist. Für alle derzeit existierenden Arten von Dashcams gilt außerdem, dass eine Erhebung personenbezogener Daten durch im Bild erfasste Fußgänger und KFZ-Kennzeichen angenommen werden muss. Somit liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen vor, dessen Verhältnismäßigkeit im Hinblick auf die genannten Sicherheitsbedürfnisse der Dashcam-Benutzer umstritten ist. Im Vergleich dazu stellen sogenannte *Crashcams* eine

[1] Fraunhofer IOSB, paul-georg.wagner@iosb.fraunhofer.de
[2] Fraunhofer IOSB, pascal.birnstill@iosb.fraunhofer.de
[3] Fraunhofer IOSB, erik.krempel@iosb.fraunhofer.de
[4] Zentrum für Angewandte Rechtswissenschaft (ZAR) am Karlsruher Institut für Technologie und an der Goethe-Universität Frankfurt a. M. bei Prof. Dr. Indra Spiecker gen. Döhmann, LL. M. sowie an der dortigen Forschungsstelle Datenschutz, sebastian.bretthauer@kit.edu
[5] Fraunhofer IOSB & Karlsruher Institut für Technologie (KIT), juergen.beyerer@iosb.fraunhofer.de

datenschutzfreundlichere Methode dar, da diese nur ereignisbezogen aufzeichnen, etwa durch Beschleunigungssensoren ausgelöst. Durch Verwendung eines Ringpuffers, der im Ereignisfall nicht mehr überschrieben wird, kann eine Crashcam Videobilder im Zeitraum von bspw. jeweils einer Minute vor und nach dem Ereignis aufnehmen. Allerdings ist auch bei diesen Kameras eine Erhebung personenbezogener Daten kaum zu vermeiden.

Während in Deutschland noch keine obergerichtliche Entscheidung vorliegt, sind Dashcams in Österreich bereits seit 2012 unzulässig. Weiterhin erklärte das Bundesverwaltungsgericht in Wien 2015 auch eine Crashcam für unzulässig, die zum Schutz der Privatsphäre erfasster Personen mit reduzierter Auflösung betrieben wurde. Das Gericht sah es nicht als erwiesen an, dass die geringe Auflösung der Kamera eine unrechtmäßige Erhebung personenbezogener Daten wirksam verhindere, und erbat explizit eine Stellungnahme des Klägers, weshalb die Kamera datenschutzrelevante Bereiche von Bildern wie etwa Gesichter und KFZ-Kennzeichen nicht unkenntlich mache. Technisch kann festgestellt werden, dass entsprechende Anonymisierungsverfahren existieren, aber für eine Integration in transportable Kameras zu rechenintensiv sind.

Dieser Beitrag stellt einen Ansatz vor, der die zur Anonymisierung benötigte Bildauswertung auf sichere Weise an einen separaten, leistungsfähigen Rechner auslagert. Hierzu wird ein spezielles Speichermedium eingesetzt, das Videos sofort verschlüsselt. Ein Zugriff auf das Speichermedium ist nur über einen Rechner mit Mechanismen der Datenfluss- und Nutzungskontrolle möglich. Diese stellen sicher, dass die Aufzeichnungen der Dashcam vor dem Zugriff durch den Benutzer anonymisiert werden. Weiterhin wird gewährleistet, dass der Benutzer aufgezeichnete Daten weder modifizieren noch löschen kann.

2 Verwandte Arbeiten

Rinner und Winkler[6] stellen mit dem Prototyp *TrustEYE.M4* eine vertrauenswürdige Kamera mit integrierten Privacy-Enhancing-Technologies (PET) vor. Diese basiert auf einem Raspberry PI, einem preiswerten Miniaturrechner, der die erfassten Daten sofort verarbeitet bevor diese gespeichert oder übertragen werden. Die verfügbare Rechenleistung ist jedoch limitiert und es können nur einfache Verfahren zur Anonymisierung genutzt werden. Ob hierdurch eine Anonymisierung erreicht werden kann, die einen hinreichenden Schutz personenbezogener Bildbereiche bietet, zugleich aber auch für den Nachvollzug von Verkehrsunfällen ausreichendes Material liefert, ist unklar.

Soll die Anonymisierung der Dashcam-Videos an einen separaten Rechner ausgelagert werden, so muss auf ein portables Speichermedium aufgezeichnet werden, das der Benutzer selbst an den vorbereiteten Rechner anschließt. Hierbei muss sichergestellt werden, dass der Benutzer nicht auf die Videodaten zugreifen kann, bevor diese anonymisiert wurden. Mittels Mechanismen der Nutzungskontrolle[7][8] können Nutzungen von Daten in einer kontrollierten Umgebung kontinuierlich überwacht werden – auch über Systemgrenzen

[6] Rinner und Winkler, Privacy-protecting Smart Cameras, ICDSC 2015.
[7] Park und Sandhu, Towards Usage Control Models: Beyond Traditional Access Control, SACMAT 2002.
[8] Pretschner et al. , Distributed Usage Control, Commun. ACM, 49(9), 2006.

hinweg. Bei der Nutzungskontrolle handelt es sich um eine Verallgemeinerung der Zugriffskontrolle, wobei die Kontrolle über Nutzungen von Daten auch nach dem dem initialen Zugriff noch möglich ist. Hierzu ist allerdings eine kontinuierliche Überwachung der zu schützenden Daten erforderlich, weshalb die Nutzungskontrolle darüber hinaus häufig mit einer Datenflusskontrolle erweitert wird. Durch die Datenflusskontrolle können Nutzungsrestriktionen nicht nur in Abhängigkeit von Systemereignissen, sondern ebenso in Form von (un-)zulässigen Datenflüssen formuliert werden.[9]

Zur Anonymisierung datenschutzrelevanter Bildbereiche sind geeignete Bildauswertealgorithmen und Anonymisierungstechniken erforderlich. Hinreichend leistungsstarke Bildauswertealgorithmen, die datenschutzkritische Bildbereiche in Echtzeit detektieren können, sind jedoch im Allgemeinen sehr rechenintensiv und somit nur bedingt für den Einsatz in mobilen Kamerasystemen geeignet. So erreichten Janard und Marurngsith mit einer Local-Binary-Pattern-Gesichtserkennung auf dem Raspberry PI lediglich etwa 17 QVGA-Bilder (320x240 Pixel) pro Sekunde.[10] Auch einige Anonymisierungstechniken sind mit Miniaturrechnern nicht in Echtzeit zu bewerkstelligen. So war für *TrustEYE.M4* eine eigene Implementierung des Privacy-Filters nötig, da sich die Standardalgorithmen der OpenCV-Bibliothek für den Raspberry PI als zu komplex herausgestellt haben.

3 Rechtliche Perspektive

3.1 Unter geltendem Datenschutzrecht

Bereits unter geltendem Datenschutzrecht wird der Einsatz von Dashcams kontrovers diskutiert. Teilweise werden Dashcams als datenschutzrechtlich zulässig erachtet,[11] teilweise hingegen als ausdrücklich unzulässig.[12] In der datenschutzrechtlichen Diskussion wird erörtert, ob Datenschutzrecht gar nicht anwendbar sei, falls die Nutzung einer Dashcam eine ausschließlich persönliche oder familiäre Tätigkeit darstellen würde,[13] ob und inwiefern überhaupt personenbezogene Daten durch die Dashcam-Aufnahme betroffen seien[14] und ob und wie Dashcams generell mit § 6 b BDSG in Einklang gebracht werden können.[15] Eine pauschale Antwort ist jedenfalls nicht möglich, insbesondere unter Berücksichtigung der verschiedenen technischen Gestaltungsmöglichkeiten von Dashcams.[16] Dieser technische Aspekt wird bisher von der Rechtsprechung zu Unrecht nicht berücksichtigt.[17]

So kommt der technischen Gestaltung von Dashcams aber gerade eine besonders überragende Bedeutung bei der datenschutzrechtlichen Bewertung zu. Entscheidend ist die

[9] Harvan und Pretschner, State-based Usage Control Enforcement with Data Flow Tracking Using System Call Interposition, NSS 2009.
[10] Janard/Marurngsith, Accelerating real-time face detection on a raspberry pi telepresence robot, INTECH 2015.
[11] Wirsching, NZV 2016, 13 (16); Knyrim/Trieb, ZD 2014, 547 ff; Fuchs, ZD 2015, 212 (217).
[12] Ernst, CR 2015, 620 (624); Reibach, DuD 2012, 157 (160); AG München, Urt. v. 13.08.2014 – 345 C.
[13] Ernst, CR 2015, 620 (622); Reibach, DuD 2012, 157 ff.; Balzer/Nugel, NJW 2014, 1622 (1625); Fuchs, ZD 2015, 212 (214 ff.).
[14] Balzer/Nugel, NJW 2014, 1622 (1625); Fuchs, ZD 2015, 212 (213 ff.).
[15] Ernst, CR 2015, 620 (623); Balzer/Nugel, NJW 2014, 1622 (1626 ff.).
[16] In diese Richtung auch Knyrim/Trieb, ZD 2014, 547 (547).
[17] Knyrim/Trieb, ZD 2014, 547 (547 ff.).

technische Ausgestaltung des Aufnahmesystems, insbesondere was die Auflösung der Bilder angeht, den Speicherzeitpunkt, die Speicherdauer der Aufnahmen, die Zugriffsmöglichkeiten auf die gespeicherten Daten sowie die allgemeine technische Architektur der Dashcam.[18] Eine dauerhafte Speicherung von Klarbildern aus einer Dashcam ist jedenfalls unzulässig, da dies einen besonders schwerwiegenden Eingriff in Persönlichkeitsrechte der von der Dashcam Betroffenen darstellt.[19] Künftig muss deshalb der technischen Spezifikation bei der datenschutzrechtlichen Zulässigkeitsbewertung eine wesentlich größere Bedeutung beigemessen werden. Das gilt bereits ohnehin für das geltende Datenschutzrecht und erst Recht für die ab 2018 kommende Europäische Datenschutzgrundverordnung.

3.2 Unter der kommenden Datenschutz-Grundverordnung (DS-GVO)

Ab dem 25. Mai 2018 gilt die DS-GVO in jedem Mitgliedstaat unmittelbar (Art. 288 AEUV, Art. 99 Abs. 2 DS-GVO), sodass die Datenschutzrichtlinie und die in ihrer Folge bzw. Umsetzung erlassenen nationalen Datenschutzgesetze ihre Geltung verlieren (Art. 94 Abs. 1 DS-GVO). Ausnahmen kommen allerdings dort in Betracht, wo die DS-GVO Öffnungsklauseln bereithält, die den nationalen Staaten dann auch weiterhin eigene Befugnisse einräumen.[20] Die datenschutzrechtliche Zulässigkeit von Dashcams richtet sich gleichwohl nach der DS-GVO, da derartige videoüberwachungsähnliche Systeme überwiegend von Privatpersonen genutzt werden - einmal abgesehen von der Nutzung in Polizeiautos -, sodass auch keine Öffnungsklausel für den öffentlichen Bereich in Betracht kommt (vgl. etwa Art. 2 Abs. 2 d) und Art. 6 Abs. 2 DS-GVO). Andere Öffnungsklauseln sind ebenfalls nicht ersichtlich.[21] Ebenso unterfällt die Nutzung von Dashcams nicht dem „Familienprivileg“ nach Art. 2 Abs. 2 (c) DS-GVO, da die Dashcam-Aufzeichnung nicht ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeit erfolgt, soll sie doch überwiegend als Beweismittel in einem späteren Prozess eingesetzt werden.[22] Für die klassische Videoüberwachung hat dies der Europäische Gerichtshof bereits so auch ausdrücklich festgestellt.[23]

Damit verbleibt es bei den sehr allgemein gehaltenen Regelungen der DS-GVO, da es an einer spezifischen Videoüberwachungsnorm fehlt.[24] In Betracht kommt Art. 6 Abs. 1 (f) DS-GVO, der jedoch nur auf eine Interessenabwägung zwischen dem Dashcam-Betreiber und dem Betroffenen abstellt und keine weiteren eingrenzenden Tatbestandsmerkmale aufweist. Bisherige Regelungen in einzelnen europäischen Mitgliedstaaten zur Videoüberwachung haben jedoch gerade solche expliziten weiteren einschränkenden Tatbestandsmerkmale.[25] Damit ist aber fraglich, ob ein derart offen und weit gefasster Erlaubnistatbestand, wie ihn Art. 6 Abs. 1 (f) DS-GVO darstellt, überhaupt hinreichend bestimmt

[18] So bereits Knyrim/Trieb, ZD 2014, 547 (548); Balzer/Nugel, NJW 2014, 1622 (1627).
[19] VG Ansbach, Urt. v. 12.08.2014 – AN 4 K 13.01634 = ZD 2014, 590 (593).
[20] Ausführlich hierzu Benecke/Wagner, DVBl 2016, 600 ff.
[21] Ausführlich Benecke/Wagner, DVBl 2016, 600 (604 Fn. 27).
[22] Vgl. hierzu ausführlich Reibach, DuD 2012, 157 ff.
[23] EuGH, Urt. v. 11.12.2014 – C-212/13 = CR 2015, 101 ff. (m. Anm. Bretthauer).
[24] Vgl. bereits dazu Bretthauer/Krempel/Birnstill, CR 2015, 239 (242).
[25] Vgl. etwa hierzu § 6 b BDSG, § 50 a ff ÖDSG, §§ 16 ff. Litauisches Datenschutzgesetz, § 26 Dänisches Datenschutzgesetz, § 6 a Liechtensteinisches Datenschutzgesetz und §§ 36 ff. Norwegisches Datenschutzgesetz.

ist im Sinne des Art. 52 Abs. 1 EU-Grundrechte-Charta, um eine derartig grundrechtssensible Technologie zu regulieren.[26] Der rechtliche Maßstab läuft ausschließlich auf eine reine Interessenabwägung hinaus. Für den Dashcam-Betreiber lässt sich sein Interesse an einer effektiven Beweismittelführung in einem Unfallprozess und einer effektiven Strafverfolgung bei einer möglichen Unfallflucht des Gegners anführen.[27] Die von der Dashcam Betroffenen können sich auf den Schutz personenbezogener Daten nach Art. 7, 8 EU-Gr-Charta berufen. In diese Abwägung muss aber ebenso die technische Spezifikation der Dashcam eingestellt werden, sodass datenschutzfreundliche Techniken Berücksichtigung finden können (vgl. Erwägungsgrund 78 DS-GVO und Art. 25 DS-GVO).

Führt man sich die in den einzelnen Mitgliedstaaten derzeit vorhandenen Regelungen zur Videoüberwachung vor Augen und überträgt man die aus dem deutschen Verfassungsrecht bekannten Anforderungen an die Bestimmtheit von Rechtsnormen auf Art. 6 Abs. 1 f) DS-GVO im Hinblick auf den Einsatz von Dashcams, so erweist sich die Regelung als zu unbestimmt, da es neben der Interessenabwägung an weiteren eingrenzenden Tatbestandsmerkmalen fehlt. Die Nutzung von Dashcams ist dann im privaten Bereich jedenfalls nicht mehr von der DS-GVO gedeckt.

4 Systemmodell

Das im Folgenden spezifizierte und formalisierte System arbeitet mit einer handelsüblichen Dashcam und einem Speichermedium, auf welches Video- und Metadaten geschrieben werden. Videos werden solange als klassifizierte Daten behandelt, bis eine entsprechende Softwarekomponente datenschutzrelevante Bereiche entfernt oder anonymisiert hat. Diese Deklassifikation erfolgt auf einem separaten Rechner. Während der Übertragung vom Speichermedium auf die Deklassifikationskomponente müssen die Daten adäquat geschützt werden. Die folgenden Abschnitte gehen auf Schutzziele, Angreifer und Vertrauensbeziehungen im betrachteten Szenario ein.

Schutzziele Schutzgüter sind personenbezogene Merkmale, die in aufgezeichneten Videodaten eingebettet sind, insbesondere Gesichter und KFZ-Kennzeichen. Hinzu kommen Metadaten der Videos, wie etwa Zeitstempel oder GPS-Positionsdaten. Wichtigstes Schutzziel ist die Vertraulichkeit der Videodaten bzw. der darin enthaltenen personenbezogenen Daten. Ein weiteres Schutzziel ist die Integrität der Daten (einschließlich der Metadaten). Sollen diese als Beweismittel vorgebracht werden können, muss sichergestellt sein, dass sie nicht manipuliert wurden. Schließlich muss die Authentizität von Benutzern mit erweiterten Berechtigungen (bspw. Strafverfolgungsbehörden) gewährleistet werden.

[26] So bereits Bretthauer/Krempel, in: Schweighofer/Kummer/Hötzendorfer (Hrsg.), Transparenz – Tagungsband des 17. Internationalen Rechtsinformatik Symposions, 2014, S. 525, 532; zu den Anforderungen nach Art. 52 EU-Grundrechte-Charta im Einzelnen vgl. Rieckhoff, Der Vorbehalt des Gesetzes im Europarecht, 2007, S. 155 ff.

[27] So etwa Ernst, CR 2015, 620 (623).

Angreifermodell Im Mittelpunkt steht ein Angreifer, der datenschutzrelevante Inhalte aufgezeichneter Videos an eine interessierte dritte Partei weitergeben möchte. Dieser sog. *Privacy-Attacker* hat Zugriff auf die Kamera, das verschlüsselte Speichermedium und den zur Deklassifikation der Videodaten verwendeten Rechner. Gegenüber diesem Angreifer darf das System keine datenschutzrelevanten Inhalte preisgeben. Dies wird insbesondere dadurch erschwert, dass es sich beim Privacy-Attacker nicht um einen externen Dritten handelt, sondern um den Benutzer der Dashcam selbst. (Diese ambivalente Betrachtung des Benutzers ist typisch für Einsatzszenarien der Nutzungskontrolle.) Dennoch kann ein Dashcam-System nur datenschutzgerecht sein, wenn es gegenüber dem Privacy-Attacker widerstandsfähig ist.

Ein *Modifying-Attacker* verfolgt das Ziel, aufgezeichnete Video- und/oder Metadaten zu seinem Vorteil zu verändern. Schutzmechanismen gegen ihn müssen daher die Integrität der klassifizierten Videos und der Metadaten sicherstellen. Ein Schutz der deklassifizierten Videos oder exportierter Metadaten ist nicht notwendig. Auch der Modifying-Attacker hat Zugriff auf das Speichermedium und das Deklassifikationssystem.

Ein ähnliches Ziel verfolgt der sog. *Destructive-Attacker*, der unvorteilhafte Video- bzw. Metadaten zerstören möchte, etwa nach einem selbst verschuldeten Verkehrsunfall. Da eine mechanische Zerstörung des Speichermediums nicht verhindert werden kann, wird dieser Angreifer durch die Annahme beschränkt, dass er Daten für Dritte undetektierbar löschen möchte. Ein Schutz der deklassifizierten Videos oder exportierter Metadaten ist nicht notwendig. Der Destructive-Attacker hat Zugriff auf das Speichermedium und das Deklassifikationssystem, sieht jedoch von mechanischer Zerstörung ab.

Vertrauensmodell Im betrachteten Szenario interagieren die im Folgenden beschriebenen Akteure mit dem Dashcam-System. Der *Betreiber* benutzt das System, um bei einem möglichen Verkehrsunfall die Aufzeichnungen der Kamera als Beweismittel zu nutzen. Neben der Nutzung als Betreiber kann er als Privacy-Attacker, Modifying-Attacker und Destructive-Attacker agieren. Da das System dem Betreiber nicht vertraut, ihn sogar als möglichen Angreifer betrachtet, muss er nicht explizit am System authentifiziert werden.

Die *Strafverfolgungsbehörde* hat ein rechtmäßiges Interesse an den aufgezeichneten Videodaten, um diese gegebenenfalls als Beweismittel in einem Prozess vorzubringen. Ihr ist es erlaubt, auf die klassifizierten Videos zuzugreifen. Dies geschieht üblicherweise auf eine richterliche Anordnung hin, da solche Zugriffe einen Eingriff in die Persönlichkeitsrechte erfasster Personen darstellen. Der Strafverfolgungsbehörde wird vollumfänglich vertraut, d.h. ihr ist es gestattet, die Schutzmechanismen des Systems zu deaktivieren. Die Authentifizierung dieses Akteurs gegenüber dem System ist daher essentiell.

Der *Administrator* nimmt das Deklassifikationssystem in Betrieb. An diesem legt er initial die Zugriffsrechte für alle Akteure fest. Dem Administrator muss voll vertraut werden. Im Folgenden wird angenommen, dass der Administrator nur bei der Inbetriebnahme Zugang zum System hat, sodass er für die weitere Sicherheitsanalyse des Systemmodells keine Rolle spielt. Abschnitt 7 geht auf einige grundlegende Vorkehrungen ein, die der Administrator bei der Inbetriebnahme des Deklassifikationssystems treffen muss.

5 Systemspezifikation

In den folgenden Abschnitten wird das konkrete System spezifiziert. Dafür werden die einzelnen Komponenten und ihre Interaktionen untereinander definiert. Schließlich wird eine mögliche Implementierung des entwickelten Systemmodells vorgestellt.

5.1 Systemkomponenten

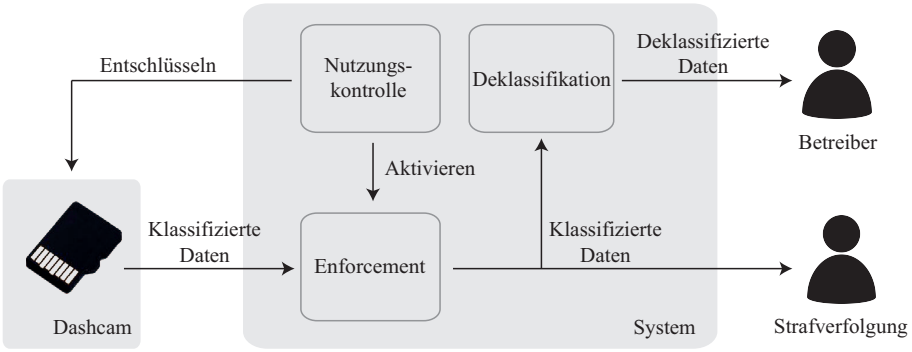

Abb. 1: Realisierung des Systemmodells

Das Systemmodell unterscheidet zwischen der *Kamera* an sich und einem *Speicher*, typischerweise einer SD-Karte, auf dem die erfassten Daten für die weitere Verarbeitung vorgehalten werden. Für das Modell ist es unerheblich, wie Videos mit potentiell datenschutzrelevanten Bereichen in den Speicher gelangen. Von der Kamera selbst wird daher im Folgenden abstrahiert. Der in Abb. 1 dargestellte Ansatz kann somit für alle handelsüblichen Geräte genutzt werden. Der Speicher ist dagegen von herausragender Bedeutung. Da er die klassifizierten Videos speichert, muss er sicherstellen, dass nur dann auf die Daten zugegriffen wird, wenn diese auf dem zugreifenden System geschützt sind.

Die Komponente *Deklassifikation* liest klassifizierte Videos, also Videos mit möglicherweise datenschutzrelevanten Bereichen, und nutzt eine Deklassifikationsfunktion, um eine deklassifizierte Repräsentation der Videos zu erzeugen. Dies geschieht in der Regel durch eine Anonymisierung der datenschutzrelevanten Bildbereiche, etwa durch Schwärzen oder Verpixeln. Nur deklassifizierte Videos dürfen das System verlassen, um dem Benutzer angezeigt zu werden. Die klassifizierten Daten hingegen dürfen die Deklassifikationskomponente keinesfalls verlassen.

Da der einzig rechtmäßige Zugriff auf den Speicher durch die Deklassifikationskomponente erfolgt, müssen alle weiteren Zugriffe darauf verhindert werden. Eine mögliche Lösung hierfür besteht darin, beiden Komponenten ein gemeinsames Geheimnis zu geben und damit die vorhandenen Daten zu verschlüsseln. Ein weitaus flexiblerer Ansatz ist es jedoch, die Deklassifikationskomponente und den Speicher nur lose miteinander zu koppeln. Um dies zu erreichen wird eine weitere Komponente, die *Nutzungskontrolle*, eingeführt. Diese Komponente stellt Datenverbindungen zwischen dem Speicher und beliebig vielen Deklassifikatoren her, vorausgesetzt diese nutzen ausreichend gute Deklassifikationsfunktionen,

um die datenschutzrelevanten Bereiche zu schützen. Authentifiziert sich ein entsprechender Benutzer, in unserem Beispiel eine Strafverfolgungsbehörde, an der Nutzungskontrolle, erhält dieser ebenfalls Zugriff auf die noch nicht anonymisierten Daten. In diesem Fall wird davon ausgegangen, dass die entsprechende Instanz die erhaltenen Daten verantwortungsvoll nutzt und nicht für Unbefugte zugänglich macht.

Den eigentlichen Kern des Systems bildet die *Enforcement*-Komponente. Sie überwacht die vom Speicher in das System fließenden klassifizierten Daten und unterbindet eine missbräuchliche Verwendung innerhalb des Systems. Die Enforcement-Komponente überwacht hierzu sämtliche Datenflüsse, die auf dem System auftreten, und unterbindet diejenigen Operationen, die klassifizierte Daten an den Betreiber weitergeben könnten.

5.2 Interaktion

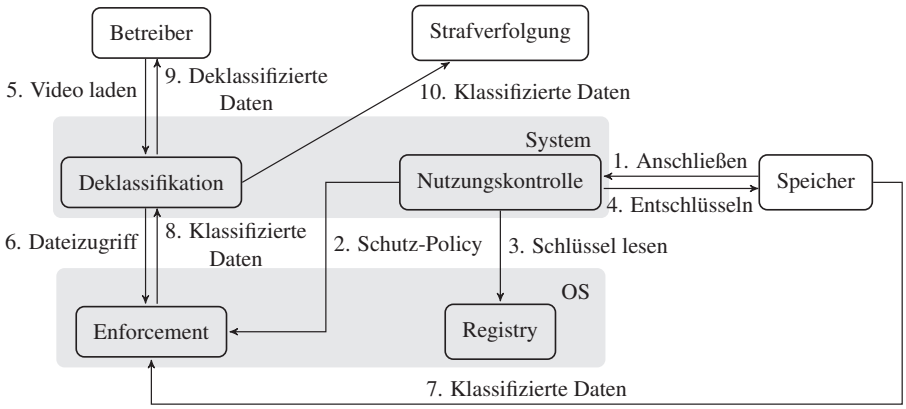

Abb. 2: Überblick über die Systeminteraktion

Abb. 2 zeigt die Interaktion der Komponenten, sobald der Betreiber seinen Speicher an einen Rechner anschließt, auf dem das Deklassifikationssystem aktiv ist. Der Speicher besteht aus einer verschlüsselten SD-Karte, auf der klassifizierte Daten in Form von Dashcam-Videos vorhanden sind. Das Entschlüsseln der SD-Karte geschieht mittels eines zufällig generierten gemeinsamen Geheimnisses (Schlüssel), das dem Betreiber selbst nicht bekannt sein darf und das daher durch die Nutzungskontrolle in einer geschützten Umgebung abgespeichert wird, etwa als verschlüsselter Eintrag in der Registry. Der Speicher kann dementsprechend nur an einem Rechner betrieben werden, der mit einer vertrauenswürdigen Nutzungskontrolle ausgestattet ist. Neben der Verwendung eines symmetrischen Verfahrens zur Verschlüsselung der Speicherkarte ist auch der Einsatz eines asymmetrischen Verfahrens, bei welchem sich der private Schlüssel in der Nutzungskontrolle und der öffentliche Schlüssel auf der Speicherkarte befindet, möglich. Allerdings ist dieses Design mit den meisten verfügbaren asymmetrisch verschlüsselnden Speicherkarten nicht umsetzbar, da der private Schlüssel in der Regel nicht exportiert werden kann.

Ist auf dem Rechner eine Nutzungskontrolle verfügbar, so erkennt diese den verschlüsselten Speicher und aktiviert die Enforcement-Komponente. Diese Aktivierung erfolgt mit Hilfe

einer Schutz-Policy, welche das angeschlossene Speichergerät eindeutig identifiziert. Nach der Aktivierung dieser Schutzmechanismen unterliegen sämtliche Datenflüsse von und auf den Speicher der Kontrolle der Enforcement-Komponente. Daher kann die Nutzungskontrolle nun das gemeinsame Geheimnis verwenden, um den Speicher zu entschlüsseln. Ab diesem Zeitpunkt liegen die klassifizierten Daten auf dem Speicher im Klartext vor und können von beliebigen Systemprozessen ausgelesen werden. Dies zu verhindern obliegt der Enforcement-Komponente, welche sämtliche Lesezugriffe auf den entschlüsselten Speicher überwacht und nur solche mit authentifiziertem Ziel zulässt (d.h. ausgehend von der Deklassifikationskomponente oder der Strafverfolgungsbehörde). Schreibzugriffe auf den Speicher werden ebenfalls untersagt, insbesondere auch für die Strafverfolgungsbehörden. Damit stellt die Enforcement-Komponente sicher, dass die klassifizierten Daten von der Speicherkarte lediglich in die Deklassifikationskomponente und zu Strafverfolgungsbehörden fließen können. Der Betreiber der Dashcam kann die klassifizierten Daten an keiner Stelle abgreifen, da die Deklassifikationskomponente die Videos nur in deklassifizierter Form, also anonymisiert, darstellt. Es wird somit sichergestellt, dass sowohl die Vertraulichkeit als auch die Integrität der klassifizierten Daten geschützt ist. Lediglich der Strafverfolgungsbehörde erlaubt die Enforcement-Komponente nach expliziter Authentifizierung an der Nutzungskontrolle, lesend auf die klassifizierten Daten zuzugreifen.

5.3 Implementierung

Bei der Implementierung des beschriebenen Systems ist insbesondere der Entwurf der Nutzungskontrolle und der Enforcement-Komponente entscheidend. Die Nutzungskontrolle wurde als Windows-Dienst realisiert, welcher stets im Hintergrund auf angeschlossene Speichermodule lauscht, für jene die Schutzmechanismen aktiviert und weitere Steuerungsaufgaben übernimmt. Die Enforcement-Komponente besteht aus einem Dateisystem-Filtertreiber für Windows, welcher sich im Kernel registriert, sämtliche Dateizugriffe im System filtert und gegebenenfalls untersagt (vgl. Abb. 2). Dieser Treiber blockiert, sobald die Speicherkarte entschlüsselt wurde, sämtliche unerwünschten Datenflüsse im System.

Als Deklassifkationskomponente wird nun ein Programm benötigt, das in der Lage ist, datenschutzkritische Bereiche der Videos zu detektieren und zu anonymisieren. Durch die lose Kopplung zwischen Nutzungskontrolle und Deklassifkationskomponente kann für diese Aufgabe jedes geeignete Drittprogramm eingesetzt werden.

Weiter ist zu klären, wie die Kamera Videos auf die verschlüsselte Speicherkarte schreiben kann, ohne das zur Ver-/Entschlüsselung benötigte Geheimnis zu kennen. Dies wird durch den sog. *Postbox-Mode* der Karte möglich, der das Schreiben von Daten auch ohne Authentifizierung erlaubt, nicht jedoch das Lesen oder Modifizieren. Die Kamera kann somit Überwachungsvideos aufzeichnen, die zu jedem Zeitpunkt auf der Speicherkarte in verschlüsselter Form aufbewahrt werden. Wird ein asymmetrisches Verschlüsselungsverfahren eingesetzt, entfällt diese Problematik.

Ferner schreiben Dashcams dauerhaft auf die verwendete Speicherkarte. Sobald der Speicher voll ist, werden die ältesten Videos überschrieben. Dies kann durch den Destructive-

Attacker ausgenutzt werden, um unerwünschte Videos zu löschen. Dem Problem der begrenzten Kapazität von Speicherkarten kann wie folgt begegnet werden. Werden ereignisbasiert aufzeichnende Crashcams benutzt, ist der begrenzte Speicherplatz unproblematisch, da auf eine Speicherkarte über 200 Unfallvideos gespeichert werden können. Diese anlassbezogene Speicherung ist auch aus Datenschutzgründen vorzuziehen. Alternativ kann das Deklassifikationssytem um einen Modus erweitert werden, der alle Videos von der Speicherkarte löscht, bei denen die zugehörigen Metadaten keine Auffälligkeiten aufweisen wie etwa außergewöhnliche Beschleunigungen. Somit wird eine volle Speicherkarte wieder nutzbar, ohne dass Videos von Unfällen vom Benutzer gelöscht werden können.

6 Formalisierung

6.1 Datenflussmodel

Zur Formalisierung von Datenflusseigenschaften eignet sich das formale Datenflussmodell von Harvan und Pretschner.[28] Dieses wird durch ein Tupel $(D, C, F, \Sigma, \sigma_i, P, A, R)$ beschrieben. D ist die Menge der *Daten*, die vom System überwacht werden. C ist die Menge der *Container* im System, bspw. Dateien, Systemprozesse oder Netzwerkverbindungen. $P \subseteq C$ ist die Menge der *Prozesse*, die Aktionen auslösen können. Prozesse sind Container, da sie Daten im Speicher oder in CPU-Registern vorhalten können. F ist die Menge der *Namen*, über die Container identifiziert werden können, bspw. Dateinamen $F_{fn} \subseteq F$ oder Dateideskriptoren $F_{dsc} \subseteq F$. Der aktuelle Zustand des Modells wird durch $\Sigma = (C \to 2^D) \times (C \to 2^C) \times (P \times F \to C)$ beschrieben und besteht aus drei Relationen. Die *Speicherrelation* $s : C \to 2^D$ bildet ab, welche Daten in welchen Containern enthalten sind. Die *Aliasrelation* $l : C \to 2^C$ enthält Container, die implizit aktualisiert werden, sobald Daten in einen anderen Container fließen. Die *Namensrelation* $f : P \times F \to C$ bildet ab, unter welchen prozessspezifischen Kennungen Container identifizierbar sind. $\sigma_i = (s_i, l_i, f_i) \in \Sigma$ beschreibt den initialen Zustand des Modells. Hier enthält die Speicherrelation die initialen Repräsentationen der überwachten Daten. Die Menge A enthält die im System durchführbaren Aktionen, die Änderungen der Speicher-, Alias-, oder Namensrelation indizieren. Diese Änderungen werden in der (deterministischen) Übergangsrelation $R \subseteq \Sigma \times P \times A \times \Sigma$ beschrieben. Aktualisierungen der Relationen s, l und f werden im Folgenden in der Notation von Harvan und Pretschner[27] dargestellt: Sei $m : S \to T$ eine Relation und $x \in X \subseteq S$ eine Variable. Dann ist $m[x \leftarrow expr]_{x \in X} = m'$ mit $m' : S \to T$ definiert als

$$m'(y) = \begin{cases} expr & \text{falls } y \in X \\ m(y) & \text{sonst.} \end{cases}$$

Harvan und Pretschner formalisieren explizite Datenflüsse innerhalb des Betriebssystems.[27] Modifikationen auf R werden daher durch System-Calls induziert. Da durch Anpassungen der Formalisierungen des *read*- und des *write*-System-Calls das Verhalten des De-

[28] Harvan und Pretschner, State-based Usage Control Enforcement with Data Flow Tracking Using System Call Interposition, NSS 2009.

klassifikationssystems spezifiziert werden kann, werden diese im Folgenden in ihrer ursprünglichen Form zitiert.

$$\begin{aligned}&\forall s \in [C \to 2^D], \forall l \in [C \to 2^C], \forall f \in [P \times F \to C], \forall p \in P, \forall e \in F_{dsc} : \\ &\big((s,l,f), p, read(e), (s[t \leftarrow s(t) \cup s(f(p,e))]_{t \in l^*(p)}, l, f)\big) \in R\end{aligned} \tag{1}$$

$$\begin{aligned}&\forall s \in [C \to 2^D], \forall l \in [C \to 2^C], \forall f \in [P \times F \to C], \forall p \in P, \forall e \in F_{dsc} : \\ &\big((s,l,f), p, write(e), (s[t \leftarrow s(t) \cup s(p)]_{t \in l^*(f(p,e))}, l, f)\big) \in R\end{aligned} \tag{2}$$

Gl. 1 beschreibt die Semantik eines *read*-System-Calls. Dieses Ereignis modifiziert die Speicherrelation s dergestalt, dass jedes Datum aus dem gelesenen Container (konservativ überapproximiert) in die reflexiv-transitive Hülle l^* des aufrufenden Prozess-Containers p fließt. Analog beschreibt Gl. 2 die Semantik von *write*-System-Calls.

Mittels dieser Formalisierungen können bereits Daten im System bewegt werden. Im Unterschied zu Harvan und Pretschner[27] wird im Folgenden eine weitere Interpretation der Datenmenge D verwendet. Diese umfasst nicht nur Daten, die durch Policies der Nutzungskontrolle geschützt werden, sondern alle verfügbaren Daten. Dies ist erforderlich, um zwischen klassifizierten Daten, die das System weder verlassen noch vom Betreiber eingesehen werden dürfen, und unklassifizierten Daten unterscheiden zu können. $D = D_{cl} \dot{\cup} D_{decl}$ sei daher aus zwei disjunkten Mengen der klassifizierten bzw. deklassifizierten Daten zusammengesetzt. Klassifizierte Daten können mittels der nicht-injektiven Deklassifikationsfunktion $decl : D_{cl} \to D_{decl}$ in unklassifizierte Daten konvertiert werden. Zusätzlich sei $D_{prot} \subseteq D$ die Menge der unklassifizierten Daten, die der Betreiber lesen, aber nicht modifizieren oder löschen darf (Metadaten wie Zeitstempel oder GPS-Daten). Da die Integrität der klassifizierten Daten sichergestellt werden muss, gilt $D_{cl} \subseteq D_{prot}$.

Im nächsten Schritt sind nun diejenigen Container im System zu definieren, die klassifizierte Daten enthalten dürfen. Entsprechend repräsentieren $c_{storage} \in C$ und $c_{decl} \in P$ den Speicher der Kamera (Speichermedium) bzw. den Systemprozess der Deklassifikationskomponente. Die Nutzungskontrollkomponente wird nicht als separater Container betrachtet, da sie als überwachende Instanz agiert und selbst keine Daten verarbeitet. Damit kann nun spezifiziert werden, wie die Deklassifikationsfunktion von der Deklassifikationskomponente benutzt wird. Dazu wird die Formalisierung der *read*-Operation so erweitert, dass klassifizierte Daten in die Deklassifikationskomponente hineinfließen können, wo dann eine deklassifizierte Repräsentation der Daten erzeugt wird.

$$\begin{aligned}&\forall s \in [C \to 2^D], \forall l \in [C \to 2^C], \forall f \in [P \times F \to C], \forall p \in P, \forall e \in F_{dsc}, f(p,e) = c_{decl} : \\ &\big((s,l,f), p, read(e), (s[t \leftarrow s(t) \cup s_{decl}(f(p,e))]_{t \in l^*(p)}, l, f)\big) \in R\end{aligned} \tag{3}$$

Gl. 3 drückt aus, dass für jede *read*-Operation auf dem Deklassifikationscontainter c_{decl} jeweils auch die deklassifizierten Repräsentationen der Daten zurückgegeben werden. Dies

wird mittels einer modifizierten Speicherrelation $s_{decl} : C \to 2^{D_{decl}}$ erreicht, die automatisch die entsprechenden Daten deklassifiziert. Sie ist definiert als:

$$s_{decl}(c) = \left\{ d \middle| d \in \left(s(c) \setminus D_{cl} \right) \right\} \cup \left\{ decl(d) \middle| d \in \left(s(c) \cap D_{cl} \right) \right\} \tag{4}$$

Analog wird die *write*-Operation erweitert (vgl. Gl. 5), sodass diese ebenfalls deklassifizierte Daten schreibt, falls sie aus dem Deklassifikationscontainer stammen.

$$\begin{aligned} &\forall s \in [C \to 2^D], \forall l \in [C \to 2^C], \forall f \in [P \times F \to C], \forall e \in F_{dsc} : \\ &\left((s, l, f), c_{decl}, write(e), (s[t \leftarrow s(t) \cup s_{decl}(c_{decl})]_{t \in l^*(f(c_{decl}, e))}, l, f) \right) \in R \end{aligned} \tag{5}$$

Mittels dieser erweiterten Definitionen der *read*- bzw. *write*-Operation können Daten nun in einer deklassifizierten Form angefordert werden. Noch immer können aber klassifizierte Daten die Deklassifikationskomponente verlassen. Um dies zu verhindern, werden im Folgenden die für die Sicherheit des Systems erforderlichen System-Policies spezifiziert. Davor sei allerdings noch der initiale Zustand $\sigma_i = (s_i, l_i, f_i) \in \Sigma$ in Gl. 6 angegeben.

$$\begin{aligned} s_i(c_{storage}) \cap D_{cl} &\neq \emptyset \\ s_i(C \setminus \{c_{storage}\}) \cap D_{prot} &= \emptyset \end{aligned} \tag{6}$$

Somit wird davon ausgegangen, dass klassifizierte Daten initial nur auf der Speicherkarte vorhanden sind, während noch keine schützenswerten Daten im System existieren.

6.2 System-Policies

Basierend auf dem angegebenen formalen Systemmodell können formale Nutzungskontroll-Policies spezifiziert werden, um die Nutzungen von klassifizierten Daten im System einzuschränken. Wie von Harvan und Pretschner beschrieben,[27] sind solche Policies zustandsbasiert. Sie spezifizieren nicht, welche Ereignisse unterbunden bzw. zugelassen werden sollen, sondern vielmehr welche unzulässigen Systemzustände zu vermeiden sind.

Die wichtigste Policy im betrachteten System verfolgt das Schutzziel der Vertraulichkeit und verlangt, dass klassifizierte Daten nicht durch den Betreiber betrachtet oder verarbeitet werden dürfen. Daher dürfen im formalen Modell ausschließlich die Container $c_{storage}$ als Quelle und c_{decl} als Deklassifizierungskomponente klassifizierte Daten enthalten.

$$\forall c \in C \setminus \{c_{storage}, c_{decl}\} : s(c) \cap D_{cl} = \emptyset \tag{7}$$

Die in Gl. 7 dargestellte Policy ist hinreichend, um unerwünschte Datennutzungen auszuschließen. Weiterhin sollen keine Aliasbeziehungen für diese beiden Container existieren, da klassifizierte Daten ansonsten entlang der Aliasbeziehungen abfließen könnten. Auch wenn Gl. 7 bereits implizite Flüsse klassifizierter Daten in Alias-Container verhindert, kann mit der Policy in Gl. 8 zusätzlich bereits das Entstehen entsprechender Aliasbeziehungen unterbunden werden.

$$l(c_{storage}) \cup l(c_{decl}) = \emptyset \tag{8}$$

Obgleich die in Gl. 7 dargestellte Policy bereits alle Vertraulichkeitsanforderungen erfüllt, ist es ungünstig, über die gesamte Menge C der Container quantifizieren zu müssen. Da für den initialen Zustand angenommen wurde, dass nur $c_{storage}$ klassifizierte Daten enthält, kann die Policy in Gl. 7 auch als Restriktion für Datenflüsse zwischen $c_{storage}$ und c_{decl} ausgedrückt werden. Die Policy in Gl. 9 besagt, dass Daten aus dem Container $c_{storage}$ nur in den Container c_{decl} fließen dürfen. Die in Gl. 10 und 11 dargestellten Policies verlangen, dass nur deklassifizierte Daten aus c_{decl} heraus fließen können.

$$\forall\big((s,l,f),p,read(e),(\bar{s},l,f)\big) \in R : f(p,e) = c_{storage} \implies l^*(p) = \{c_{decl}\} \tag{9}$$

$$\forall\big((s,l,f),p,read(e),(\bar{s},l,f)\big) \in R : f(p,e) = c_{decl} \implies \bar{s}[l^*(p)] \subseteq D_{decl} \tag{10}$$

$$\forall\big((s,l,f),p,write(e),(\bar{s},l,f)\big) \in R : p = c_{decl} \implies \bar{s}\left[l^*\big(f(p,e)\big)\right] \subseteq D_{decl} \tag{11}$$

Im Unterschied zur Alias- und Namensrelation wird die Speicherrelation bei den betrachteten *read*- und *write*-Operationen zu $\bar{s}$ modifiziert. Wenn wir o.B.d.A. annehmen, dass $p \notin \{c_{storage}, c_{decl}\}$ in der Policy in Gl. 10 und 11 gilt, so wird ersichtlich, dass ein System, das Gl. 9, 10 und 11 erfüllt, auch Gl. 7 erfüllt. Die Policies sind allerdings nicht äquivalent, da durch die Policies in Gl. 9, 10 und 11 ein Zugriff auf unklassifizierte Daten, die initial in $c_{storage}$ vorliegen, ebenfalls unterbunden wird. Wie im Folgenden gezeigt wird, eignet sich diese an Datenflüssen orientierte Spezifikation besser für die technische Umsetzung als die Policy in Gl. 7. Weiterhin kann auf die Nutzung von l^* in der Policy in Gl. 9 verzichtet werden, wenn gleichzeitig Gl. 8 gefordert wird.

Schließlich ist noch das Schutzziel der Integrität gegenüber einem Modifying-Attacker oder einem Destructive-Attacker (vgl. Abschnitt 4) zu behandeln. Diese sollen geschützte Daten weder verändern noch löschen können. Hierfür muss zu jedem Zeitpunkt gelten:

$$s_i(c_{storage}) \cap D_{prot} = s(c_{storage}) \cap D_{prot} \tag{12}$$

Die Policy in Gl. 12 verlangt, dass geschützte Daten, die initial auf dem Speichermedium vorliegen, für alle Zeit unverändert bleiben. Sie verhindert außerdem, dass neue geschützte Daten erzeugt werden, bspw. gefälschte GPS-Positionsdaten. Wegen $D_{cl} \subseteq D_{prot}$ stellt die Policy in Gl. 12 insbesondere sicher, dass auch klassifizierte Daten weder verändert noch vom ursprünglichen Speichermedium gelöscht werden können.

Der Akteur Strafverfolgungsbehörde taucht in der angegebenen Formalisierung des Systems nicht auf. Die zustandsbasierte Sicht auf das System eignet sich nur bedingt, um Benutzerautorisierungen auszudrücken. Es wird daher angenommen, dass eine Infrastruktur zur Verwaltung von Benutzerrechten auf dem formalisierten System aufsetzt und entscheiden kann, ob die angegebenen Policies durchzusetzen sind oder nicht.

7 Sicherheitsanalyse

Ausgehend von der Formalisierung eines Systems, das die Anwendung von Deklassifikationsfunktionen sicherstellt, können nun dessen Sicherheitseigenschaften in Bezug auf das Angreifermodell analysiert werden.

In Bezug auf den Datenschutz stellt sich zunächst die Frage, ob das System robust gegen einen Privacy-Attacker ist, d.h. ob das Schutzziel der Vertraulichkeit erfüllt ist. Gemäß der Policies in Gl. 9, 10 und 11 können klassifizierte Daten nur im Speicher der Kamera, sowie in der Deklassifikationskomponente existieren. Der Betreiber kann Daten nur einsehen, falls diese zuvor durch eine Deklassifikationskomponente anonymisiert wurden. Aufgrund dieser Eigenschaften ist sichergestellt, dass klassifizierte Daten niemals in unanonymisierter Form das System verlassen. Dem Privacy-Attacker, und damit auch dem Betreiber der Dashcam, ist es nicht möglich klassifizierte Daten zu extrahieren, womit das Schutzziel der Vertraulichkeit erfüllt ist.

Für das Schutzziel der Integrität sind vor allem der Modifying-Attacker und der Destructive-Attacker relevant. Gemäß der Policy in Gl. 12 ist es nicht möglich, Daten auf dem Speicher der Kamera zu modifizieren oder zu löschen. Das System ist somit robust gegen Modifying-Attacker und ebenso gegen Destructive-Attacker, wobei hier vom mechanischen Zerstören der Speicherkarte abgesehen werden muss.

Damit die Analyse der Angreifer valide ist, müssen einige Annahmen an die Betriebsumgebung des implementierten Systems gemacht werden. Zunächst muss vorausgesetzt werden, dass das verwendete Betriebssystem die Integrität der einzelnen Komponenten sichert. Dies bedeutet insbesondere, dass der Betreiber der Dashcam auf dem Anonymisierungssystem keine Administratorrechte besitzt und der Zugriff auf die Programm- und Konfigurationsdateien der Systemkomponenten eingeschränkt ist. Auch das gemeinsame Geheimnis, welches auf dem Anonymisierungssystem gespeichert ist, muss vor dem Auslesen durch den Betreiber geschützt werden, bspw. durch Einsatz der Windows Data Protection API. Neben den Softwarekomponenten muss auch das physische System gesichert werden. Der Betreiber der Dashcam darf keinen direkten Zugriff auf die Festplatte des Anonymisierungssystems erhalten, ansonsten könnte er sich selbst Administratorrechte verschaffen. Diese Art des Umgehens von Sicherheitsmechanismen kann besonders wirksam durch den Einsatz eines sog. Trusted-Platform-Modules (TPM) verhindert werden.

8 Fazit

In diesem Beitrag wurde ein System entwickelt, das die Vertraulichkeit und die Integrität datenschutzrelevanter Bildbereiche gewährleistet. Mechanismen der Datenflusskontrolle lassen klassifizierte Daten von einem sicheren Speichermedium ausschließlich in die Deklassifikationskomponente fließen. Dort werden sie vor einem Zugriff durch den Betreiber anonymisiert, sodass dieser zu keinem Zeitpunkt die Möglichkeit hat, die Klarvideodaten einzusehen. Durch die Auslagerung der Anonymisierung auf einen separaten Rechner können leistungsfähige Bildauswertealgorithmen eingesetzt werden, sodass (i) personenbezogene Daten nach dem Stand der Technik minimiert werden, und (ii) jede handelsübliche Dashcam um Datenschutzmechanismen erweitert werden kann. Ein datenschutzgerechter Betrieb von Dashcams erscheint somit unter den in Abschnitt 7 genannten Annahmen möglich.