Thomas Winkler

# Vertrauenswürdige Videoüberwachung

## Sichere intelligente Kameras mit Trusted Computing

Im Straßenverkehr, im Einkaufszentrum, in der U-Bahn: Videoüberwachung ist ein fester Bestandteil unseres Alltags. Während für Kamerabetreiber Sicherheitsaspekte wie die Integrität und Authentizität von Videodaten im Vordergrund stehen, sorgen sich viele Bürger um den Schutz ihrer Privatsphäre. Das TrustCAM-Projekt untersucht, wie intelligente Kamerasysteme diese unterschiedlichen Bedürfnisse unter Verwendung von Trusted Computing erfüllen können.

### 1 Intelligente Kameras

Kamerasysteme für die Videoüberwachung haben in den vergangenen Jahren einen starken Wandel durchlaufen. Ursprünglich analoge Systeme sind mittlerweile vollständig auf digitale Techniken umgestellt. Inzwischen werden auch immer öfter sogenannte „intelligente Kameras" eingesetzt. Dabei handelt es sich um eingebettete Rechnersysteme, die Bilder und Videos direkt verarbeiten und analysieren können. Ein wesentlicher Vorteil ist, dass sich dadurch die Menge der zu übertragenden Daten erheblich reduzieren lässt. Auch der Personalaufwand kann verringert werden: Wenn Kameras selbständig ungewöhnliche Ereignisse erkennen, müssen die Videoströme nicht mehr permanent von Menschen beobachtet werden. Intelligente Kamerasysteme bringen aber nicht nur Vorteile, sondern werfen auch neue Fragen auf. Da Videodaten nun in digitaler Form vorliegen, können sie sehr einfach archiviert, indiziert und durchsucht werden. Datenschützer sehen durch diese Eigenschaften die Privatsphäre zunehmend in Gefahr.

Intelligente Kameras können aber auch genutzt werden um diesem Problem offensiv zu begegnen. Mit den verfügbaren Ressourcen ist es möglich, Sicherheitsfunktionalität direkt in die Kamera zu integrieren [1, 2]. Daten können somit noch bevor sie das System verlassen geschützt werden.

Das TrustCAM-Projekt [3] am Institut für Vernetzte und Eingebettete Systeme der Alpen-Adria Universität Klagenfurt [4] setzt sich mit genau dieser Thematik auseinander. Im Rahmen des Projekts wurde ein Kameraprototyp mit umfassenden Sicherheitsfunktionen auf Basis von *Trusted Computing* (TC) entwickelt. Dieser Artikel führt in die Grundlagen von TC ein und illustriert wie diese Technik für ein vertrauenswürdiges Kamerasystem eingesetzt werden kann.

**Thomas Winkler**

Assistent am Institut für Vernetzte und Eingebettete Systeme der Alpen-Adria Universität Klagenfurt. Er beschäftigt sich bereits seit Mitte 2005 mit Trusted Computing. Seit 2007 forscht er an intelligenten, eingebetteten Kamerasystemen und setzt sich insbesondere mit Fragen der Sicherheit sowie dem Schutz der Privatsphäre auseinander.
E-Mail: thomas.winkler@aau.at

### 2 Trusted Computing

Trusted Computing ist eine Sicherheitstechnik, die in der Vergangenheit mehrfach kontrovers diskutiert wurde.[1] Nach Bereinigung anfänglicher Missverständnisse und Fehleinschätzungen ist die Technik nun soweit gereift, dass erste praktische Anwendungen in die Realität umgesetzt werden. TC umfasst eine Reihe von Spezifikationen, die von der *Trusted Computing Group* (TCG) [5] herausgegeben und gepflegt werden. Die Vorläuferorganisation der TCG – die *Trusted Computing Platform Alliance* (TCPA) – wurde im Jahr 1999 gegründet und in weiterer Folge im Jahr 2003 in TCG umbenannt. Die TCG ist ein Industriekonsortium, in dem viele namhafte Größen der IT-Industrie wie zum Beispiel AMD, Intel, Microsoft, IBM oder HP, vertreten sind. Die TCG umfasst weit über 100 Mitglieder aus den Bereichen der Industrie und Forschung.

Da Vertrauen (engl. *Trust*) zentrales Ziel der TC-Initiative ist, stellt sich die Frage, wie Vertrauen im Kontext eines Computer-Systems zu verstehen ist. Die TCG selbst beantwortet diese Frage so:

> *"Trust is the expectation that a device will behave in a particular manner for a specific purpose."*

Vertrauen ist also laut TCG die Erwartungshaltung, dass sich ein Gerät, das für einen bestimmten Einsatzzweck, in einer ganz bestimmten Art und Weise verhält. Überträgt man diese Überlegung auf Computer, so zeigt sich, dass deren Verhalten von der darauf ausgeführten Software bestimmt wird. Daraus leitet sich eines der zentralen Ziele von TC ab: Die Erfassung der auf einem Computersystem ausgeführten Software sowie die sichere Berichterstattung über den aufgezeichneten Systemzustand an Dritte.

#### 2.1 Trusted Platform Module

Das Kernelement von TC bildet das *Trusted Platform Module* (TPM). Das TPM ist ein Microchip, der genau spezifizierte Sicherheitsfunktionen in Form einer Hardwarekomponente zur Verfügung stellt. In einem typischen PC-System ist das TPM als fester Bestandteil auf die Hauptplatine aufgelötet. Der Grund, bei TC einen Hardware-basierten Ansatz zu verfolgen, resul-

1 Siehe DuD-Schwerpunkthefte 9/2004 und 9/2005.

tiert aus der Annahme, dass Hardware deutlich schwieriger manipulierbar ist als eine reine Softwarelösung. Das TPM beinhaltet die folgenden Funktionseinheiten:

- *I/O-Einheit*: Sie dient zur Kommunikation mit dem eigentlichen Computersystem. Als rein passives Bauelement kann das TPM niemals aktiv in Abläufe des Computers eingreifen.
- *Ausführungseinheit*: Hier werden die eingehenden Befehle verarbeitet.
- *RSA-Schlüsselerzeugung*: Das TPM nutzt RSA als asymmetrischen Verschlüsselungsalgorithmus. Die Schlüssellänge aktueller TPM Implementierungen beträgt maximal 2048 Bits.
- *RSA-Einheit*: Hardwareeinheit für RSA-Ver- und -Entschlüsselung. Beim Signieren können die Daten mit einem Zeitstempel auf Basis eines internen, monotonen Zählers versehen werden.
- *SHA-1-Einheit*: Komponente zur Erzeugung von SHA-1 Prüfsummen.
- *Zufallszahlengenerator*: Das TPM ist mit einem Hardware-basierten Zufallszahlengenerator ausgestattet.
- *Flüchtiger und nichtflüchtiger Speicher*: Für den Betrieb verfügt das TPM intern sowohl über flüchtigen als auch über nichtflüchtigen Speicher. In letzterem werden spezielle kryptografische Schlüssel abgelegt.

Im Auslieferungszustand ist das TPM inaktiv und muss vom Benutzer aktiviert und in Betrieb genommen werden. Jedes TPM wird ab Werk mit einer eindeutigen Kennung in Form eines RSA-Schlüssels, dem sogenannten *Endorsement Key* (EK) geliefert. Der private EK kann weder zurückgesetzt noch aus dem TPM exportiert werden. Während der Inbetriebnahme wird ein weiterer spezieller RSA-Schlüssel – der sogenannte *Storage Rootkey* (SRK) – erzeugt. Auch der private SRK verlässt niemals das TPM, kann aber vom Besitzer wieder gelöscht werden. Dazu ist die Kenntnis eines speziellen Passworts erforderlich, welches bei der Inbetriebnahme festgelegt wird.

## 2.2 Roots of Trust

Trusted Computing definiert mehrere sogenannte Wurzeln des Vertrauens (engl. *Roots of Trust*). Nachfolgend werden diese näher beschrieben.

**Root of Trust for Storage**

Mit dem bei der Inbetriebnahme erzeugten SRK kann das TPM zur sicheren Datenverschlüsselung genutzt werden. Benutzer können zu diesem Zweck eigene TPM-Schlüssel erzeugen. Für einen solchen RSA-Schlüssel sind beim Erzeugen ein Passwort und ein Elternschlüssel anzugeben. Im einfachsten Fall ist dieser Elternschlüssel der SRK.

Der Elternschlüssel ist notwendig, um eine praktische Limitierung des TPMs zu umgehen. Idealerweise sollten alle vom TPM erstellten kryptographischen Schlüssel stets im TPM gespeichert werden und somit dessen Schutz niemals verlassen. Allerdings ist der interne, nichtflüchtige Speicher des TPMs begrenzt. Deshalb werden Benutzerschlüssel aus dem TPM exportiert und z. B. auf der Festplatte abgelegt. Damit die privaten Teile dieser Schlüssel nicht ungeschützt sind, werden sie vor dem Export mit ihrem öffentlichen Elternschlüssel verschlüsselt. Es ergibt sich eine Schlüsselhierarchie, an deren Spitze der SRK steht. Dieser kann seinerseits jedoch nicht aus dem TPM exportiert werden. Durch dieses Verfahren ist sichergestellt, dass private Benutzerschlüssel durch das TPM geschützt sind und nur in diesem verwendet werden können, auch wenn sie auf externem Massenspeicher liegen.

Bei der Datenverschlüsselung unterscheidet TC zwei Arten. In der ersten Variante, dem sogenannten Binding, werden Daten mit einem öffentlichen TPM-Schlüssel verschlüsselt. Nur jener TPM-Chip, zu dem der private Schlüssel gehört, kann die Daten auch wieder entschlüsseln. Damit ist sichergestellt, dass die Daten nur auf einem ganz bestimmten Rechner – jenem, der das TPM enthält – entschlüsselt werden können.

Die zweite Form der Verschlüsselung, die von TC unterstützt wird, nennt sich Sealing. Dabei handelt es sich um eine Erweiterung des Binding. Die Datenentschlüsselung durch das TPM ist nur dann möglich, wenn sich das System in einem bestimmten, bei der Verschlüsselung festgelegten Zustand befindet. Andernfalls verweigert das TPM die Entschlüsselung. Wie die Erfassung und Speicherung dieses Systemzustands erfolgt, wird nachfolgend beschrieben.

**Root of Trust for Measurement**

Wie bereits erwähnt bietet TC die Möglichkeit, den Systemzustand zu erfassen. Zu diesem Zweck verfügt das TPM über 24 sogenannte Platform Configuration Registers (PCRs). Dabei handelt es sich um jeweils 20 Bytes große Speicherbereiche, die beim Systemstart zurückgesetzt werden. Jede Softwarekomponente des Systems wird, bevor sie ausgeführt wird, in diese PCRs „gemessen". Messen bedeutet in diesem Zusammenhang, dass die SHA-1-Prüfsumme der auszuführenden Komponente berechnet und in ein PCR gespeichert wird. Auf PCRs kann jedoch nicht direkt zugegriffen werden, sondern nur über eine als *PCR Extend* bezeichnete TPM-Funktion. Diese ist wie folgt definiert:

*PCR[i] = SHA-1(PCR[i] || Messwert).*
*Messwert = SHA-1(Programm).*

Das bedeutet, dass beim *PCR Extend* der Messwert des auszuführenden Programms an den aktuellen Inhalt des PCR-Registers angehängt wird und für diese Daten dann die SHA-1-Prüfsumme berechnet wird. Diese wird in Folge im PCR-Register abgelegt. Daraus ergibt sich die Eigenschaft, dass mit konstantem Speicher eine beliebig lange Kette von Messwerten gespeichert werden kann. Außerdem wird dadurch nicht nur verzeichnet, welche Programme ausgeführt worden sind, sondern auch, in welcher Reihenfolge dies erfolgt ist.

Mit diesem Verfahren, bei dem stets die nachfolgende Software-Komponente zuerst in ein PCR gemessen und erst dann ausgeführt wird, ergibt sich eine Vertrauenskette, die sogenannte *Chain of Trust*. Allerdings benötigt man für diese Kette einen Startpunkt, der die erste Messung vornimmt. In einem PC-System ist diese statische *Root of Trust for Measurement* (RTM) als nicht modifizierbarer Teil des *Basic Input Output System* (BIOS) realisiert. Beim Systemstart misst die statische RTM den variablen Teil des BIOS und gibt dann die Kontrolle an diesen ab. So wird Schritt für Schritt bis zur Applikationsebene weiter verfahren. Eine wesentliche Eigenschaft dieses auch als *Trusted Boot* bezeichneten Vorgangs ist, dass lediglich protokolliert wird, welche Software ausgeführt wird. TC kann jedoch nicht aktiv in Systemabläufe eingreifen um beispielsweise die Ausführung eines bestimmten Programms zu unterbinden.

**Root of Trust for Reporting**

Den in den PCRs erfassten Systemzustand kann man an Dritte melden (engl. *reporting*). Mit diesem, auch als Attestierung bezeichneten Verfahren kann ein Kommunikationspartner Eigenschaften eines Rechners wie z. B. Freiheit des Systems von Schadsoftware überprüfen. Bei der

Attestierung werden die aktuellen PCR-Inhalte vom TPM digital signiert. Damit diese Signatur für den Empfänger von Wert ist, muss dieser nachvollziehen können, dass die Signatur auch tatsächlich von einem TPM stammt, in dem die PCR-Werte vor Manipulation geschützt aufgezeichnet worden sind. Der naheliegende Ansatz wäre, die PCR-Werte mit dem EK zu signieren. Für diesen wird vom TPM-Hersteller ein entsprechendes *Public Key Zertifikat* mitgeliefert. Damit wären aber alle Attestierungen eines bestimmten TPMs auf dieses zurückführbar. Zum Schutz der Privatsphäre der Nutzer werden deshalb Stellvertreter vom EK abgeleitet. Von diesen sogenannten *Attestation Identity Keys* kann der Benutzer beliebig viele erstellen und somit eine Rückverfolgung vermeiden.

### 2.3 Aktuelle Anwendungen

Schätzungen der TCG gehen davon aus, dass bis 2010 ca. 250 Millionen TPM-Chips verkauft wurden. Auch wenn heute in sehr vielen Computern TPMs verbaut sind, bleibt die tatsächliche Nutzung hinter den Erwartungen zurück. Erst nach und nach werden praxistaugliche Anwendungen verfügbar, die das TPM beispielsweise zur sicheren Speicherung von vertraulichen Daten nutzen. So bietet z. B. Bitlocker – Microsofts Lösung zur Verschlüsselung von Festplatten – die Möglichkeit, das TPM zu nutzen. Die Messung und Attestierung des Systemzustands wird bisher allenfalls in Nischenanwendungen durchgeführt. Dies liegt nicht zuletzt daran, dass der Systemzustand aktueller Desktopsysteme derart komplex ist, dass ein vollständiges Nachvollziehen der gemessenen Prüfsummen kaum möglich ist. Kürzlich kündigte Google an, dass ein TPM Voraussetzung für den Betrieb seines kommenden Chrome-Betriebssystems sein wird. Dabei soll ein abgewandeltes Konzept namens *Verified Boot* zum Einsatz kommen. Dessen Ziel ist es nicht, den Systemzustand an Dritte zu melden. Vielmehr soll dem Benutzer garantiert werden, dass das System in einem vertrauenswürdigen Zustand ist.

## 4 Trusted Computing in der Videoüberwachung

Im TrustCAM-Projekt werden TC-Konzepte auf ein eingebettetes, intelligentes Kamerasystem angewendet. Die Fragestellungen leiten sich dabei von den klassischen Zielen der IT-Sicherheit ab und werden auf den konkreten Anwendungsbereich übertragen. Bei der Realisierung ist stets zu beachten, dass die Echtzeitfähigkeit des Bildverarbeitungssystems durch die eingeführten Sicherheitsmechanismen möglichst wenig beeinträchtigt werden soll. Nachfolgend werden wichtige Sicherheitsüberlegungen zusammengefasst:

- *Integrität*: Ziel ist es, Manipulationen an übertragenen oder gespeicherten Bildern zu erkennen. Von besonderem Interesse ist dieser Aspekt, wenn es um die Ahndung von Gesetzesübertretungen geht (z. B. Verkehrskameras). Dabei genügt es oft nicht, sich auf Einzelbilder zu konzentrieren, sondern es ist notwendig gesamte Videosequenzen zu betrachten. Schon durch einfaches umsortieren von Bildern eines Videos kann dessen Bedeutung grundlegend verfälscht werden. Bei einer Einzelbild-basierten Integritätsprüfung bliebe diese Manipulation unerkannt.
- *Authentizität*: In vielen Fällen ist es notwendig nachprüfen zu können, ob Bilder und Videos authentisch sind. Es gilt hier sicherzustellen, dass die vorliegenden Daten tatsächlich von einer bestimmten, am fraglichen Ort installierten Kamera stammen.
- *Aktualität und Zeitstempel*: Ziel ist es, Angriffe zu verhindern, bei denen vorab mitgeschnittenes, gültiges Videomaterial von einem Angreifer zu einem späteren Zeitpunkt in das System eingespeist wird. Über die Garantie der Aktualität hinausgehend erfordern viele Anwendungen (z. B. Strafverfolgung) außerdem, dass Bild- und Videodaten mit sicheren Zeitstempeln versehen werden.
- *Vertraulichkeit*: Wenn Bilddaten über ein Netzwerk übertragen oder in einer Datenbank gespeichert werden, ist dafür zu sorgen, dass sie von Dritten nicht mitgeschnitten, abgespielt und verwendet werden können.
- *Zugriffs-Autorisierung*: Vertrauliches Videomaterial soll nur für autorisiertes Personal zugreifbar sein. Der Zugriff ist durch entsprechende Maßnahmen wie z. B. Passwörter oder Smartcards zu sichern. Zugriffe und Zugriffsversuche sollten darüber hinaus vom System protokolliert werden.
- *Schutz der Privatsphäre*: Ein wesentlicher Aspekt ist, dass ein Kamerasystem dem Betriebspersonal nur jene Informationen zugänglich macht, die auch tatsächlich benötigt werden. In vielen Fällen ist es wichtiger, das Verhalten von Personen beobachten und einschätzen zu können als deren Identität zu kennen. Intelligente Kameras sind dafür bestens geeignet, weil persönliche Informationen noch bevor Daten das System verlassen unkenntlich gemacht oder entfernt werden können.
- *Zustimmung und Feedback*: Videoüberwachungsanlagen werden üblicherweise durch Aufkleber oder Hinweisschilder gekennzeichnet. Moderne Kommunikationsmittel wie z. B. Smartphones könnten genutzt werden, um Passanten aktiv über installierte Überwachungssysteme aufzuklären sowie Feedback über deren Einsatzzweck und Eigenschaften zu geben.
- *Verfügbarkeit*: In manchen Fällen werden Kamerasysteme als Teil der kritischen Informationsinfrastruktur betrachtet. Daher kann es notwendig sein, Schutzmechanismen gegen *Denial of Service*-Angriffe zu integrieren, um Garantien zur Verfügbarkeit der Dienste machen zu können.

### 4.1 Integrität und Authentizität

Abbildung 1 zeigt ein System aus mehreren Kameras, die jeweils mit einem TPM, bezeichnet als $TPM_K$, ausgestattet sind. Das Kontrollzentrum ist ebenfalls mit einem TPM – genannt $TPM_Z$ – ausgestattet. Bei der Installation einer Kamera wird in deren $TPM_K$ ein nicht übertragbarer Signaturschlüssel $K_{SIG}$ erzeugt. Der öffentliche Teil wird in der Datenbank des Kontrollzentrums abgelegt. Weiter werden im $TPM_Z$ des Kontrollzentrums für jede installierte Kamera mehrere Schlüssel $K_{BIND[1...N]}$ für das Binding von Daten erzeugt. Die öffentlichen Teile werden auf der Kamera hinterlegt.

Um sicherzustellen, dass empfangene Bild- und Videodaten auch tatsächlich von einer ganz bestimmten Kamera stammen, werden ausgehende Daten von den Kameras digital signiert. Dazu wird die SHA-1-Prüfsumme des Bildes berechnet und vom $TPM_K$ der Kamera unter Verwendung des privaten Signaturschlüssels $K_{SIG}$ digital signiert. Im Kontrollzentrum wird der zur erwarteten Kamera gehörende, öffentliche Schlüssel aus der Datenbank geladen. Danach wird die an die Bilddaten angehängte Signatur geprüft und die enthalte-

**Abbildung 1 | Ein Netzwerk bestehend aus intelligenten Kameras, die Informationen und Videos an eine Kontrolleinheit übermitteln. Jede Kamera sowie auch das Kontrollzentrum ist mit einem TPM Chip ausgestattet.**

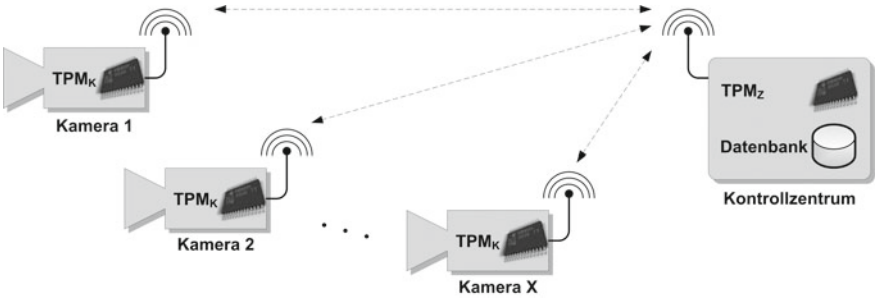
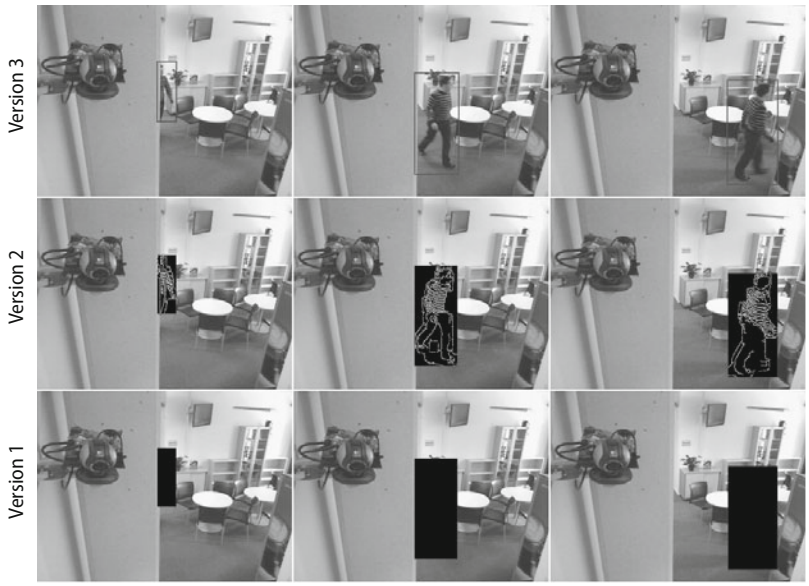



**Abbildung 2 | Die oberste Zeile zeigt vollständige Bilder mit einer von der Kamera detektierten Person. In der mittleren Zeile wird die Identität der Person unkenntlich gemacht. Das Verhalten der Person bleibt aber erkennbar. In der untersten Zeile werden von der Kamera alle personenbezogenen Informationen aus den Bildern entfernt.**




ne SHA-1-Prüfsumme mit dem vom Empfänger berechneten SHA-1-Wert der Bilddaten verglichen.

Ist diese Prüfung erfolgreich, so ist für den Empfänger sichergestellt, dass (1) die Bilddaten nicht manipuliert wurden und (2) die Daten tatsächlich von der erwarteten Kamera stammen. Dies wird dadurch garantiert, dass der private Teil von $K_{SIG}$ ausschließlich im $TPM_K$ dieser Kamera nutzbar ist und aus diesem TPM nicht im Klartext exportiert oder in ein anderes TPM übertragen werden kann.

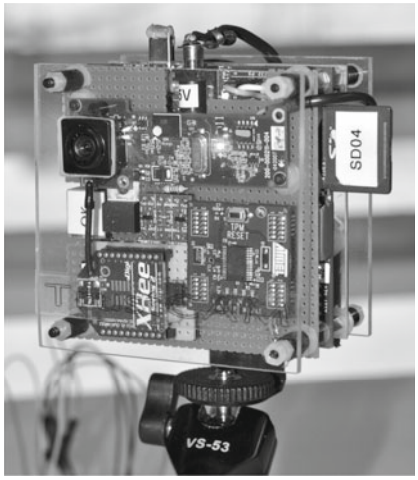
Die beschriebene Vorgehensweise hat allerdings die Einschränkung, dass aktuelle TPM-Implementierungen nicht schnell genug sind, um jedes einzelne Frame eines Videos zu signieren. Die schnellsten verfügbaren TPMs benötigen für das Signieren ca. 350ms. Damit würde die effektive Bildwiederholrate von 25 auf weniger als 3 Bilder pro Sekunde sinken. Deshalb werden im TrustCAM-System Bildgruppen anstatt einzelner Bilder signiert. Dabei werden die Prüfsummen der Einzelbilder, ähnlich der *PCR Extend*-Funktion, akkumuliert. Danach wird dieser akkumulierte Hash vom TPM signiert. Damit gelingt es nicht nur, die Geschwindigkeitsprobleme des TPM zu umgehen, sondern es ist auch nicht mehr möglich unbemerkt Bilder innerhalb einer Gruppe zu vertauschen. Um die Reihenfolge der Gruppen sicherzustellen, wird auch die Prüfsumme der jeweils vorhergehenden Gruppe mit in die Signatur aufgenommen.

### 4.2 Vertraulichkeit, Privatsphäre, Zugriffskontrolle

Um die Privatsphäre von überwachten Personen zu wahren, verfolgt das TrustCAM-Projekt den Ansatz, personenbezogene Daten schon auf der Kamera zu erkennen und entsprechend zu schützen. Als personenbezogen werden dabei jene Informationen eingestuft, die Rückschlüsse auf die Identität von Personen erlauben. Dazu gehören beispielsweise Gesichter oder auch Autokennzeichen. Die zugehörigen Bildregionen können beispielsweise gänzlich entfernt oder verschwommen bzw. verpixelt dargestellt werden. Ist für eine Anwendung lediglich das Verhalten der beobachteten Personen von Interesse, dann sind die verbleibenden Informationen ausreichend. In Ausnahmefällen kann es jedoch vorkommen, dass Informationen zur Identität der beobachteten Personen benötigt werden. Ein solcher Fall wäre zum Beispiel die Aufklärung einer Straftat. Um zugleich dieser Anforderung zu genügen, realisiert das TrustCAM-Projekt ein mehrstufiges System zum Schutz der Privatsphäre. Im ersten Schritt werden von der Kamera auf Basis einer Bewegungsdetektion zu schützende Bildbereiche, wie zum Beispiel Personen, identifiziert. Dies ist exemplarisch in der obersten Zeile von Abbildung 2 gezeigt. Im nächsten Schritt werden diese sensiblen Bereiche aus dem Bild ausgeschnitten (Abbildung 2, unterste Zeile). Die sensiblen Bilddaten werden von der Kamera mittels Kantendetektion so modifiziert, dass zwar das Verhalten von Personen erkennbar bleibt, deren Identität aber verborgen wird (Abbildung 2, mittlere Zeile). Somit ergeben sich drei Versionen der Videodaten: In Version 1 (Abbildung 2, unterste Zeile) ist lediglich die Position von Personen erkennbar. Identität und Verhalten bleiben verborgen. In Version 2 (Abbildung 2, mittlere Zeile) ist das Verhalten von Personen beobachtbar. Und in Version 3 (Abbildung 2, oberste Zeile) sind sowohl Verhalten als auch Identität erkennbar.

Diese drei Versionen werden an das Kontrollzentrum übermittelt. Zuvor müssen die sensiblen Bildbereiche noch entsprechend geschützt werden. Dazu werden AES-Sitzungsschlüssel erzeugt. Mit je einem dieser Schlüssel werden die sensiblen Regionen aus Version 3 (Originalvideo) sowie der vorverarbeiteten Version 2 verschlüsselt. Die beiden AES-Schlüssel

**Abbildung 3 | TrustCAM-Prototyp**




werden mit den öffentlichen Teilen von $K_{BIND1}$ und $K_{BIND2}$ verschlüsselt. Die zugehörigen privaten Schlüssel sind durch $TPM_Z$ geschützt. Für die Entschlüsselung der Bilddaten ist somit Zugang zum Kontrollzentrum erforderlich. Dieser sollte auf einen kleinen Kreis autorisierter Personen beschränkt sein.

Unter dem Kontrollpersonal ist darüber hinaus eine Abstufung der Zugriffsrechte möglich. Personal auf niedriger Stufe ohne Kenntnis der Passwörter für $K_{BIND1}$ oder $K_{BIND2}$ kann nur Version 1 der Videodaten einsehen, in der lediglich Präsenz und Position von Personen im Sichtfeld der Kamera erkennbar ist. Personal auf einer höheren Sicherheitsebene mit Kenntnis des Passworts für den privaten Teil von $K_{BIND1}$ erhält Zugriff auf Version 2 der Videodaten, in der zusätzlich zu Präsenz und Position auch das Verhalten von Personen erkennbar ist. Version 3, in der auch die Identität von Personen sichtbar ist, erfordert das Passwort für $K_{BIND2}$ und ist höheren Instanzen (z. B. Supervisor oder Behörden) vorbehalten.

### 4.3 TrustCAM Prototyp

Abbildung 3 zeigt den TrustCAM-Prototyp. Das System basiert auf einer OMAP 3530 CPU von Texas Instruments mit ARM und DSP Prozessorkernen, 256 MB Arbeitsspeicher, 256 MB Flashspeicher, einem Atmel TPM 1.2 sowie einem VGA Farb-CMOS-Sensor.

Auf diesem Prototyp sind nicht nur die zuvor beschriebenen Konzepte zur Sicherstellung von Integrität, Authentizität und Vertraulichkeit umgesetzt, sondern es wird auch eine *Chain of Trust* aufgebaut. Anders als auf einem konventionellen PC werden allerdings nicht alle Teile des Systems mitsamt den Softwarebibliotheken und Applikationen separat in die PCRs des TPM gemessen. Abgesehen vom mehrstufigen Bootloader und dem Betriebssystemkern wird das Basisdateisystem der Kamera als Ganzes gemessen. Da das Dateisystem weniger als 30 MB umfasst, wird dadurch der Startvorgang kaum verlängert.

Um nicht nur den Gesamtzustand der Kamera an den Betreiber melden zu können, werden darüber hinaus die ausgeführten Bildverarbeitungsapplikationen mit in die Messkette aufgenommen. Der aktuelle Systemzustand wird in Form eines sogenannten *Lifebeat* periodisch vom Kontrollzentrum aus abgefragt. Als Teil dieses Lifebeats wird unter Verwendung der monotonen Zähler des TPM auch eine Reboot-Erkennung durchgeführt.

Evaluierungen der Systemleistung haben gezeigt, dass die im Prototyp realisierten Sicherheitsfunktionen nur geringen Einfluss auf die Gesamtleistung des Systems haben. Die Bildwiederholraten reduzieren sich bei aktiver Datenverschlüsselung und Signierung um lediglich ein halbes Bild pro Sekunde.

## 5 Zusammenfassung und Ausblick

Überwachungskameras sind heute in vielen Bereichen des täglichen Lebens präsent. Sehr oft werden Sicherheitsfragen oder der Schutz der Privatsphäre nur am Rande berücksichtigt. Für eingebettete Systeme wie z. B. intelligente Kameras stellen Trusted Computing und das TPM eine attraktive Lösung dar, um Sicherheitsfunktionen auf vergleichsweise einfache Art zu integrieren. Einer der wesentlichen Vorteile ist die sichere Speicherung der verwendeten kryptographischen Schlüssel, die andernfalls nur schwierig realisierbar ist.

Die Konzepte der Erfassung des Systemzustands sowie der Attestierung haben sich bisher für PC Systeme nicht durchsetzen können. Geschuldet ist dies in erster Linie der Größe und der Komplexität der verwendeten Betriebssysteme und Applikationen. Bei eingebetteten Systemen ist einerseits der Umfang der Software weitaus geringer, andererseits ist diese wesentlich homogener und weitgehend unter der Kontrolle der Hersteller bzw. Betreiber. Attestierung ist somit in diesem Umfeld durchaus als praktisch verwendbarer Mechanismus zur Systemüberwachung anzusehen.

Sicherheit und Schutz der Privatsphäre in der Videoüberwachung sind Themenbereiche, die gegenwärtig in der Forschung vermehrt Beachtung finden. Das hier vorgestellte TrustCAM-System ist ein Ansatz, ausgewählte Aspekte prototypisch zu realisieren. Weitere Informationen und technische Hintergründe sind beispielsweise in [3, 6] beschrieben. Um ein solches System in praktischen Anwendungsszenarien einzusetzen, bedarf es jedoch noch umfassender weiterer Arbeiten. So sind zukünftig Fragen der Skalierbarkeit, der dynamischen Rekonfiguration, des sicheren Einspielens von Softwareupdates oder des Schutzes gegen *Denial of Service*-Angriffe zu untersuchen.

Abschließend bleibt festzuhalten, dass moderne, intelligente Kamerasysteme besonders im Bereich der Privatsphäre viele Fragen aufwerfen, aber auch ganz neue Möglichkeiten eröffnen. Die Vorverarbeitung von sensiblen Informationen direkt bei der Aufnahme, gepaart mit etablierten Konzepten aus der IT-Sicherheit, lässt die Vision vertrauenswürdiger Überwachungskameras in greifbare Nähe rücken.

## Referenzen

[1] D.N. Serpanos und A. Papalambrou, "Security and Privacy in Distributed Smart Cameras," Proceedings of the IEEE, Okt. 2008, S. 1678-1687.

[2] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, A. Ekin, J. Connell, C.F. Shu, and M. Lu, "Enabling Video Privacy through Computer Vision," IEEE Security & Privacy Magazine, Vol. 3, 2005, S. 50-57.

[3] T. Winkler und B. Rinner, "TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera based on Trusted Computing," Proceedings of the International Conference on Advanced Video and Signal-Based Surveillance, 2010, S. 593-600.

[4] Institut für Vernetzte und Eingebettete Systeme, Alpen-Adria Universität Klagenfurt, http://nes.aau.at

[5] Trusted Computing Group Website, http://www.trustedcomputinggroup.org

[6] T. Winkler und B. Rinner, "Securing Embedded Smart Cameras with Trusted Computing," EURASIP Journal on Wireless Communications and Networking, Vol. 2011, 2011, 20 Seiten.