A Systematic Approach Towards User-Centric Privacy and Security for Smart Camera Networks

Thomas Winkler
Pervasive Computing / Institute of Networked
and Embedded Systems (NES)
Lakeside Park B02b
9020 Klagenfurt, Austria
thomas.winkler@uni-klu.ac.at

Bernhard Rinner
Pervasive Computing / Institute of Networked
and Embedded Systems (NES)
Lakeside Park B02b
9020 Klagenfurt, Austria
bernhard.rinner@uni-klu.ac.at

ABSTRACT

The majority of research in the field of camera networks is targeted at distributed and cooperative processing, advanced computer vision algorithms or the development of embedded, ubiquitous camera systems. Privacy and security are topics that are often overlooked or considered as an afterthought. With the digitalization of visual surveillance, data can easily be stored and accessed. This raises the question how confidential data can be protected, authenticity and integrity can be ensured and access can be restricted. This work discusses security and privacy issues relevant in the context of visual surveillance and camera networks. We try to capture the state of the art on these aspects in the available literature and highlight areas that require special consideration. We present a concept of a privacy-preserving camera system based on Trusted Computing. In our system-level approach, we consider privacy and security as primary goals without limiting the overall usefulness of a camera system.

Categories and Subject Descriptors

I.4.9 [**Image Processing and Computer Vision**]: Applications; K.6.5 [**Security and Protection**]: Authentication, Unauthorized Access; K.4.1 [**Public Policy Issues**]: Privacy

General Terms

Security

Keywords

Smart Cameras, Privacy, Security, Trusted Computing

1. INTRODUCTION AND MOTIVATION

Visual surveillance is undergoing a shift from traditional, analog CCTV cameras towards fully digitized systems. This promises to increase effectiveness of systems since no constant monitoring by human operators is required. Captured video is analyzed autonomously and alarms are issued in case of unusual events. Systems that implement some of these capabilities are already commercially available [13].

The introduction of digital video surveillance, however, does not only have positive aspects. A number of open issues exist when it comes to privacy of monitored people and security of systems against attacks and abuse. Contrary to analog systems, digital video can easily be stored, indexed, retrieved and cross-referenced [5]. This opens new possibilities to, e.g., derive behavior patterns not only for suspected criminals but also for ordinary, innocent people.

Recent discussions in Europe about the legitimacy of services such as Google Street View [12], raise public awareness of capabilities and potential risks of digital imaging. We believe that it is only a question of time until digital video surveillance will be in the focus of public and media attention. Therefore, we advocate that researchers take an open and pro-active approach towards privacy protection and security in camera systems. In this area, we see especially high potential for smart cameras since security and privacy should not be addressed as an afterthought but need to be integrated into the processing chain as close to the sensor as possible. To date, several solutions for selected problems exist that, e.g., hide human faces [7, 14] or extract and encrypt sensitive image regions [19]. But a lot of work still remains to be done towards truly integrated, privacy-protecting and secure smart cameras.

With this work we contribute to this effort in three ways: First, in section 2, we collect desirable properties of a secure and privacy-preserving camera system. Second, in section 3, we review related work on privacy and security in visual surveillance. We classify existing approaches based on their properties and discuss shortcomings and gaps that need to be filled. Third, in section 4, we sketch a concept for a system level approach for a trustworthy, embedded smart camera. We address both, security needs of system operators and privacy concerns of monitored users. Section 5, outlines future work and concludes the paper.

2. PRIVACY AND SECURITY IN VISUAL SURVEILLANCE

In the following section we discuss common system security properties and their meaning for smart cameras. Thereafter, we address the critical issue of privacy in visual surveillance and outline potential ways of user involvement.

ICDSC 2010 August 31 – September 4, 2010, Atlanta, GA, USA
Copyright 2010 ACM 978-1-4503-0317-0/10/08 ...$10.00.

2.1 General Security Aspects

General security requirements for smart cameras are not substantially different from those of other computing systems. The following discussion of security properties is loosely based on previous work by Serpanos and Papalambrou [20] and Senior et al. [19]. We, however, provide slightly different interpretations and extend some of the properties in ways previously not considered. Note that these general security properties not only offer benefits for camera operators. They also are a fundamental requirement for the design of advanced, user-centric security features such as privacy protection.

- **Integrity.** Image data from cameras can be intentionally altered by attackers during transmission or when stored in a database. Integrity protection allows consumers to detect manipulation. It can be realized with checksums and digital signatures for images and videos sequences.
- **Authenticity.** In many applications such as traffic monitoring and law enforcement, the origin of information is important. For a camera system, this is equivalent to knowing the source of a video stream. This can be done by explicit authentication of cameras belonging to a network and embedding this information into videos.
- **Freshness and Timestamping.** To avoid replay attacks where recorded video sequences are injected into a network to replace the live video stream, freshness of images must be guaranteed. Timestamping is one way to realize this freshness property. Moreover, timestamping is a desired feature in, e.g., enforcement applications where evidence is required when an image was taken.

  Often overlooked is the issue of correct order of frames of a video stream. Re-ordering of images by an attacker could substantially change the meaning of a video. Again, timestamping allows to detect such modifications.
- **Confidentiality.** Images and videos that are transmitted over a network or stored in a database, need to be protected such that attackers can not view or use the original video. Typically, this is achieved by encryption.
- **Access Authorization.** Access to confidential image data must be limited to persons with adequate security clearance. For access to highly sensitive data, involvement of more than one operator should be required to prevent misuse. If a video stream contains different levels of information (e.g., full video, annotations, ...), access should be managed separately for each level. Finally, all access to confidential data should be logged.
- **Availability.** A camera network should provide certain guarantees about availability of system services under various conditions. Specifically, reasonable resistance against denial of service attacks should be provided.

Clearly, these security properties partially depend on each other. For example, it is meaningless to provide data confidentiality without implementing appropriate authorization mechanisms for access to confidential data.

2.2 Privacy in Visual Surveillance

Cameras allow to extend the field of view of observers into areas where they are not physically present. This “virtual presence” of an observer is not necessarily noticed by monitored persons. In the resulting, but misleading feeling of privacy, persons might act differently than they would in the obvious presence of other people. This example makes it apparent, that privacy in video surveillance is an issue that needs special consideration. But when trying to identify what forms of privacy protection are appropriate, the picture becomes less clear. One reason is that there is no common definition of privacy. As discussed in [19, 16], the notion of privacy is highly subjective and what is acceptable depends on the individual person as well as cultural attitudes.

The problem of protecting an area against capturing by cameras, is addressed by Truong et al. [23]. In their capture-resistive environment, camera phones are prevented from taking images. Emitted IR light is retro-reflected by the mobile phone’s image sensor. These reflections are detected by the system and used to localize the mobile phone which is then neutralized by intense, directed light emitted by a video beamer. While this is an interesting approach to preserve privacy in selected areas, it is not practical for large deployments. Therefore, many researchers focus on the opposite approach where cameras actively detect and protect privacy sensitive image regions. The challenge is to provide adequate privacy protection without removing too much information such that the system becomes unusable for the intended purpose. As discussed by Cavallaro [5], it is usually more important to be able to observe the behavior of a person than knowing the actual identity. This is achieved by identification and obfuscation of personally identifiable information such as people’s faces. Only in situations where, e.g., a law was violated, this personal information is of interest and should still be available to authorized parties. In the following, we discuss functionality typically found in proposals for privacy-aware camera systems:

- **Detection of Sensitive Regions.** This denotes the capability of a system to detect privacy sensitive image regions. These are, e.g., human faces [7, 14] or vehicle licence plates. If this system component does not work reliably, privacy is at risk. A single frame of a video sequence where sensitive regions are not properly detected, can break privacy protection for the entire sequence.
- **Blanking.** One way to deal with sensitive image regions is to completely remove them from the image leaving behind blank areas [18]. While providing perfect user privacy, the usefulness of the system is reduced since not even basic user behavior can be observed. Some approaches suggest to fill blank regions with background data from related frames or by inpainting techniques [9].
- **Obfuscation and Scrambling.** The purpose of obfuscation is to reduce the level of detail in sensitive image regions such that persons can no longer be identified. Proposed approaches apply, e.g., mosaicing, pixelation, blurring [10, 25] or high, lossy compression.

Image scrambling is a technique where sensitive regions in, e.g., JPEG compressed images are obscured by pseudo-randomly modifying the region's DCT coefficients [11].

- **Abstraction.** This popular technique replaces sensitive image regions with, e.g., bounding boxes or, in case of persons, with silhouettes and stick-figures [19]. Another form of abstraction is meta-information that is attached to a video. This can be object properties such as position and dimensions, but also names of identified persons [22].
- **Encryption.** Data encryption is frequently used to keep sensitive regions confidential [2, 28, 8]. While the primary goal is to protect against external attacks, encryption can also help against misuse by legitimate system operators. In combination with multiple privacy levels, it can be ensured that normal operators only get access to obfuscated or abstracted data which often is sufficient for their requirements. Access to higher levels, such as unmodified video data, might be limited to supervisors or governmental agencies. Contrary to simple blanking, obfuscation, abstraction and abstraction, the encryption of sensitive image regions is reversible and allows to reconstruct the original image.
- **Multiple Privacy Levels.** This denotes that one single video stream can contain different levels of information. In the context of privacy, these could be the original, unmodified sensitive image regions, an obfuscated version with blurred faces and an abstracted version only showing the borders of objects. This allows to present different information to observers with different security clearance. The individual data representations must be protected against access from unauthorized observers.

Note that there is partial overlap between privacy protection and data confidentiality. Depending on the actual implementation, privacy protection is a subset of data confidentiality since some parts of the original information, e.g., are removed or encrypted. Typically, data confidentiality is a stronger property since no distinction is made between personal or behavioral data as it is done in privacy protection. In a real system, both – confidentiality and privacy protection – are required. Data confidentiality mechanisms protect all data against eavesdropping when, e.g., transmitted over a wireless network. Privacy protection allows to reveal behavioral information to legitimate observers while personal data is protected.

2.3 User Involvement

To increase acceptance of camera installations in public areas, privacy protection is an important step. Current implementations provide no feedback and users have to blindly trust that camera systems behave as advertised. Ideally, this behavior should be verifiable by users. Furthermore, an ideal system should give users control over their personal video data. Specifically, user involvement includes the following points:

- **User Consent and Control.** Typical camera installations are marked with signs or stickers that advertise their presence. User consent to video surveillance is given implicitly by acknowledging these signs when entering the area. As these signs are easily overlooked, consent should be sought more actively. Users could be automatically notified, e.g., via their mobile phone. Moreover, monitored people should remain in control of personal data captured by the system. If data is disclosed to a third party, explicit user permission should be required.
- **User Feedback.** In current systems, users have to trust operators to protect their privacy. To establish this trust, Senior et al. [19] suggest that surveillance equipment should be certified and the results should be made visible, e.g., by stickers attached to cameras. But for users it is difficult to evaluate if this certification is still valid. The software of a smart camera might have been changed by the operator without recertification of the system. Therefore, an ideal system should be able to accurately report its current status to users. This report should include information on what personal data is captured, processed, stored and delivered to observers.

3. RELATED WORK

Only little literature exists that targets general security questions in the context of smart camera networks. One noteworthy exception is the work of Serpanos and Papalambrou [20] which provides an extensive discussion of security aspects. Most other related work, which we cover in the following two sections, is focused on privacy issues. We distinguish between work aimed at privacy protection and work that additionally proposes approaches for user involvement. Thereafter, we present a comparison and classification of the reviewed works and identify shortcomings and gaps that need to be filled.

3.1 Privacy Protection in Visual Surveillance

Senior et al.[19] discuss critical aspects of a secure surveillance system including what data is available and in what form (e.g., raw images vs. metadata), who has access to data and in what form (e.g., plain vs. encrypted) and how long it is stored. User privacy is a major concern that is addressed in the proposed system concept. Incoming videos are analyzed and sensitive information is extracted. The extracted data is re-rendered and multiple streams with different levels of data abstraction are created. By encryption of streams, multi-level access authorization is realized. The authors suggest that video analysis, processing and encryption could either be done by a dedicated privacy console or directly by the cameras.

Cavallaro [5, 4] argues that digitalization of video surveillance introduces new privacy threats. Therefore, personal and behavioral data should be separated directly on the camera. While system operators only get access to behavioral data, a separate stream containing personal data is made available to law enforcement authorities. A benefit of this strict separation is prevention of operator misuse. Possible implementation approaches are not discussed in this work.

Moncrieff et al. [16] argue that most proposed systems rely on predefined security policies and are either too intrusive or too limited. Therefore, they suggest to apply dynamic data hiding techniques. By context based adaptation, the system could remove or abstract privacy sensitive information during normal operation while in case of an emergency, the full, unmodified video stream is automatically made available. This way, the system remains usable for the intended purpose but protects privacy during normal operation.

Boult [2] argues that many existing approaches are targeted at removing privacy sensitive image data without providing mechanisms to reconstruct the original image. Based on this observation, he proposes a system concept called PICO that relies on cryptography to protect selected image regions such as faces. It allows to monitor actions of a person without revealing his/her identity. The faces are only decrypted if, e.g., a crime was committed by the person. Encryption is supposed to be done as part of image compression and uses a combination of symmetric and asymmetric cryptography. Additionally, it is suggested to compute checksums of frames or sub-sequences to ensure data integrity. In related work, Chattopadhyay and Boult present PrivacyCam [6], a camera system based on a Blackfin DSP clocked at 400 MHz, 32 MB of SDRAM and an Omnivision OV7660 color CMOS sensor. uClinux is used as operating system. Regions of interest are identified based on a background subtraction model and resulting regions are encrypted using an AES session key.

Dufaux and Ebrahimi [11] suggest to scramble sensitive image regions. After detection of relevant areas, images are transformed using DCT. The signs of the coefficient of sensitive regions are then flipped pseudo-randomly. The seed for the pseudo random number generator is encrypted. Decryption is only possible for persons who are in possession of the corresponding decryption key. According to the authors, main benefits are minimal performance impact and that video streams with scrambled regions can still be viewed with standard players. A similar approach is discussed by Baaziz et al. [1] where in a first step motion detection is performed followed by content scrambling. To ensure data integrity, an additional watermark is embedded into the image which allows to detect manipulation of image data. Limited reconstruction of manipulated image regions is possible due to redundancy introduced by the watermark. Yabuta et al. [28] also propose a system where DCT encoded image data is modified. They however do not scramble regions of interest but extract them before DCT encoding and encrypt them. These encrypted regions are then embedded into the DCT encoded background by modifying the DCT coefficients.

Tansuriyavong et al. [22] present a system used in an office scenario that blanks the silhouettes of persons. Additionally, the system integrates face recognition to identify previously registered persons. Configuration options allow to choose what information should be disclosed - full images, silhouettes, names of known persons or any combination thereof.

3.2 Privacy Protection with User Involvement

Privacy protection can be further enhanced by involvement of monitored users. Several approaches have been presented that allow to selectively remove known, trusted users from captured video. Some go even further and give monitored persons control over who is able to access personal video data. Due to limited reliability of computer vision for detection of personal image data, many researchers rely on portable devices carried by users for identification and localization.

Brassil [3] proposes a Privacy Enabling Device (PED) that gives users control over their personal data. When activated, the PED records the location of the person together with timestamps. The recorded data is then uploaded to a clearinghouse. Before a camera operator discloses videos to a third party, he is obligated to contact the clearinghouse. If any active PED was in the vicinity of the camera at the time in question, video data has to be anonymized. As there is no feedback, users have to trust camera operators to follow the advertised procedures.

Contrary to the approach of Brassil, Wickramasuriya et al. [25] perform realtime monitoring of the environment to increase user privacy. In particular, they suggest to use motion sensors to guard rooms or areas. If motion is detected, an RFID reader is triggered that tries to read the RFID tag carried by the person that entered the area. If no RFID tag can be found or the security level of the tag does not grant access to the area, a camera that oversees the region is turned on to record video. Image regions containing persons with valid RFID tags are blanked such that only potential intruders remain visible.

Chinomi et al. [10] also use RFID technology to detect known users. RFID readers, deployed together with cameras, are used to localize RFID tags carried by users based on signal strength. This location information is then mapped to moving objects detected by the cameras. As the RFID tag identifies the person, his/her privacy policy can be retrieved from a database. This policy defines the relationship between the monitored person and potential observers. Based on that, different levels of data abstraction can be generated and displayed by the system. Abstractions range from a simple dot showing only the location of the person, over silhouettes and blurred image data to the full disclosure of the original image.

Cheung et al. [8] follow a similar approach but extend the idea in several ways. Localization is based on active RFID tags carried by users. Corresponding motion regions are extracted from the video and encrypted with the user's public encryption key. This key is retrieved from a database via the user ID read form the RFID tag. The blank regions in the remaining image are filled with background image data using video inpainting as described by Cheung et al. [9]. The encrypted regions then are embedded into the compressed background image using data hiding techniques [17] similar to steganography. Since decryption of privacy sensitive image regions requires access to the user's private key, user consent and active cooperation is necessary to reconstruct the original image. A dedicated mediator establishes contact between users and observers who are interested in the video data.

It must be noted, that none of the described approaches that rely on RFID for localization of trusted users address the issue of RFID security. In an actual system, countermeasures against, e.g., cloning of tags is a critical requirement. Moreover, it is apparent that these approaches are only applicable to well defined monitoring scenarios (e.g., a hospital) but can not easily be used in general public places.

An approach that does not need special, electronic devices carried by persons is presented by Schiff et al. [18]. Their "respectful cameras" use visual markers such as yellow hard hats worn by persons to identify privacy sensitive image regions. Specifically, the authors suggest to remove person's faces from the images. For marker detection and

	General Security						Privacy Protection						User Inv.		
	Integrity	Authenticity	Freshness / Timestamping / Ordering	Confidentiality	Authorization / Access Control	Availability	Sensitive Regions	Blanking	Obfuscation / Scrambling	Abstraction	Encryption	Multi-Level	Consent and Control	Feedback	System Level Integration
Baaziz [1]	●	○	○	◐	○	○	●	○	●	○	◐	○	○	○	○
Boult [2] + Chattopadhyay [6]	◐	○	○	◐	○	○	●	○	○	○	●	○	○	○	◐
Brassil [3]	○	○	○	○	○	○	◐	●	◐	○	○	○	●	○	○
Cavallaro [5, 4]	○	○	○	○	●	○	●	●	○	●	○	●	○	○	○
Cheung et al. [8, 9, 17]	○	○	○	◐	●	○	●	●	○	○	●	○	●	○	○
Chinomi et al. [10]	○	○	○	○	◐	○	●	●	●	●	○	●	●	○	○
Dufaux + Ebrahimi [11]	○	○	○	◐	●	○	●	○	●	○	●	○	○	○	○
Moncrieff et al. [16]	○	○	○	○	○	○	◐	◐	◐	◐	○	●	○	○	○
Schiff et al. [18]	○	○	○	○	○	○	●	●	○	○	○	○	●	○	○
Senior et al. [19]	○	○	○	●	●	○	●	○	○	●	●	●	○	◐	◐
Spindler et al. [21]	○	○	○	◐	○	○	●	●	○	○	●	○	◐	○	○
Tansuriyavong [22]	○	○	○	○	○	○	●	●	○	●	○	●	○	○	○
Wickramasuriya et al. [25]	○	○	○	○	○	○	●	●	●	●	○	●	●	○	○
Yabuta et al. [28]	○	○	○	◐	○	○	●	●	○	○	●	○	○	○	○
TrustCAM Concept (sec. 4)	●	●	●	●	●	○	●	●	◐	●	●	●	○	●	●

Table 1: Security and privacy properties of related work on visual surveillance and our TrustCAM concept (see section 4). The properties correspond to those described in section 2. The *System Level Integration* column reflects if the work tries to incorporate general security and privacy protection into a smart camera platform. White bullets represent unsupported properties, grey bullets denote partially realized properties and black bullets stand for fully covered properties.

tracking, probabilistic AdaBoost and particle filtering are used. Spindler et al. [21] propose to apply similar ideas for a building automation and monitoring system. Personal data is obfuscated based on individual privacy settings. For user identification and localization, the authors suggest to use computer vision. For the prototype however, this component was not implemented but replaced by manual selection of privacy sensitive regions.

3.3 Classification and Observations

In table 1 we present a classification of the related works we summarized in the previous sections. It is based on the system security and privacy properties we discussed in section 2.

It is apparent that general system security is not considered by most approaches. Integrity protection for image data is only mentioned by Baaziz et al. and Boult. Authenticity and freshness/timestamping of images is not addressed by any of the reviewed works. Confidentiality of image data is considered by less than half of the concepts. In most cases, partial confidentiality is achieved by encryption of selected image regions for privacy protection. Only Senior et al. target full confidentiality by encryption of all data sent by cameras. Access control for confidential data is mentioned in less than half of the concepts. Finally, system availability is not considered in any of the proposals. Reasons might be that availability is difficult to define and is very application specific.

Privacy protection is an important feature in all approaches. There seems to be consensus that this is best achieved by identification of sensitive image regions. The majority of works considers blanking of regions as an appropriate way to protect privacy. Obfuscation/scrambling and abstraction of data both are considered by about half of the proposals. The same holds true for the support of multiple privacy levels and encryption of sensitive image regions.

About half of the approaches try to actively involve monitored users by seeking consent or giving some control over the use of personal data. The approach of Cheung et al. stands out as, by design, access to personal data requires active user involvement. In most approaches, users have to trust that the system behaves as advertised by the operator. The only work that mentions limited user feedback is from Senior et al. who propose the certification of surveillance equipment.

The *System Level Integration* column of table 1 highlights those approaches where at least partial effort was made towards a holistic, embedded smart camera security solution. Chattopadhyay and Boult demonstrated detection and encryption of sensitive image regions with their PrivacyCam prototype. Senior et al. probably presented one of the most comprehensive approaches towards security and privacy in camera networks. Moreover, they consider deployment on embedded camera systems.

In conclusion, all reviewed approaches provide some form of privacy protection. User involvement is addressed by several researchers but user feedback is typically not provided. Furthermore, little effort is spent on the integration of privacy protection with underlying system security. Therefore, we see two major topics that need to be addressed in future work:

- **User Feedback.** Currently, users have to trust that cameras behave as advertised. Feedback should be given on how personal data is used and protected by the system.
- **System Level Integration.** Most approaches for privacy protection do not consider the underlying system. We however argue, that system security is a fundamental requirement for successful realization of high-level features such as privacy protection. Therefore, privacy and system level security should always be addressed in combination.

4. A SYSTEM-LEVEL CONCEPT FOR SECURITY AND PRIVACY PROTECTION WITH USER-FEEDBACK

In this section we sketch the overall concept for our system-level approach for trustworthy, embedded smart cameras called TrustCAM. In related work we discuss details and provide first evaluation results for selected aspects such as secure video streaming [26] and user feedback [27]. As a basis for our work, we rely on Trusted Computing (TC) which is a hardware security solution built around a microchip called Trusted Platform Module (TPM) [24]. TPMs are available from multiple manufacturers and implement a well defined and widely reviewed set of functions. It allows to generate RSA key pairs which can be used to securely store or sign data. An important property is that private RSA keys never can be exported from the TPM as plaintext. If a key is marked as non-migratable upon creation, it also can not be transferred to another TPM. This guarantees that data signed with such a key, comes from the system the TPM belongs to. Likewise, data encrypted with the public part of a non-migratable TPM key can only be decrypted on the system the contains the TPM with the matching private key. In TC terminology, the encrypted data is said to be *bound* to that TPM. Additionally, key usage is protected with a password. Another important capability of a TPM is to *measure* the status of a platform. This means that every software component executed on a system is logged into so called Platform Configuration Registers (PCRs) inside the TPM. These PCRs can not be overwritten but are *extended* which means that measurements are accumulated. PCRs can only be reset by rebooting the system. To be able to reproduce the accumulated PCR values, a PCR log with the individual measurements is kept on mass storage. If each component is measured before execution, a *chain of trust* is established starting at the BIOS or bootloader going up to the application level. By signing the PCR values inside the TPM with a special type of key called Attestation Identity Key (AIK), the current platform state can be reported to a verifier. This reporting mechanism is called *attestation.* In addition to this core functionality, a TPM supports timestamping, monotonic counters and random number generation.

We propose to integrate a TPM, subsequently called TPM_C, into our embedded smart cameras. Cameras are operated from a central control station that is also equipped with a TPM called TPM_S. During setup, where cameras are under full control of the operating personnel, a set of keys is generated on TPM_C and TPM_S. Specifically, a non-migratable signing key K_{SIG} is created on TPM_C and multiple, non-migratable binding keys $K_{BIND1...N}$ are generated on TPM_S. For platform attestation, a dedicated key called K_{AIK} is generated by TPM_C. The public parts of K_{SIG} and K_{AIK} are stored in the database of the control station while the public parts of $K_{BIND1...N}$ are stored on the camera.

Figure 1 shows an example camera network demonstrating three main security functions: (1) A trusted lifebeat that allows operators to reliably check the status of a camera. (2) Secure and privacy-preserving streaming of videos. (3) User feedback about what the camera does and how personal data is managed. Note that even though the three services are depicted separately, they are offered by every camera.

4.1 Trusted Lifebeat

The trusted lifebeat, built on TC attestation, allows operators to check the status of a system. Lifebeat requests are sent periodically by the control station to the cameras. To avoid replay attacks, the request contains freshly generated random data. This data is included when the camera's TPM_C signs the current PCR values with K_{AIK}. The signed PCRs are returned to the control station where (1) the signature is checked using $K_{AIK_{pub}}$ of the intended camera and (2) the reported PCRs are evaluated. This way operators can check if the camera's state is known and trustworthy or if unknown applications have been executed, e.g., as part of an attack.

4.2 Privacy-Preserving and Secure Video Streaming

To support different privacy levels, we perform motion detection to identify regions of interest (ROI). These ROI are extracted from the original image leaving behind blank areas as shown in figure 1. In our concept, we currently perform edge detection to support an intermediate level between revealing no sensitive data and disclosing the original ROI. Note that any number of intermediate levels is possible. To guarantee confidentiality, both – the original ROI and the edge-detected ROI – are encrypted with AES session keys K_{AES1} and K_{AES2}, respectively. The encrypted ROI images are embedded into the JPEG-compressed background as custom EXIF data. The AES session keys are bound to TPM_S with the public binding keys $K_{BIND1...N_{pub}}$. K_{AES1} of the original ROI is encrypted twice using $K_{BIND1_{pub}}$ followed by $K_{BIND2_{pub}}$. K_{AES2} of the edge-detected ROI is encrypted only with $K_{BIND3_{pub}}$. This setup realizes two important security properties. First, the non-migratable private keys $K_{BIND1...N}$ can only be used inside TPM_S. This ensures that access to the control station is an absolute requirement for decrypting confidential data. Second, double encryption of K_{AES1} ensures that the operator who knows the password for K_{BIND1} and the one who knows the pass-

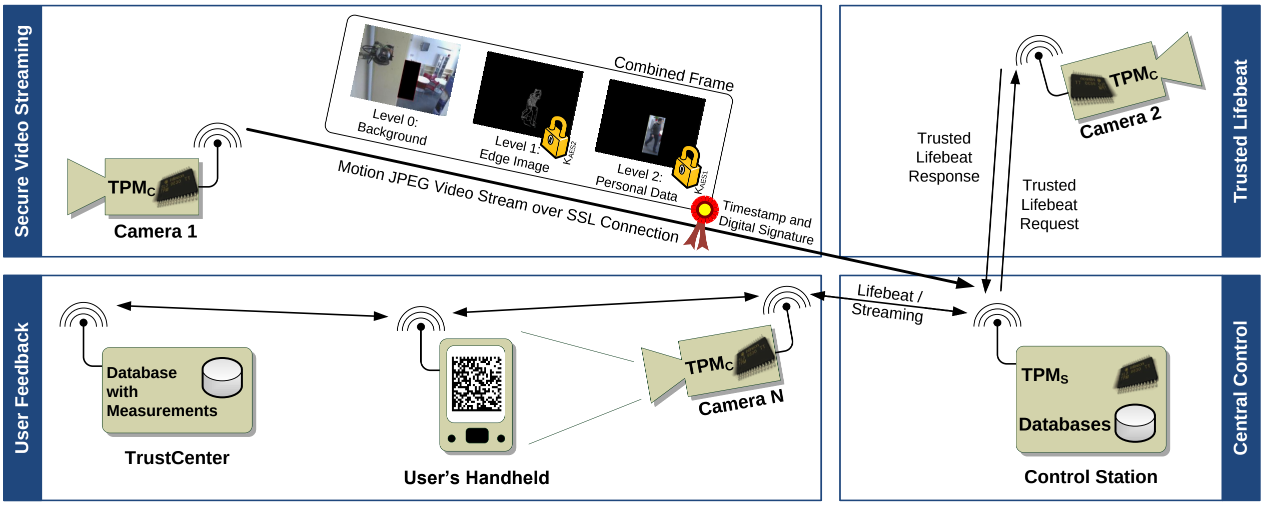


Figure 1: A network of trustworthy, TPM equipped cameras. From the central control station, the status of a camera can be reliably checked via a trusted lifebeat. Secure video streaming ensures confidentiality, integrity, authenticity and freshness of image data. Furthermore, multi-level privacy protection and per-level access control are supported. Using a handheld device, users can query the status of a camera and check if personal data is properly protected.

word for K_{BIND2} have to cooperate for ROI decryption.

Before images are streamed to the control station, they are signed with K_{SIG}. This signature not only allows to check the integrity of an image, it also demonstrates its authenticity: Since the private part of K_{SIG} can only be used inside the camera's TPM_C, the verifier at the control station gets assurance that the signed image actually comes from this specific camera. If required, image signing can be extended with timestamps using the TPM timestamping functionality.

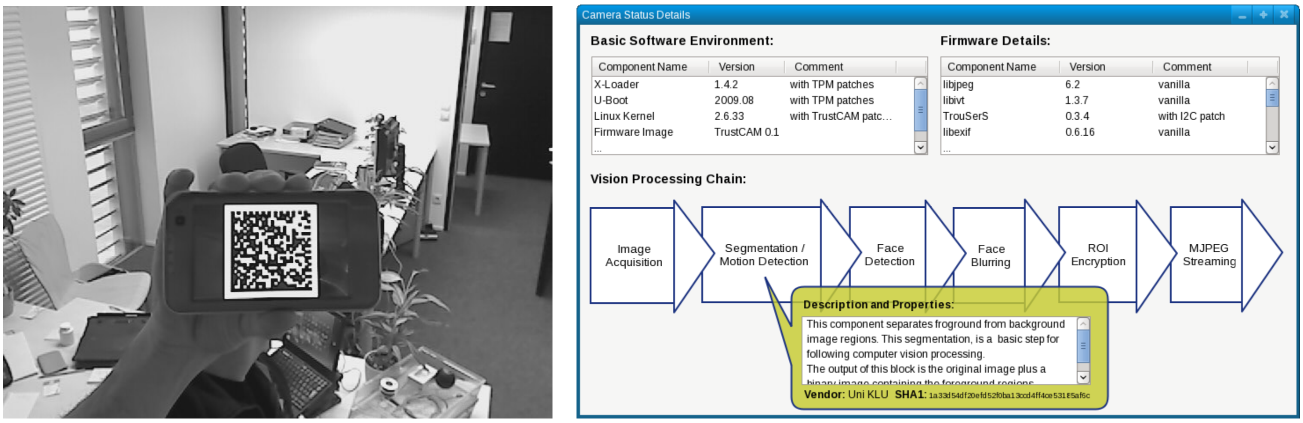
4.3 User Feedback

An important feature is user feedback to actively demonstrate what a system is doing and how personal data is managed. One of the primary challenges is to establish an authentic communication channel to the camera. Wireless networking, as supported by many of today's systems, is no ideal choice. It is difficult to determine if the response actually comes from the intended camera. Similar to approaches for secure pairing of mobile phones [15], we suggest to use visual communication for camera selection and secure channel establishment.

A user is equipped with a handheld device that is capable to display 2D barcodes. This barcode encodes a request for the camera to report its system status by means of TC attestation. The users points the handheld with the displayed barcode towards the camera as shown in figure 2(a). Next, the camera decodes the request and performs the attestation using K_{AIK}. The signed PCRs that represent the software state of the camera are returned to the user together with the PCR log. The PCR values by themselves are of little meaning to the user. What is required is a database where known measurements for software components are stored together with a description and a list of properties. In our model, this services is provided by a trusted third party subsequently called TrustCenter. The user submits the signed PCR values and the PCR log to the TrustCenter. First, the TrustCenter must verify the signature of the PCR values. Next, the individual measurements that lead to the signed PCR values have to be checked against the database of the TrustCenter and a report containing descriptions and properties of the corresponding applications is generated. The report is signed and sent back to the user.

To be able to generate such a report, the TrustCenter has to know the measurements of applications potentially running on a camera. To achieve that, we assume the cooperation of camera operators by disclosing the camera firmware, including the source code, to the TrustCenter. The TrustCenter can then review the applications and store the corresponding measurements together with a description of application properties in its database. We believe that both, camera operators and users can benefit from such a model. On the one hand, operators can demonstrate their commitment to privacy protection while their intellectual property rights are protected since source code only is disclosed to the TrustCenter and not the general public. On the other hand, users benefit from the system since they can learn what the cameras in their environment are doing and how they handle personal data.

Once the attestation is successfully completed, the results are shown to the user. One way to display such a report is presented in figure 2(b). It provides general information about the operating system environment including the bootloader, the kernel and root filesystem. Furthermore, the report lists the content of the filesystem including system libraries and their versions. Additionally, it shows the processing pipeline of the vision tasks running on the camera. By clicking on the individual blocks, users get a detailed description about what the block is doing. We acknowledge that this information might not be easy to interpret to average users. Educated users, acting as opinion leaders, however should be able to interpret the provided information. We believe that this is an important first step towards more transparency in visual surveillance.



Camera Status Details

Basic Software Environment:

Component Name	Version	Comment
X-Loader	1.4.2	with TPM patches
U-Boot	2009.08	with TPM patches
Linux Kernel	2.6.33	with TrustCAM patc...
Firmware Image	TrustCAM 0.1	
...		

Firmware Details:

Component Name	Version	Comment
libjpeg	6.2	vanilla
libivt	1.3.7	vanilla
TrouSerS	0.3.4	with I2C patch
libexif	0.6.16	vanilla
...		

Vision Processing Chain:

Description and Properties:

This component separates froground from background image regions. This segmentation, is a basic step for following computer vision processing.
The output of this block is the original image plus a binary image containing the foreground regions.

Vendor: Uni KLU **SHA1:** 1a33d54df20efd52f0ba13ccd4ff4ce53185af6c

(a) A visual attestation request as seen by the camera.

(b) An attestation result example. It lists the camera's software and presents the computer vision processing flow. Details are available when clicking on the blocks.

Figure 2: An attestation request displayed on the user's handheld and a proposal for presenting attestation results received from the TrustCenter.

Note that we outlined only the basic concept of our user feedback mechanism and omitted several details. These specifically include the validation of signed PCR values as well as countermeasures against potential cuckoo attacks. Background information and technical details can be found in [27].

4.4 Discussion and Comparison

First results from a prototype implementation suggest that the impact of the added security features on camera performance is moderate [26]. Compared to other approaches, our concept covers most of the security and privacy properties listed in table 1. We currently do not support user consent/control primarily due to the lack of reliable user localization and identification. We however consider to proactively notify users about the presence of cameras in an area, e.g., via the users' mobile phones. Finally, we do not yet address availability and resistance against denial of service attacks. This however is an important issue for user triggered actions such as the proposed feedback. Unlimited, excessive use of such a functionality might easily overload a camera.

5. CONCLUSIONS

In this work we discussed security and privacy features desirable for visual surveillance systems. We reviewed and classified existing approaches that address these topics. Classification results show that privacy protection is seen as a critical issue by many researchers. Unfortunately, most related work is decoupled from general system security considerations. We however argue that this gap needs to be filled to reach the goal of a truly privacy-preserving and trustworthy camera system. Currently we are working on such an integrated prototype system to demonstrated the feasibility of our proposed concepts.

To conclude, we believe that security and privacy in camera networks are very important issues with many research opportunities. They could be future driving factors for the deployment of embedded, smart cameras. With their onboard processing capabilities, privacy protection and security can be moved where they belong: As close to the sensor as possible.

6. REFERENCES

[1] N. Baaziz, N. Lolo, O. Padilla, and F. Petngang. Security and Privacy Protection for Automated Video Surveillance. In *Proceedings of the International Symposium on Signal Processing and Information Technology*, pages 17–22, 2007.

[2] T. E. Boult. PICO: Privacy through Invertible Cryptographic Obscuration. In *Proceedings of the Workshop on Computer Vision for Interactive and Intelligent Environments*, pages 27–38, 2005.

[3] J. Brassil. Using Mobile Communications to Assert Privacy from Video Surveillance. In *Proceedings of the Parallel and Distributed Processing Symposium*, page 8, 2005.

[4] A. Cavallaro. Adding Privacy Constraints to Video-Based Applications. In *Proceedings of the European Workshop on the Integration of Knowledge, Semantics and Digital Media Technology*, page 8, 2004.

[5] A. Cavallaro. Privacy in Video Surveillance. *IEEE Signal Processing Magazine*, 24(2):166–168, March 2007.

[6] A. Chattopadhyay and T. E. Boult. PrivacyCam: A Privacy Preserving Camera Using uCLinux on the Blackfin DSP. In *Proceedings of the Conference on Computer Vision and Pattern Recognition*, page 8, 2007.

[7] D. Chen, Y. Chang, R. Yan, and J. Yang. Tools for Protecting the Privacy of Specific Individuals in Video. *EURASIP Journal of Applied Signal Processing*, 2007(1):107–116, January 2007.

[8] S. C. S. Cheung, J. K. Paruchuri, and T. P. Nguyen. Managing Privacy Data in Pervasive Camera Networks. In *Proceedings of the International Conference on Image Processing*, pages 1676–1679, 2008.

[9] S.-C. S. Cheung, J. Zhao, and M. V. Venkatesh. Efficient Object-Based Video Inpainting. In

Proceedings of the International Conference on Image Processing, pages 705–708, 2006.

[10] K. Chinomi, N. Nitta, Y. Ito, and N. Babaguchi. PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction. In *Proceedings of the Int. Multimedia Modeling Conf.*, page 144, 2008.

[11] F. Dufaux and T. Ebrahimi. Scrambling for Video Surveillance with Privacy. In *Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop*, pages 160–166, 2006.

[12] M. Hadem and J. Kuri. Google Street View: Rechtsverletzung im Sekundentakt? (in German), March 2010. last visisted: April 2010.

[13] A. Hampapur. Smart Video Surveillance for Proactive Security. *IEEE Signal Processing Magazine*, 25(4):136–134, July 2008.

[14] I. Martinez-Ponte, X. Desurmont, J. Meessen, and J. F. Delaigle. Robust Human Face Hiding Ensuring Privacy. In *Proceedings of the Internat. Workshop on Image Analysis for Multimedia Interactive Services*, page 4, 2005.

[15] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. *Int. Journal of Security and Networks*, 4(1/2):43–56, 2009.

[16] S. Moncrieff, S. Venkatesh, and G. West. Dynamic Privacy in Public Surveillance. *IEEE Computer*, 42(9):22–28, Sept. 2009.

[17] J. K. Paruchuri and S. C. S. Cheung. Joint Optimization of Data Hiding and Video Compression. In *Proceedings of the International Symposium on Circuits and Systems*, pages 3021–3024, 2008.

[18] J. Schiff, M. Meingast, D. K. Mulligan, S. Sastry, and K. Y. Goldberg. Respectful Cameras: Selecting Visual Markers in Real-Time to Address Privacy Concerns. In *Proceedings of the International Conference on Intelligent Robots and Systems*, pages 971–978, 2007.

[19] 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*, 3(3):50–57, May/June 2005.

[20] D. N. Serpanos and A. Papalambrou. Security and Privacy in Distributed Smart Cameras. *Proceedings of the IEEE*, 96(10):1678–1687, October 2008.

[21] T. Spindler, C. Wartmann, L. Hovestadt, D. Roth, L. van Gool, and A. Steffen. Privacy in Video Surveilled Areas. In *Proceedings of the International Conference on Privacy, Security and Trust*, page 10, 2006.

[22] S. Tansuriyavong and S. Hanaki. Privacy Protection by concealing Persons in circumstantial Video Image. In *Proceedings of the Workshop on Perceptive User Interfaces*, pages 1–4, 2001.

[23] K. Truong, S. Patel, J. Summet, and G. Abowd. Preventing Camera Recording by Designing a Capture-Resistant Environment. In *Proceedings of the Int. Conference on Ubiquitous Computing*, pages 73–86, 2005.

[24] Trusted Computing Group. TPM Main Specification Version 1.2, Level 2, Revision 103, July 2007.

[25] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian. Privacy Protecting Data Collection in Media Spaces. In *Proceedings of the International Conference on Multimedia*, pages 48–55, 2004.

[26] T. Winkler and B. Rinner. TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera based on Trusted Computing. In *Proceedings of the Conference on Advanced Video and Signal-Based Surveillance*, 2010.

[27] T. Winkler and B. Rinner. User-Based Attestation for Trustworthy Visual Sensor Networks. In *Proceedings of the Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 2010.

[28] K. Yabuta, H. Kitazawa, and T. Tanaka. A New Concept of Security Camera Monitoring with Privacy Protection by Masking Moving Objects. In *Proceedings of the Pacific-Rim Conf. on Multimedia*, page 12, 2005.