Computer Standards & Interfaces 44 (2016) 137–143

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers

Kyungroul Lee, Hyeungjun Yeuk, Jaein Kim, Hyungjoon Park, Kangbin Yim *

Department of Information Security Engineering, Soonchunhyang University, 646 Eupnae, Shinchang, Asan 336-745 Korea

ARTICLE INFO

Article history:
Received 20 February 2015
Received in revised form 2 June 2015
Accepted 25 June 2015
Available online 14 July 2015

Keywords:
Video surveillance system
Key management technique
Privacy masking and restoring
User authentication

ABSTRACT

In this paper, we surveyed technical elements of video surveillance systems and proposed several countermeasures to effectively manage a number of keys for image encryption, privacy protection and user authentication. In addition, we proposed several solutions for potential problems that could arise when the system adopts a privacy masking policy for each user. The proposed solutions selectively implement a Kerberos approach, a round keys approach and a double hash chain approach. For secure video surveillance systems, protecting privacy and providing accessibility through strong user authentication and prioritized authorization is expected.

1. Introduction

According to the increase of the crime rate, public peace management is expected to have a better solution against the increasing criminalities. What is most considered to be useful are video surveillance systems. Practically, video equipment and facilities are greatly increased such as CCTVs (closed-circuit television) and networked cameras, which can minimize the limitations of time and space. Thereupon, these systems are growing into an intelligent framework [1]. For this reason, people are concerned about intrusions of privacy because they are exposed to many cameras during their day-to-day life. In this situation, diverse researches are required to solve these social problems [2].

In the past analog environment using VCRs (video cassette recorder), it was hard to access image information because only administrators had specific permissions in a closed area. This reason originated from the environment which was constructed using analog CCTVs to obtain the image information. But now, diverse applications for video surveillance systems are combined with digital cameras and the related network systems. This developing tendency has positively influenced the related systems to easily obtain video images. In contrast, it also has negative influence such that the collected digital images are no longer safe from third parties with malicious behaviors such as insider threats, hacking attacks, and so on, making the images available for second and third means [3]. In order to counteract this problem, the system has three requirements: intrusion prevention of network cameras, counterfeiting and falsification prevention of images and cryptography technology to protect the images.

There have been many related researches to meet these requirements, including user authentication for accessing network cameras [4], encryption/decryption of the images [5], privacy masking for images [6] and so on. To apply these solutions, many kinds of keys are needed and related management policies need to be studied. In addition, a safe distribution mechanism for the keys is needed to protect the keys from exposure to third parties. Therefore, in this paper, we propose management and distribution methods for encryption and decryption keys to protect images or to place and remove privacy masks and suggest an efficient streaming method for images with privacy information to each user that has different authority.

2. Evaluation history of video surveillance system and research trends in video security

A camera is essential in the video surveillance system, the camera has advanced from analog to digital, and now it changes to the network camera that is combined with the network infrastructure. Table 1 shows the evaluation history of the video surveillance system.

The development history of camera for a video surveillance system is summarized as follows. First one was the analog CCTV using VCRs, second one was also the analog CCTV using DVRs (digital video recorders), third one was the analog CCTV with networked DVRs, fourth one was the networked system using video servers and finally we have networked frameworks using IP cameras [7].

By combining a video surveillance system with the network infrastructure from closed environment to open environment, cameras can be exposed to vulnerabilities such as hacking, sniffing and DoS (denial

* Corresponding author. Tel.:+82 10 8958 9080.
E-mail addresses: goodyug@sch.ac.kr (H. Yeuk), boxbop@sch.ac.kr (J. Kim), nemo@sch.ac.kr (H. Park), yim@sch.ac.kr (K. Yim).

http://dx.doi.org/10.1016/j.csi.2015.06.006
0920-5489/

Table 1
Evaluation history of video surveillance system.

Evaluation history	Description
Analog CCTV using VCRs	This is totally analog-based system to connect the VCR to an analog camera with a coaxial cable and to use an analog tape for recording
Analog CCTV using DVRs	This system is an analog-based system with a DVR and it records the obtained video image digitally to a hard disk instead of a videotape
Analog CCTV with networked DVRs	This is able to connect to the network by adding Ethernet ports with existing DVR function and to adjust or display the collected video images remotely through networked DVRs
Network system using a video server	This system is an Ethernet-based network environment in which an analog camera is connected to a video server
Networked framework using IP cameras	This system is a totally digital-based system without analog elements that transfers video images through a network

of service) to steal or block images. In order to resolve this vulnerability, we researched video distribution servers that securely transmits images without DoS to protect images for many users [8]. The server solves unintentional DoS problems by handling many clients instead of cameras basically and effectively distributes images to multiple users. Furthermore, it is able to minimize information leakage from network cameras to an attacker who is in the dark-side by acting as a proxy server that conceals the location and IP address of the network camera.

In the past, the video surveillance system was a type of distribution server that simply shares video images of cameras to multiple users, and then a system was developed that integrated control systems because camera security, encryption and decryption of image [7,9–13] and a central control system are required. The network camera has requisite drawbacks. When a number of users connect to the camera, it is impossible to handle because basically the camera is configured as an embedded system with processes that have low performance [13,14]. Thus, a video distribution server is required to collect and record images from many networked cameras and to distribute these images when many users connect to the cameras in real time. This resolves overhead by multi-accessing. In addition, as the video image is changed from analog to digital, many related researches have been studied to prepare infrastructure that integrates management solutions according to how the image will be used. Video security is used for video surveillance and the traditional video surveillance system receives the video image from cameras to a central control room and then it is recorded by the DVR. However, new systems are now more exquisite and intelligent so past systems that were not standardized cannot adapt to change. Consequently, a network-based system that can easily be interworked into various applications dominates video surveillance systems.

A CMS (centralized management system) is an integrated management system for remotely networking existing DVRs, video servers, network cameras and so on. This system manages all kind of functions of DVRs, video servers and network cameras through software and it has the advantage that many functions such as recording, backup, PTZ (pan-tilt-zoom) camera control and so on are performed concurrently. Likewise, it is possible to monitor, in real time, the network status, record status, event detection, motion detection and so on, and if specific motion is detected, the situation is notified to the administrator intelligently.

3. Structure of video surveillance systems with privacy masking

The proposed video surveillance system in this paper contains a key management server that generates keys for user authentication and privacy masking. The generated keys are managed through a database and the key management server distributes the generated keys upon the request of a camera or a user. Fig. 1 shows the related processes.

In video surveillance systems, keys for cameras and users are managed individually, and thus these are very extensive and produce loads of information. Fig. 2 shows the key distribution process when cameras and users are managed separately.

1. Step 1. If N is the number of users, the network camera requests user's keys at the key management server for masking image that is selected from users for privacy protection.
2. Step 2. The key management server searches for the registered user and generates the user's keys (N).
3. Step 3. Whole generated keys (N) are transferred to the camera and the corresponding key (K_A, K_B, K_N) is sent to the user.

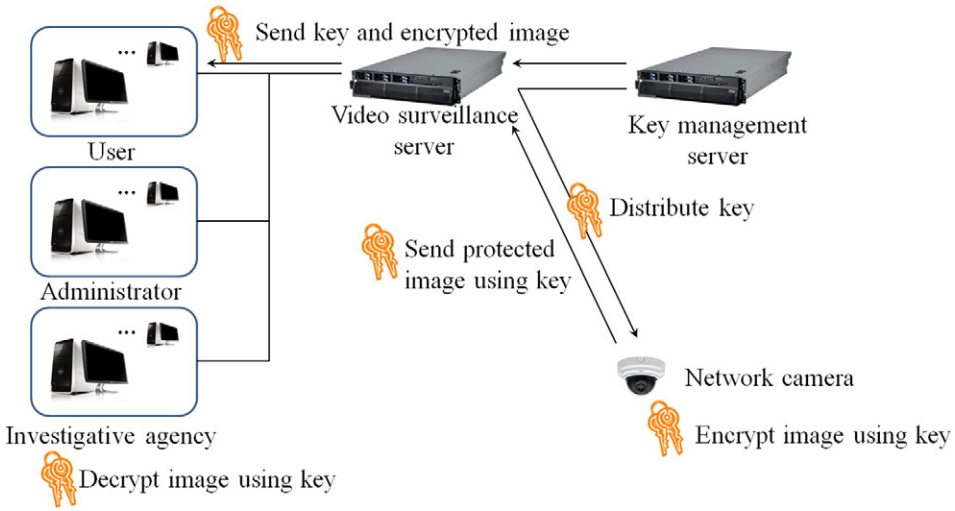

Fig. 1. Whole structure and processes on the proposed video surveillance system.